Mọi người có thể up source này lên quizlet dưới định dạng của quizlet rồi comment link được không ạ?

CyberOps Associate (Version 1.0) – Modules 1 – 2: Threat Actors and Defenders Group Exam Answers

1. Which personnel in a SOC is assigned the task of verifying whether an alert triggered by monitoring software represents a true security incident?

- **Tier 1 personnel**
- Tier 2 personnel
- Tier 3 personnel
- SOC Manager

2. After a security incident is verified in a SOC, an incident responder reviews the incident but cannot identify the source of the incident and form an effective mitigation procedure. To whom should the incident ticket be escalated?

- **the SOC manager to ask for other personnel to be assigned**
- an alert analyst for further analysis
- a cyberoperations analyst for help
- a SME for further investigation

3. Which two services are provided by security operations centers? (Choose two.)

- responding to data center physical break-ins
- monitoring network security threats
- managing comprehensive threat solutions
- **ensuring secure routing packet exchanges**
- **providing secure Internet connections**

4. Which organization is an international nonprofit organization that offers the CISSP certification?

- CompTIA
- **(ISC)²**
- IEEE
- GIAC

Explanation: (ISC)² is an international nonprofit organization that offers the CISSP certification.

5. What is a benefit to an organization of using SOAR as part of the SIEM system?

- SOAR was designed to address critical security events and high-end investigation.
- SOAR would benefit smaller organizations because it requires no cybersecurity analyst involvement once installed.
- **SOAR automates incident investigation and responds to workflows based on playbooks.**
- SOAR automation guarantees an uptime factor of "5 nines".

Explanation: SIEM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats. SOAR technology does the same as SIEMs but it also includes automation. SOAR integrates threat intelligence and automates incident investigation. SOAR also responds to events using response workflows based on previously developed playbooks.

6. Which personnel in a SOC are assigned the task of hunting for potential threats and implementing threat detection tools?

- **Tier 3 SME**
- Tier 2 Incident Reporter
- Tier 1 Analyst
- SOC Manager

Explanation: In a SOC, Tier 3 SMEs have expert-level skills in network, endpoint, threat intelligence, and malware reverse engineering (RE). They are deeply involved in hunting for potential security threats and implementing threat detection tools.

7. An SOC is searching for a professional to fill a job opening. The employee must have expert-level skills in networking, endpoint, threat intelligence, and malware reverse engineering in order to

search for cyber threats hidden within the network. Which job within an SOC requires a professional with those skills?

- Incident Responder
- Alert Analyst
- SOC Manager
- **Threat Hunter**

Explanation: Tier 3 professionals called Threat Hunters must have expert-level skills in networking, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing the processes of malware to determine the impact of the malware and how it can be removed.

8. Which three are major categories of elements in a security operations center? (Choose three.)

- **technologies**
- Internet connection
- **processes**
- data center
- **people**
- database engine

Explanation: The three major categories of elements of a security operations center are people, processes, and technologies. A database engine, a data center, and an Internet connection are components in the technologies category.

9. Which KPI metric does SOAR use to measure the time required to stop the spread of malware in the network?

- MITR
- **Time to Control**
- MITC
- MTTD

Explanation:
The common key performance indicator (KPI) metrics compiled by SOC managers are as follows:
• Dwell Time: the length of time that threat actors have access to a network before they are detected and the access of the threat actors stopped

• Mean Time to Detect (MTTD): the average time that it takes for the SOC personnel to identify that valid security incidents have occurred in the network
• Mean Time to Respond (MTTR): the average time that it takes to stop and remediate a security incident
• Mean Time to contain (MTTC): the time required to stop the incident from causing further damage to systems or data
• Time to Control the time required to stop the spread of malware in the network

10. Which three technologies should be included in a SOC security information and event management system? (Choose three.)

- **security monitoring**
- **threat intelligence**
- proxy service
- firewall appliance
- intrusion prevention
- **log management**

Explanation: Technologies in a SOC should include the following:
Event collection, correlation, and analysis
Security monitoring
Security control
Log management
Vulnerability assessment
Vulnerability tracking
Threat intelligence
Proxy server, VPN, and IPS are security devices deployed in the network infrastructure.

11. The term cyber operations analyst refers to which group of personnel in a SOC?

- **Tier 1 personnel**
- Tier 3 personnel
- Tier 2 personnel
- SOC managers

Explanation: In a typical SOC, the Tier 1 personnel are called alert analysts, also known as cyberoperations analysts.

12. How does a security information and event management system (SIEM) in a SOC help the personnel fight against security threats?

- by analyzing logging data in real time
- **by combining data from multiple technologies**
- by integrating all security devices and appliances in an organization
- by dynamically implementing firewall rules

Explanation: A security information and event management system (SIEM) combines data from multiple sources to help SOC personnel collect and filter data, detect and classify threats, analyze and investigate threats, and manage resources to implement preventive measures.

13. What job would require verification that an alert represents a true security incident or a false positive?

- **Alert Analyst**
- Threat Hunter
- SOC Manager
- Incident Reporter

Explanation: A Cybersecurity Analyst monitors security alert queues and uses a ticketing system to assign alerts to a queue for an analyst to investigate. Because the software that generates alerts can trigger false alarms, one job of the Cybersecurity Analyst would be to verify that an alert represents a true security incident.

14. When a user turns on the PC on Wednesday, the PC displays a message indicating that all of the user files have been locked. In order to get the files unencrypted, the user is supposed to send an email and include a specific ID in the email title. The message also includes ways to buy and submit bitcoins as payment for the file decryption. After inspecting the message, the technician suspects a security breach occurred. What type of malware could be responsible?

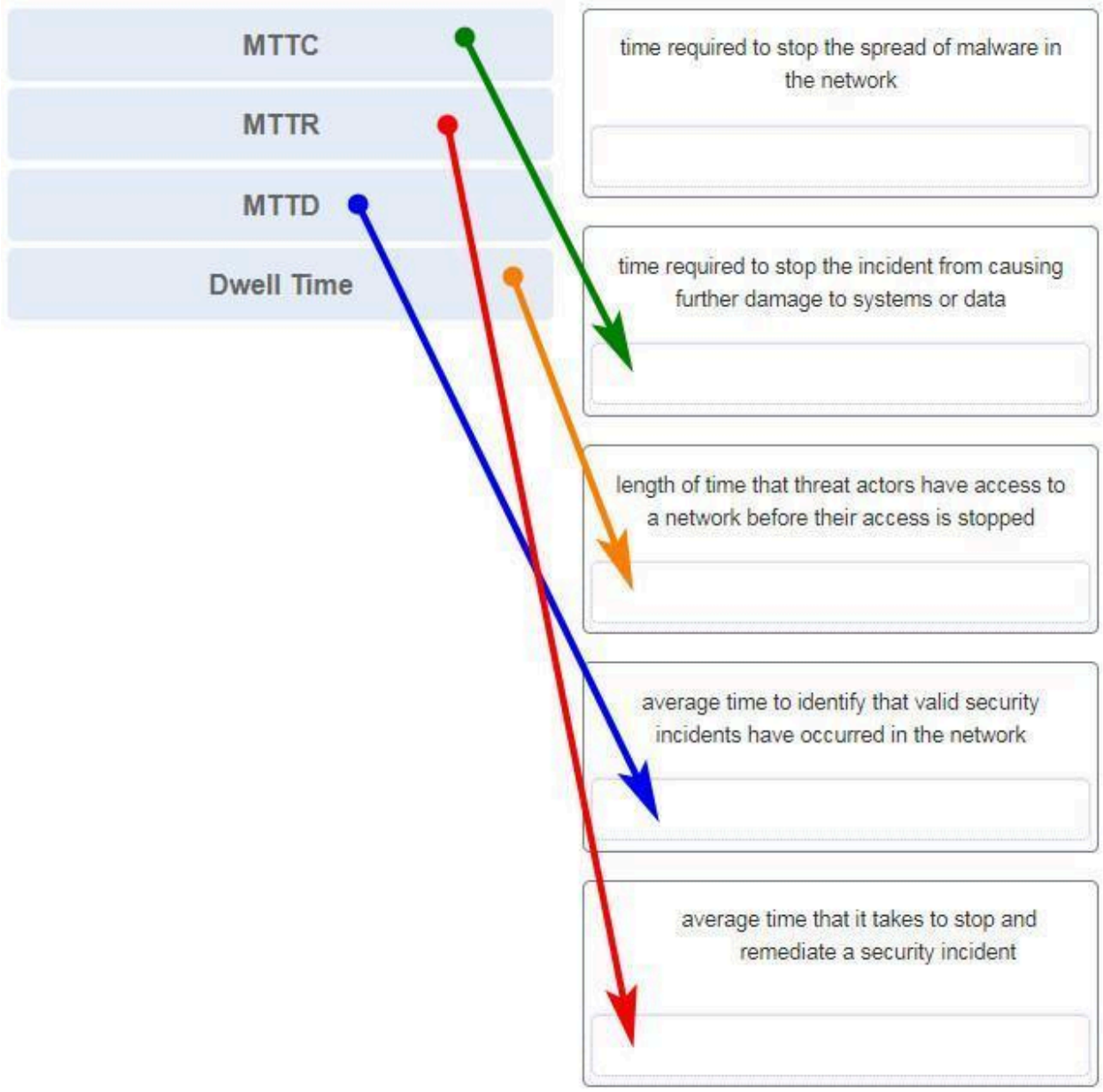
- Trojan
- spyware
- adware
- **ransomware**

Explanation: Ransomware requires payment for access to the computer or files. Bitcoin is a type of digital currency that does not go through a particular bank.

15. An employee connects wirelessly to the company network using a cell phone. The employee then configures the cell phone to act as a wireless access point that will allow new employees to connect to the company network. Which type of security threat best describes this situation?

- **rogue access point**
- cracking
- spoofing
- denial of service

16. Match the SOC metric to the description. (Not all options are used.)



Explanation: SOCs use many metrics as performance indicators of how long it takes personnel to locate, stop, and remediate security incidents.

- Dwell Time
- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Mean Time to Contain (MTTC)
- Time to Control

17. A group of users on the same network are all complaining about their computers running slowly. After investigating, the technician determines that these computers are part of a zombie network. Which type of malware is used to control these computers?

- **botnet**
- spyware
- virus
- rootkit

18. Which statement describes cyberwarfare?

- **It is Internet-based conflict that involves the penetration of information systems of other nations.**
- It is simulation software for Air Force pilots that allows them to practice under a simulated war scenario.
- Cyberwarfare is an attack carried out by a group of script kiddies.
- It is a series of personal protective equipment developed for soldiers involved in nuclear war

Explanation: Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. Organized hackers are typically involved in such an attack.

19. Why do IoT devices pose a greater risk than other computing devices on a network?

- **Most IoT devices do not receive frequent firmware updates.**
- Most IoT devices do not require an Internet connection and are unable to receive new updates.
- IoT devices cannot function on an isolated network with only an Internet connection.
- IoT devices require unencrypted wireless connections.

Explanation: IoT devices commonly operate using their original firmware and do not receive updates as frequently as laptops, desktops, and mobile platforms.

20. What are two examples of personally identifiable information (PII)? (Choose two.)

- first name
- IP address

- language preference
- **street address**
- **credit card number**

Explanation: Personally identifiable information (PII) is any data that could potentially identify and track a specific individual. A credit card number and street address are the best examples of PII.

21. What is the dark web?

- It is a website that reports the most recent activities of cybercriminals all over the world.
- It is a website that sells stolen credit cards.
- It is part of the internet where a person can obtain personally identifiable information from anyone for free
- **It is part of the internet that can only be accessed with special software.**

Explanation: One of the more lucrative goals of cybercriminals is obtaining lists of personally identifiable information that can then be sold on the dark web. The dark web can only be accessed with special software and is used by cybercriminals to shield their activities. Stolen PII can be used to create fake accounts, such as credit cards and short-term loans.

22. A company has just had a cybersecurity incident. The threat actor appeared to have a goal of network disruption and appeared to use a common security hack tool that overwhelmed a particular server with a large amount of traffic. This traffic rendered the server inoperable. How would a certified cybersecurity analyst classify this type of threat actor?

- terrorist
- hacktivist
- state-sponsored
- **amateur**

Explanation: Amateurs or script kiddies use common, existing tools found on the internet to launch attacks. Hacktivists disrupt services in protest against organizations or governments for a particular political or social idea. State-sponsored threat actors use cyberspace for

industrial espionage or interfering with another country in some way. Terrorist groups attack for a specific cause.

23. A user calls the help desk complaining that the password to access the wireless network has changed without warning. The user is allowed to change the password, but an hour later, the same thing occurs. What might be happening in this situation?

- **rogue access point**
- password policy
- weak password
- user error
- user laptop

Explanation: Man-in-the-middle attacks are a threat that results in lost credentials and data. These type of attacks can occur for different reasons including traffic sniffing.

24. Which regulatory law regulates the identification, storage, and transmission of patient personal healthcare information?

- FISMA
- **HIPAA**
- PCI-DSS
- GLBA

Explanation: The Health Insurance Portability and Accountability Act (HIPAA) requires that all patient personally identifiable healthcare information be stored, maintained, and transmitted in ways that ensure patient privacy and confidentiality.

25. A worker in the records department of a hospital accidentally sends a medical record of a patient to a printer in another department. When the worker arrives at the printer, the patient record printout is missing. What breach of confidentiality does this situation describe?

- EMR
- PII
- PSI
- **PHI**

Explanation: Protected Health Information (PHI) includes patient name, addresses, visiting dates and more. The Health Insurance Portability and Accountability Act (HIPAA) regulates and provides severe penalties for breaches of PHI. EMRs (Electronic Medical Records) are documents created and maintained by the medical community that contain PHI. Personally identifiable information (PII) is any information that can be used to positively identify an individual, such as name and social security number. Personal Security Information (PSI) is related to information about an individual such as passwords, access keys, and account details.

26. Which cyber attack involves a coordinated attack from a botnet of zombie computers?

- **DDoS**
- MITM
- address spoofing
- ICMP redirect

Explanation: DDoS is a distributed denial-of-services attack. A DDoS attack is launched from multiple coordinated sources. The sources of the attack are zombie hosts that the cybercriminal has built into a botnet. When ready, the cybercriminal instructs the botnet of zombies to attack the chosen target.

27. What is the main purpose of cyberwarfare?

- to protect cloud-based data centers
- to develop advanced network devices
- **to gain advantage over adversaries**
- to simulate possible war scenarios among nations

Explanation: Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. The main purpose of cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

28. What type of cyberwarfare weapon was Stuxnet?

- botnet
- virus
- **worm**

- ransomware

Explanation: The Stuxnet worm was an excellent example of a sophisticated cyberwarfare weapon. In 2010, it was used to attack programmable logic controllers that operated uranium enrichment centrifuges in Iran.

29. Which example illustrates how malware might be concealed?

- A hacker uses techniques to improve the ranking of a website so that users are redirected to a malicious site.
- An attack is launched against the public website of an online retailer with the objective of blocking its response to visitors.
- A botnet of zombies carry personal information back to the hacker.
- **An email is sent to the employees of an organization with an attachment that looks like an antivirus update, but the attachment actually consists of spyware.**

Explanation: An email attachment that appears as valid software but actually contains spyware shows how malware might be concealed. An attack to block access to a website is a DoS attack. A hacker uses search engine optimization (SEO) poisoning to improve the ranking of a website so that users are directed to a malicious site that hosts malware or uses social engineering methods to obtain information. A botnet of zombie computers is used to launch a DDoS attack.

30. What websites should a user avoid when connecting to a free and open wireless hotspot?

- websites to check account fees
- websites to check product details
- websites to check stock prices
- **websites to make purchases**

Explanation: Many free and open wireless hotspots operate with no authentication or weak authentication mechanisms. Attackers could easily capture the network traffic in and out of such a hotspot and steal user information. Therefore, users who use free and open wireless hotspots to connect to websites should avoid giving any personal information to the websites.

31. In a smart home, an owner has connected many home devices to the Internet, such as the refrigerator and the coffee maker. The owner is concerned that these devices will make the wireless network vulnerable to attacks. What action could be taken to address this issue?

- Configure mixed mode wireless operation.
- **Install the latest firmware versions for the devices.**
- Assign static IP addresses to the wireless devices.
- Disable the SSID broadcast.

Explanation: The Internet of Things (IoT) is facilitating the connection of different kinds of devices to the internet, like home devices such as coffee makers and refrigerators, and also wearable devices. In order to make these devices secure and not vulnerable to attacks, they have to be updated with the latest firmware.

CyberOps Associate (Version 1.0) – Modules 3 – 4: Operating System Overview Group Exam

1. When a user makes changes to the settings of a Windows system, where are these changes stored?

- **win.ini**
- Control Panel

- boot.ini
- Registry

2. Which user account should be used only to perform system management and not as the account for regular use?

- guest
- **power user**
- standard user
- administrator

3. What is the purpose of entering the netsh command on a Windows PC?

- **to configure networking parameters for the PC**
- to change the computer name for the PC
- to create user accounts
- to test the hardware devices on the PC

Explanation: The **netsh.exe** tool can be used to configure networking parameters for the PC from a command prompt.

4. Which type of Windows PowerShell command performs an action and returns an output or object to the next command that will be executed?

- **cmdlets**
- functions
- routines
- scripts

Explanation: The types of commands that PowerShell can execute include the following:

- **cmdlets** – perform an action and return an output or object to the next command that will be executed
- **PowerShell scripts** – files with a .ps1 extension that contain PowerShell commands that are executed
- **PowerShell functions** – pieces of code that can be referenced in a script

5. A user creates a file with `.ps1` extension in Windows. What type of file is it?

- PowerShell documentation
- PowerShell cmdlet
- **PowerShell script**
- PowerShell function

Explanation: The types of commands that PowerShell can execute include the following:
cmdlets – perform an action and return an output or object to the next command that will be executed
PowerShell scripts – files with a .ps1 extension that contain PowerShell commands that are executed
PowerShell functions – pieces of code that can be referenced in a script

6. What are two benefits of using an ext4 partition instead of ext3? (Choose two.)

- an increase in the number of supported devices
- **improved performance**
- compatibility with NTFS
- **increase in the size of supported files**
- decreased load time
- compatibility with CDFS

Explanation: Based on the ex3 file system, an ext4 partition includes extensions that improve performance and an increase in the of supported files. An ext4 partition also supports journaling, a file system feature that minimizes the risk of file system corruption if power is suddenly lost to the system.

7. Consider the result of the ls -l command in the Linux output below. What are the file permissions assigned to the sales user for the analyst.txt file?

```
ls -l analyst.txt

-rwxrw-r-- sales staff 1028 May 28 15:50 analyst.txt
```

- **read, write, execute**

- write only
- read only
- read, write

Explanation: The file permissions are always displayed in the User Group and Other order. In the example displayed, the file has the following permissions:
The dash (–) means that this is a file. For directories, the first dash would replaced with a "d".
The first set of characters is for user permission (rwx).
The user, sales, who owns the file can read, write and execute the file.
The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.
The third set of characters is for any other user or group permissions (r–). Any other user or group on the computer can only read the file.

8. Which Linux command can be used to display the name of the current working directory?

- sudo
- ps
- **pwd**
- chmod

9. Consider the result of the `ls -l` command in the Linux output below. What are the file permissions assigned to the sales user for the `analyst.txt` file?

- write only
- read, write
- read only
- **read, write, execute**

10. A Linux system boots into the GUI by default, so which application can a network administrator use in order to access the CLI environment?

- system viewer
- file viewer
- package management tool
- **terminal emulator**

Explanation: A terminal emulator is an application program a user of Linux can use in order to access the CLI environment.

11. What is the well-known port address number used by DNS to serve requests?

- 25
- **53**
- 110
- 60

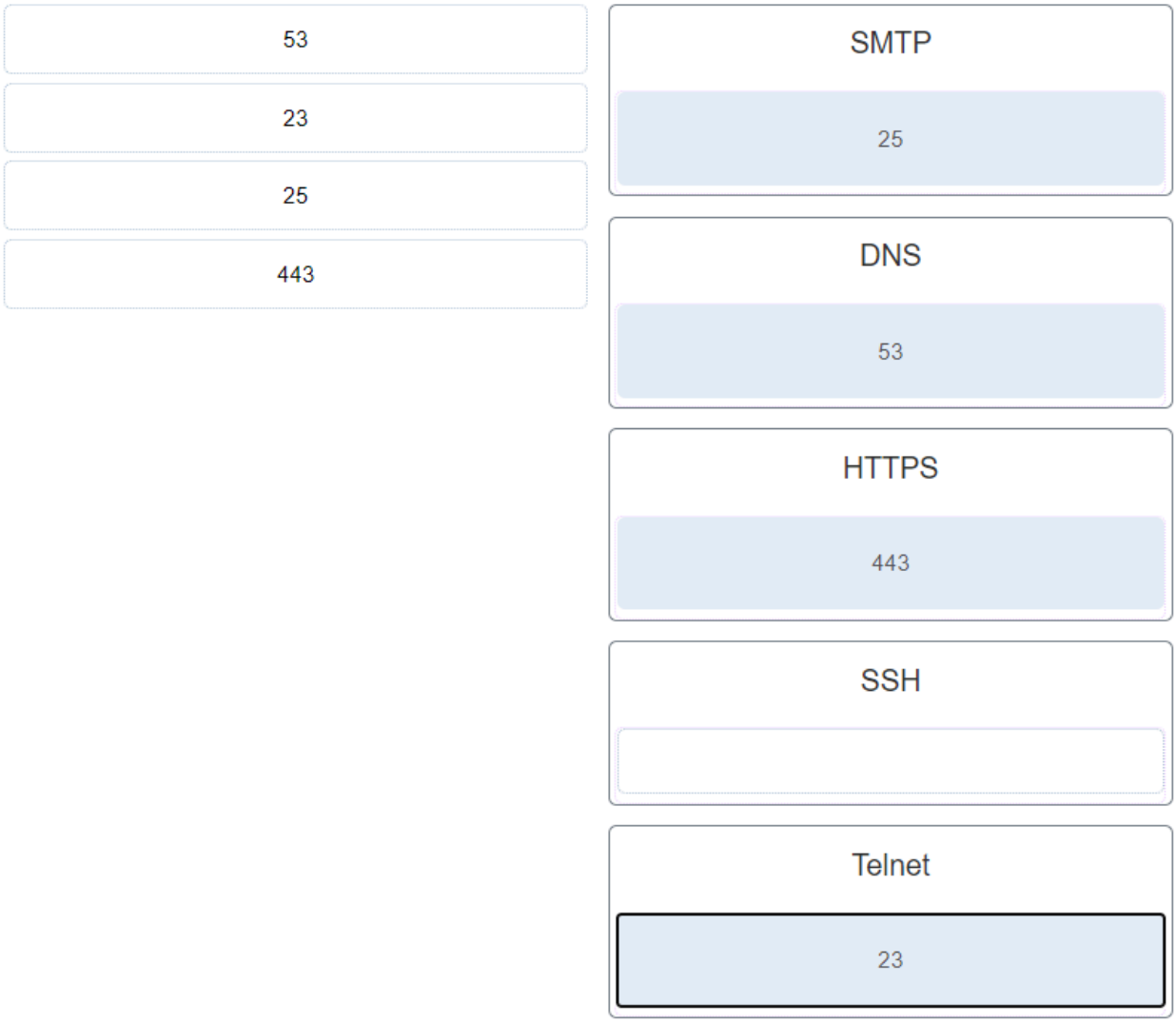
Explanation: Port numbers are used in TCP and UDP communications to differentiate between the various services running on a device. The well-known port number used by DNS is port 53.

12. Which user can override file permissions on a Linux computer?

- any user that has 'group' permission to the file
- only the creator of the file
- any user that has 'other' permission to the file
- **root user**

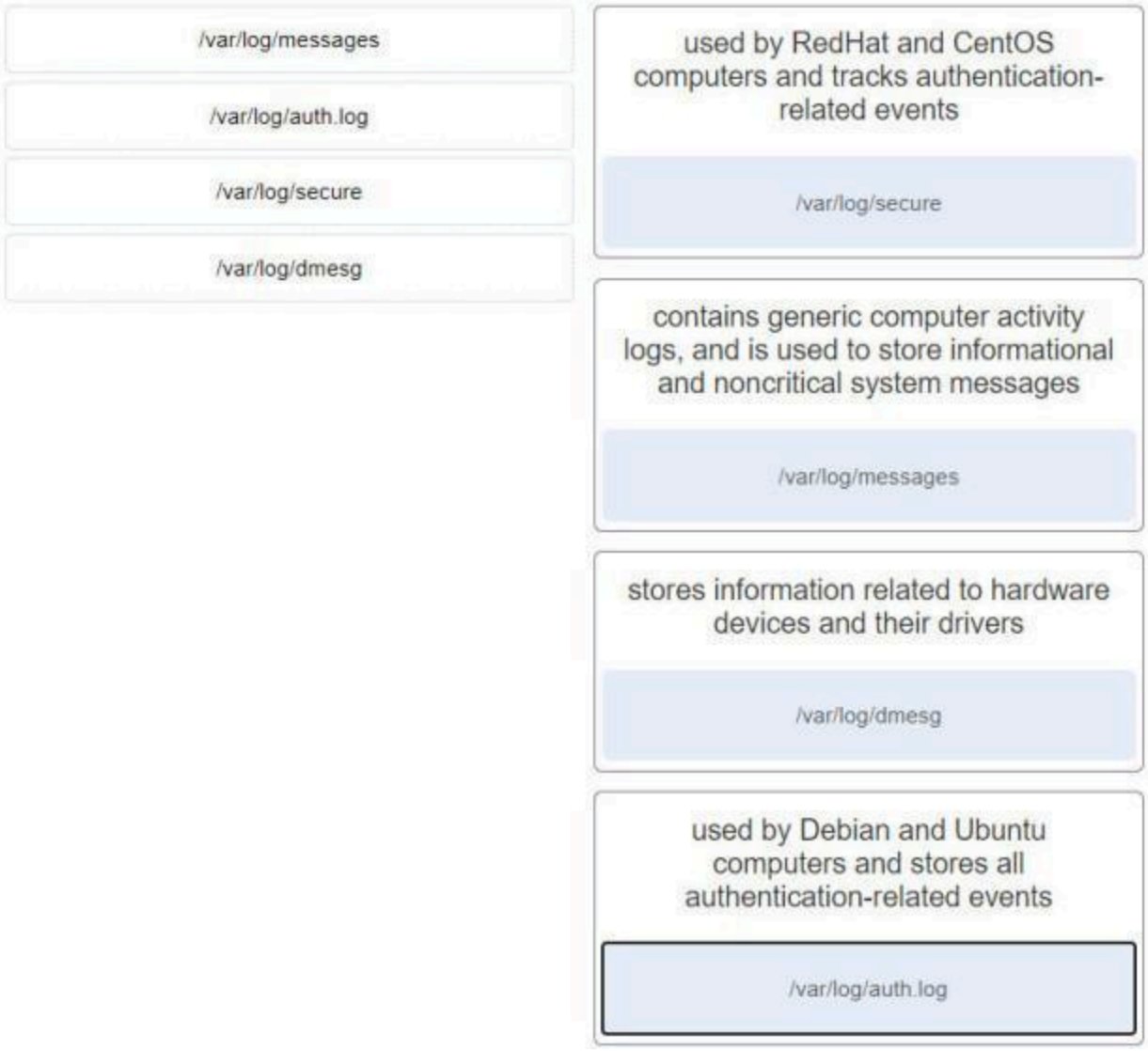
Explanation: A user has as much rights to a file as the file permissions allow. The only user that can override file permission on a Linux computer is the root user. Because the root user has the power to override file permissions, the root user can write to any file.

13. Match the commonly used ports on a Linux server with the corresponding service.



- SMTP: **25**
- DNS: **53**
- HTTPS: **443**
- SSH: **22**
- TELNET: **23**

14. Match typical Linux log files to the function.

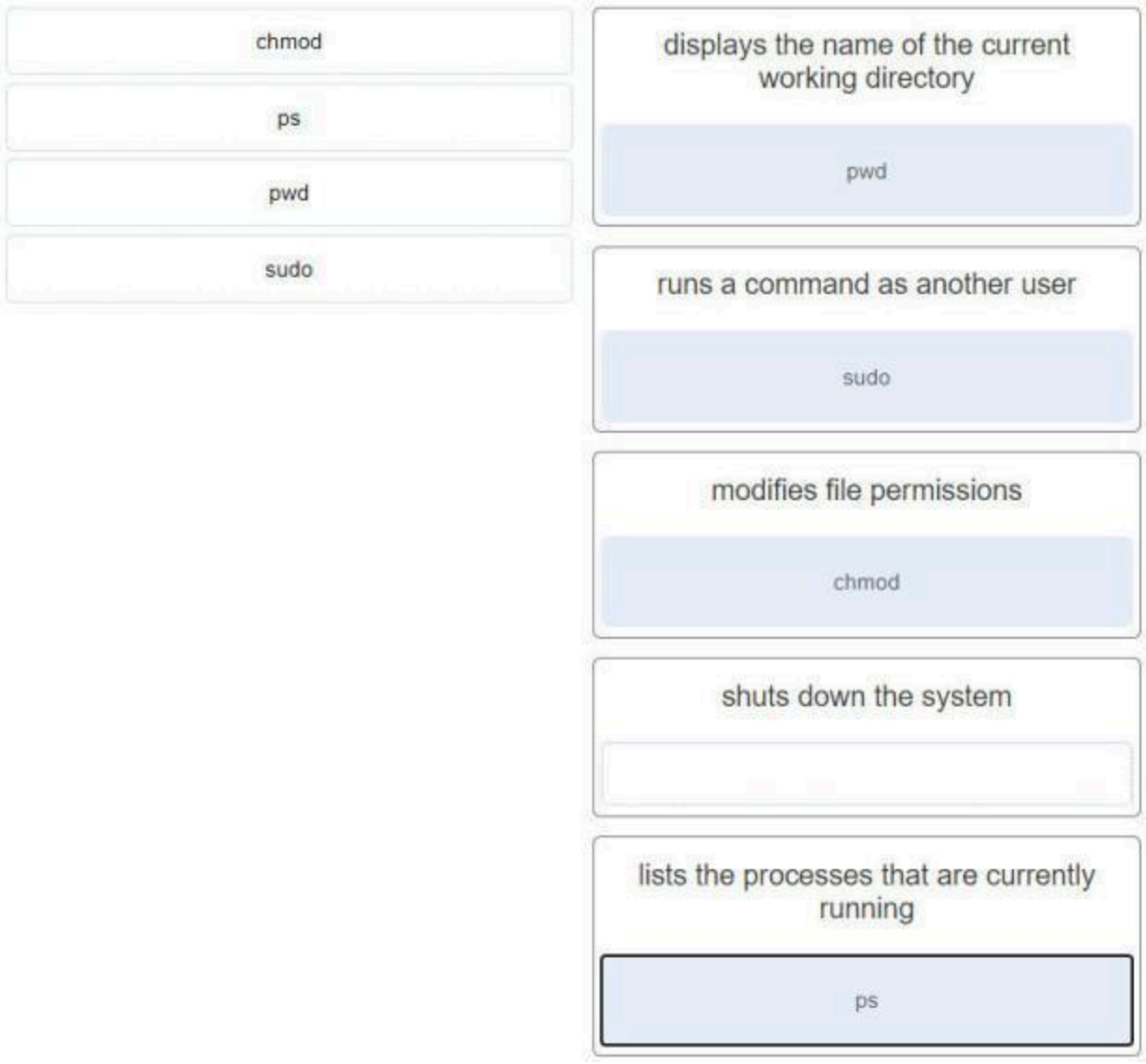


- used by RedHat and CentOS computers and tracks authentication-related events: **/var/log/secure**
- contains generic computer activity logs, and is used to store informational and noncritical system messages: **/var/log/messages**
- stores information related to hardware devices and their drivers: **/var/log/dmesg**
- used by Debian and Ubuntu computers and stores all authentication-related events: **/var/log/auth.log**

15. Which type of tool allows administrators to observe and understand every detail of a network transaction?

- log manager
- malware analysis tool
- ticketing system
- **packet capture software**

16. Match the Linux command to the function. (Not all options are used.)



- Displays the name of the current working directory: **pwd**
- runs a command as another user: **sudo**
- modifies file permissions: **chmod**

- shuts down the system: **Empty**
- lists the processes that are currently running: **ps**

17. What are two advantages of the NTFS file system compared with FAT32? (Choose two.)

- NTFS is easier to configure.
- **NTFS supports larger files.**
- NTFS allows faster formatting of drives.
- NTFS allows the automatic detection of bad sectors.
- NTFS allows faster access to external peripherals such as a USB drive.
- **NTFS provides more security features.**

Explanation: The file system has no control over the speed of access or formatting of drives, and the ease of configuration is not file system-dependent.

18. Why is Kali Linux a popular choice in testing the network security of an organization?

- It is a network scanning tool that prioritizes security risks.
- **It is an open source Linux security distribution containing many penetration tools.**
- It can be used to test weaknesses by using only malicious software.
- It can be used to intercept and log network traffic.

Explanation: Kali is an open source Linux security distribution that is commonly used by IT professionals to test the security of networks.

19. Match the octal value to the file permission description in Linux. (Not all options are used.)

000	write only
001	010
010	read and execute
101	101
110	read and write
	110
	execute only
	001
	write and execute
	no access
	000

- write only ~~> **010**
- read and execute ~~> **101**
- read and write ~~> **110**
- execute only ~~> **001**
- write and execute ~~> **NOT SCORED**
- no access ~~> **000**

20. A PC user issues the netstat command without any options. What is displayed as the result of this command?

- a historical list of successful pings that have been sent
- **a list of all established active TCP connections**
- a network connection and usage report
- a local routing table

Explanation: When used by itself (without any options), the netstat command will display all the active TCP connections that are available.

21. Which two commands could be used to check if DNS name resolution is working properly on a Windows PC? (Choose two.)

- **nslookup cisco.com**
- net cisco.com
- ipconfig /flushdns
- nbtstat cisco.com
- **ping cisco.com**

Explanation: The `ping` command tests the connection between two hosts. When ping uses a host domain name to test the connection, the resolver on the PC will first perform the name resolution to query the DNS server for the IP address of the host. If the ping command is unable to resolve the domain name to an IP address, an error will result.

Nslookup is a tool for testing and troubleshooting DNS servers.

22. A technician has installed a third party utility that is used to manage a Windows 7 computer. However, the utility does not automatically start whenever the computer is started. What can the technician do to resolve this problem?

- Set the application registry key value to one.
- Use the Add or Remove Programs utility to set program access and defaults.
- **Change the startup type for the utility to Automatic in Services .**
- Uninstall the program and then choose Add New Programs in the Add or Remove Programs utility to install the application.

Explanation: The Services console in Windows OS allows for the management of all the services on the local and remote computers.

The setting of Automatic in the Services console enables the chosen service to start when the computer is started.

23. Which statement describes the function of the Server Message Block (SMB) protocol?

- It is used to stream media contents.
- It is used to manage remote PCs.
- It is used to compress files stored on a disk.
- **It is used to share network resources.**

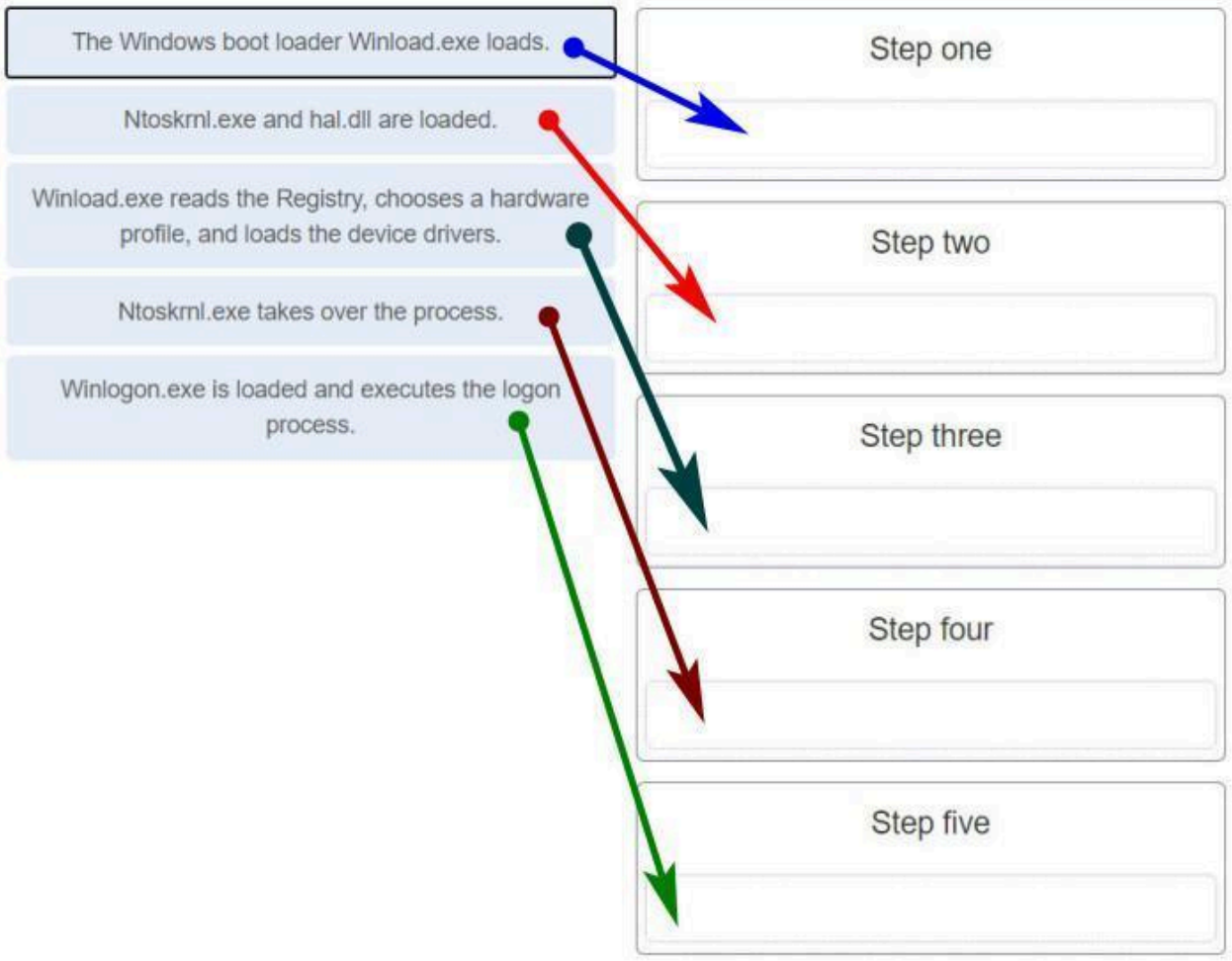
Explanation: The Server Message Block (SMB) protocol is primarily used by Microsoft to share network resources.

24. What is the purpose of using the net accounts command in Windows?

- to display information about shared network resources
- to show a list of computers and network devices on the network
- to start a network service
- **to review the settings of password and logon requirements for users**

Explanation: These are some common net commands:
net accounts – sets password and logon requirements for users
net start – starts a network service or lists running network services
net use – connects, disconnects, and displays information about shared network resources
net view – shows a list of computers and network devices on the network
When used without options, the net accounts command displays the current settings for password, logon limitations, and domain information.

25. Match the Windows 10 boot sequence after the boot manager (bootmgr.exe) loads.



- Step one: The Windows boot loader Winload.exe loads
- Step two: Ntosknl.exe and hal.dll are loaded
- Step three: Winload.exe reads the registry, chooses a hardware profile, and loads the device drivers.
- Step four: Ntoskrnl.exe takes over the process.
- Step five: Winlogon.exe is loaded and excutes the logon process.

26. A user creates a file with .ps1 extension in Windows. What type of file is it?

- PowerShell function
- PowerShell cmdlet
- PowerShell documentation
- **PowerShell script**

Explanation: The types of commands that PowerShell can execute include the following:

- cmdlets – perform an action and return an output or object to the next command that will be executed
- PowerShell scripts – files with a .ps1 extension that contain PowerShell commands that are executed
- PowerShell functions – pieces of code that can be referenced in a script

27. A user logs in to Windows with a regular user account and attempts to use an application that requires administrative privileges. What can the user do to successfully use the application?

- Right-click the application and choose Run as Priviledge .
- Right-click the application and choose Run as Superuser .
- **Right-click the application and choose Run as Administrator .**
- Right-click the application and choose Run as root .

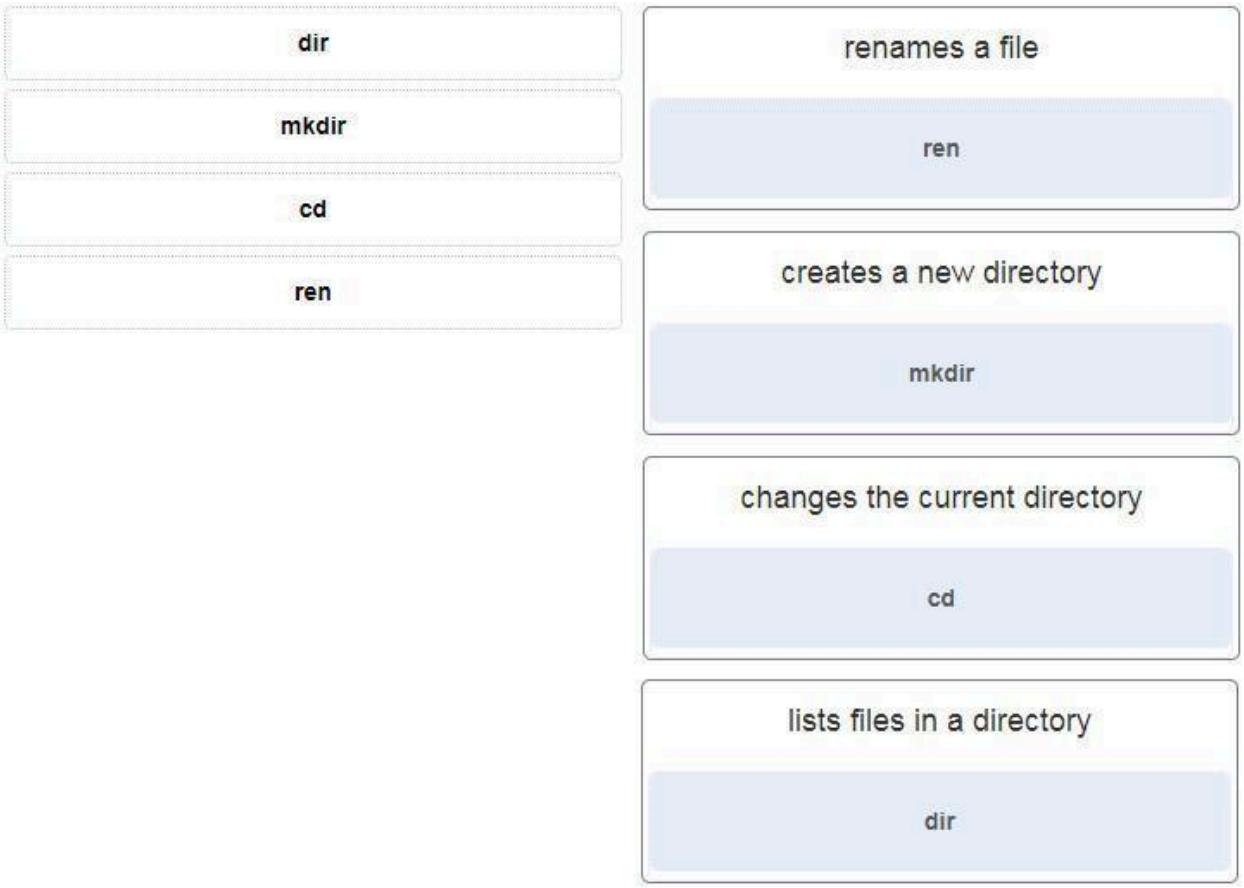
Explanation: As a security best practice, it is advisable not to log on to Windows using the Administrator account or an account with administrative privileges. When it is necessary to run or install software that requires the privileges of the Administrator, the user can right-click the software in the Windows File Explorer and choose **Run as Administrator** .

28. An IT technician wants to create a rule on two Windows 10 computers to prevent an installed application from accessing the public Internet. Which tool would the technician use to accomplish this task?

- Local Security Policy
- Computer Management
- **Windows Defender Firewall with Advanced Security**
- DMZ

Explanation: Windows Firewall with Advanced Security or the Windows 10 Windows Defender Firewall with Advanced Security is used to create inbound and outbound rules, connection security rules such as security traffic between two computers, and monitoring any active connection security rules.

29. Match the Windows command to the description.



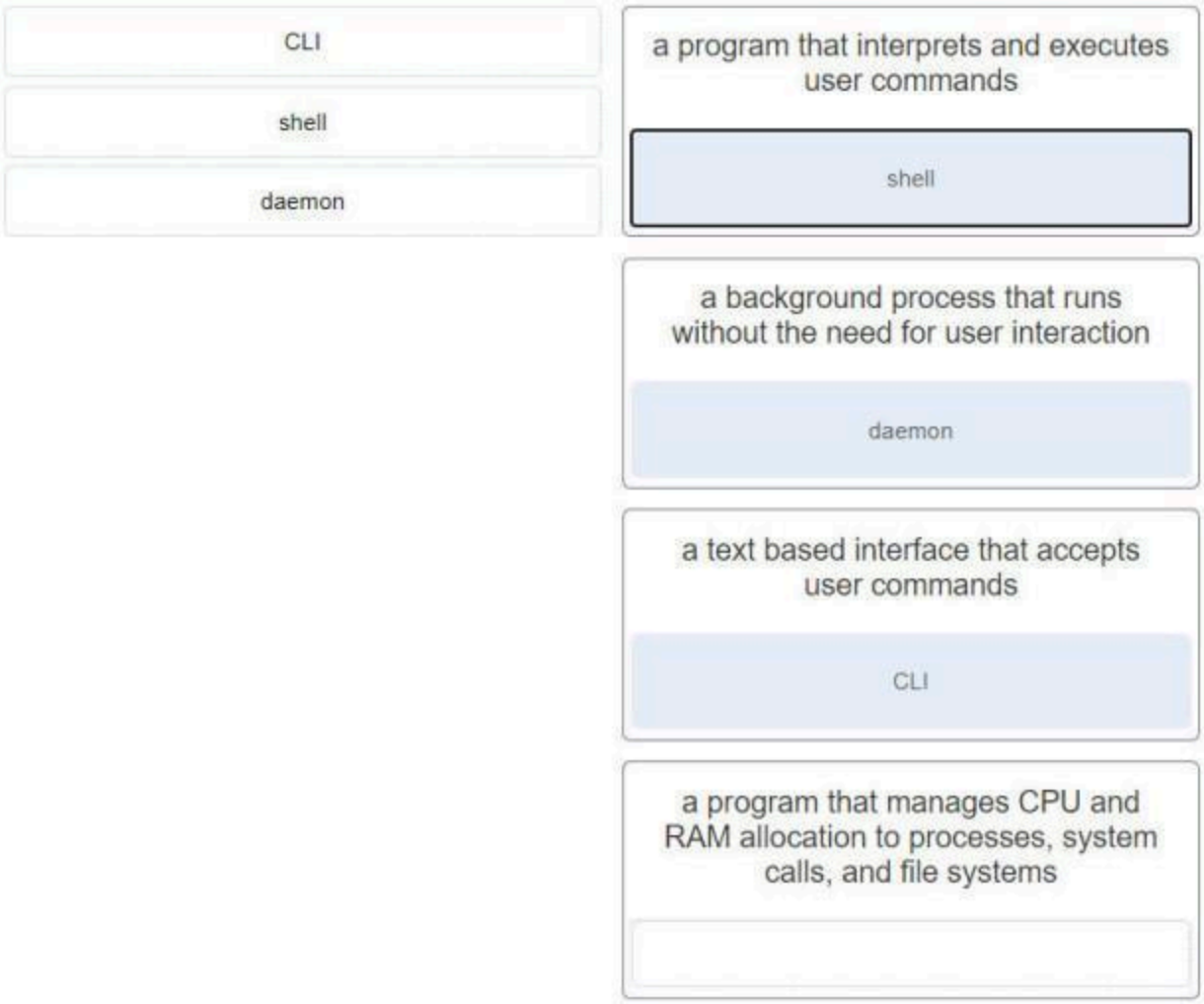
- renames a file ~~> ren
- creates a new directory ~~> mkdir
- changes the current directory ~~> cd
- lists files in a directory ~~> dir

30. What technology was created to replace the BIOS program on modern personal computer motherboards?

- **UEFI**
- MBR
- CMOS
- RAM

Explanation: As of 2015, most personal computer motherboards are shipped with UEFI as the replacement for the BIOS program.

31. Match the Linux system component with the description. (Not all options are used.)



- **CLI** : a text based interface that accepts user commands
- **shell** : a program that interprets and executes user commands
- **daemon** : a background process that runs without the need for user interaction
- **(Empty)** : a program that manages CPU and RAM allocation to processes, system calls, and file systems

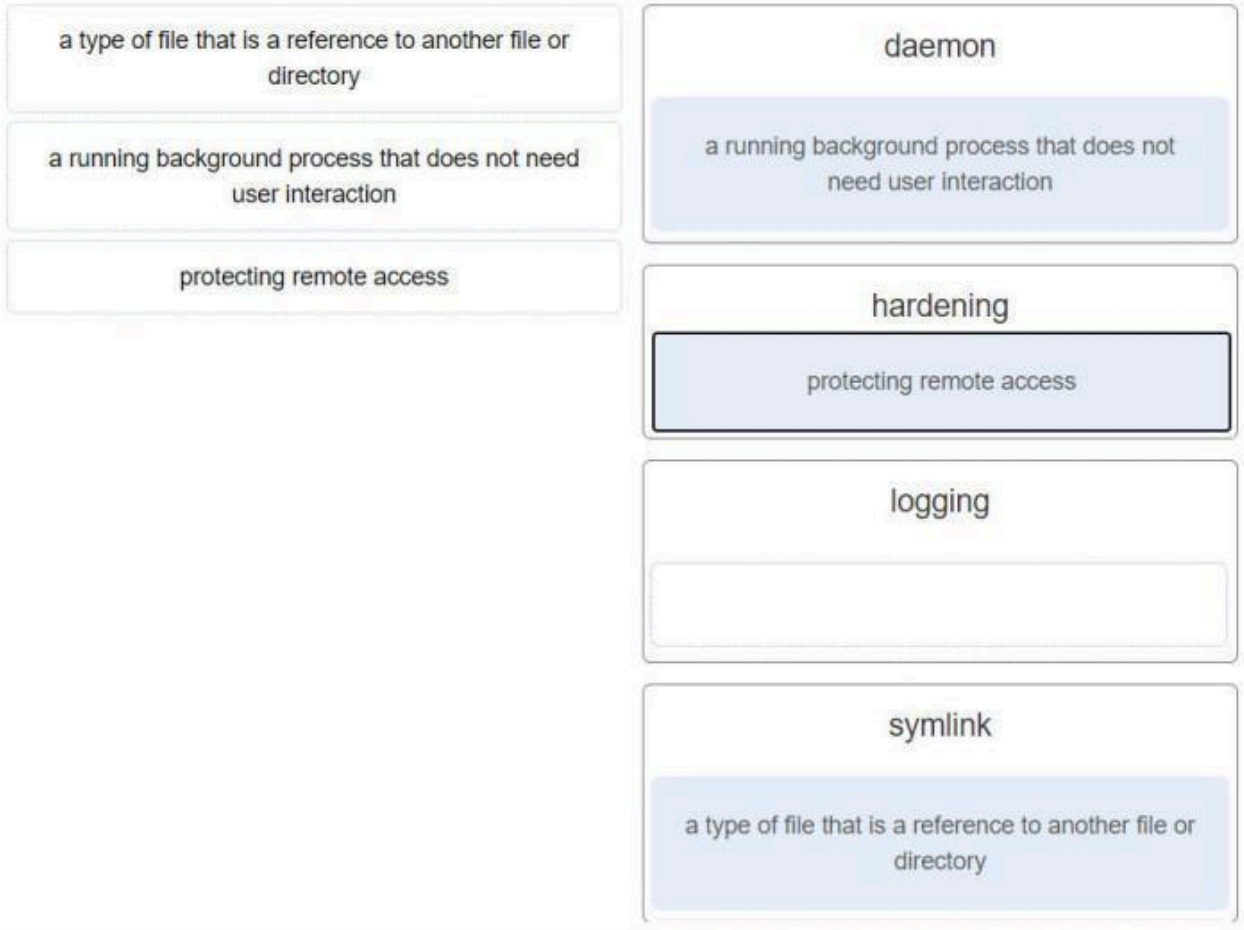
32. What is the outcome when a Linux administrator enters the man man command?

- The **man man** command configures the network interface with a manual address
- The **man man** command opens the most recent log file

- The **man man** command provides a list of commands available at the current prompt
- **The `man man` command provides documentation about the man command**

Explanation: The man command is short for manual and is used to obtain documentation about a Linux command. The command man man would provide documentation about how to use the manual.

33. Match the description to the Linux term. (Not all options are used.)



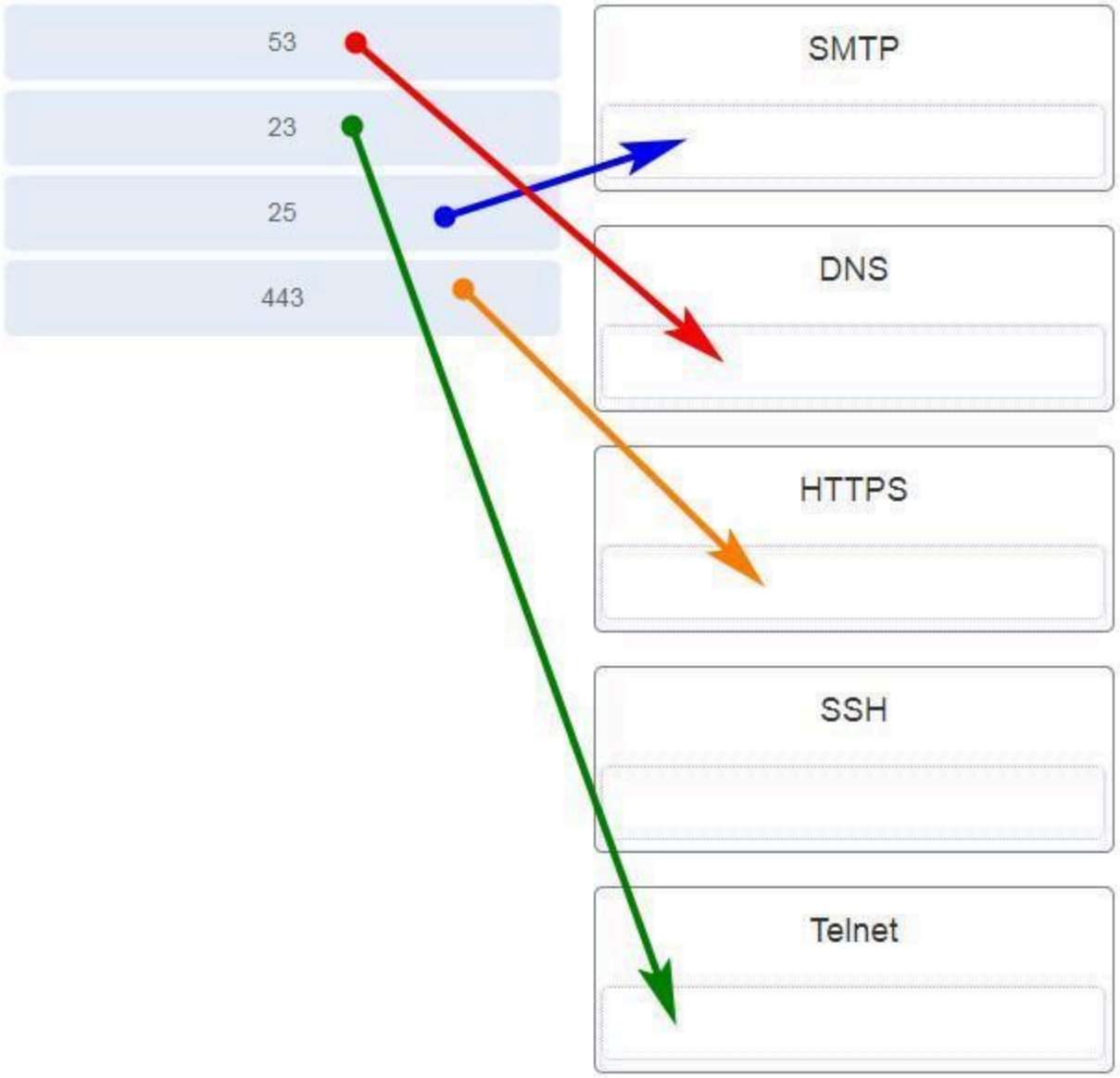
- a type of file that is a reference to another file or directory ~~> symlink
- a running background process that does not need user interaction ~~> daemon
- protecting remote access ~~> hardening
- (Empty) ~~>logging

34. Why is Linux considered to be better protected against malware than other operating systems?

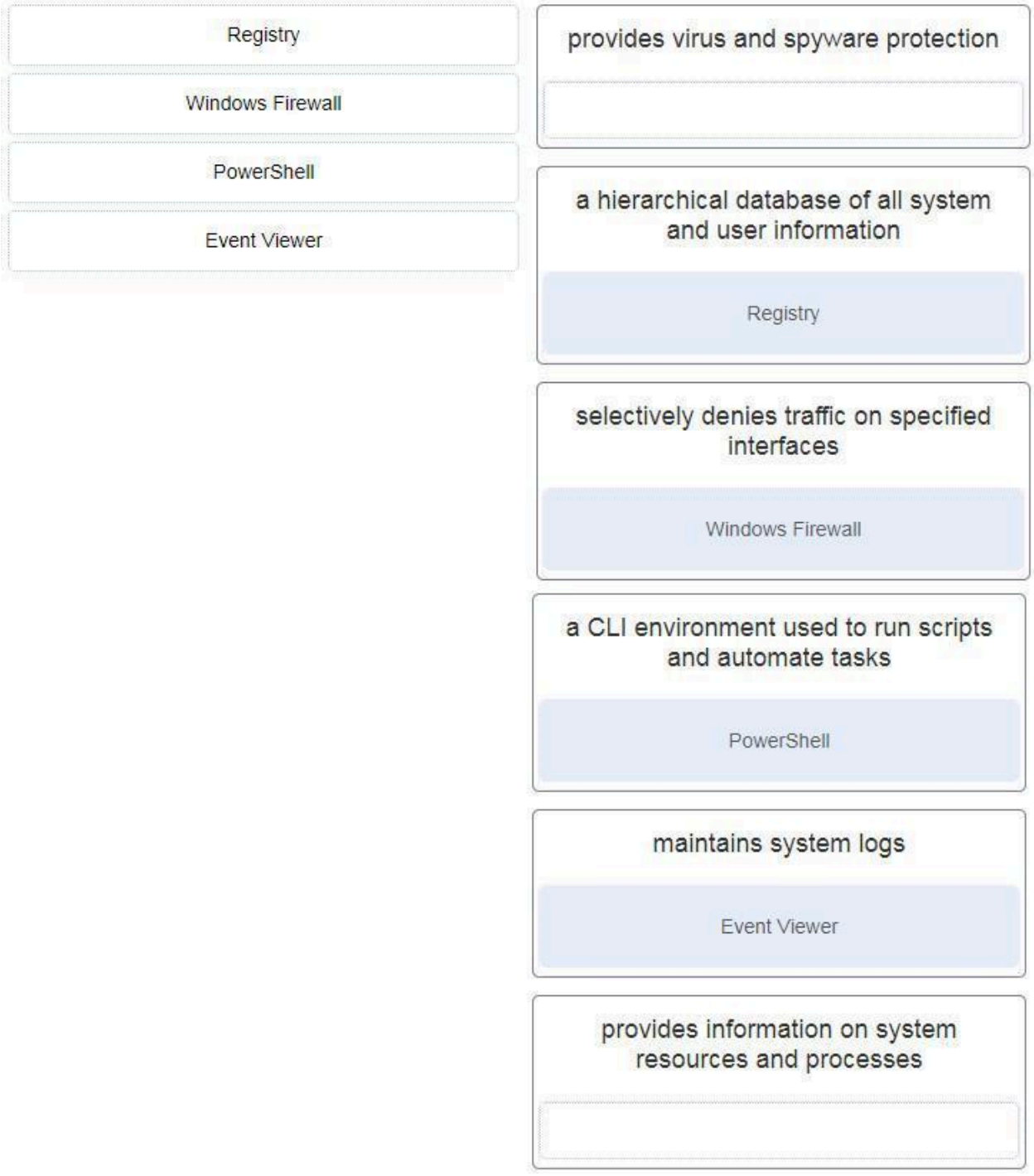
- customizable penetration and protection tools
- fewer deployments
- **file system structure, file permissions, and user account restrictions**
- integrated firewall

Explanation: The Linux operating design including how the file system is structured, standard file permissions, and user account restrictions make Linux a better protected operating system. However, Linux still has vulnerabilities and can have malware installed that affects the operating system.

35. Match the commonly used ports on a Linux server with the corresponding service. (Not all options are used.)



36. Match the Windows system tool with the description. (Not all options are used.)



- Registry : **a hierarchical database of all system and user information**
- Windows Firewall : **selectively denies traffic on specified interfaces**

- PowerShell : **a CLI environment used to run scripts and automate tasks**
- Event Viewer : **maintains system logs**
- (Empty) : **provides information on system resources and processes**
- (Empty) : **provides virus and spyware protection**

37. In the Linux shell, which character is used between two commands to instruct the shell to combine and execute these two commands in sequence?

- $
- #
- %
- **|**

Explanation: In the Linux shell, several commands can be combined to perform a complex task. This technique is known as piping. The piping process is indicated by inserting the character "|" between two consecutive commands.

38. Which Windows tool can be used by a cybersecurity administrator to secure stand-alone computers that are not part of an active directory domain?

- PowerShell
- Windows Defender
- Windows Firewall
- **Local Security Policy**

Explanation: Windows systems that are not part of an Active Directory Domain can use the Windows Local Security Policy to enforce security settings on each stand-alone system.

39. Why would a network administrator choose Linux as an operating system in the Security Operations Center (SOC)?

- It is easier to use than other operating systems.
- More network applications are created for this environment.
- It is more secure than other server operating systems.
- **The administrator has more control over the operating system.**

Explanation: There are several reasons why Linux is a good choice for the SOC.
Linux is open source.
The command line interface is a very powerful environment.
The user has more control over the operating system.
Linux allows for better network communication control.

40. Which two methods can be used to harden a computing device? (Choose two.)

- Allow default services to remain enabled.
- Allow USB auto-detection.
- **Enforce the password history mechanism.**
- Update patches on a strict annual basis irrespective of release date.
- **Ensure physical security.**

Explanation: The basic best practices for device hardening are as follows:
Ensure physical security.
Minimize installed packages.
Disable unused services.
Use SSH and disable the root account login over SSH.
Keep the system updated.
Disable USB auto-detection.
Enforce strong passwords.
Force periodic password changes.
Keep users from reusing old passwords.
Review logs regularly.

CyberOps Associate (Version 1.0) – Modules 5 – 10: Network Fundamentals Group Exam

1. A host is transmitting a broadcast. Which host or hosts will receive it?

- the closest neighbor on the same network
- all hosts in the same network
- all hosts on the Internet

- **a specially defined group of hosts**

2. Which statement describes a characteristic of cloud computing?

- **Applications can be accessed over the Internet by individual users or businesses using any device, anywhere in the world.**
- Devices can connect to the Internet through existing electrical wiring.
- Investment in new infrastructure is required in order to access the cloud.
- A business can connect directly to the Internet without the use of an ISP.

3. A network administrator can successfully ping the server at www.cisco.com, but cannot ping the company web server located at an ISP in another city. Which tool or command would help identify the specific router where the packet was lost or delayed?

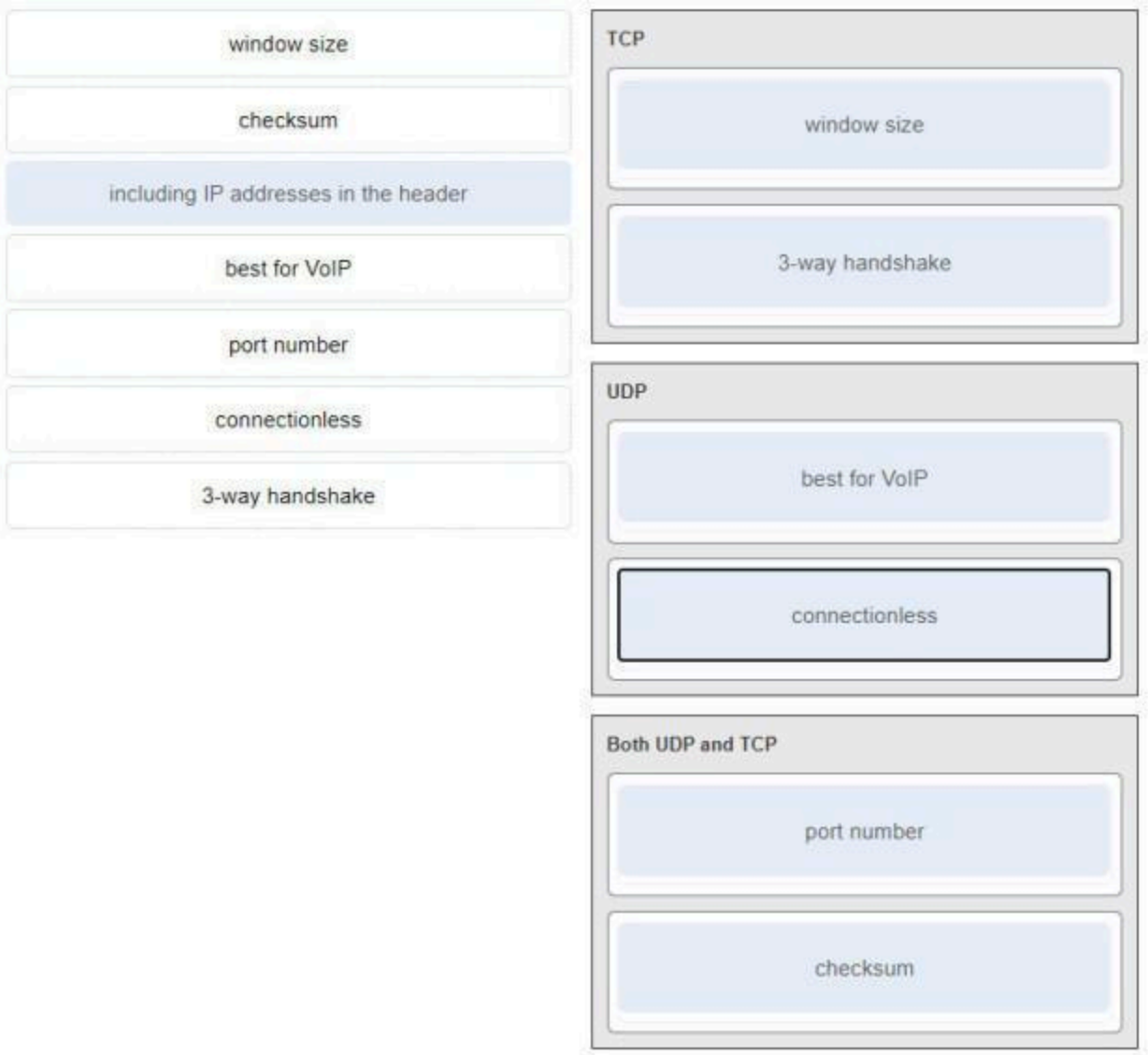
- netstat
- telnet
- **ipconfig**
- traceroute

4. What type of information is contained in an ARP table?

- domain name to IP address mappings
- switch ports associated with destination MAC addresses
- routes to reach destination networks
- **IP address to MAC address mappings**

Explanation: ARP tables are used to store mappings of IP addresses to MAC addresses. When a network device needs to forward a packet, the device knows only the IP address. To deliver the packet on an Ethernet network, a MAC address is needed. ARP resolves the MAC address and stores it in an ARP table.

5. Match the characteristic to the protocol category. (Not all options are used.)



TCP:

- 3-wayhandshake
- window size

UDP:

- connectionless
- best for VoIP

Both UDP and TCP:

- Port number

- checksum

Explanation: TCP uses 3-way handshaking as part of being able to provide reliable communication and window size to provide data flow control. UDP is a connectionless protocol that is great for video conferencing. Both TCP and UDP have port numbers to distinguish between applications and application windows and a checksum field for error detection.

6. When a wireless network in a small office is being set up, which type of IP addressing is typically used on the networked devices?

- **private**
- public
- network
- wireless

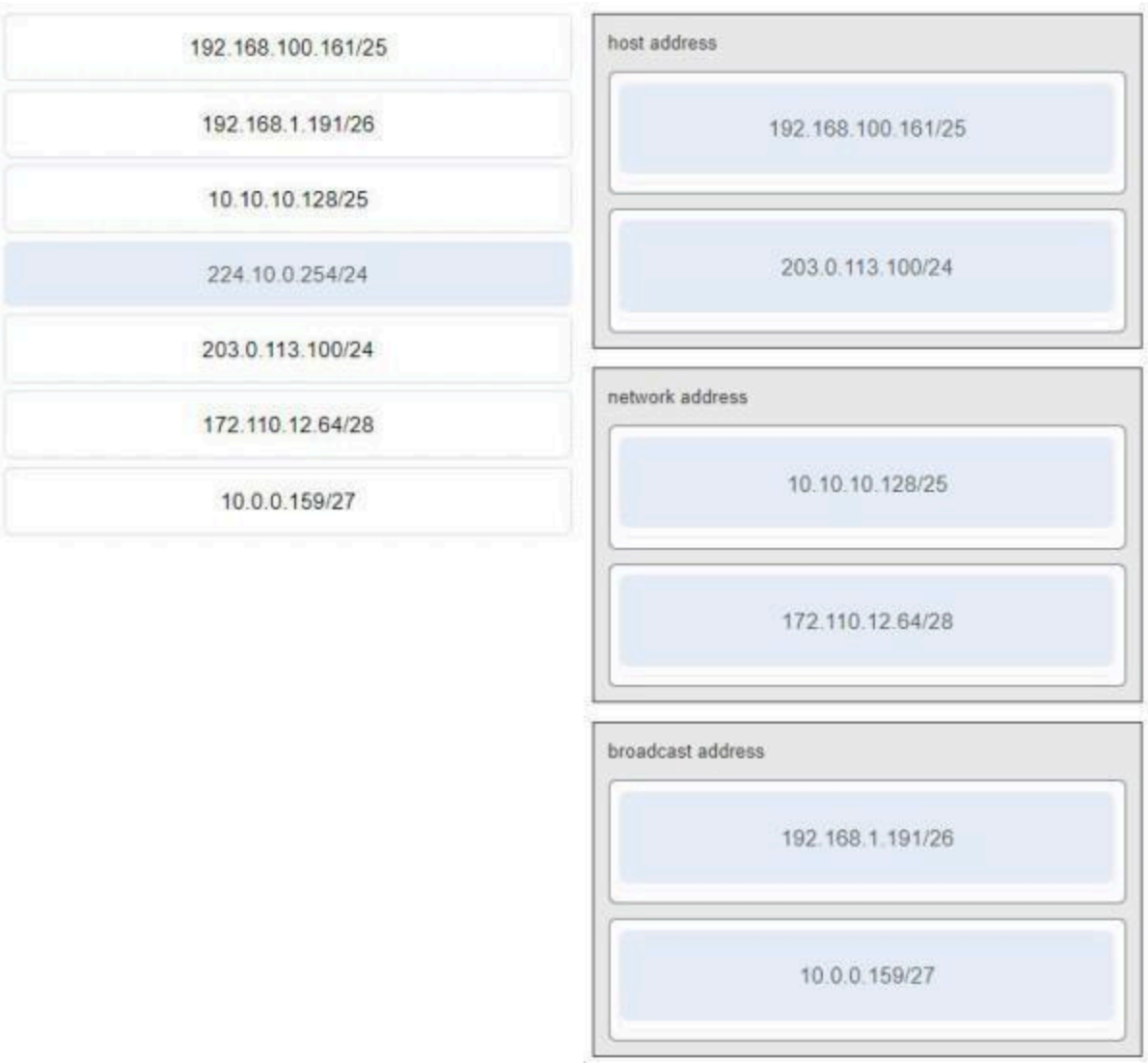
Explanation: In setting up the wireless network in a small office, it is a best practice to use private IP addressing because of the flexibility and easy management it offers.

7. Which two parts are components of an IPv4 address? (Choose two.)

- logical portion
- **host portion**
- broadcast portion
- subnet portion
- **network portion**
- physical portion

Explanation: An IPv4 address is divided into two parts: a network portion – to identify the specific network on which a host resides, and a host portion – to identify specific hosts on a network. A subnet mask is used to identify the length of each portion.

8. Match each IPv4 address to the appropriate address category. (Not all options are used.)



host address:

- 192.168.100.161/25
- 203.0.113.100/24

network address:

- 10.10.10.128/25
- 172.110.12.64/28

broadcast address:

- 192.168.1.191/26
- 10.0.0.159/27

9. A cybersecurity analyst believes an attacker is spoofing the MAC address of the default gateway to perform a man-in-the-middle attack. Which command should the analyst use to view the MAC address a host is using to reach the default gateway?

- route print
- ipconfig /all
- netstat -r
- **arp -a**

Explanation: ARP is a protocol used with IPv4 to map a MAC address to an associated specific IP address. The command arp -a will display the MAC address table on a Windows PC.

10. A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?

- the network domain of the destination host
- the MAC address of the destination host
- the IP address of the default gateway
- **the MAC address of the default gateway**

Explanation: A frame is encapsulated with source and destination MAC addresses. The source device will not know the MAC address of the remote host. An ARP request will be sent by the source and will be responded to by the router. The router will respond with the MAC address of its interface, the one which is connected to the same network as the source.

11. What addresses are mapped by ARP?

- destination IPv4 address to the source MAC address
- **destination MAC address to a destination IPv4 address**
- destination MAC address to the source IPv4 address
- destination IPv4 address to the destination host name

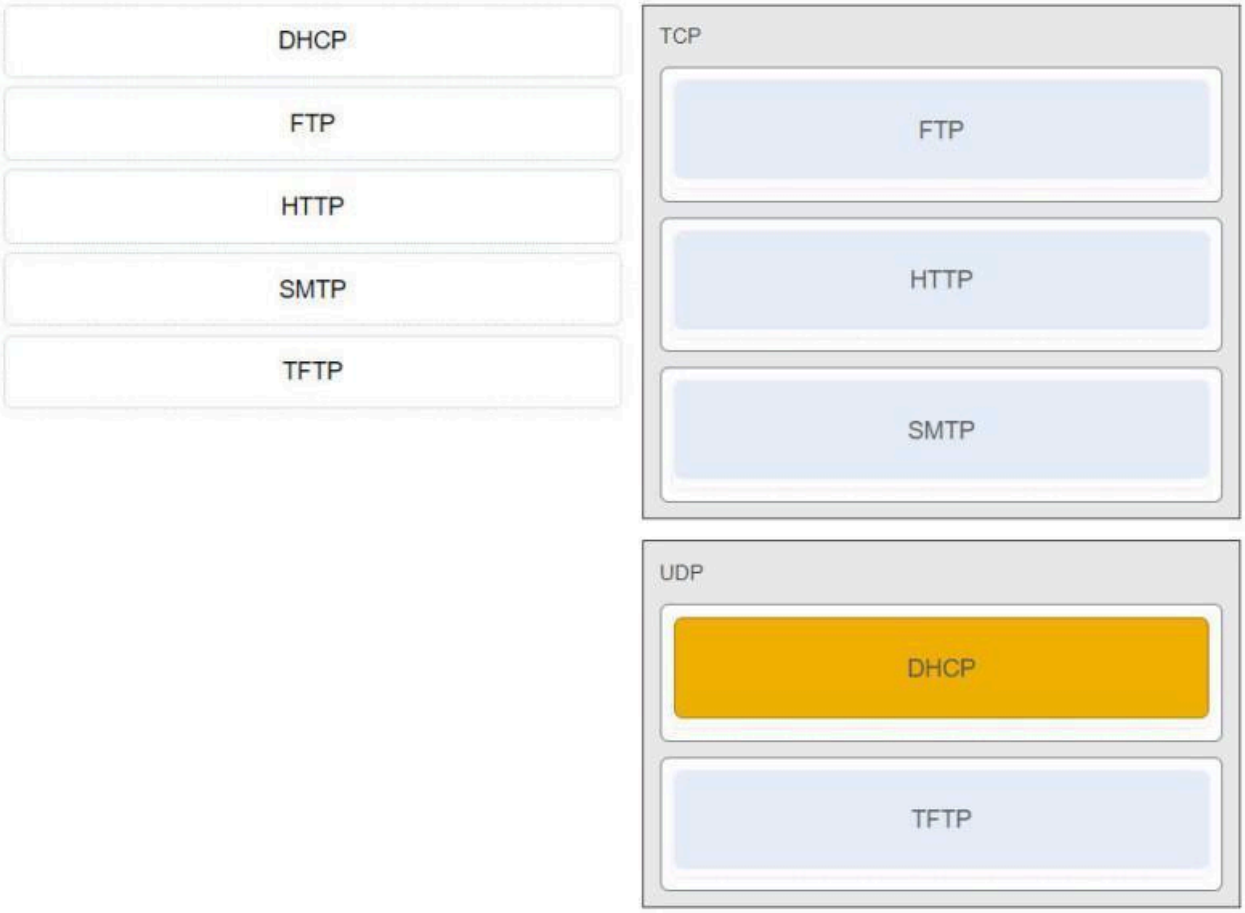
Explanation: ARP, or the Address Resolution Protocol, works by mapping a destination MAC address to a destination IPv4 address. The host knows the destination IPv4 address and uses ARP to resolve the corresponding destination MAC address.

12. What type of information is contained in a DNS MX record?

- the IP address of an authoritative name server
- the FQDN of the alias used to identify a service
- **the domain name mapped to mail exchange servers**
- the IP address for an FQDN entry

Explanation: MX, or mail exchange messages, are used to map a domain name to several mail exchange servers that all belong to the same domain.

13. Match the application protocols to the correct transport protocols.



- **TCP**: FTP, HTTP, SMTP.
- **UDP**: TFTP, DHCP.

14. A PC is downloading a large file from a server. The TCP window is 1000 bytes. The server is sending the file using 100-byte segments.

How many segments will the server send before it requires an acknowledgment from the PC?

- 1000 segments
- 100 segments
- 1 segment
- **10 segments**

Explanation: With a window of 1000 bytes, the destination host accepts segments until all 1000 bytes of data have been received. Then the destination host sends an acknowledgment.

15. A user issues a ping 192.168.250.103 command and receives a response that includes a code of 1 . What does this code represent?

- port unreachable
- network unreachable
- protocol unreachable
- **host unreachable**

16. Which two commands can be used on a Windows host to display the routing table? (Choose two.)

- **netstat -r**
- show ip route
- netstat -s
- **route print**
- tracert

Explanation: On a Windows host, the `route print` or `netstat -r` commands can be used to display the host routing table. Both commands generate the same output. On a router, the `show ip route` command is used to display the routing table. The `netstat -s` command is used to display per-protocol statistics.
The `tracert` command is used to display the path that a packet travels to its destination.

17. What is the full decompressed form of the IPv6 address 2001:420:59:0:1::a/64?

- 2001:4200:5900:0:1:0:0:a000
- 2001:0420:0059:0000:0001:0000:000a
- 2001:0420:0059:0000:0001:000a

- **2001:0420:0059:0000:0001:0000:0000:000a**
- 2001:420:59:0:1:0:0:a
- 2001:4200:5900:0000:1000:0000:0000:a000

Explanation: To decompress an IPv6 address, the two rules of compression must be reversed. Any 16-bit hextet that has less than four hex characters is missing the leading zeros that were removed. An IPv6 address should have a total of 8 groups of 16-bit hextets, a (::) can be replaced with consecutive zeros that were removed.

18. A user issues a ping 2001:db8:FACE:39::10 command and receives a response that includes a code of 2 . What does this code represent?

- host unreachable
- port unreachable
- network unreachable
- **protocol unreachable**

Explanation: When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable. The message will include a code that indicates why the packet could not be delivered. These are some of the Destination Unreachable codes for ICMPv4:

0 : net unreachable
1 : host unreachable
2 : protocol unreachable
3 : port unreachable

19. What message informs IPv6 enabled interfaces to use stateful DHCPv6 for obtaining an IPv6 address?

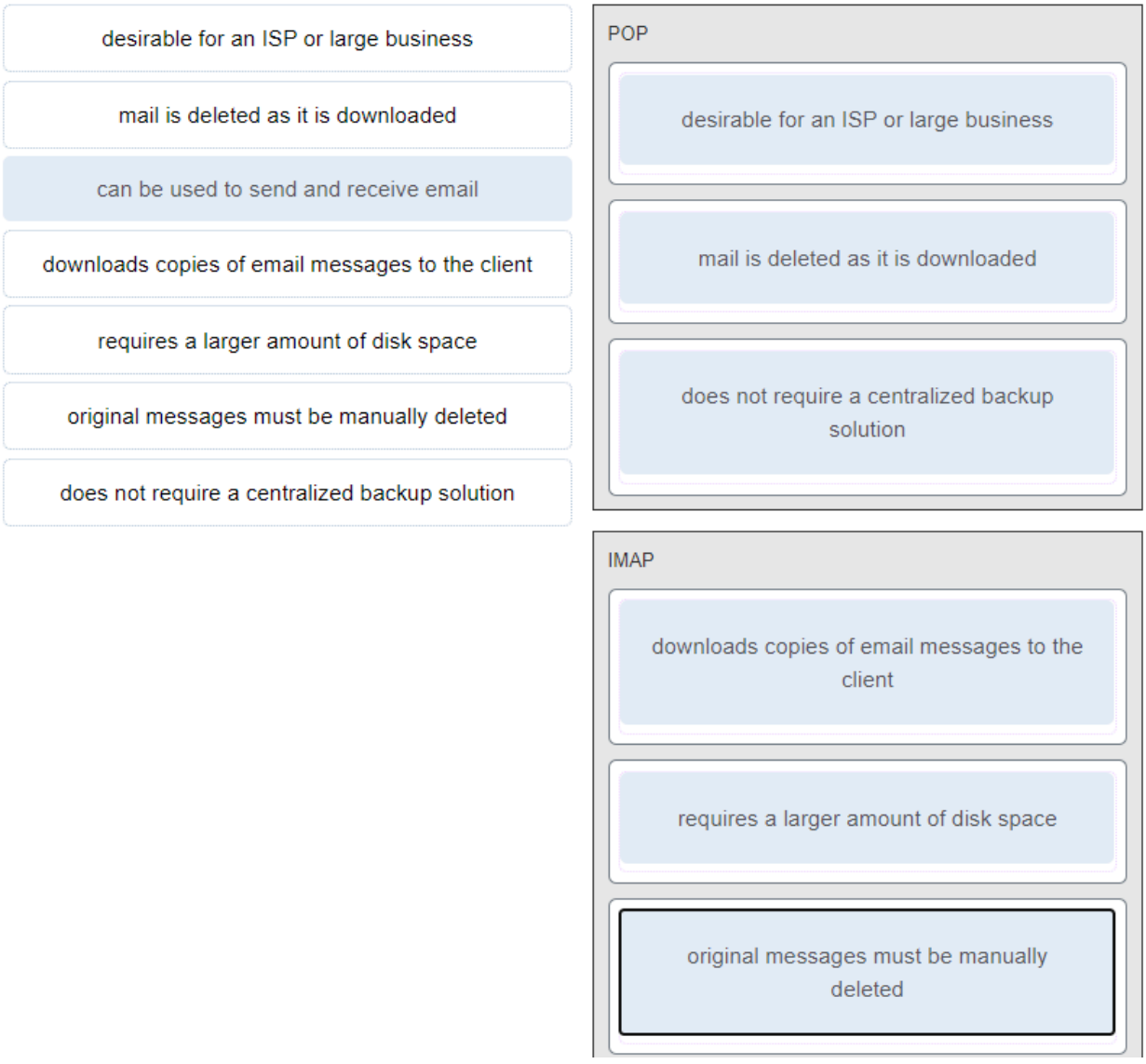
- the ICMPv6 Router Solicitation
- the DHCPv6 Advertise message
- the DHCPv6 Reply message
- **the ICMPv6 Router Advertisement**

Explanation: Before an IPv6 enabled interface will use stateful DHCPv6 to obtain an IPv6 address, the interface must receive an ICMPv6 Router Advertisement with the managed configuration flag (M flag) set to 1.

20. Refer to the exhibit. From the perspective of users behind the NAT router, what type of NAT address is 209.165.201.1?

- **inside global**
- inside local
- outside global
- outside local

21. Match each characteristic to the appropriate email protocol. (Not all options are used.)



POP:

- does not require a centralized backup solution.
- mail is deleted as it is downloaded.
- desirable for an ISP or large business.

IMAP:

- download copies of messages to be the client.
- original messages must be manually deleted.
- requires a larger a mount of disk space.

22. What is done to an IP packet before it is transmitted over the physical medium?

- It is tagged with information guaranteeing reliable delivery.
- It is segmented into smaller individual pieces.
- **It is encapsulated in a Layer 2 frame.**
- It is encapsulated into a TCP segment.

Explanation: When messages are sent on a network, the encapsulation process works from the top of the OSI or TCP/IP model to the bottom. At each layer of the model, the upper layer information is encapsulated into the data field of the next protocol. For example, before an IP packet can be sent, it is encapsulated in a data link frame at Layer 2 so that it can be sent over the physical medium.

23. Which PDU is processed when a host computer is de-encapsulating a message at the transport layer of the TCP/IP model?

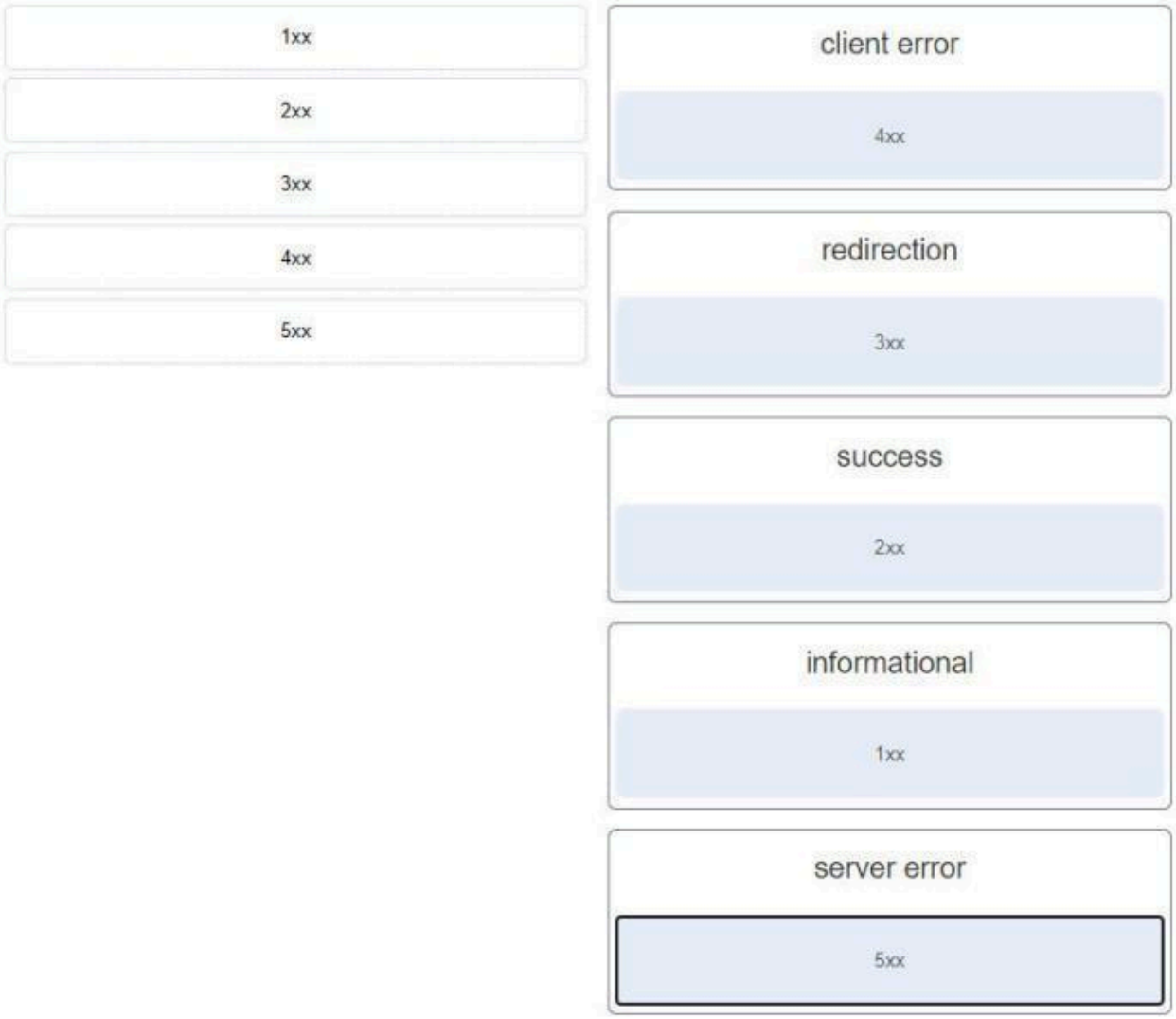
- **segment**
- packet
- frame
- bits

Explanation: At the transport layer, a host computer will de-encapsulate a segment to reassemble data to an acceptable format by the application layer protocol of the TCP/IP model.

14. What is the purpose of ICMP messages?

- to inform routers about network topology changes
- to ensure the delivery of an IP packet
- **to provide feedback of IP packet transmissions**
- to monitor the process of a domain name to IP address resolution

25. Match the HTTP status code group to the type of message generated by the HTTP server.



- **client error:** ~~> 4xx
- **redirection:** ~~> 3xx
- **success:** ~~> 2xx
- **informational:** ~~> 1xx
- **server error:** ~~> 5xx

26. What network service uses the WHOIS protocol?

- HTTPS
- **DNS**
- SMTP

- FTP

Explanation: WHOIS is a TCP-based protocol that is used to identify the owners of internet domains through the DNS system.

27. What action does a DHCPv4 client take if it receives more than one DHCPOFFER from multiple DHCP servers?

- It sends a DHCPNAK and begins the DHCP process over again.
- It accepts both DHCPOFFER messages and sends a DHCPACK.
- It discards both offers and sends a new DHCPDISCOVER.
- **It sends a DHCPREQUEST that identifies which lease offer the client is accepting.**

Explanation: If there are multiple DHCP servers in a network, it is possible for a client to receive more than one DHCPOFFER. In this scenario, the client will only send one DHCPREQUEST, which includes the server from which the client is accepting the offer.

28. Which networking model is being used when an author uploads one chapter document to a file server of a book publisher?

- peer-to-peer
- **client/server**
- master-slave
- point-to-point

Explanation: In the client/server network model, a network device assumes the role of server in order to provide a particular service such as file transfer and storage. In the client/server network model, a dedicated server does not have to be used, but if one is present, the network model being used is the client/server model. In contrast, a peer-to-peer network does not have a dedicated server.

29. Which protocol is a client/server file sharing protocol and also a request/response protocol?

- FTP
- UDP
- TCP
- **SMB**

Explanation: The Server Message Block (SMB) is a client/server file sharing protocol that describes the structure of shared network resources such as directories, files, printers, and serial ports. SMB is also a request/response protocol.

30. How is a DHCPDISCOVER transmitted on a network to reach a DHCP server?

- **A DHCPDISCOVER message is sent with the broadcast IP address as the destination address.**
- A DHCPDISCOVER message is sent with a multicast IP address that all DHCP servers listen to as the destination address.
- A DHCPDISCOVER message is sent with the IP address of the default gateway as the destination address.
- A DHCPDISCOVER message is sent with the IP address of the DHCP server as the destination address.

31. What is a description of a DNS zone transfer?

- **transferring blocks of DNS data from a DNS server to another server**
- the action taken when a DNS server sends a query on behalf of a DNS resolver
- forwarding a request from a DNS server in a subdomain to an authoritative source
- finding an address match and transferring the numbered address from a DNS server to the original requesting client

Explanation: When a server requires data for a zone, it will request a transfer of that data from an authoritative server for that zone. The process of transferring blocks of DNS data between servers is known as a zone transfer.

32. What are the two sizes (minimum and maximum) of an Ethernet frame? (Choose two.)

- 128 bytes
- **64 bytes**
- 1024 bytes
- 56 bytes
- **1518 bytes**

33. A user who is unable to connect to the file server contacts the help desk. The helpdesk technician asks the user to ping the IP address of the default gateway that is configured on the workstation. What is the purpose for this ping command?

- to resolve the domain name of the file server to its IP address
- to request that gateway forward the connection request to the file server
- to obtain a dynamic IP address from the server
- **to test that the host has the capability to reach hosts on other networks**

Explanation: The `ping` command is used to test connectivity between hosts. The other options describe tasks not performed by ping . Pinging the default gateway will test whether the host has the capability to reach hosts on its own network and on other networks.

34. A user gets an IP address of 192.168.0.1 from the company network administrator. A friend of the user at a different company gets the same IP address on another PC. How can two PCs use the same IP address and still reach the Internet, send and receive email, and search the web?

- ISPs use Domain Name Service to change a user IP address into a public IP address that can be used on the Internet.
- Both users must be using the same Internet Service Provider.
- Both users must be on the same network.
- **ISPs use Network Address Translation to change a user IP address into an address that can be used on the Internet.**

Explanation: As user traffic from behind an ISP firewall reaches the gateway device, Network Address Translation changes private IP addresses into a public, routable IP address. Private user addresses remain hidden from the public Internet, and thus more than one user can have the same private IP address, regardless of ISP.

35. How many host addresses are available on the 192.168.10.128/26 network?

- 30
- 32
- 60

- **62**
- 64

36. What are the three ranges of IP addresses that are reserved for internal private use? (Choose three.)

- 64.100.0.0/14
- **192.168.0.0/16**
- 192.31.7.0/24
- **172.16.0.0/12**
- **10.0.0.0/8**
- 127.16.0.0/12

37. Which process failed if a computer cannot access the internet and received an IP address of 169.254.142.5?

- DNS
- IP
- HTTP
- **DHCP**

38. Which statement describes a feature of the IP protocol?

- IP relies on Layer 2 protocols for transmission error control.
- MAC addresses are used during the IP packet encapsulation.
- **IP relies on upper layer services to handle situations of missing or out-of-order packets.**
- IP encapsulation is modified based on network media.

Explanation: IP protocol is a connection-less protocol, considered unreliable in terms of end-to-end delivery. It does not provide error control in the cases where receiving packets are out-of-order or in cases of missing packets. It relies on upper layer services, such as TCP, to resolve these issues.

39. What is a basic characteristic of the IP protocol?

- **connectionless**
- media dependent
- user data segmentation
- reliable end-to-end delivery

40. Which statement describes the ping and tracert commands?

- Both ping and tracert can show results in a graphical display.
- Ping shows whether the transmission is successful; tracert does not.
- **Tracert shows each hop, while ping shows a destination reply only.**
- Tracert uses IP addresses; ping does not.

41. A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?

- cloud computing
- video conferencing
- online collaboration
- **bring your own device**

42. Match each description to its corresponding term. (Not all options are used.)

message encoding

message sizing

message encapsulation

the process of determining when to begin sending messages on a network	
the process of converting information from one format into another acceptable for transmission	message encoding
the process of placing one message format inside another message format	message encapsulation
the process of unpacking one message format from another message format	
the process of breaking up a long message into individual pieces before being sent over the network	message sizing

- **message encoding** : the process of converting information from one format into another acceptable for transmission
- **message sizing** : the process of breaking up a long message into individual pieces before being sent over the network
- **message encapsulation** : the process of placing one message format inside another message format

- **(Empty)** : the process of determining when to begin sending messages on a network
- **(Empty)** : the process of unpacking one message format from another message format

43. Which method would an IPv6-enabled host using SLAAC employ to learn the address of the default gateway?

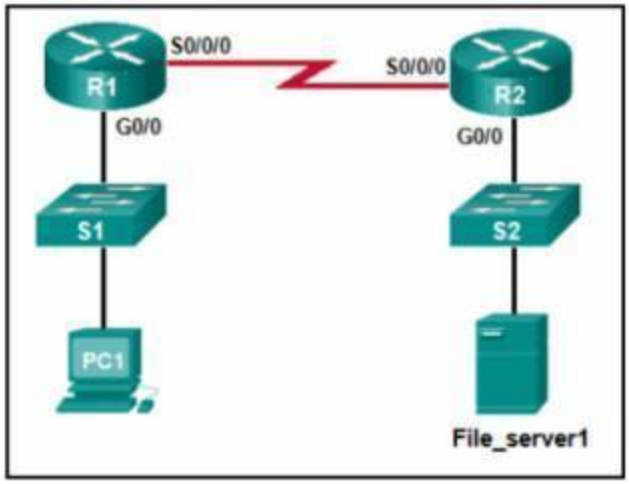
- **router advertisement messages received from the link router**
- router solicitation messages received from the link router
- neighbor advertisement messages received from link neighbors
- neighbor solicitation messages sent to link neighbors

44. Which type of transmission is used to transmit a single video stream such as a web-based video conference to a select number of users?

- anycast
- broadcast
- unicast
- **multicast**

Explanation: An anycast is used with IPv6 transmissions. A unicast is a transmission to a single host destination. A broadcast is a transmission sent to all hosts on a destination network.

45. Refer to the exhibit. PC1 attempts to connect to File_server1 and sends an ARP request to obtain a destination MAC address. Which MAC address will PC1 receive in the ARP reply?



- the MAC address of the GO/O interface on R2
- the MAC address of S2
- the MAC address of S1
- the MAC address of File_server1
- **the MAC address of the GO/O interface on R1**

Explanation: PC1 must have a MAC address to use as a destination Layer 2 address. PC1 will send an ARP request as a broadcast and R1 will send back an ARP reply with its G0/0 interface MAC address. PC1 can then forward the packet to the MAC address of the default gateway, R1.

46. What is the result of an ARP poisoning attack?

- Network clients are infected with a virus.
- Network clients experience a denial of service.
- Client memory buffers are overwhelmed.
- **Client information is stolen.**

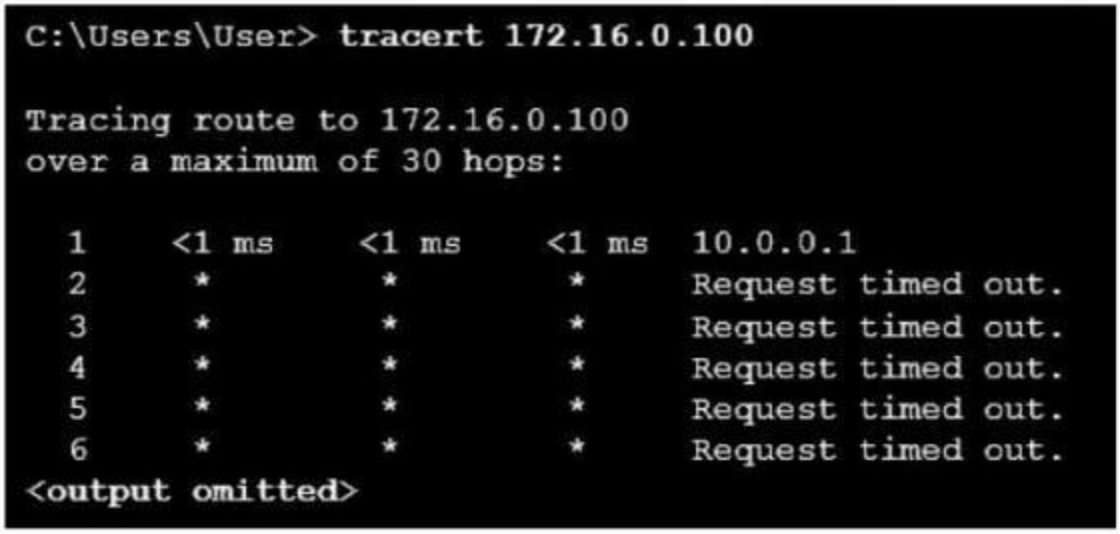
Explanation: ARP poisoning is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway. The attacker, who is effectively doing an MITM attack, pretends to be the default gateway and sends an ARP reply to the transmitter of the ARP request. The receiver of the ARP reply will add the wrong MAC address to the ARP table and will send the packets to the attacker. Therefore, all traffic to the default gateway will funnel through the attacker device.

47. What is the function of the HTTP GET message?

- to upload content to a web server from a web client
- to retrieve client email from an email server using TCP port 110
- **to request an HTML page from a web server**
- to send error information from a web server to a web client

48. Refer to the exhibit. This PC is unable to communicate with the host at 172.16.0.100. What information can be gathered from the

displayed output?



- The target host is turned off.
- **The communication fails after the default gateway.**
- 172.16.0.100 is only a single hop away.
- This PC has the wrong subnet configured on its NIC

Explanation: The `tracert` command shows the path a packet takes through the network to the destination. In this example, only a response from the first router in the path is received, and all other responses time out. The first router is the default gateway for this host, and because a response is received from the router, it can be assumed that this host is on the same subnet as the router.

49. A user issues a ping 192.168.250.103 command and receives a response that includes a code of 1. What does this code represent?

- network unreachable
- port unreachable
- protocol unreachable
- **host unreachable**

50. Which two operations are provided by TCP but not by UDP? (Choose two.)

- **retransmitting any unacknowledged data**
- **acknowledging received data**
- reconstructing data in the order received
- identifying the applications

- tracking individual conversations

Explanation: Numbering and tracking data segments, acknowledging received data, and retransmitting any unacknowledged data are reliability operations to ensure that all of the data arrives at the destination. UDP does not provide reliability. Both TCP and UDP identify the applications and track individual conversations. UDP does not number data segments and reconstructs data in the order that it is received.

51. A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?

- when the router receives an ICMP Time Exceeded message
- when the RTT value reaches zero
- when the values of both the Echo Request and Echo Reply messages reach zero
- when the host responds with an ICMP Echo Reply message
- **when the value in the TTL field reaches zero**

Explanation: When a router receives a traceroute packet, the value in the TTL field is decremented by 1. When the value in the field reaches zero, the receiving router will not forward the packet, and will send an ICMP Time Exceeded message back to the source.

52. A network administrator is testing network connectivity by issuing the ping command on a router. Which symbol will be displayed to indicate that a time expired during the wait for an ICMP echo reply message?

- U
- .
- !
- $

Explanation: When the `ping` command is issued on a router, the most common indicators are as follows:
! – indicates receipt of an ICMP echo reply message
. – indicates a time expired while waiting for an ICMP echo reply message
U – an ICMP message of unreachability was received

53. A technician is configuring email on a mobile device. The user wants to be able to keep the original email on the server, organize it into folders, and synchronize the folders between the mobile device and the server. Which email protocol should the technician use?

- SMTP
- MIME
- POP3
- **IMAP**

54. At which OSI layer is a source MAC address added to a PDU during the encapsulation process?

- application layer
- presentation layer
- **data link layer**
- transport layer

55. Which value, that is contained in an IPv4 header field, is decremented by each router that receives a packet?

- **Time-to-Live**
- Fragment Offset
- Header Length
- Differentiated Services

Explanation: When a router receives a packet, the router will decrement the Time-to-Live (TTL) field by one. When the field reaches zero, the receiving router will discard the packet and will send an ICMP Time Exceeded message to the sender.

56. What are three responsibilities of the transport layer? (Choose three.)

- **identifying the applications and services on the client and server that should handle transmitted data**
- conducting error detection of the contents in frames
- **meeting the reliability requirements of applications, if any**
- directing packets towards the destination network
- formatting data into a compatible form for receipt by the destination devices

- **multiplexing multiple communication streams from many users or applications on the same network**

Explanation: The transport layer has several responsibilities. Some of the primary responsibilities include the following:
Tracking the individual communication streams between applications on the source and destination hosts
Segmenting data at the source and reassembling the data at the destination
Identifying the proper application for each communication stream through the use of port numbers
Multiplexing the communications of multiple users or applications over a single network
Managing the reliability requirements of applications

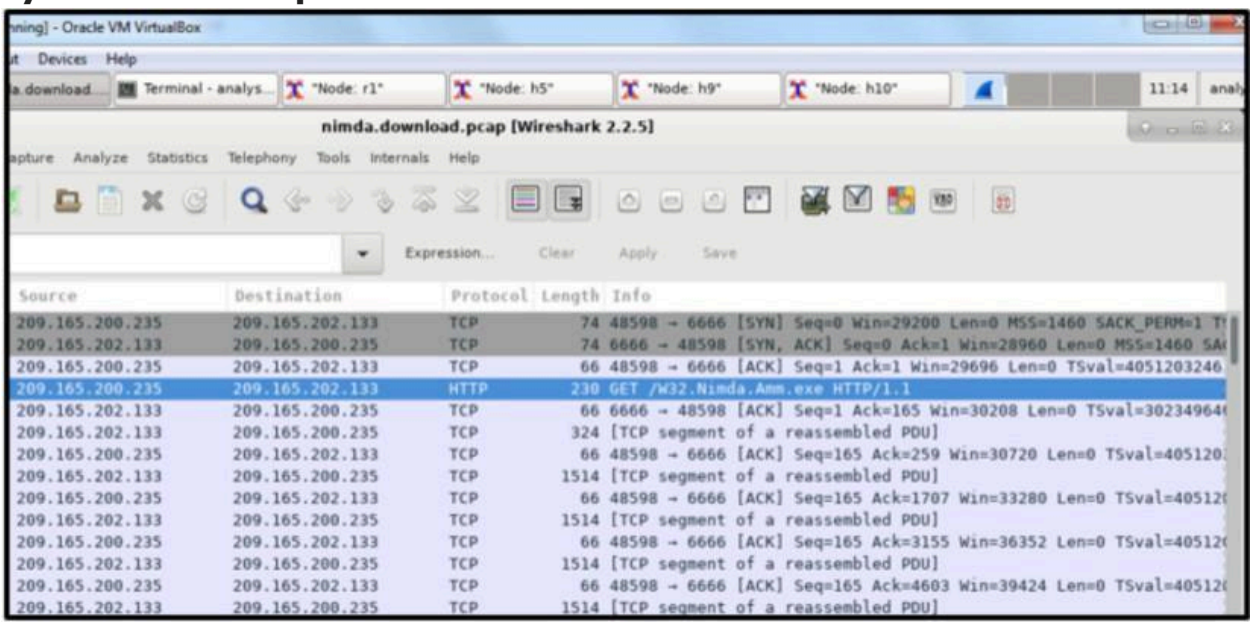
57. How does network scanning help assess operations security?

- **It can detect open TCP ports on network systems.**
- It can detect weak or blank passwords.
- It can simulate attacks from malicious sources.
- It can log abnormal activity.

Explanation: Network scanning can help a network administrator strengthen the security of the network and systems by identifying open TCP and UDP ports that could be targets of an attack.

58. Refer to the exhibit. A network security analyst is examining captured data using Wireshark. The captured frames indicate that a host is downloading malware from a server. Which source port is used

by the host to request the download?



- 66
- 1514
- 6666
- **48598**

Explanation: During the TCP three-way handshake process, the output shows that the host uses source port 48598 to initiate the connection and request the download.

59. What are three responsibilities of the transport layer? (Choose three.)

- **identifying the applications and services on the client and server that should handle transmitted data**
- conducting error detection of the contents in frames
- **meeting the reliability requirements of applications, if any**
- directing packets towards the destination network
- formatting data into a compatible form for receipt by the destination devices
- **multiplexing multiple communication streams from many users or applications on the same network**

Explanation: The transport layer has several responsibilities. Some of the primary responsibilities include the following:
Tracking the individual communication streams between applications

on the source and destination hosts
Segmenting data at the source and reassembling the data at the destination
Identifying the proper application for each communication stream through the use of port numbers
Multiplexing the communications of multiple users or applications over a single network
Managing the reliability requirements of applications

60. Which two ICMP messages are used by both IPv4 and IPv6 protocols? (Choose two.)

- **route redirection**
- neighbor solicitation
- router solicitation
- router advertisement
- **protocol unreachable**

Explanation: The ICMP messages common to both ICMPv4 and ICMPv6 include: host confirmation, destination (net, host, protocol, port) or service unreachable, time exceeded, and route redirection. Router solicitation, neighbor solicitation, and router advertisement are new protocols implemented in ICMPv6.

61. What mechanism is used by a router to prevent a received IPv4 packet from traveling endlessly on a network?

- It checks the value of the TTL field and if it is 100, it discards the packet and sends a Destination Unreachable message to the source host.
- **It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Time Exceeded message to the source host.**
- It checks the value of the TTL field and if it is 0, it discards the packet and sends a Destination Unreachable message to the source host.
- It increments the value of the TTL field by 1 and if the result is 100, it discards the packet and sends a Parameter Problem message to the source host.

62. A device has been assigned the IPv6 address of 2001:0db8:cafe:4500:1000:00d8:0058:00ab/64. Which is the host identifier of the device?

- 2001:0db8:cafe:4500:1000:00d8:0058:00ab
- 00ab
- 2001:0db8:cafe:4500
- **1000:00d8:0058:00ab**

Explanation: The address has a prefix length of /64. Thus the first 64 bits represent the network portion, whereas the last 64 bits represent the host portion of the IPv6 address.

63. What three application layer protocols are part of the TCP/IP protocol suite? (Choose three.)

- **DHCP**
- PPP
- **FTP**
- **DNS**
- NAT
- ARP

Explanation: DNS, DHCP, and FTP are all application layer protocols in the TCP/IP protocol suite. ARP and PPP are network access layer protocols, and NAT is an internet layer protocol in the TCP/IP protocol suite.

64. A computer can access devices on the same network but cannot access devices on other networks. What is the probable cause of this problem?

- The computer has an invalid IP address.
- The cable is not connected properly to the NIC.
- The computer has an incorrect subnet mask.
- **The computer has an invalid default gateway address.**

Explanation: The default gateway is the address of the device a host uses to access the Internet or another network. If the default gateway is missing or incorrect, that host will not be able to communicate outside the local network. Because the host can access other hosts on the local

network, the network cable and the other parts of the IP configuration are working.

CyberOps Associate (Version 1.0) – Modules 11 – 12: Network Infrastructure Security Group Exam

1. For which discovery mode will an AP generate the most traffic on a WLAN?

- passive mode
- mixed mode
- active mode
- **open mode**

2. Which parameter is commonly used to identify a wireless network name when a home wireless AP is being configured?

- **ad hoc**
- SSID
- BESS
- ESS

3. Which two protocols are considered distance vector routing protocols? (Choose two.)

- ISIS
- RIP
- **BGP**
- **EIGRP**
- OSPF

4. Which AAA component can be established using token cards?

- **authentication**
- accounting
- authorization
- auditing

Explanation: The authentication component of AAA is established using username and password combinations, challenge and response questions, and token cards. The authorization component of AAA determines which resources the user can access and which operations the user is allowed to perform. The accounting and auditing component of AAA keeps track of how network resources are used.

5. Which statement describes a VPN?

- VPNs use open source virtualization software to create the tunnel through the Internet.
- VPNs use dedicated physical connections to transfer data between remote users.
- VPNs use logical connections to create public networks through the Internet.
- **VPNs use virtual connections to create a private network through a public network.**

Explanation: A VPN is a private network that is created over a public network. Instead of using dedicated physical connections, a VPN uses virtual connections routed through a public network between two network devices.

6. What is an advantage of HIPS that is not provided by IDS?

- **HIPS protects critical system resources and monitors operating system processes.**
- HIPS deploys sensors at network entry points and protects critical network segments.
- HIPS monitors network processes and protects critical files.
- HIPS provides quick analysis of events through detailed logging.

Explanation: Network-based IDS (NIDS) sensors are typically deployed in offline mode. They do not protect individual hosts. Host-based IPS (HIPS) is software installed on a single host to monitor and analyze suspicious activity. It can monitor and protect operating system and critical system processes that are specific to that host. HIPS can be thought of as a combination of antivirus software, antimalware software, and a firewall.

7. Which statement describes a difference between RADIUS and TACACS+?

- RADIUS separates authentication and authorization whereas TACACS+ combines them as one process.
- RADIUS is supported by the Cisco Secure ACS software whereas TACACS+ is not.
- RADIUS uses TCP whereas TACACS+ uses UDP.
- **RADIUS encrypts only the password whereas TACACS+ encrypts all communication.**

8. What are two disadvantages of using an IDS? (Choose two.)

- **The IDS does not stop malicious traffic.**
- The IDS works offline using copies of network traffic.
- The IDS has no impact on traffic.
- The IDS analyzes actual forwarded packets.
- **The IDS requires other devices to respond to attacks.**

Explanation: The disadvantage of operating with mirrored traffic is that the IDS cannot stop malicious single-packet attacks from reaching the target before responding to the attack. Also, an IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack. An advantage of an IDS is that by working offline using mirrored traffic, it has no impact on traffic flow.

9. Which statement describes one of the rules that govern interface behavior in the context of implementing a zone-based policy firewall configuration?

- An administrator can assign interfaces to zones, regardless of whether the zone has been configured.
- An administrator can assign an interface to multiple security zones.
- **By default, traffic is allowed to flow among interfaces that are members of the same zone.**
- By default, traffic is allowed to flow between a zone member interface and any interface that is not a zone member.

Explanation: An interface can belong to only one zone. Creating a zone is the first step in configuring a zone-based policy firewall. A zone cannot be assigned to an interface if the zone has not been created. Traffic can never flow between an interface that is assigned to a zone and an interface that has not been assigned to a zone.

10. Which technique is necessary to ensure a private transfer of data using a VPN?

- **encryption**
- virtualization
- scalability
- authorization

Explanation: Confidential and secure transfers of data with VPNs require data encryption.

11. Which two devices would commonly be found at the access layer of the hierarchical enterprise LAN design model? (Choose two.)

- modular switch
- Layer 3 device
- **Layer 2 switch**
- firewall
- **access point**

Explanation: While some designs do route at the access layer, the two devices that should always be placed at the access layer of the hierarchical design model are an access point and a Layer 2 switch. A modular switch is commonly used at the core layer. Routing by a Layer 3 device is commonly used in the distribution layer. The firewall is a device in the Internet edge network design.

12. Which two statements are true about NTP servers in an enterprise network? (Choose two.)

- There can only be one NTP server on an enterprise network.
- **NTP servers at stratum 1 are directly connected to an authoritative time source.**
- NTP servers control the mean time between failures (MTBF) for key network devices.
- **NTP servers ensure an accurate time stamp on logging and debugging information.**
- All NTP servers synchronize directly to a stratum 1 time source.

Explanation: Network Time Protocol (NTP) is used to synchronize the time across all devices on the network to make sure accurate timestamping on devices for managing, securing and troubleshooting. NTP networks use a hierarchical system of time sources. Each level in

this hierarchical system is called a stratum. The stratum 1 devices are directly connected to the authoritative time sources.

13. In the data gathering process, which type of device will listen for traffic, but only gather traffic statistics?

- **NetFlow collector**
- NMS
- SNMP agent
- syslog server

Explanation: A NetFlow collector is the device that receives traffic statistics from networking devices. NetFlow only gathers traffic statistics, unlike syslog and SNMP which can collect various network events.

14. Which two protocols are link-state routing protocols? (Choose two.)

- **ISIS**
- EIGRP
- BGP
- RIP
- **OSPF**

15. What is the function of the distribution layer of the three-layer network design model?

- providing direct access to the network
- providing secure access to the Internet
- **aggregating access layer connections**
- providing high speed connection to the network edge

Explanation: The function of the distribution layer is to provide connectivity to services and to aggregate the access layer connections

16. What two components of traditional web security appliances are examples of functions integrated into a Cisco Web Security Appliance? (Choose two.)

- email virus and spam filtering
- VPN connection
- firewall
- **web reporting**

- **URL filtering**

Explanation: The Cisco Web Security Appliance is a secure web gateway which combines advanced malware protection, application visibility and control, acceptable use policy controls, reporting, and secure mobility functions. With traditional web security appliances, these functions are typically provided through multiple appliances. It is not a firewall appliance in that it only filters web traffic. It does not provide VPN connections, nor does it provide email virus and spam filtering; the Cisco Email Security Appliance provides these functions.

17. What are two types of addresses found on network end devices? (Choose two.)

- return
- **IP**
- **MAC**
- TCP
- UDP

Explanation: Intermediary devices use two types of addresses when sending messages to the final destination device, MAC and IP addresses. TCP and UDP are protocols used at Layer 4 to identify what port numbers are being used on the source and destination devices. A return address is used when mailing a letter, not in networking.

18. What is a characteristic of the WLAN passive discover mode?

- The client must know the name of the SSID to begin the discover process.
- The client begins the discover process by sending a probe request.
- The beaconing feature on the AP is disabled.
- **The AP periodically sends beacon frames containing the SSID.**

Explanation: In passive mode, the wireless clients learn what networks and APs are available. The client learns this information from beacon frames, sent by the APs, that contain the WLAN SSID, supported standards, and security settings.

19. What is a characteristic of a routed port that is configured on a Cisco switch?

- It supports subinterfaces.
- It is associated with a single VLAN.
- It runs STP to prevent loops.
- **It is assigned an IP address.**

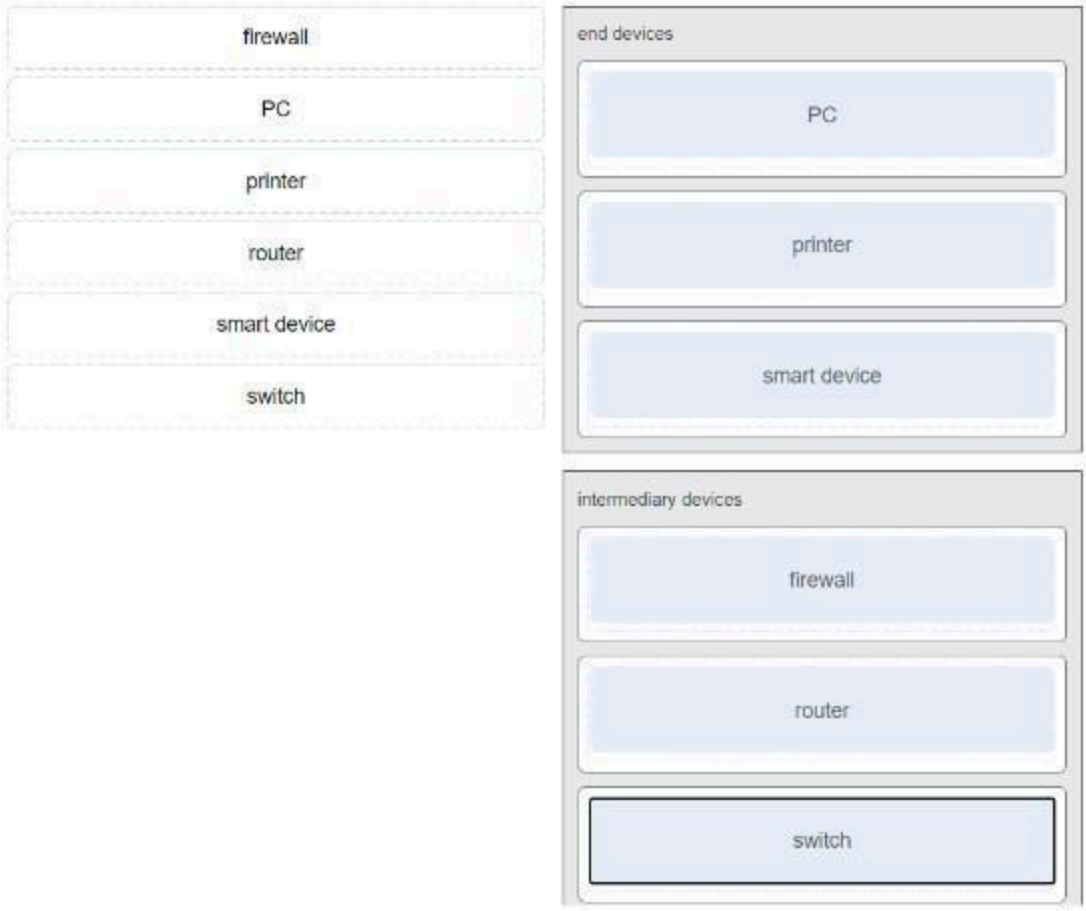
Explanation: Routed ports on a Cisco switch behave similarly to those on a router. They are configured with an IP address and forward Layer 3 packets. Unlike Layer 2 switch interfaces, routed ports do not support STP, nor do they support subinterfaces as routers do.

20. What action does an Ethernet switch take when it receives a frame with an unknown Layer 2 source address?

- It forwards the frame out all interfaces except the interface on which it was received.
- It forwards the frame to the default gateway.
- **It records the source address in the address table of the switch.**
- It drops the frame.

Explanation: When an Ethernet switch receives a frame with an unknown Layer 2 address, the switch records that address in the address table.

21.. Match each device to a category.



22. What is a host-based intrusion detection system (HIDS)?

- It detects and stops potential direct attacks but does not scan for malware.
- It is an agentless system that scans files on a host for potential malware.
- It identifies potential attacks and sends alerts but does not stop the traffic.
- **It combines the functionalities of antimalware applications with firewall protection.**

Explanation: Accurrent HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall protection. An HIDS not only detects malware but also prevents it from executing.

Because the HIDS runs directly on the host, itis considered an agent-based system.

23. What type of route is created when a network administrator manually configures a route that has an active exit interface?

- directly connected
- **static**
- local
- dynamic

Explanation: A static route is one that is manually configured by the network administrator.

24. Which characteristic describes a wireless client operating in active mode?

- must be configured for security before attaching to an AP
- broadcasts probes that request the SSID
- ability to dynamically change channels
- **must know the SSID to connect to an AP**

25. Which routing protocol is used to exchange routes between internet service providers?

- OSPF
- EIGRP
- ISIS
- **BGP**
- RIP

Explanation: BGP is a path vector routing protocol and it is used by internet service providers to exchange routes.

26. What is the first step in the CSMA/CA process when a wireless client is attempting to communicate on the wireless network?

- The client sends an RTS message to the AP.
- The client sends a test frame onto the channel.
- **The client listens for traffic on the channel.**
- The AP sends a CTS message to the client.

Explanation: When a wireless client is attempting to communicate on the network, it will first listen to the channel to be sure it is idle. Next, the client sends an RTS message to the AP to request dedicated access to the network. The AP will then send a CTS message granting access to the client. The client will then transmit data.

27. What Wi-Fi management frame is regularly broadcast by APs to announce their presence?

- authentication
- **beacon**
- probe
- association

Explanation: Beacon frames are broadcast periodically by the AP to advertise its wireless networks to potential clients. Probing, association, and authentication frames are only sent when a client is associating to the AP.

28. What are the three parts of all Layer 2 frames? (Choose three.)

- source and destination IP address
- **payload**
- sequence number
- **frame check sequence**
- time-to-live
- **header**

Explanation: Layer 2 frames have three components: the header, the payload, and a frame check sequence at the end.

29. What is the first step in the CSMA/CA process when a wireless client is attempting to communicate on the wireless network?

- The client sends an RTS message to the AP.
- The client sends a test frame onto the channel.
- **The client listens for traffic on the channel.**
- The AP sends a CTS message to the client.

Explanation: When a wireless client is attempting to communicate on the network, it will first listen to the channel to be sure it is idle. Next, the client sends an RTS message to the AP to request dedicated access to

the network. The AP will then send a CTS message granting access to the client. The client will then transmit data.

30. In which memory location is the routing table of a router maintained?

- ROM
- flash
- NVRAM
- **RAM**

Explanation: The routing table of a router is maintained in RAM, which is volatile memory. If a router loses power or is rebooted, the content of RAM is lost and the routing table must be rebuilt.

31. Lightweight access points forward data between which two devices on the network? (Choose two.)

- wireless router
- default gateway
- **wireless LAN controller**
- autonomous access point
- **wireless client**

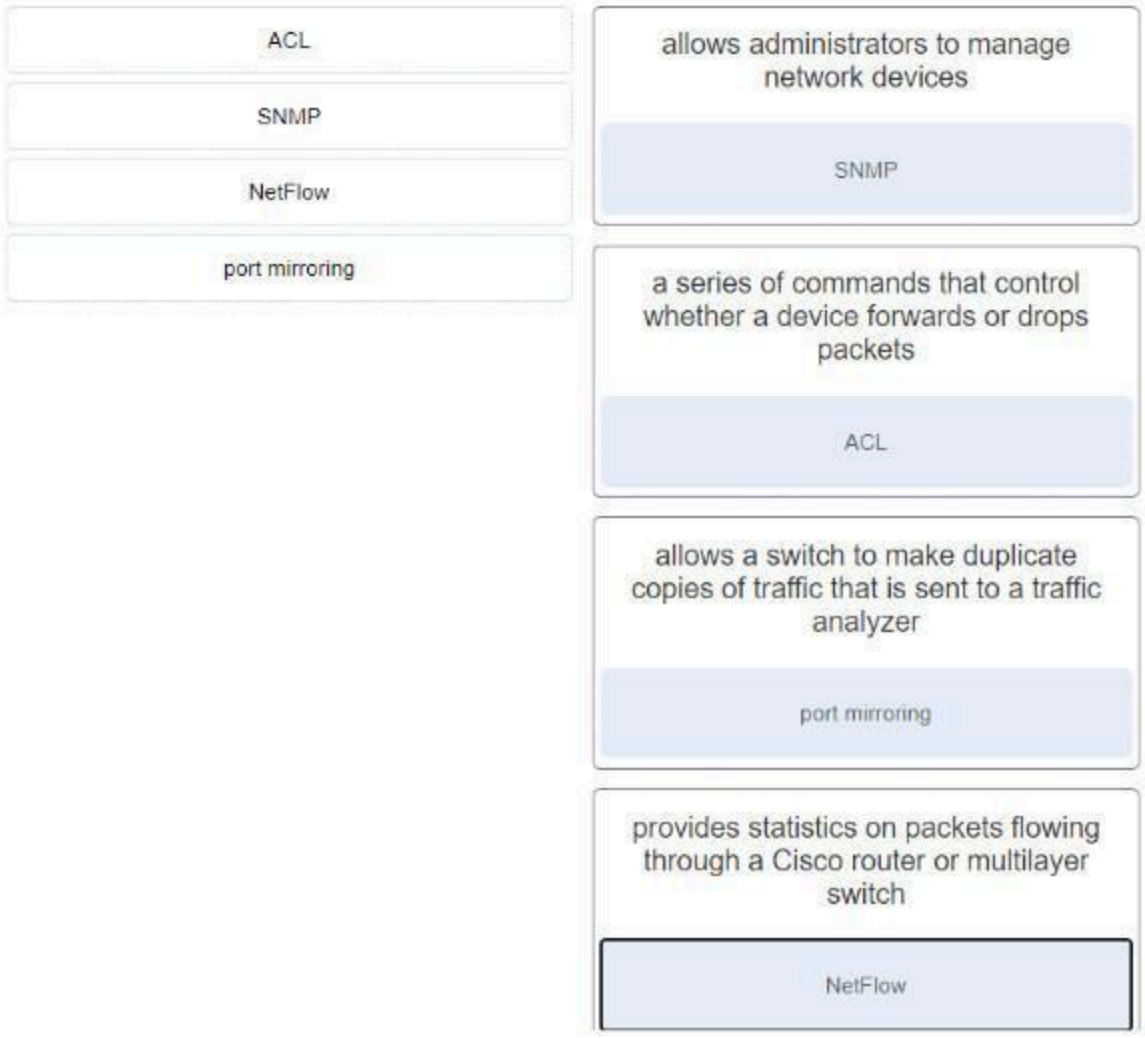
Explanation: In a wireless deployment that is using lightweight access points (LWAPs), the LWAP forwards data between the wireless clients and the wireless LAN controller (WLC).

32. A Cisco router is running IOS 15. What are the two routing table entry types that will be added when a network administrator brings an interface up and assigns an IP address to the interface? (Choose two.)

- route that is manually entered by a network administrator
- **local route interface**
- route that is learned via OSPF
- **directly connected interface**
- route that is learned via EIGRP

Explanation: A local route interface routing table entry is found when a router runs IOS 15 or higher or if IPv6 routing is enabled. Whenever an interface is addressed and enabled (made active), a directly connected interface is automatically shown in the routing table.

33. Match the secunty service with the description.



34. Match the network security device type with the descnption.

35. What Wi-Fi management frame is regularly broadcast by APs to announce their presence?

- authentication
- **beacon**
- probe
- association

Explanation: Beacon frames are broadcast periodically by the AP to advertise its wireless networks to potential clients. Probing, association, and authentication frames are only sent when a client is associating to the AP.

36. What is a function of SNMP?

- synchronizes the time across all devices on the network

- captures packets entering and exiting the network interface card
- **provides a message format for communication between network device managers and agents**
- provides statistical analysis on packets flowing through a Cisco router or multilayer switch

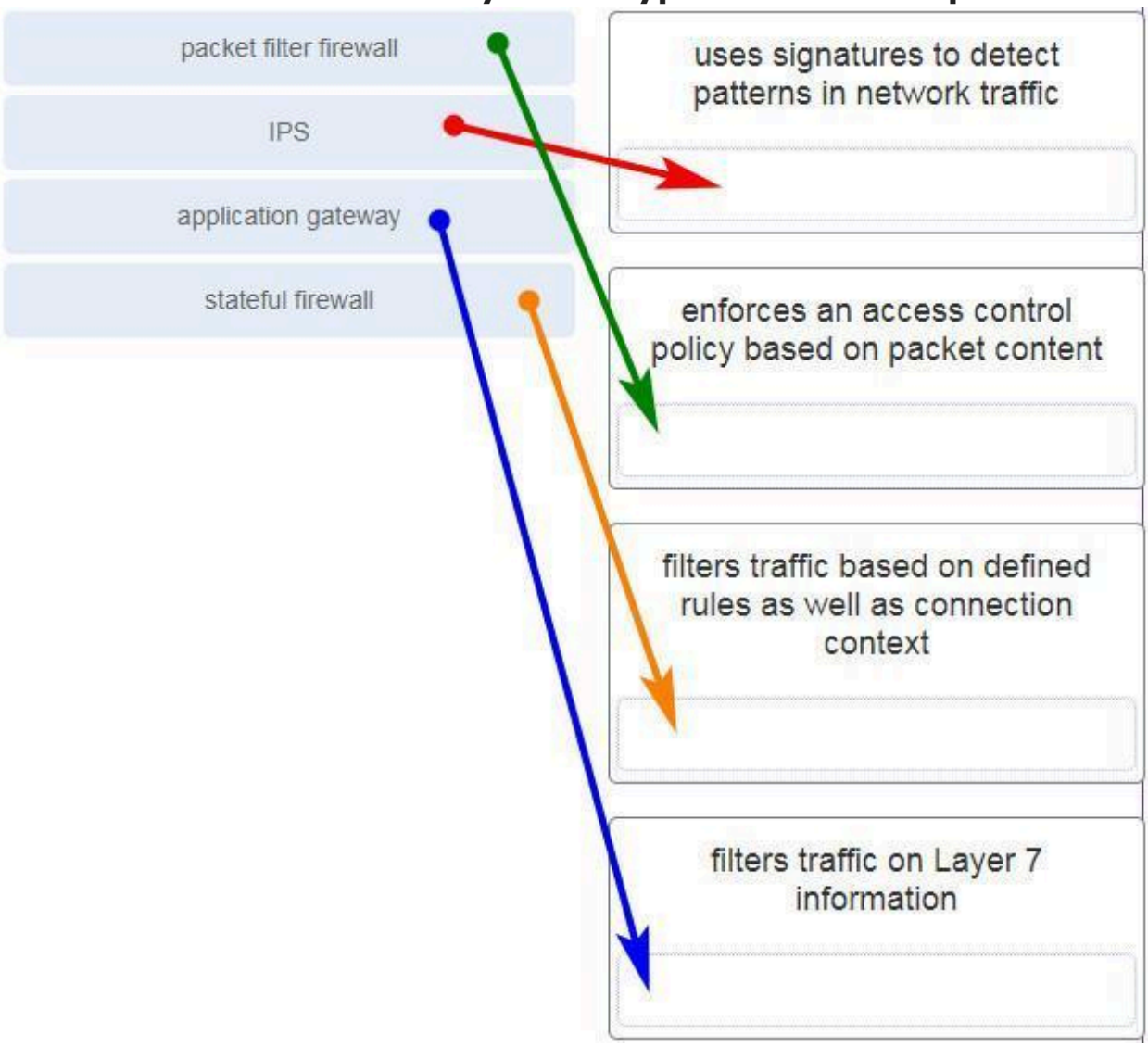
Explanation: SNMP is an application layer protocol that allows administrators to manage devices on the network by providing a messaging format for communication between network device managers and agents.

37. What is a characteristic of a hub?

- operates at Layer 2
- **regenerates signals received on one port out all other ports**
- subdivides the network into collision domains
- uses CSMA/CA to avoid collisions

Explanation: A hub is a Layer 1 device that regenerates signals out all ports other than the ingress port. All ports on a hub belong to the same collision domain. Hubs use CSMA/CD to detect collisions on the network.

38. Match the network security device type with the description.



39. Which firewall feature is used to ensure that packets coming into a network are legitimate responses to requests initiated from internal hosts?

- application filtering
- **stateful packet inspection**
- packet filtering
- URL filtering

Explanation: Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests originating from hosts inside the network. Packet filtering can be used to

permit or deny access to resources based on IP or MAC address. Application filtering can permit or deny access based on port number. URL filtering is used to permit or deny access based on URL or on keywords.

40. What is used on WLANs to avoid packet collisions?

- SVIs
- STP
- **CSMA/CA**
- VLANs

Explanation: WLANs are half-duplex networks which means that only one client can transmit or receive at any given moment. WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) to determine when to send data on the network to avoid packet collisions.

41. What information within a data packet does a router use to make forwarding decisions?

- the destination MAC address
- the destination host name
- the destination service requested
- **the destination IP address**

Explanation: A Layer 3 device like a router uses a Layer 3 destination IP address to make a forwarding decision.

1. Which is an example of social engineering?

- an unidentified person claiming to be a technician collecting user information from employees
- the infection of a computer by a virus carried by a Trojan
- an anonymous programmer directing a DDoS attack on a data center
- **a computer displaying unauthorized pop-ups and adware**

2. What is a significant characteristic of virus malware?

- A virus is triggered by an event on the host system.
- Virus malware is only distributed over the Internet.
- **A virus can execute independently of the host system.**

- Once installed on a host system, a virus will automatically propagate itself to other systems.

3. Which access attack method involves a software program that attempts to discover a system password by the use of an electronic dictionary?

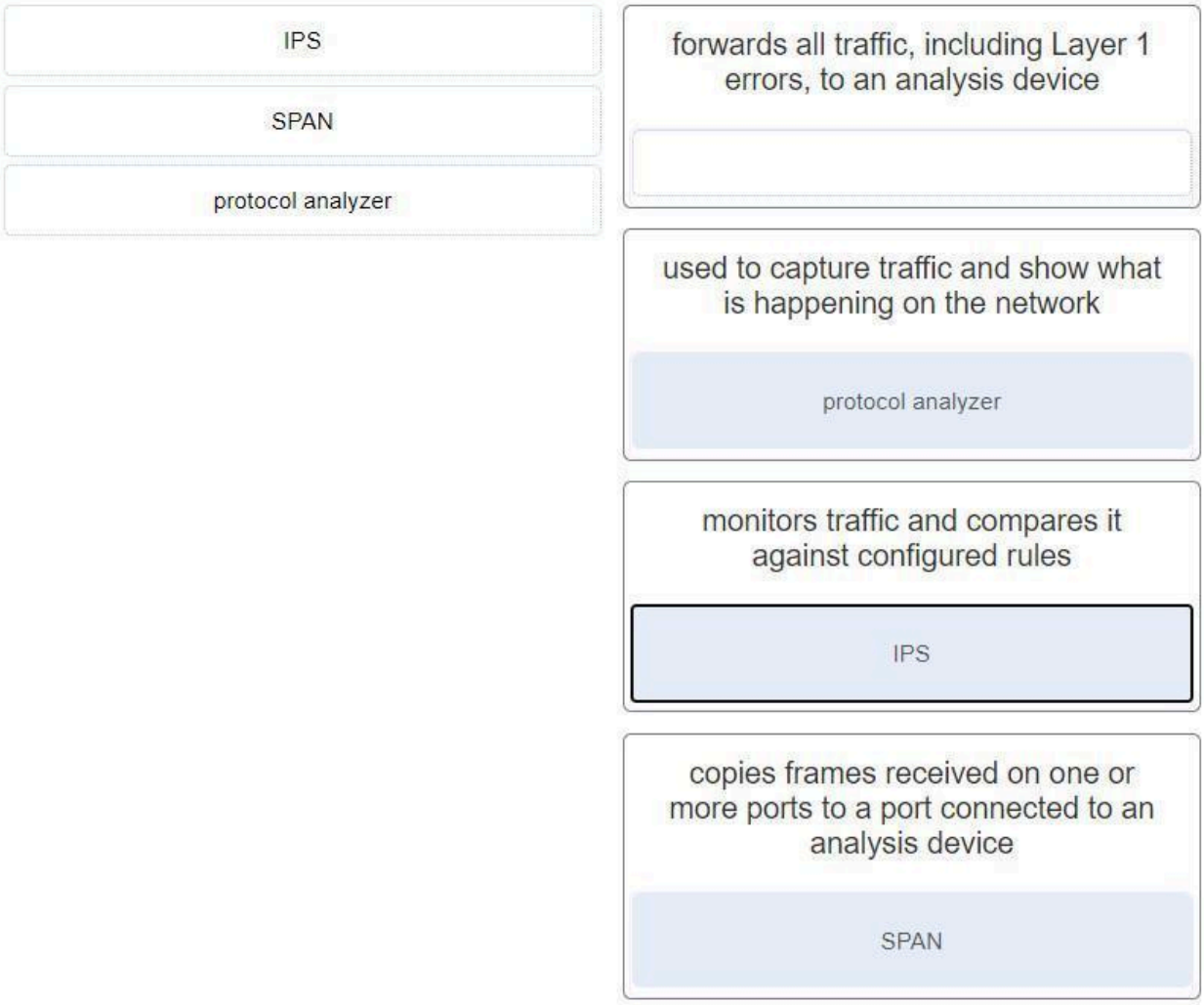
- brute-force attack
- IP spoofing attack
- denial of service attack
- **port redirection attack**
- buffer overflow attack
- packet sniffer attack

4. Which statement describes an operational characteristic of NetFlow?

- **NetFlow collects basic information about the packet flow, not the flow data itself.**
- NetFlow captures the entire contents of a packet.
- NetFlow flow records can be viewed by the tcpdump tool.
- NetFlow can provide services for user access control.

Explanation: NetFlow does not capture the entire contents of a packet. Instead, NetFlow collects metadata, or data about the flow, not the flow data itself. NetFlow information can be viewed with tools such as **nfdump** and FlowViewer.

5. Match the network monitoring solution with a description. (Not all options are used.)



6. Which technology is a proprietary SIEM system?

- StealthWatch
- NetFlow collector
- SNMP agent
- **Splunk**

Explanation: Security Information Event Management (SIEM) is a technology that is used in enterprise organizations to provide real-time reporting and long-term analysis of security events. Splunk is a proprietary SIEM system.

7. What are three functionalities provided by SOAR? (Choose three.)

- **It automates complex incident response procedures and investigations.**
- It provides 24×7 statistics on packets that flow through a Cisco router or multilayer switch.
- **It uses artificial intelligence to detect incidents and aid in incident analysis and response.**
- It presents the correlated and aggregated event data in real-time monitoring and long-term summaries.
- It provides a complete audit trail of basic information about every IP flow forwarded on a device.
- **It provides case management tools that allow cybersecurity personnel to research and investigate incidents.**

8. Which devices should be secured to mitigate against MAC address spoofing attacks?

- Layer 7 devices
- Layer 4 devices
- Layer 3 devices
- **Layer 2 devices**

Explanation: Layer 2 attacks such as MAC address spoofing can be mitigated by securing Layer 2 devices.

9. A network administrator is checking the system logs and notices unusual connectivity tests to multiple well-known ports on a server. What kind of potential network attack could this indicate?

- access
- denial of service
- information theft
- **reconnaissance**

Explanation: A reconnaissance attack is the unauthorized discovery and mapping of systems, services, or vulnerabilities. One of the most common reconnaissance attacks is performed by using utilities that automatically discover hosts on the networks and determine which ports are currently listening for connections.

10. What is a vulnerability that allows criminals to inject scripts into web pages viewed by users?

- **Cross-site scripting**

- XML injection
- buffer overflow
- SQL injection

Explanation: Cross-site scripting (XSS) allows criminals to inject scripts that contain malicious code into web applications.

11. Why would a rootkit be used by a hacker?

- to try to guess a password
- to reverse engineer binary files
- **to gain access to a device without being detected**
- to do reconnaissance

Explanation: Hackers use rootkits to avoid detection as well as hide any software installed by the hacker.

12. What causes a buffer overflow?

- sending too much information to two or more interfaces of the same device, thereby causing dropped packets
- **attempting to write more data to a memory location than that location can hold**
- sending repeated connections such as Telnet to a particular device, thus denying other data sources
- downloading and installing too many software updates at one time
- launching a security countermeasure to mitigate a Trojan horse

Explanation: By sending too much data to a specific area of memory, adjacent memory locations are overwritten, which causes a security issue because the program in the overwritten memory location is affected.

13. Which type of security threat would be responsible if a spreadsheet add-on disables the local software firewall?

- DoS
- **Trojan horse**
- buffer overflow
- brute-force attack

14. Which two types of hackers are typically classified as grey hat hackers? (Choose two.)

- **hacktivists**
- cyber criminals
- **vulnerability brokers**
- script kiddies
- state-sponsored hackers

15. A white hat hacker is using a security tool called Skipfish to discover the vulnerabilities of a computer system. What type of tool is this?

- debugger
- **fuzzer**
- vulnerability scanner
- packet sniffer

Explanation: Fuzzers are tools used by threat actors when attempting to discover the vulnerabilities of a computer system. Examples of fuzzers include Skipfish, Wapiti, and W3af.

16. Which two functions are provided by NetFlow? (Choose two.)

- It uses artificial intelligence to detect incidents and aid in incident analysis and response.
- **It provides a complete audit trail of basic information about every IP flow forwarded on a device.**
- **It provides 24×7 statistics on packets that flow through a Cisco router or multilayer switch.**
- It allows an administrator to capture real-time network traffic and analyze the entire contents of packets.
- It presents correlated and aggregated event data in real-time monitoring and long-term summaries.

Explanation: NetFlow is a Cisco IOS technology that provides statistics and complete audit trails on TCP/IP flows on the network. Some of the capabilities of NetFlow include the following: 24×7 network and security monitoring, network planning, traffic analysis, identification of network bottlenecks, and IP accounting for billing purposes.

17. Which statement describes the function of the SPAN tool used in a Cisco switch?

- It is a secure channel for a switch to send logging to a syslog server.
- It provides interconnection between VLANs over multiple switches.
- It supports the SNMP trap operation on a switch.
- **It copies the traffic from one switch port and sends it to another switch port that is connected to a monitoring device.**

18. What are two evasion methods used by hackers? (Choose two.)

- scanning
- access attack
- **resource exhaustion**
- phishing
- **encryption**

19. Which attack involves threat actors positioning themselves between a source and destination with the intent of transparently monitoring, capturing, and controlling the communication?

- **man-in-the-middle attack**
- DoS attack
- ICMP attack
- SYN flood attack

20. What is the goal of a white hat hacker?

- validating data
- modifying data
- stealing data
- **protecting data**

Explanation: White hat hackers are actually "good guys" and are paid by companies and governments to test for security vulnerabilities so that data is better protected.

21. Once a cyber threat has been verified, the US Cybersecurity Infrastructure and Security Agency (CISA) automatically shares the cybersecurity information with public and private organizations. What is this automated system called?

- **AIS**
- NCSA
- ENISA
- NCASM

Explanation: Governments are now actively promoting cybersecurity. For instance, the US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost. CISA use a system called Automated Indicator Sharing (AIS). AIS enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified. CISA offers many resources that help to limit the size of the United States attack surface.

22. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?

- spam
- anonymous keylogging
- DDoS
- **social engineering**

23. Which two characteristics describe a worm? (Chose two)

- **is self-replicating**
- **travels to new computers without any intervention or knowledge of the user**
- infects computers by attaching to software code
- hides in a dormant state until needed by an attacker
- executes when software is run on a computer

Explanation: Worms are self-replicating pieces of software that consume bandwidth on a network as they propagate from system to system. They do not require a host application, unlike a virus. Viruses, on the other hand, carry executable malicious code which harms the target machine on which they reside.

24. What kind of ICMP message can be used by threat actors to create a man-in-the-middle attack?

- ICMP echo request

- ICMP unreachable
- **ICMP redirects**
- ICMP mask reply

Explanation: Common ICMP messages of interest to threat actors include the following:
ICMP echo request and echo reply: used to perform host verification and DoS attacks
ICMP unreachable: used to perform network reconnaissance and scanning attacks
ICMP mask reply: used to map an internal IP network
ICMP redirects: used to lure a target host into sending all traffic through a compromised device and create a man-in-the-middle attack
ICMP router discovery: used to inject bogus route entries into the routing table of a target host

25. What are two purposes of launching a reconnaissance attack on a network? (Choose two.)

- to escalate access privileges
- to prevent other users from accessing the system
- **to scan for accessibility**
- **to gather information about the network and devices**
- to retrieve and modify data

Explanation: Gathering information about a network and scanning for access is a reconnaissance attack. Preventing other users from accessing a system is a denial of service attack. Attempting to retrieve and modify data, and attempting to escalate access privileges are types of access attacks.

26. Which type of network attack involves randomly opening many Telnet requests to a router and results in a valid network administrator not being able to access the device?

- DNS poisoning
- man-in-the-middle
- **SYN flooding**
- spoofing

Explanation: The TCP SYN Flood attack exploits the TCP three-way handshake. The threat actor continually sends TCP SYN session request

packets with a randomly spoofed source IP address to an intended target. The target device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections and denies TCP services.

27. What functionality is provided by Cisco SPAN in a switched network?

- **It mirrors traffic that passes through a switch port or VLAN to another port for traffic analysis.**
- It prevents traffic on a LAN from being disrupted by a broadcast storm.
- It protects the switched network from receiving BPDUs on ports that should not be receiving them.
- It copies traffic that passes through a switch interface and sends the data directly to a syslog or SNMP server for analysis.
- It inspects voice protocols to ensure that SIP, SCCP, H.323, and MGCP requests conform to voice standards.
- It mitigates MAC address overflow attacks.

Explanation: SPAN is a Cisco technology used by network administrators to monitor suspicious traffic or to capture traffic to be analyzed.

28. An attacker is redirecting traffic to a false default gateway in an attempt to intercept the data traffic of a switched network. What type of attack could achieve this?

- MAC address snoopin
- DHCP snooping
- MAC address starvation
- **DHCP spoofing**

29. What would be the target of an SQL injection attack?

- DHCP
- DNS
- email
- **database**

Explanation: SQL is the language used to query a relational database. Cybercriminals use SQL injections to get information, create fake or malicious queries, or to breach the database in some other way.

30. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?

- social engineering
- adware
- **DDoS**
- phishing
- spyware

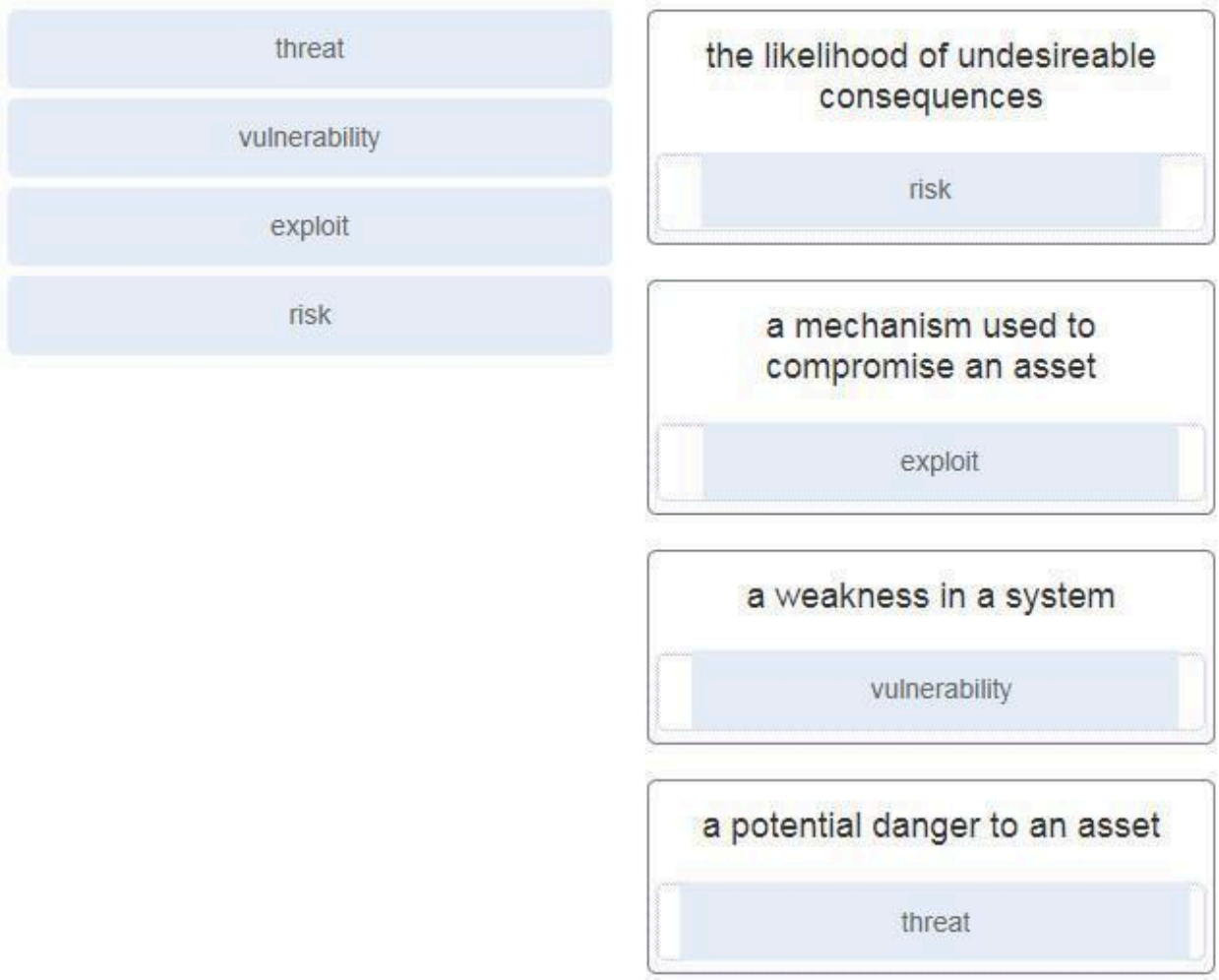
Explanation: Phishing, spyware, and social engineering are security attacks that collect network and user information. Adware consists, typically, of annoying popup windows. Unlike a DDoS attack, none of these attacks generate large amounts of data traffic that can restrict access to network services.

31. Why would an attacker want to spoof a MAC address?

- so that the attacker can capture traffic from multiple VLANs rather than from just the VLAN that is assigned to the port to which the attacker device is attached
- **so that a switch on the LAN will start forwarding frames to the attacker instead of to the legitimate host**
- so that a switch on the LAN will start forwarding all frames toward the device that is under control of the attacker (that can then capture the LAN traffic)
- so that the attacker can launch another type of attack in order to gain access to the switch

Explanation: MAC address spoofing is used to bypass security measures by allowing an attacker to impersonate a legitimate host device, usually for the purpose of collecting network traffic.

32. Match the security concept to the description.



33. What is the significant characteristic of worm malware?

- Worm malware disguises itself as legitimate software.
- Once installed on a host system, a worm does not replicate itself.
- A worm must be triggered by an event on the host system.
- **A worm can execute independently of the host system.**

34. What are the three major components of a worm attack? (Choose three.)

- **a payload**
- **a propagation mechanism**
- an infecting vulnerability
- a probing mechanism
- **an enabling vulnerability**

- a penetration mechanism

35. A user is curious about how someone might know a computer has been infected with malware. What are two common malware behaviors? (Choose two.)

- The computer emits a hissing sound every time the pencil sharpener is used.
- The computer beeps once during the boot process.
- **The computer gets increasingly slower to respond.**
- No sound emits when an audio CD is played.
- **The computer freezes and requires reboots.**

Explanation: Common symptoms of computers infected with malware:
Appearance of files, applications, or desktop icons
Security tools such as antivirus software or firewalls turned off or changed
System crashes
Emails spontaneously sent to others
Modified or missing files
Slow system or browser response
Unfamiliar processes or services running
Unknown TCP or UDP ports open
Connections made to unknown remote devices

36. Which two types of attacks are examples of reconnaissance attacks? (Choose two.)

- brute force
- **port scan**
- **ping sweep**
- man-in-the-middle
- SYN flood

37. An administrator discovers a vulnerability in the network. On analysis of the vulnerability the administrator decides the cost of managing the risk outweighs the cost of the risk itself. The risk is accepted, and no action is taken. What risk management strategy has been adopted?

- risk transfer
- **risk acceptance**

- risk reduction
- risk avoidance

38. Which protocol is exploited by cybercriminals who create malicious iFrames?

- **HTTP**
- DNS
- ARP
- DHCP

Explanation: An HTML element known as an inline frame or iFrame allows the browser to load a different web page from another source.

39. How can a DNS tunneling attack be mitigated?

- by preventing devices from using gratuitous ARP
- **by using a filter that inspects DNS traffic**
- by securing all domain owner accounts
- by using strong passwords and two-factor authentication

Explanation: To be able to stop DNS tunneling, a filter that inspects DNS traffic must be used. Also, DNS solutions such as Cisco OpenDNS block much of the DNS tunneling traffic by identifying suspicious domains.

40. What is the function of a gratuitous ARP sent by a networked device when it boots up?

- to request the netbios name of the connected system
- to request the MAC address of the DNS server
- to request the IP address of the connected network
- **to advise connected devices of its MAC address**

Explanation: A gratuitous ARP is often sent when a device first boots up to inform all other devices on the local network of the MAC address of the new device.

41. What is the result of a passive ARP poisoning attack?

- Data is modified in transit or malicious data is inserted in transit.
- Network clients experience a denial of service.
- **Confidential information is stolen.**
- Multiple subdomains are created.

Explanation: ARP poisoning attacks can be passive or active. The result of a passive attack is that cybercriminals steal confidential information. With an active attack, cybercriminals modify data in transit or they inject malicious data.

42. What are two methods used by cybercriminals to mask DNS attacks? (Choose two.)

- reflection
- shadowing
- **domain generation algorithms**
- **fast flux**
- tunneling

43. Match the security tool with the description. (Not all options apply.)

IDA Pro

Netfilter

NetStumbler

Socat

Helix

This is a forensic tool that can be used by white hat hackers to find any trace of evidence existing in a particular computer system.

Helix

This is a debugger tool that can be used by black hats to reverse engineer binary files when writing exploits. It can also be used by white hats when analyzing malware.

IDA Pro

This is a packet crafting tool that uses specially crafted forged packets to probe and test the robustness of a firewall.

Socat

This is a wireless hacking tool that can be used to hack into a wireless network to detect security vulnerabilities.

NetStumbler

44. Match the type of cyberattackers to the description. (Not all options are used.)

gather intelligence or commit sabotage on specific goals on behalf of their government

discover exploits and report them to vendors

make political statements in order to create an awareness of issues that are important to them

hacktivists

make political statements in order to create an awareness of issues that are important to them

script kiddies

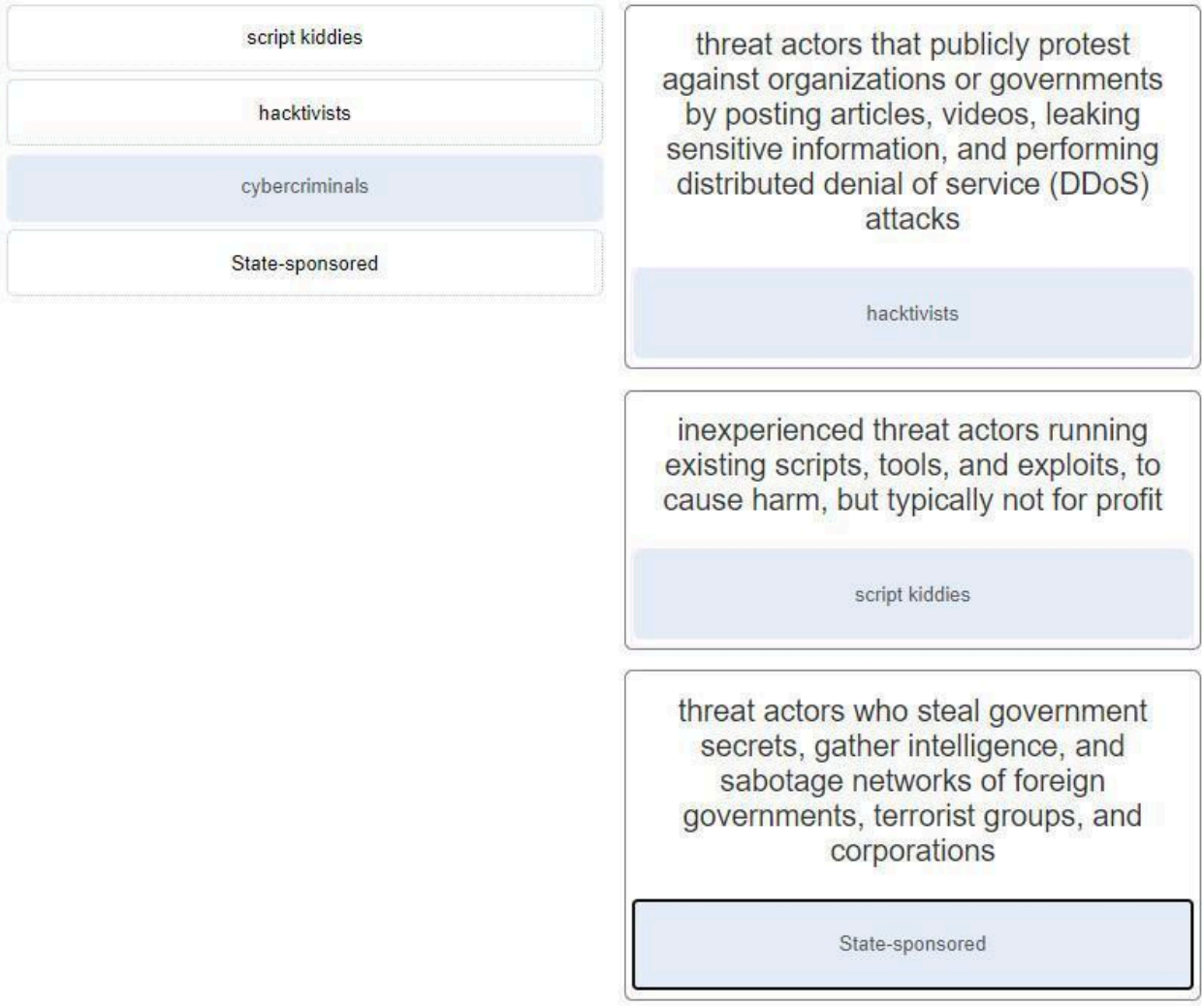
vulnerability brokers

discover exploits and report them to vendors

state-sponsored attackers

gather intelligence or commit sabotage on specific goals on behalf of their government

45. Match the threat actors with the descriptions. (Not all options are used.)



- **hacktivists** : threat actors that publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks
- **script kiddies** : inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit
- **State-sponsored** : threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations

46. What scenario describes a vulnerability broker?

- a teenager running existing scripts, tools, and exploits, to cause harm, but typically not for profit
- **a threat actor attempting to discover exploits and report them to vendors, sometimes for prizes or rewards**
- a threat actor publicly protesting against governments by posting articles and leaking sensitive information
- a State-Sponsored threat actor who steals government secrets and sabotages networks of foreign governments

Explanation: Vulnerability brokers typically refers to grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.

47. In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?

- **DoS**
- session hijacking
- MITM
- address spoofing

16. Which field in the IPv6 header points to optional network layer information that is carried in the IPv6 packet?

- traffic class
- version
- flow label
- **next header**

Explanation: Optional Layer 3 information about fragmentation, security, and mobility is carried inside of extension headers in an IPv6 packet. The next header field of the IPv6 header acts as a pointer to these optional extension headers if they are present.

48. Which type of attack is carried out by threat actors against a network to determine which IP addresses, protocols, and ports are allowed by ACLs?

- social engineering
- denial of service
- phishing
- **reconnaissance**

Explanation: Packet filtering ACLs use rules to filter incoming and outgoing traffic. These rules are defined by specifying IP addresses, port numbers, and protocols to be matched. Threat actors can use a reconnaissance attack involving port scanning or penetration testing to determine which IP addresses, protocols, and ports are allowed by ACLs.

49. Which cyber attack involves a coordinated attack from a botnet of zombie computers?

- ICMP redirect
- MITM
- **DDoS**
- address spoofing

Explanation: DDoS is a distributed denial-of-services attack. A DDoS attack is launched from multiple coordinated sources. The sources of the attack are zombie hosts that the cybercriminal has built into a botnet. When ready, the cybercriminal instructs the botnet of zombies to attack the chosen target.

50. What technique is a security attack that depletes the pool of IP addresses available for legitimate hosts?

- reconnaissance attack
- **DHCP starvation**
- DHCP spoofing
- DHCP snooping

51 Which type of Trojan horse security breach uses the computer of the victim as the source device to launch other attacks?

- **proxy**
- FTP
- DoS
- data-sending

Explanation: The attacker uses a proxy Trojan horse attack to penetrate one device and then use that device to launch attacks on other devices. The Dos Trojan horse slows or halts network traffic. The FTP trojan horse enables unauthorized file transfer services when port 21 has been compromised. A data-sending Trojan horse transmits data back to the hacker that could include passwords.

52. What are two examples of DoS attacks? (Choose two.)

- **buffer overflow**
- SQL injection
- port scanning
- phishing
- **ping of death**

Explanation: The buffer overflow and ping of death DoS attacks exploit system memory-related flaws on a server by sending an unexpected amount of data or malformed data to the server.

CyberOps Associate (Version 1.0) – Modules 18 – 20: Network Defense Group Exam

1. How does BYOD change the way in which businesses implement networks?

- BYOD requires organizations to purchase laptops rather than desktops.
- **BYOD provides flexibility in where and how users can access network resources.**
- BYOD users are responsible for their own network security, thus reducing the need for organizational security policies.
- BYOD devices are more expensive than devices that are purchased by an organization.

2. Which type of business policy establishes the rules of conduct and the responsibilities of employees and employers?

- employee
- data
- **company**
- security

3. What device would be used as the third line of defense in a defense-in-depth approach?

- host
- firewall

- **internal router**
- edge router

4. What does the incident handling procedures security policy describe?

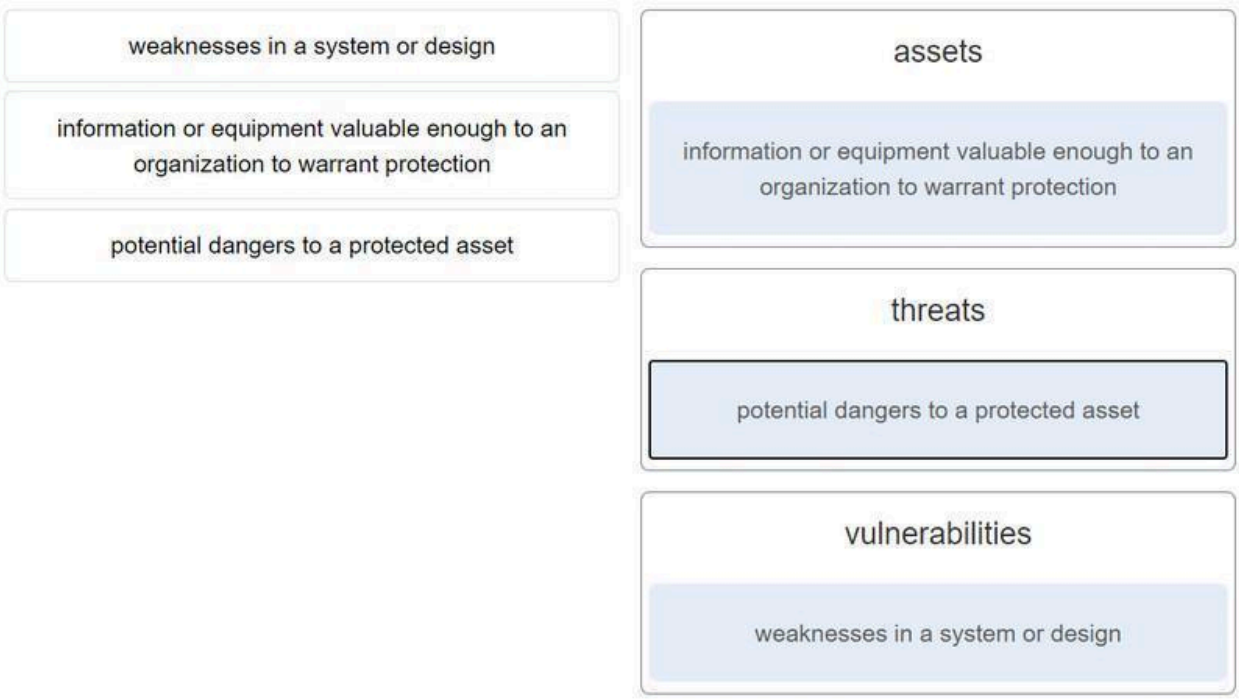
- **It describes how security incidents are handled.**
- It describes the procedure for auditing the network after a cyberattack.
- It describes the procedure for mitigating cyberattacks.
- It describes how to prevent various cyberattacks.

5. What is the benefit of a defense-in-depth approach?

- All network vulnerabilities are mitigated.
- The need for firewalls is eliminated.
- Only a single layer of security at the network core is required.
- **The effectiveness of other security measures is not impacted when a security mechanism fails.**

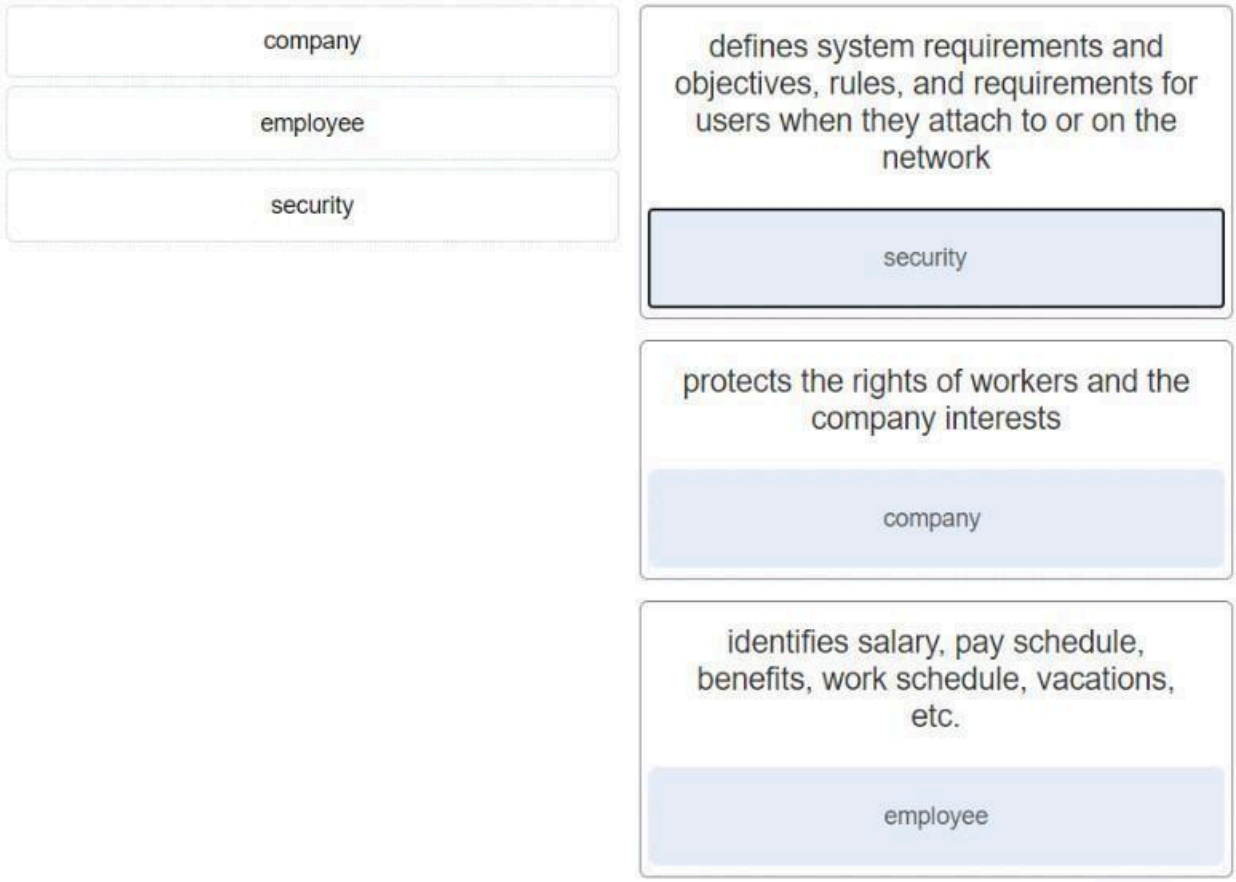
Explanation: The benefit of the defense-in-depth approach is that network defenses are implemented in layers so that failure of any single security mechanism does not impact other secuirty measures.

6. Match the term to the description.



Match the term to the description

7. Match the type of business policy to the description.



- defines system requirements and objectives, rules, and requirements for users when they attach to or on the network ==> **security**
- protects the rights of workers and the company interests ==> **company**
- identifies salary, pay schedule, benefits, work schedule, vacations, etc. ==> **employee**

8. Why is asset management a critical function of a growing organization against security threats?

- **It identifies the ever increasing attack surface to threats.**
- It allows for a build of a comprehensive AUP.
- It serves to preserve an audit trail of all new purchases.
- It prevents theft of older assets that are decommissioned.

Explanation: Asset management is a critical component of a growing organization from a security aspect. Asset management consists of

inventorying all assets, and then developing and implementing policies and procedures to protect them. As an organization grows, so does the attack surface in terms of security threats. Each of these assets can attract different threat actors who have different skill levels and motivations. Asset management can help mitigate these threats by inventorying the risks as the attack surface grows.

9. In a defense-in-depth approach, which three options must be identified to effectively defend a network against attacks? (Choose three.)

- total number of devices that attach to the wired and wireless network
- **assets that need protection**
- **vulnerabilities in the system**
- location of attacker or attackers
- past security breaches
- **threats to assets**

Explanation: In order to prepare for a security attack, IT security personnel must identify assets that need to be protected such as servers, routers, access points, and end devices. They must also identify potential threats to the assets and vulnerabilities in the system or design.

10. What is the first line of defense when an organization is using a defense-in-depth approach to network security?

- **edge router**
- firewall
- proxy server
- IPS

Explanation: A defense-in-depth approach uses layers of security measures starting at the network edge, working through the network, and finally ending at the network endpoints. Routers at the network edge are the first line of defense and forward traffic intended for the internal network to the firewall.

11. What is the primary function of the Center for Internet Security (CIS)?

- to maintain a list of common vulnerabilities and exposures (CVE) used by security organizations
- to provide a security news portal that aggregates the latest breaking news pertaining to alerts, exploits, and vulnerabilities
- **to offer 24×7 cyberthreat warnings and advisories, vulnerability identification, and mitigation and incident responses**
- to provide vendor-neutral education products and career services to industry professionals worldwide

Explanation: CIS offers 24×7 cyberthreat warnings and advisories, vulnerability identification, and mitigation and incident responses to state, local, tribal, and territorial (SLTT) governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC).

12. What is CybOX?

- It is a specification for an application layer protocol that allows the communication of CTI over HTTPS.
- **It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations.**
- It enables the real-time exchange of cyberthreat indicators between the U.S. Federal Government and the private sector.
- It is a catalog of known security threats called Common Vulnerabilities and Exposures (CVE) for publicly known cybersecurity vulnerabilities.

Explanation: CybOX is a set of open standards that provide the specifications that aid in the automated exchange of cyberthreat intelligence information in a standardized format. It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations that support many cybersecurity functions.

13. What three goals does a BYOD security policy accomplish? (Choose three.)

- identify all malware signatures and synchronize them across corporate databases
- **identify which employees can bring their own devices**
- **identify safeguards to put in place if a device is compromised**
- identify and prevent all heuristic virus signatures

- identify a list of websites that users are not permitted to access
- **describe the rights to access and activities permitted to security personnel on the device**

14. When designing a prototype network for a new server farm, a network designer chooses to use redundant links to connect to the rest of the network. Which business goal will be addressed by this choice?

- **availability**
- manageability
- security
- scalability

Explanation: Availability is one of the components of information security where authorized users must have uninterrupted access to important resources and data.

15. When a security audit is performed at a company, the auditor reports that new users have access to network resources beyond their normal job roles. Additionally, users who move to different positions retain their prior permissions. What kind of violation is occurring?

- **least privilege**
- network policy
- password
- audit

16. Which component of the zero trust security model focuses on secure access when an API, a microservice, or a container is accessing a database within an application?

- workflow
- workforce
- **workload**
- workplace

Explanation: The workload pillar focuses on applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another. It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.

17. Which two options are security best practices that help mitigate BYOD risks? (Choose two.)

- Use paint that reflects wireless signals and glass that prevents the signals from going outside the building.
- **Keep the device OS and software updated.**
- Only allow devices that have been approved by the corporate IT team.
- **Only turn on Wi-Fi when using the wireless network.**
- Decrease the wireless antenna gain level.
- Use wireless MAC address filtering.

Explanation: Many companies now support employees and visitors attaching and using wireless devices that connect to and use the corporate wireless network. This practice is known as a bring-your-own-device policy or BYOD. Commonly, BYOD security practices are included in the security policy. Some best practices that mitigate BYOD risks include the following:

Use unique passwords for each device and account.

Turn off Wi-Fi and Bluetooth connectivity when not being used. Only connect to trusted networks.

Keep the device OS and other software updated.

Backup any data stored on the device.

Subscribe to a device locator service with a remote wipe feature.

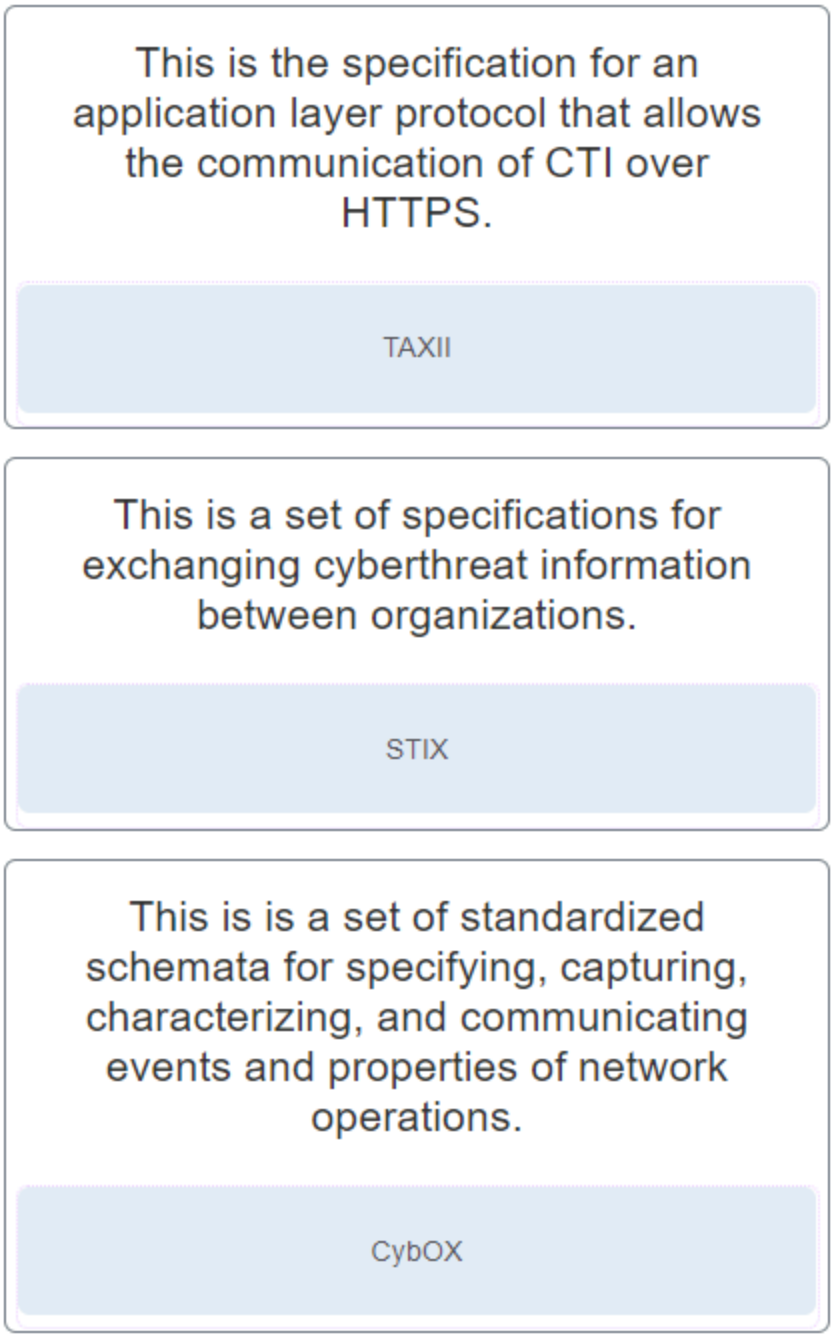
Provide antivirus software for approved BYODs.

Use Mobile Device Management (MDM) software that allows IT teams to track the device and implement security settings and software controls.

18. What is the purpose of mobile device management (MDM) software?

- It is used to create a security policy.
- **It is used to implement security policies, setting, and software configurations on mobile devices.**
- It is used to identify potential mobile device vulnerabilities.
- It is used by threat actors to penetrate the system.

19. Match the threat intelligence sharing standards with the description.



- This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. ==> **TAXII**
- This is a set of specifications for exchanging cyberthreat information between organizations. ==> **STIX**

- This is is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations. ==> **CybOX**

20. What is the primary purpose of the Forum of Incident Response and Security Teams (FIRST)?

- **to enable a variety of computer security incident response teams to collaborate, cooperate, and coordinate information sharing, incident prevention, and rapid reaction strategies**
- to provide a security news portal that aggregates the latest breaking news pertaining to alerts, exploits, and vulnerabilities
- to offer 24×7 cyberthreat warnings and advisories, vulnerability identification, and mitigation and incident response
- to provide vendor neutral education products and career services to industry professionals worldwide

Explanation: The primary purpose of the Forum of Incident Response and Security Teams (FIRST) is to enable a variety of computer security incident response teams to collaborate, cooperate, and coordinate information sharing, incident prevention, and rapid reaction between the teams.

21. What is the primary purpose of the Malware Information Sharing Platform (MISP) ?

- to publish all informational materials on known and newly discovered cyberthreats
- **to enable automated sharing of IOCs between people and machines using the STIX and other exports formats**
- to provide a set of standardized schemata for specifying and capturing events and properties of network operations
- to exchange all the response mechanisms to known threats

Explanation: Malware Information Sharing Platform (MISP) is an open source platform that enables automated sharing of IOCs between people and machines using the STIX and other exports formats.

22. Which statement describes Trusted Automated Exchange of Indicator Information (TAXII)?

- It is a set of specifications for exchanging cyber threat information between organizations.

- It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.
- It is a dynamic database of real-time vulnerabilities.
- **It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.**

23. Which organization defines unique CVE Identifiers for publicly known information-security vulnerabilities that make it easier to share data?

- Cisco Talos
- DHS
- FireEye
- **MITRE**

Explanation: The United States government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE). The CVE serves as a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

24. How does FireEye detect and prevent zero-day attacks?

- by establishing an authentication parameter prior to any data exchange
- **by addressing all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis**
- by keeping a detailed analysis of all viruses and malware
- by only accepting encrypted data packets that validate against their configured hash values

Explanation: FireEye uses a three-pronged approach combining security intelligence, security expertise, and technology. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

25. A web server administrator is configuring access settings to require users to authenticate first before accessing certain web pages. Which requirement of information security is addressed through the configuration?

- availability
- integrity

- scalability
- **confidentiality**

Explanation: Confidentiality ensures that data is accessed only by authorized individuals. Authentication will help verify the identity of the individuals.

26. What is the purpose of the network security accounting function?

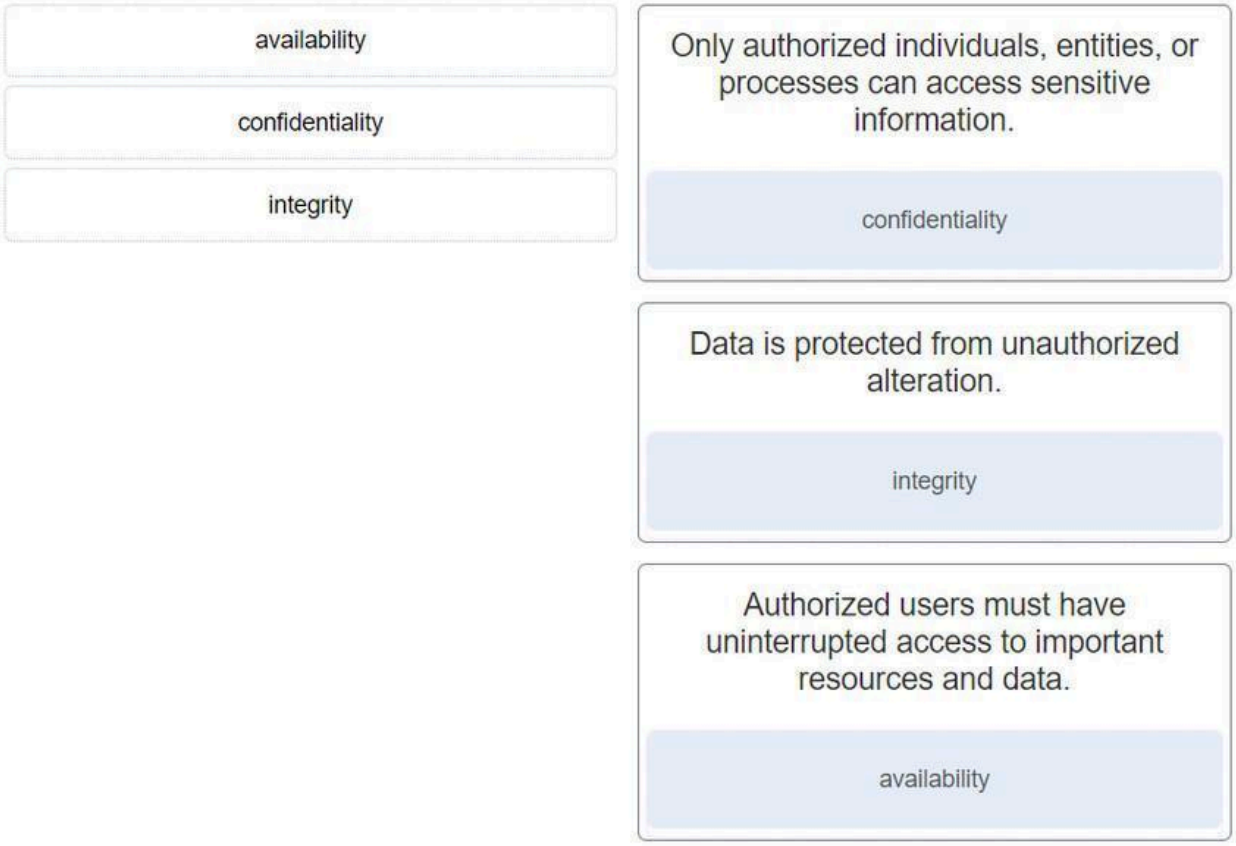
- to determine which resources a user can access
- to provide challenge and response questions
- **to keep track of the actions of a user**
- to require users to prove who they are

27. Which term describes the ability of a web server to keep a log of the users who access the server, as well as the length of time they use it?

- authentication
- **accounting**
- assigning permissions
- authorization

Explanation: Accounting records what users do and when they do it, including what is accessed, the amount of time the resource is accessed, and any changes that were made. Accounting keeps track of how network resources are used.

28. Match the information security component with the description.



- Only authorized individuals, entities, or processes can access sensitive information. : **confidentiality**
- Data is protected from unauthorized alteration. : **Integrity**
- Authorized users must have uninterrupted access to important resources and data. : **availability**

29. What are two characteristics of the RADIUS protocol? (Choose two.)

- encryption of the entire body of the packet
- **encryption of the password only**
- **the use of UDP ports for authentication and accounting**
- the separation of the authentication and authorization processes
- the use of TCP port 49

Explanation: RADIUS is an open-standard AAA protocol using UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. It combines authentication and authorization into one process.

30. Which AAA component can be established using token cards?

- accounting
- authorization
- **authentication**
- auditing

Explanation: The authentication component of AAA is established using username and password combinations, challenge and response questions, and token cards. The authorization component of AAA determines which resources the user can access and which operations the user is allowed to perform. The accounting and auditing component of AAA keeps track of how network resources are used.

31. What is a characteristic of the security artichoke, defense-in-depth approach?

- Threat actors can easily compromise all layers safeguarding the data or systems.
- **Threat actors no longer have to peel away each layer before reaching the target data or system.**
- Threat actors can no longer penetrate any layers safeguarding the data or system.
- Each layer has to be penetrated before the threat actor can reach the target data or system.

Explanation: In the security artichoke, defense-in-depth approach not every layer needs to be penetrated by the threat actor in order to get to the data or systems. Each layer provides a layer of protection while simultaneously providing a path to attack.

32. What is a characteristic of a layered defense-in-depth security approach?

- Three or more devices are used.
- Routers are replaced with firewalls.
- **One safeguard failure does not affect the effectiveness of other safeguards.**
- When one device fails, another one takes over.

Explanation: When a layered defense-in-depth security approach is used, layers of security are placed through the organization-at the edge, within the network, and on endpoints. The layers work together to

create the security architecture. In this environment, a failure of one safeguard does not affect the effectiveness of other safeguards.

33. What is the principle behind the nondiscretionary access control model?

- It applies the strictest access control possible.
- **It allows access decisions to be based on roles and responsibilities of a user within the organization.**
- It allows users to control access to their data as owners of that data.
- It allows access based on attributes of the object be to accessed.

Explanation: The nondiscretionary access control model used the roles and responsibilities of the user as the basis for access decisions.

34. Which type of access control applies the strictest access control and is commonly used in military or mission critical applications?

- Non-discretionary access control
- discretionary access control (DAC)
- attribute-based access control (ABAC)
- **mandatory access control (MAC)**

Explanation: Access control models are used to define the access controls implemented to protect corporate IT resources. The different types of access control models are as follows:

Mandatory access control (MAC) – The strictest access control that is typically used in military or mission critical applications.

Discretionary access control (DAC) – Allows users to control access to their data as owners of that data. Access control lists (ACLs) or other security measures may be used to specify who else may have access to the information.

Non-discretionary access control – Also known as role-based access control (RBAC). Allows access based on the role and responsibilities of the individual within the organization.

Attribute-based access control (ABAC) – Allows access based on the attributes of the resource to be accessed, the user accessing the resource, and the environmental factors such as the time of day.

35. Passwords, passphrases, and PINs are examples of which security term?

- identification
- access
- **authentication**
- authorization

Explanation: Authentication methods are used to strengthen access control systems. It is important to understand the available authentication methods.

36. How does AIS address a newly discovered threat?

- by creating response strategies against the new threat
- by advising the U.S. Federal Government to publish internal response strategies
- **by enabling real-time exchange of cyberthreat indicators with U.S. Federal Government and the private sector**
- by mitigating the attack with active response defense mechanisms

Explanation: AIS responds to a new threat as soon as it is recognized by immediately sharing it with U.S. Federal Government and the private sector to help them protect their networks against that particular threat.

CyberOps Associate (Version 1.0) – Modules 21 – 23: Cryptography and Endpoint Protection Group Exam

1. Which technology might increase the security challenge to the implementation of IoT in an enterprise environment?

- network bandwidth
- cloud computing
- CPU processing speed
- **data storage**

2. Which statement describes the term attack surface?

- It is the total number of attacks toward an organization within a day.
- **It is the group of hosts that experiences the same attack.**
- It is the total sum of vulnerabilities in a system that is accessible to an attacker.
- It is the network interface where attacks originate.

3. Which HIDS is an open-source based product?

- OSSEC
- **Cisco AMP**
- Tripwire
- AlienVault USM

4. What does the telemetry function provide in host-based security software?

- It updates the heuristic antivirus signature database.
- It blocks the passage of zero-day attacks.
- It enables updates of malware signatures.
- **It enables host-based security programs to have comprehensive logging functions.**

Explanation: The telemetry function allows for robust logging functionality that is essential to cybersecurity operations. Some host-based security programs will submit logs to a central location for analysis.

5. Which type of attack does the use of HMACs protect against?

- brute force
- DDoS
- DoS
- **man-in-the-middle**

Explanation: Because only the sender and receiver know the secret key, only parties that have access to that key can compute the digest of an HMAC function. This defeats man-in-the-middle attacks and provides authentication of where the data originated.

6. Which objective of secure communications is achieved by encrypting data?

- **confidentiality**
- integrity
- availability
- authentication

7. Which two statements correctly describe certificate classes used in the PKI? (Choose two.)

- **A class 4 certificate is for online business transactions between companies.**
- A class 0 certificate is more trusted than a class 1 certificate.
- **A class 0 certificate is for testing purposes.**
- The lower the class number, the more trusted the certificate.
- A class 5 certificate is for users with a focus on verification of email.

Explanation: A digital certificate class is identified by a number. The higher the number, the more trusted the certificate. The classes include the following:
Class 0 is for testing purposes in which no checks have been performed.
Class 1 is for individuals with a focus on verification of email.
Class 2 is for organizations for which proof of identity is required.
Class 3 is for servers and software signing for which independent verification and checking of identity and authority is done by the issuing certificate authority.
Class 4 is for online business transactions between companies.
Class 5 is for private organizations or governmental security.

8. A customer purchases an item from an e-commerce site. The e-commerce site must maintain proof that the data exchange took place between the site and the customer. Which feature of digital signatures is required?

- **nonrepudiation of the transaction**
- integrity of digitally signed data
- authenticity of digitally signed data
- confidentiality of the public key

Explanation: Digital signatures provide three basic security services: Authenticity of digitally signed data – Digital signatures authenticate a source, proving that a certain party has seen and signed the data in question.

Integrity of digitally signed data – Digital signatures guarantee that the data has not changed from the time it was signed.
Nonrepudiation of the transaction – The recipient can take the data to a third party, and the third party accepts the digital signature as a proof that this data exchange did take place. The signing party cannot repudiate that it has signed the data.

9. What is the purpose of a digital certificate?

- It provides proof that data has a traditional signature attached.
- It guarantees that a website has not been hacked.
- It ensures that the person who is gaining access to a network device is authorized.
- **It authenticates a website and establishes a secure connection to exchange confidential data.**

Explanation: Digital signatures commonly use digital certificates that are used to verify the identity of the originator in order to authenticate a vendor website and establish an encrypted connection to exchange confidential data. One such example is when a person logs into a financial institution from a web browser.

10. In a hierarchical CA topology, where can a subordinate CA obtain a certificate for itself?

- **from the root CA or another subordinate CA at a higher level**
- from the root CA or another subordinate CA at the same level
- from the root CA or from self-generation
- from the root CA only
- from the root CA or another subordinate CA anywhere in the tree

Explanation: In a hierarchical CA topology, CAs can issue certificates to end users and to subordinate CAs, which in turn issue their certificates to end users, other lower level CAs, or both. In this way, a tree of CAs and end users is built in which every CA can issue certificates to lower level CAs and end users. Only the root CA can issue a self-signing certificate in a hierarchical CA topology.

11. What is the purpose for using digital signatures for code signing?

- to establish an encrypted connection to exchange confidential data with a vendor website

- **to verify the integrity of executable files downloaded from a vendor website**
- to authenticate the identity of the system with a vendor website
- to generate a virtual ID

Explanation: Code signing is used to verify the integrity of executable files downloaded from a vendor website. Code signing uses digital certificates to authenticate and verify the identity of a website.

12. What technology has a function of using trusted third-party protocols to issue credentials that are accepted as an authoritative identity?

- digital signatures
- hashing algorithms
- **PKI certificates**
- symmetric keys

Explanation: Digital certificates are used to prove the authenticity and integrity of PKI certificates, but a PKI Certificate Authority is a trusted third-party entity that issues PKI certificates. PKI certificates are public information and are used to provide authenticity, confidentiality, integrity, and nonrepudiation services that can scale to large requirements.

13. In addressing a risk that has low potential impact and relatively high cost of mitigation or reduction, which strategy will accept the risk and its consequences?

- risk avoidance
- risk reduction
- **risk retention**
- risk sharing

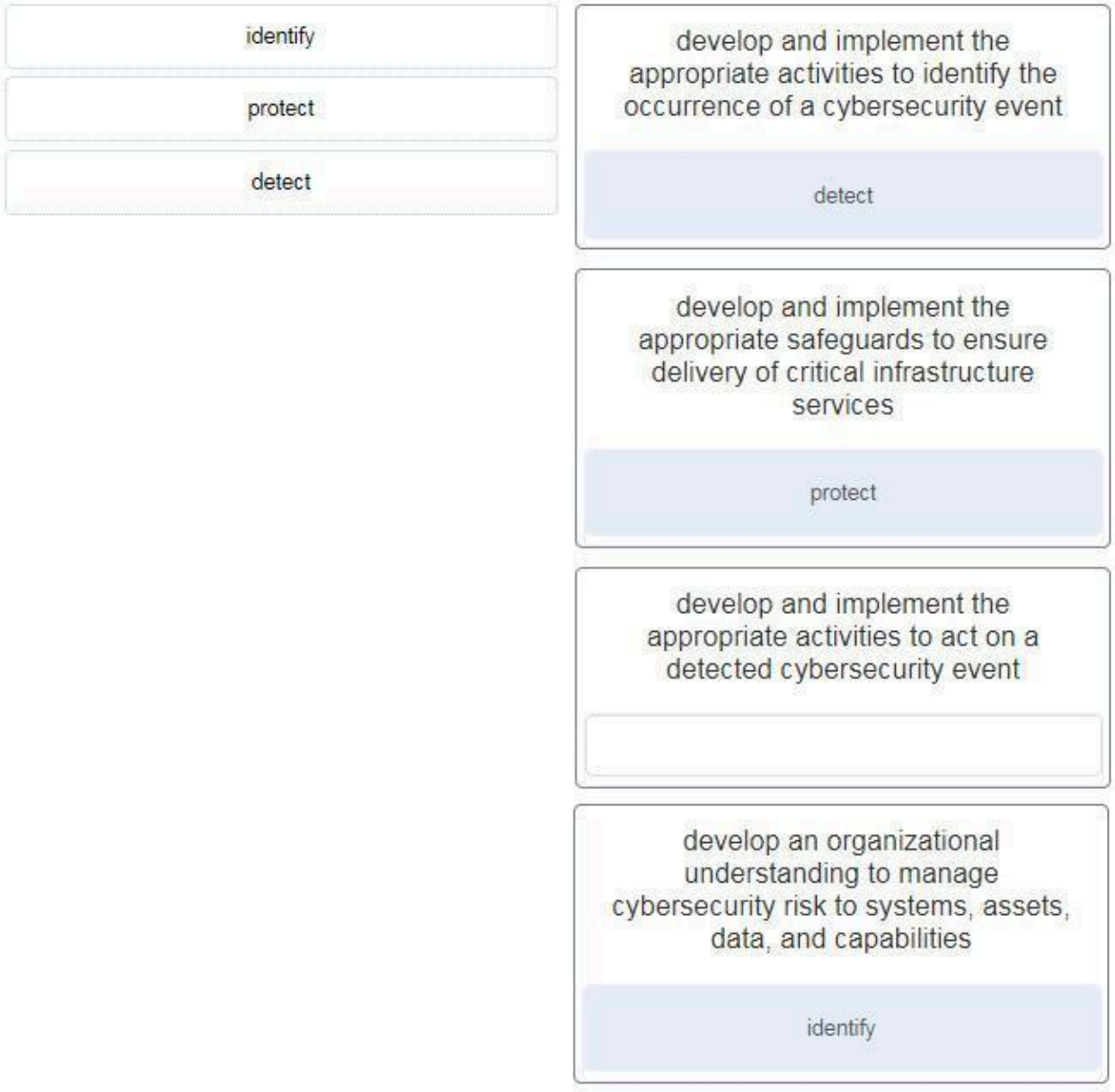
Explanation: There are four potential strategies for responding to risks that have been identified:
Risk avoidance – Stop performing the activities that create risk.
Risk reduction – Decrease the risk by taking measures to reduce vulnerability.
Risk sharing – Shift some of the risk to other parties.
Risk retention – Accept the risk and its consequences.

14. Which two classes of metrics are included in the CVSS Base Metric Group? (Choose two.)

- Confidentiality Requirement
- Modified Base
- Exploit Code Maturity
- **Exploitability**
- **Impact metrics**

Explanation: The Base Metric Group of CVSS represents the characteristics of a vulnerability that are constant over time and across contexts. It contains two classes of metrics, Exploitability and Impact.

15. Match the NIST Cybersecurity Framework core function with the description. (Not all options are used.)



- develop and implement the appropriate activities to identify the occurrence of a cybersecurity event : detect
- develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services : protect
- develop and implement the appropriate activities to act on a detected cybersecurity event

- develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
  : identify

16. A cybersecurity analyst is performing a CVSS assessment on an attack where a web link was sent to several employees. Once clicked, an internal attack was launched. Which CVSS Base Metric Group Exploitability metric is used to document that the user had to click on the link in order for the attack to occur?

- scope
- integrity requirement
- availability requirement
- **user interaction**

Explanation: The CVSS Base Metric Group has the following metrics: attack vector, attack complexity, privileges required, user interaction, and scope. The user interaction metric expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful.

17. In network security assessments, which type of test employs software to scan internal networks and Internet facing servers for various types of vulnerabilities?

- **vulnerability assessment**
- risk analysis
- strength of network security testing
- penetration testing

Explanation: In vulnerability assessment, security analysts use software to scan internal networks and Internet facing servers for various types of vulnerabilities. Tools for vulnerability assessment include the open source OpenVAS platform, Microsoft Baseline Security Analyzer, Nessus, Qualys, and Fireeye Mandiant services.

18. What are the three outcomes of the NIST Cybersecurity Framework identify core function? (Choose three.)

- information protection process and procedures
- **governance**
- mitigation
- **risk assessment**

- **asset management**
- recovery planning

Explanation: The identify core function is concerned with the development of organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It involves the following outcomes:
Asset management
Business environment
Governance
Risk assessment
Risk management strategy

19. Which statement describes the term iptables?

- It is a file used by a DHCP server to store current active IP addresses.
- **It is a rule-based firewall application in Linux.**
- It is a DHCP application in Windows.
- It is a DNS daemon in Linux.

Explanation: Iptables is an application that allows Linux system administrators to configure network access rules.

20. What is the difference between an HIDS and a firewall?

- An HIDS works like an IPS, whereas a firewall just monitors traffic.
- **An HIDS monitors operating systems on host computers and processes file system activity. Firewalls allow or deny traffic between the computer and other systems.**
- A firewall performs packet filtering and therefore is limited in effectiveness, whereas an HIDS blocks intrusions.
- An HIDS blocks intrusions, whereas a firewall filters them.
- A firewall allows and denies traffic based on rules and an HIDS monitors network traffic.

Explanation: In order to monitor local activity an HIDS should be implemented. Network activity monitors are concerned with traffic and not operating system activity.

21. Which statement describes the Cisco Threat Grid Glovebox?

- It is a network-based IDS/IPS.

- It is a host-based intrusion detection system (HIDS) solution to fight against malware.
- **It is a sandbox product for analyzing malware behaviors.**
- It is a firewall appliance.

Explanation: Cisco ThreatGrid Glovebox is a sandbox product for analyzing malware behaviors.

22. Which statement describes the policy-based intrusion detection approach?

- It compares the signatures of incoming traffic to a known intrusion database.
- **It compares the operations of a host against well-defined security rules.**
- It compares the antimalware definitions to a central repository for the latest updates.
- It compares the behaviors of a host to an established baseline to identify potential intrusion.

Explanation: With the anomaly-based intrusion detection approach, a set of rules or policies are applied to a host. Violation of these policies is interpreted to be the result of a potential intrusion.

23. What is the purpose of the DH algorithm?

- to provide nonrepudiation support
- **to generate a shared secret between two hosts that have not communicated before**
- to encrypt data traffic after a VPN is established
- to support email data confidentiality

Explanation: DH is an asymmetric mathematical algorithm that allows two computers to generate an identical shared secret, without having communicated before. Asymmetric key systems are extremely slow for any sort of bulk encryption. It is common to encrypt the bulk of the traffic using a symmetric algorithm such as DES, 3DES, or AES, and use the DH algorithm to create keys that will be used by the symmetric encryption algorithm.

24. What is a difference between symmetric and asymmetric encryption algorithms?

- Symmetric encryption algorithms are used to authenticate secure communications. Asymmetric encryption algorithms are used to repudiate messages.
- Symmetric encryption algorithms are used to encrypt data. Asymmetric encryption algorithms are used to decrypt data.
- **Symmetric encryption algorithms use pre-shared keys. Asymmetric encryption algorithms use different keys to encrypt and decrypt data.**
- Symmetric algorithms are typically hundreds to thousands of times slower than asymmetric algorithms.

Explanation: Asymmetric algorithms can use very long key lengths in order to avoid being hacked. This results in the use of significantly increased resources and time compared to symmetric algorithms.

25. When a server profile for an organization is being established, which element describes the TCP and UDP daemons and ports that are allowed to be open on the server?

- critical asset address space
- service accounts
- software environment
- **listening ports**

Explanation: A server profile will often contain the following:
Listening ports – the TCP and UDP daemons and ports that are allowed to be open on the server
User accounts – the parameters defining user access and behavior
Service accounts – the definitions of the type of service that an application is allowed to run on a server
Software environment – the tasks, processes, and applications that are permitted to run on the server

26. What is an action that should be taken in the discovery step of the vulnerability management life cycle?

- documenting the security plan
- assigning business value to assets
- **developing a network baseline**
- determining a risk profile

Explanation: During the discovery step of the vulnerability management life cycle, an inventory of all network assets is made. A network baseline is developed, and security vulnerabilities are identified.

27. In what order are the steps in the vulnerability management life cycle conducted?

- discover, assess, prioritize assets, report, remediate, verify
- discover, prioritize assets, assess, remediate, report, verify
- discover, prioritize assets, assess, remediate, verify, report
- **discover, prioritize assets, assess, report, remediate, verify**

Explanation: There are six steps in the vulnerability management life cycle:

- Discover
- Prioritize assets
- Assess
- Report
- Remediate
- Verify

28. A security professional is making recommendations to a company for enhancing endpoint security. Which security endpoint technology would be recommended as an agent-based system to protect hosts against malware?

- IPS
- **HIDS**
- blacklisting
- baselining

Explanation: A host-based intrusion detection systems (HIDS) is a comprehensive security application that provides antimalware applications, a firewall, and monitoring and reporting.

29. What is a feature of distributed firewalls?

- They all use an open sharing standard platform.
- They use only TCP wrappers to configure rule-based access control and logging systems.
- They use only iptables to configure network rules.

- **They combine the feature of host-based firewalls with centralized management.**

30. An administrator suspects polymorphic malware has successfully entered the network past the HIDS system perimeter. The polymorphic malware is, however, successfully identified and isolated. What must the administrator do to create signatures to prevent the file from entering the network again?

- **Execute the polymorphic file in the Cisco Threat Grid Glovebox.**
- Run the Cisco Talos security intelligence service.
- Use Cisco AMP to track the trajectory of a file through the network.
- Run a baseline to establish an accepted amount of risk, and the environmental components that contribute to the risk level of the polymorphic malware.

Explanation: The isolated polymorphic malware file should be run in a sandbox environment like Cisco Threat Grid Glovebox, and the activities of the file documented by the system. This information can then be used to create signatures to prevent the file from entering the network again.

31. On a Windows host, which tool can be used to create and maintain blacklists and whitelists?

- Local Users and Groups
- **Group Policy Editor**
- Task Manager
- Computer Management

Explanation: In Windows, blacklisting and whitelisting settings can be managed through the Group Policy Editor.

32. In addressing an identified risk, which strategy aims to stop performing the activities that create risk?

- risk retention
- **risk avoidance**
- risk sharing
- risk reduction

Explanation: There are four potential strategies for responding to risks that have been identified:

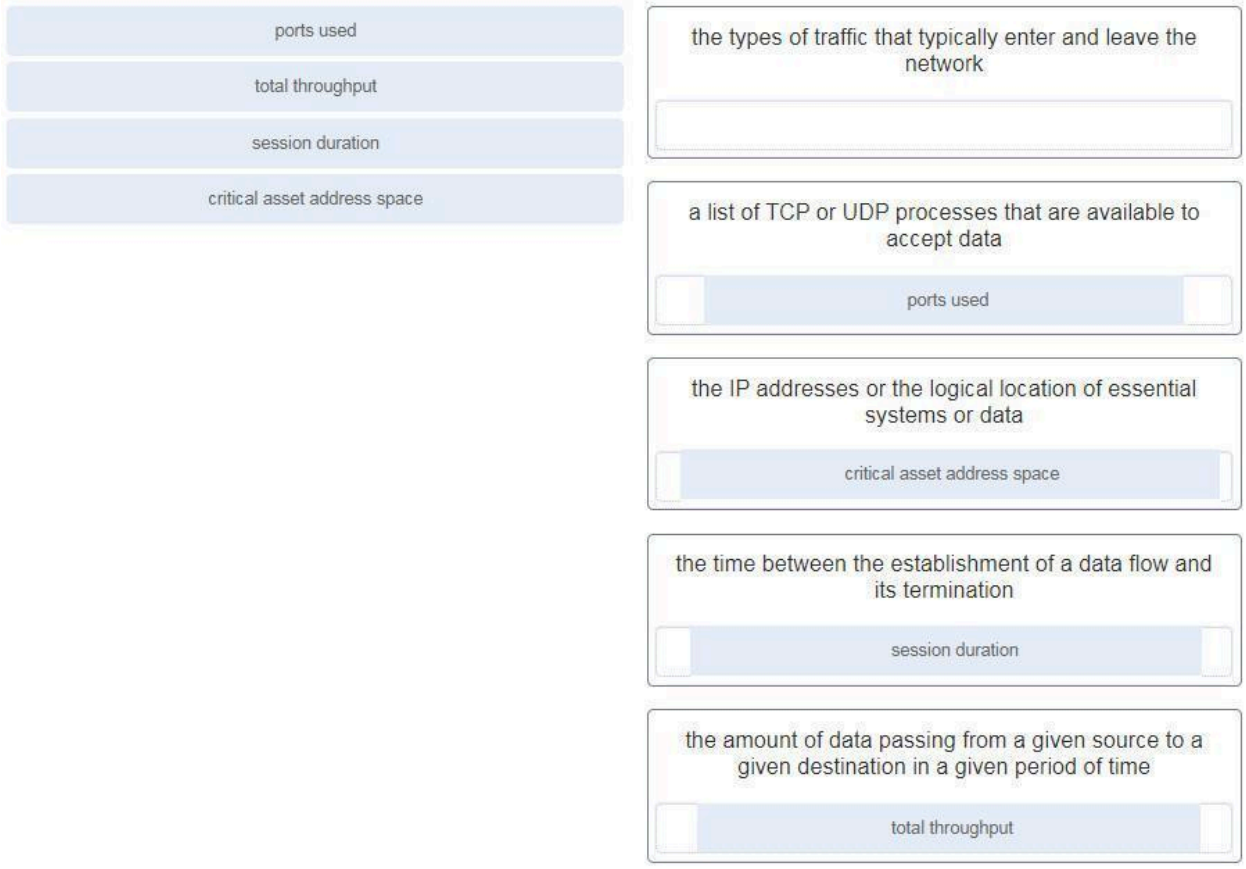
- Risk avoidance – Stop performing the activities that create risk.
- Risk reduction – Decrease the risk by taking measures to reduce vulnerability.
- Risk sharing – Shift some of the risk to other parties.
- Risk retention – Accept the risk and its consequences.

33. A company is developing a security policy for secure communication. In the exchange of critical messages between a headquarters office and a branch office, a hash value should only be recalculated with a predetermined code, thus ensuring the validity of data source. Which aspect of secure communications is addressed?

- data integrity
- data confidentiality
- non-repudiation
- **origin authentication**

Explanation: Secure communications consists of four elements:
Data confidentiality – guarantees that only authorized users can read the message
Data integrity – guarantees that the message was not altered
Origin authentication – guarantees that the message is not a forgery and does actually come from whom it states
Data nonrepudiation – guarantees that the sender cannot repudiate, or refute, the validity of a message sent

34. Match the network profile element to the description. (Not all options are used.)



Explanation: Important elements of a network profile include:

- **Total throughput** – the amount of data passing from a given source to a given destination in a given period of time
- **Session duration** – the time between the establishment of a data flow and its termination
- **Ports used** – a list of TCP or UDP processes that are available to accept data
- **Critical asset address space** – the IP addresses or the logical location of essential systems or data

35. What is blacklisting?

- **This is an application list that can dictate which user applications are not permitted to run on a computer.**
- This is a user list to prevent blacklisted users from accessing a computer.

- This is a network process list to stop a listed process from running on a computer.
- This is a Heuristics-based list to prevent a process from running on a computer.

36. Which technology is used by Cisco Advanced Malware Protection (AMP) in defending and protecting against known and emerging threats?

- network admission control
- network profiling
- website filtering and blacklisting
- **threat intelligence**

Explanation: Cisco AMP uses threat intelligence along with known file signatures to identify and block policy-violating file types and exploitations.

37. Which technique could be used by security personnel to analyze a suspicious file in a safe environment?

- **sandboxing**
- baselining
- whitelisting
- blacklisting

Explanation: Sandboxing allows suspicious files to be executed and analyzed in a safe environment. There are free public sandboxes that allow for malware samples to be uploaded or submitted and analyzed.

38. A company implements a security policy that ensures that a file sent from the headquarters office to the branch office can only be opened with a predetermined code. This code is changed every day. Which two algorithms can be used to achieve this task? (Choose two.)

- HMAC
- MD5
- **3DES**
- SHA-1
- **AES**

Explanation: The task to ensure that only authorized personnel can open a file is data confidentiality, which can be implemented with

encryption. AES and 3DES are two encryption algorithms. HMAC can be used for ensuring origin authentication. MD5 and SHA-1 can be used to ensure data integrity.

39. Which security management plan specifies a component that involves tracking the location and configuration of networked devices and software across an enterprise?

- **asset management**
- patch management
- vulnerability management
- risk management

Explanation: Asset management involves tracking the location and configuration of networked devices and software across an enterprise.

CyberOps Associate (Version 1.0) – Modules 24 – 25: Protocols and Log Files Group Exam

1. What is a feature of the tcpdump tool?

- It provides real-time reporting and long-term analysis of security events.
- It records metadata about packet flows.
- It uses agents to submit host logs to centralized management servers.
- **It can display packet captures in real time or write them to a file.**

2. Which Windows tool can be used to review host logs?

- Services
- **Event Viewer**
- Task Manager
- Device Manager

3. Which type of security data can be used to describe or predict network behavior?

- alert
- transaction
- session

- **statistical**

4. Which function is provided by the Sguil application?

- It reports conversations between hosts on the network.
- **It makes Snort-generated alerts readable and searchable.**
- It detects potential network intrusions.
- It prevents malware from attacking a host.

Explanation: Applications such as Snorby and Sguil can be used to read and search alert messages generated by NIDS/NIPS.

5. Which ICMP message type should be stopped inbound?

- source quench
- echo-reply
- **echo**
- unreachable

Explanation: The echo ICMP packet should not be allowed inbound on an interface. The echo-reply should be allowed so that when an internal device pings an external device, the reply is allowed to return.

6. How can IMAP be a security threat to a company?

- Someone inadvertently clicks on a hidden iFrame.
- Encrypted data is decrypted.
- **An email can be used to bring malware to a host.**
- It can be used to encode stolen data and send to a threat actor.

Explanation: IMAP, SMTP, and POP3 are email protocols. SMTP is used to send data from a host to a server or to send data between servers. IMAP and POP3 are used to download email messages and can be responsible for bringing malware to the receiving host.

7. Which two technologies are primarily used on peer-to-peer networks? (Choose two.)

- **Bitcoin**
- **BitTorrent**
- Wireshark
- Darknet
- Snort

Explanation: Bitcoin is used to share a distributed database or ledger. BitTorrent is used for file sharing.

8. Which protocol is exploited by cybercriminals who create malicious iFrames?

- **HTTP**
- ARP
- DHCP
- DNS

Explanation: An HTML element known as an inline frame or iFrame allows the browser to load a different web page from another source.

9. Which method is used by some malware to transfer files from infected hosts to a threat actor host?

- UDP infiltration
- **ICMP tunneling**
- HTTPS traffic encryption
- iFrame injection

Explanation: ICMP traffic from inside the company is also a threat. Some varieties of malware use ICMP packets to transfer files from infected hosts to threat actors via ICMP tunneling.

10. Why does HTTPS technology add complexity to network security monitoring?

- HTTPS dynamically changes the port number on the web server.
- HTTPS uses tunneling technology for confidentiality.
- HTTPS hides the true source IP address using NAT/PAT.
- **HTTPS conceals data traffic through end-to-end encryption.**

Explanation: With HTTPS, a symmetric key is generated by the client after the client verifies the trustworthiness of the web server. The symmetric key is encrypted with the public key of the web server and then sent to the web server. The web server uses its public key to decrypt the key. The key is then used to encrypt the data requested by the client and the data is sent to the client. This end-to-end encryption complicates inline network security monitoring. The HTTPS port number, typically 443, is configured statically on the web server.

11. Which approach is intended to prevent exploits that target syslog?

- Use a Linux-based server.
- **Use syslog-ng.**
- Create an ACL that permits only TCP traffic to the syslog server.
- Use a VPN between a syslog client and the syslog server.

Explanation: Hackers may try to block clients from sending data to the syslog server, manipulate or erase logged data, or manipulate the software used to transmit messages between the clients and the server. Syslog-ng is the next generation of syslog and it contains improvements to prevent some of the exploits.

12. Which type of attack is carried out by threat actors against a network to determine which IP addresses, protocols, and ports are allowed by ACLs?

- phishing
- denial of service
- **reconnaissance**
- social engineering

Explanation: Packet filtering ACLs use rules to filter incoming and outgoing traffic. These rules are defined by specifying IP addresses, port numbers, and protocols to be matched. Threat actors can use a reconnaissance attack involving port scanning or penetration testing to determine which IP addresses, protocols, and ports are allowed by ACLs.

13. Which two application layer protocols manage the exchange of messages between a client with a web browser and a remote web server? (Choose two.)

- **HTTP**
- **HTTPS**
- DNS
- DHCP
- HTML

Explanation: Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) are two application layer protocols that manage the content requests from clients and the responses from the web server. HTML (Hypertext Mark-up Language) is the encoding language that describes the content and display features of a web page. DNS is for

domain name to IP address resolution. DHCP manages and provides dynamic IP configurations to clients.

14. What is Tor?

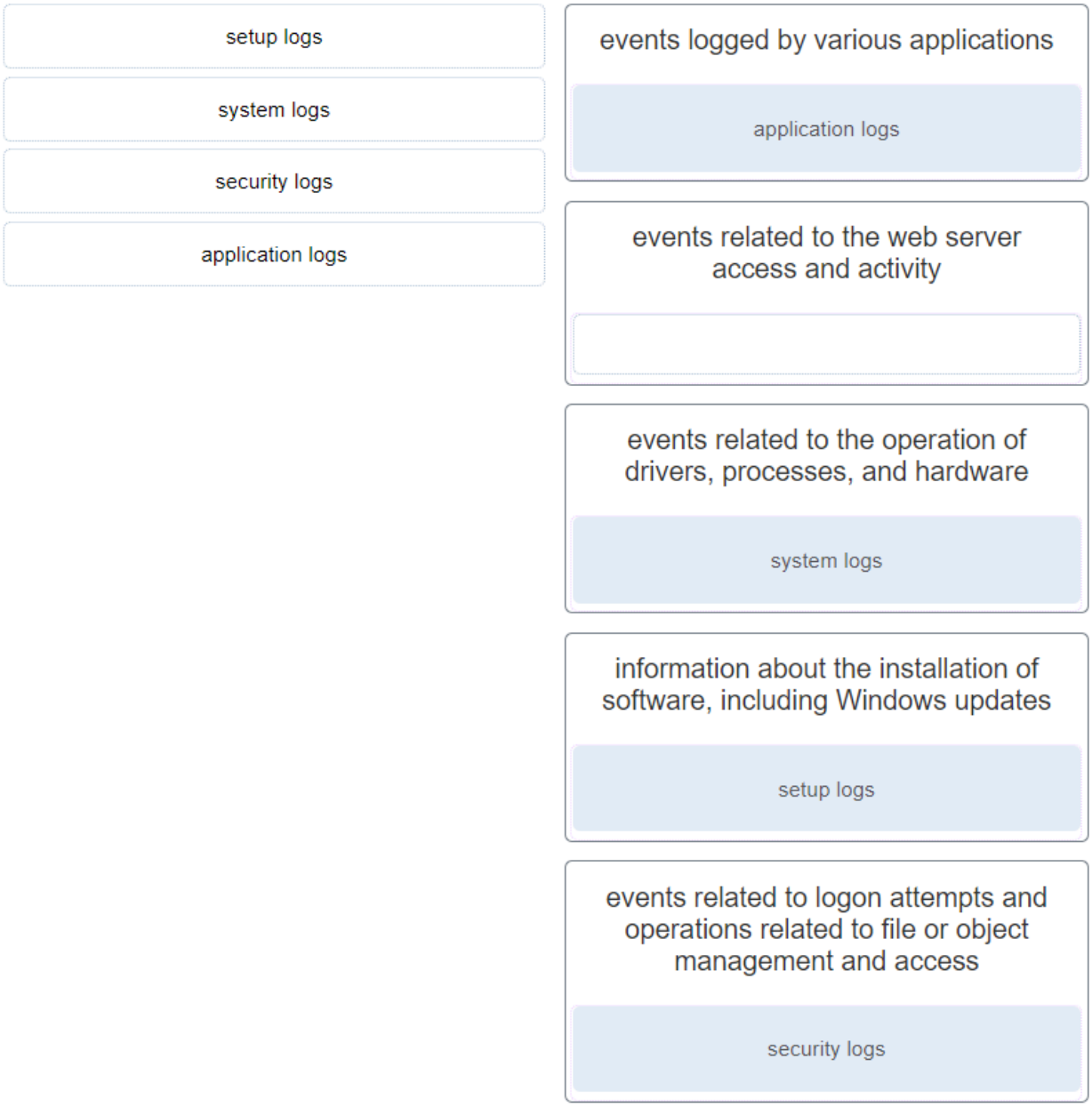
- a rule created in order to match a signature of a known exploit
- **a software platform and network of P2P hosts that function as Internet routers**
- a way to share processors between network devices across the Internet
- a type of Instant Messaging (IM) software used on the darknet

15. Which Windows log contains information about installations of software, including Windows updates?

- system logs
- application logs
- **setup logs**
- security logs

Explanation: On a Windows host, setup logs record information about the installation of software, including Windows updates.

16. Match the Windows host log to the messages contained in it. (Not all options are used.)



- events logged by various applications : **application logs**
- events related to the web server access and activity :
- events related to the operation of drivers, processes, and hardware : **system logs**
- information about the installation of software, including Windows updates : **setup logs**

- events related to logon attempts and operations related to file or object management and access : **security logs**

17. Which Cisco appliance can be used to filter network traffic contents to report and deny traffic based on the web server reputation?

- **WSA**
- AVC
- ASA
- ESA

Explanation: The Cisco Web Security Appliance (WSA) acts as a web proxy for an enterprise network. WSA can provide many types of logs related to web traffic security including ACL decision logs, malware scan logs, and web reputation filtering logs. The Cisco Email Security Appliance (ESA) is a tool to monitor most aspects of email delivery, system functioning, antivirus, antispam operations, and blacklist and whitelist decisions. The Cisco ASA is a firewall appliance. The Cisco Application Visibility and Control (AVC) system combines multiple technologies to recognize, analyze, and control over 1000 applications.

18. Which technique would a threat actor use to disguise traces of an ongoing exploit?

- Create an invisible iFrame on a web page.
- **Corrupt time information by attacking the NTP infrastructure.**
- Encapsulate other protocols within DNS to evade security measures.
- Use SSL to encapsulate malware.

Explanation: The Network Time Protocol (NTP) uses a hierarchy of time sources to provide a consistent time clock to network infrastructure devices. Threat actors may attack the NTP infrastructure in order to corrupt time information that is used in network logs.

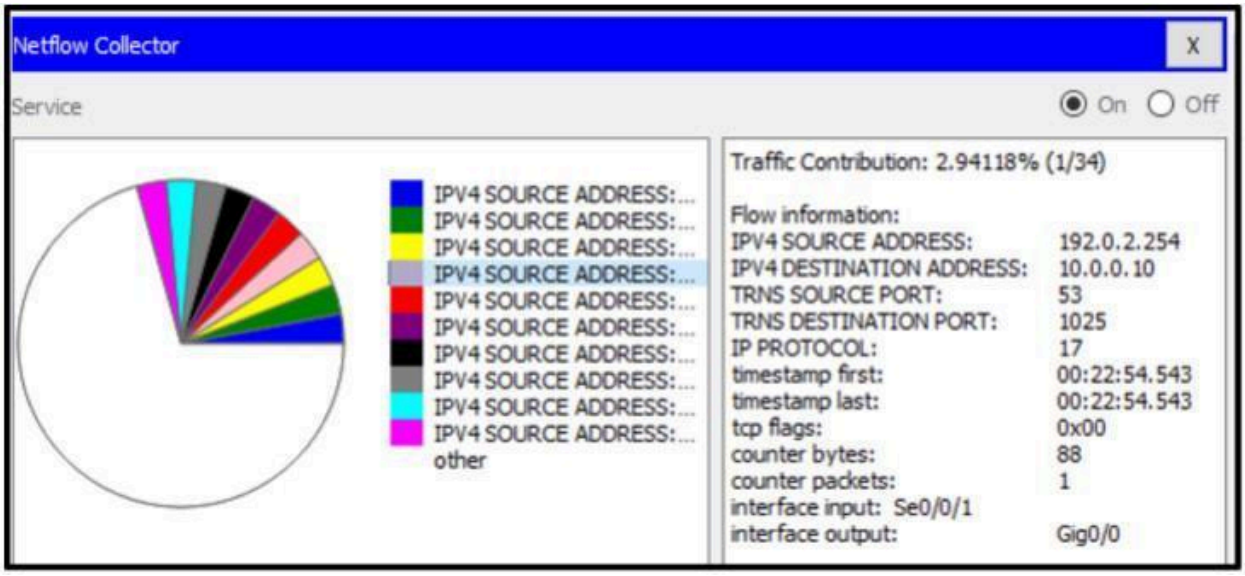
19. A system administrator runs a file scan utility on a Windows PC and notices a file lsass.exe in the Program Files directory. What should the administrator do?

- **Delete the file because it is probably malware.**
- Move it to Program Files (x86) because it is a 32bit application.

- Uninstall the lsass application because it is a legacy application and no longer required by Windows.
- Open the Task Manager, right-click on the lsass process and choose End Task .

Explanation: On Windows computers, security logging and security policies enforcement are carried out by the Local Security Authority Subsystem Service (LSASS), running as lsass.exe. It should be running from the Windows\System32 directory. If a file with this name, or a camouflaged name, such as lsass.exe, is running or running from another directory, it could be malware.

20. Refer to the exhibit. A network administrator is viewing some output on the Netflow collector. What can be determined from the output of the traffic flow shown?



- This is a UDP DNS request to a DNS server.
- **This is a UDP DNS response to a client machine.**
- This is a TCP DNS request to a DNS server.
- This is a TCP DNS response to a client machine.

Explanation: The traffic flow shown has a source port of 53 and a destination port of 1025. Port 53 is used for DNS and because the source port is 53, this traffic is responding to a client machine from a DNS server. The IP PROTOCOL is 17 and specifies that UDP is being used and the TCP flag is set to 0.

21 In a Cisco AVC system, in which module is NetFlow deployed?

- Management and Reporting
- Control
- Application Recognition
- **Metrics Collection**

Explanation: NetFlow technology is deployed in the Metrics Collection module of a Cisco AVC system to collect network flow metrics and to export to management tools.

22. What does it indicate if the timestamp in the HEADER section of a syslog message is preceded by a period or asterisk symbol?

- **There is a problem associated with NTP.**
- The timestamp represents the round trip duration value.
- The syslog message should be treated with high priority.
- The syslog message indicates the time an email is received.

Explanation: The HEADER section of the message contains the timestamp. If the timestamp is preceded by the period (.) or asterisk (*) symbols, a problem is indicated with NTP.

23. Which protocol is a name resolution protocol often used by malware to communicate with command-and-control (CnC) servers?

- IMAP
- **DNS**
- HTTPS
- ICMP

Explanation: Domain Name Service (DNS) is used to convert domain names into IP addresses. Some organizations have less stringent policies in place to protect against DNS-based threats than they have in place for other exploits.

24. Which technique is necessary to ensure a private transfer of data using a VPN?

- authorization
- scalability
- **encryption**

- virtualization

Explanation: Confidential and secure transfers of data with VPNs require data encryption.

25. Which technology would be used to create the server logs generated by network devices and reviewed by an entry level network person who works the night shift at a data center?

- **syslog**
- NAT
- ACL
- VPN

Explanation: Syslog is a daemon or service run on a server that accepts messages sent by network devices. These logs are frequently examined to detect inconsistencies and issues within the network.

26. Which statement describes a Cisco Web Security Appliance (WSA)?

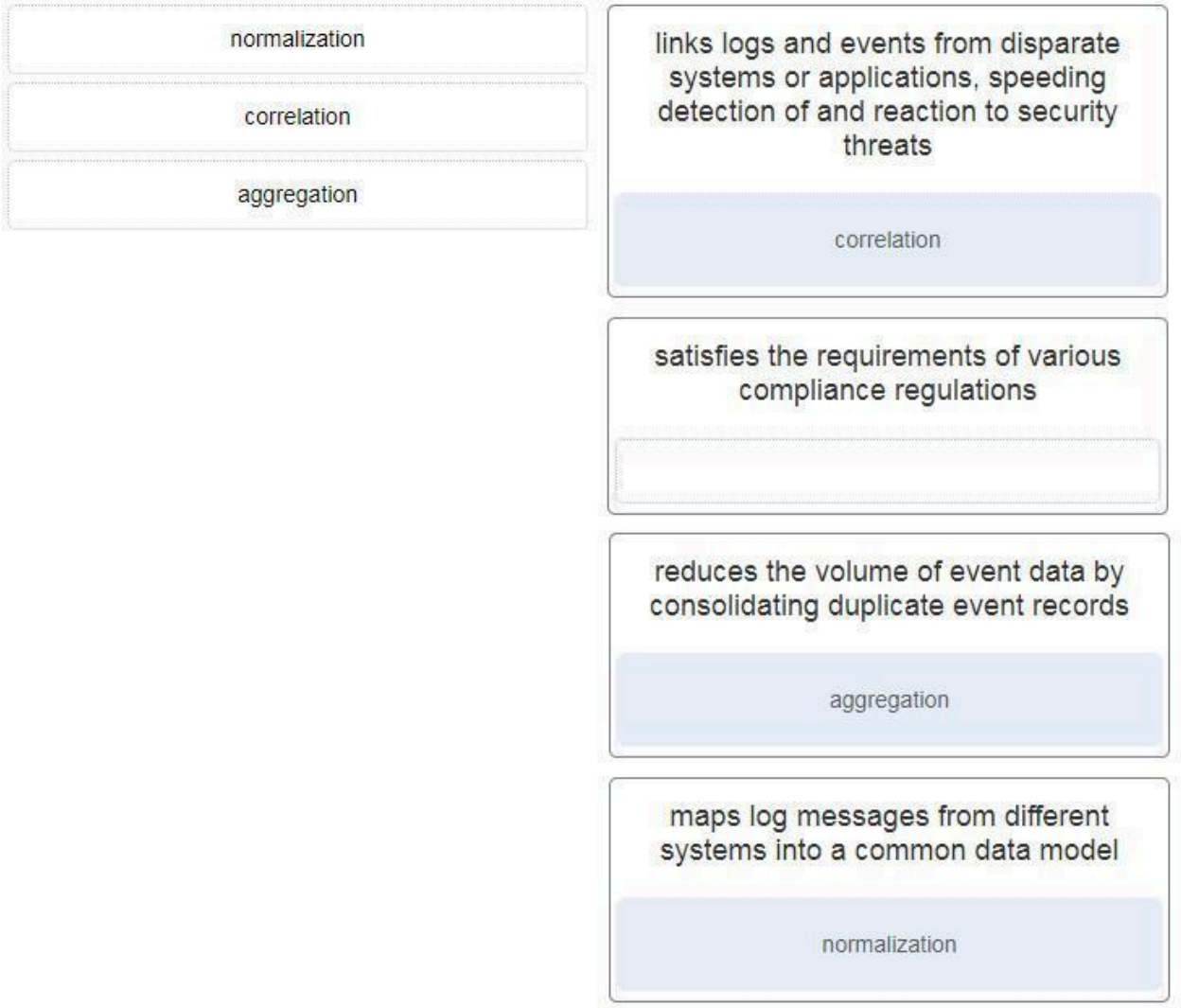
- It protects a web server by preventing security threats from accessing the server.
- It provides high performance web services.
- It acts as an SSL-based VPN server for an enterprise.
- **It functions as a web proxy.**

Explanation: Cisco Web Security Appliance (WSA) devices provide a wide range of functionalities for security monitoring. WSA effectively acts as a web proxy. It logs all inbound and outbound transaction information for HTTP traffic.

27. Which statement describes statistical data in network security monitoring processes?

- **It is created through an analysis of other forms of network data.**
- It contains conversations between network hosts.
- It shows the results of network activities between network hosts.
- It lists each alert message along with statistical information.

28. Match the SIEM function with the description.



- links logs and events from disparate systems or applications, speeding detection of and reaction to security threats : **correlation**
- satisfies the requirements of various compliance regulations :
- reduces the volume of event data by consolidating duplicate event records : **aggregation**
- maps log messages from different systems into a common data model : **normalization**

29. Which two tools have a GUI interface and can be used to view and analyze full packet captures? (Choose two.)

- nfdump

- **Wireshark**
- **Cisco Prime Network Analysis Module**
- tcpdump
- Splunk

Explanation: The Network Analysis Module of the Cisco Prime Infrastructure system and Wireshark have GUI interfaces and can display full packet captures. The tcpdump tool is a command-line packet analyzer.

30. Which statement describes session data in security logs?

- It can be used to describe or predict network behavior.
- It shows the result of network sessions.
- **It is a record of a conversation between network hosts.**
- It reports detailed network activities between network hosts.

Explanation: Session data is a record of a conversation between two network endpoints.

31. Which two options are network security monitoring approaches that use advanced analytic techniques to analyze network telemetry data? (Choose two.)

- **NBAD**
- Sguil
- NetFlow
- IPFIX
- Snorby
- **NBA**

Explanation: Network behavior analysis (NBA) and network behavior anomaly detection (NBAD) are approaches to network security monitoring that use advanced analytical techniques to analyze NetFlow or IPFIX network telemetry data.

32. How does a web proxy device provide data loss prevention (DLP) for an enterprise?

- by functioning as a firewall
- by inspecting incoming traffic for potential exploits
- **by scanning and logging outgoing traffic**

- by checking the reputation of external web servers

Explanation: A web proxy device can inspect outgoing traffic as means of data loss prevention (DLP). DLP involves scanning outgoing traffic to detect whether the data that is leaving the enterprise network contains sensitive, confidential, or secret information.

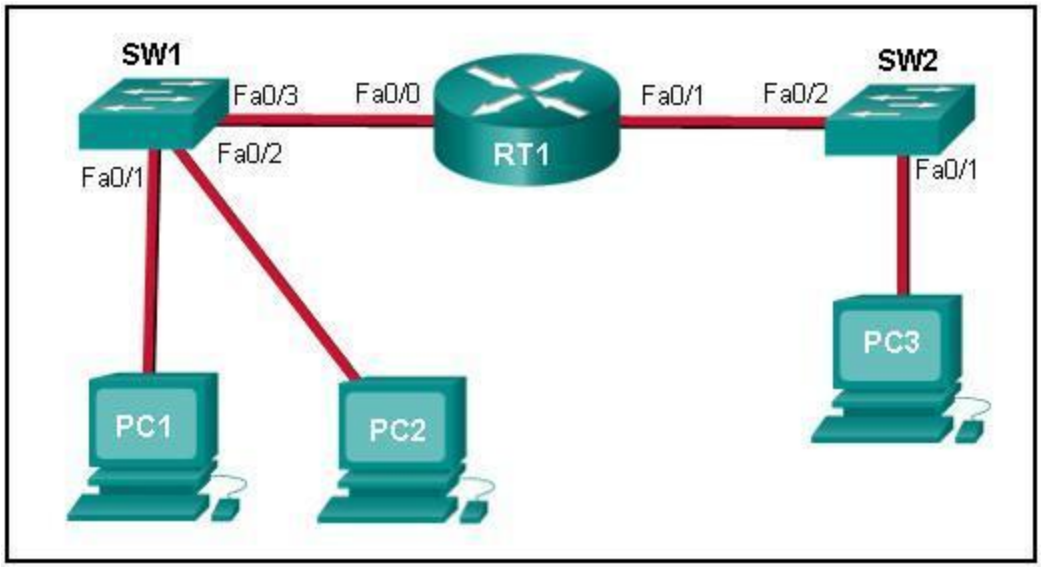
33. Which information can be provided by the Cisco NetFlow utility?

- security and user account restrictions
- IDS and IPS capabilities
- **peak usage times and traffic routing**
- source and destination UDP port mapping

Explanation: NetFlow efficiently provides an important set of services for IP applications including network traffic accounting, usage-based network billing, network planning, security, denial of service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

GPL	older rules created by Sourcefire → GPL
ET	rules created and maintained by Cisco Talos → VRT
VRT	open source rules under BSD license → ET

65. Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC3. In this scenario, what will happen next?



- RT1 will send an ARP reply with its own Fa0/1 MAC address.
- SW1 will send an ARP reply with its Fa0/1 MAC address.
- RT1 will send an ARP reply with the PC3 MAC address.

- RT1 will forward the ARP request to PC3.
- **RT1 will send an ARP reply with its own Fa0/0 MAC address.**

Explanation: When a network device has to communicate with a device on another network, it broadcasts an ARP request asking for the default gateway MAC address. The default gateway (RT1) unicasts an ARP reply with the Fa0/0 MAC address.

CyberOps Associate (Version 1.0) – CyberOps Associate 1.0 Practice Final exam Answers

1. When real-time reporting of security events from multiple sources is being received, which function in SIEM provides capturing and processing of data in a common format?

- log collection
- **normalization**
- aggregation
- compliance

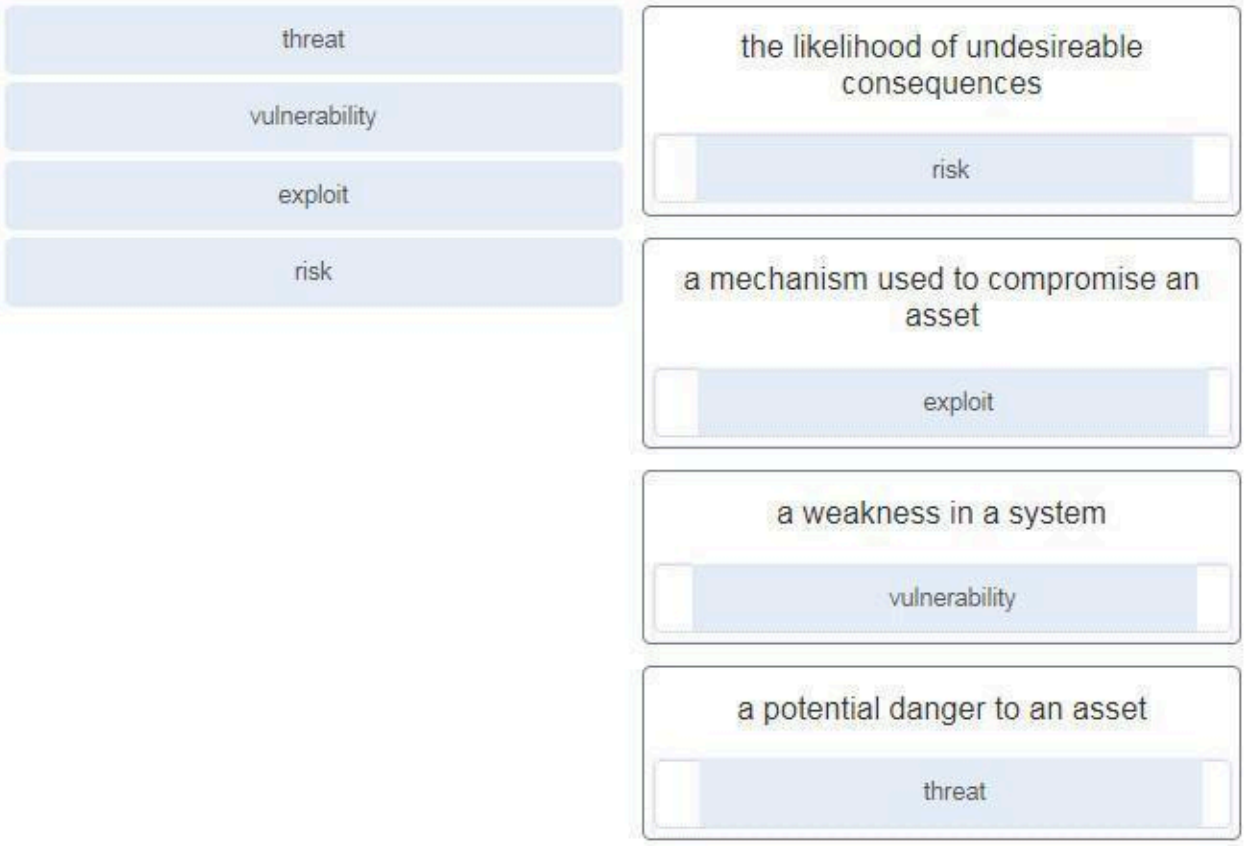
2. What is the value of file hashes to network security investigations?

- They ensure data availability.
- They assure nonrepudiation.
- They offer confidentiality.
- **They can serve as malware signatures.**

3. Which technology is an open source SIEM system?

- StealthWatch
- **ELK**
- Splunk
- Wireshark

4. Match the security concept to the description.



5. What are the two important components of a public key infrastructure (PKI) used in network security? (Choose two.)

- intrusion prevention system
- **digital certificates**
- symmetric encryption algorithms
- **certificate authority**
- pre-shared key generation

Explanation: A public key infrastructure uses digital certificates and certificate authorities to manage asymmetric key distribution. PKI certificates are public information. The PKI certificate authority (CA) is a trusted third-party that issues the certificate. The CA has its own certificate (self-signed certificate) that contains the public key of the CA.

6. Which three algorithms are designed to generate and verify digital signatures? (Choose three.)

- 3DES
- IKE
- **DSA**
- AES
- **ECDSA**
- **RSA**

Explanation: There are three Digital Signature Standard (DSS) algorithms that are used for generating and verifying digital signatures:
Digital Signature Algorithm (DSA)
Rivest-Shamir Adelman Algorithm (RSA)
Elliptic Curve Digital Signature Algorithm (ECDSA)

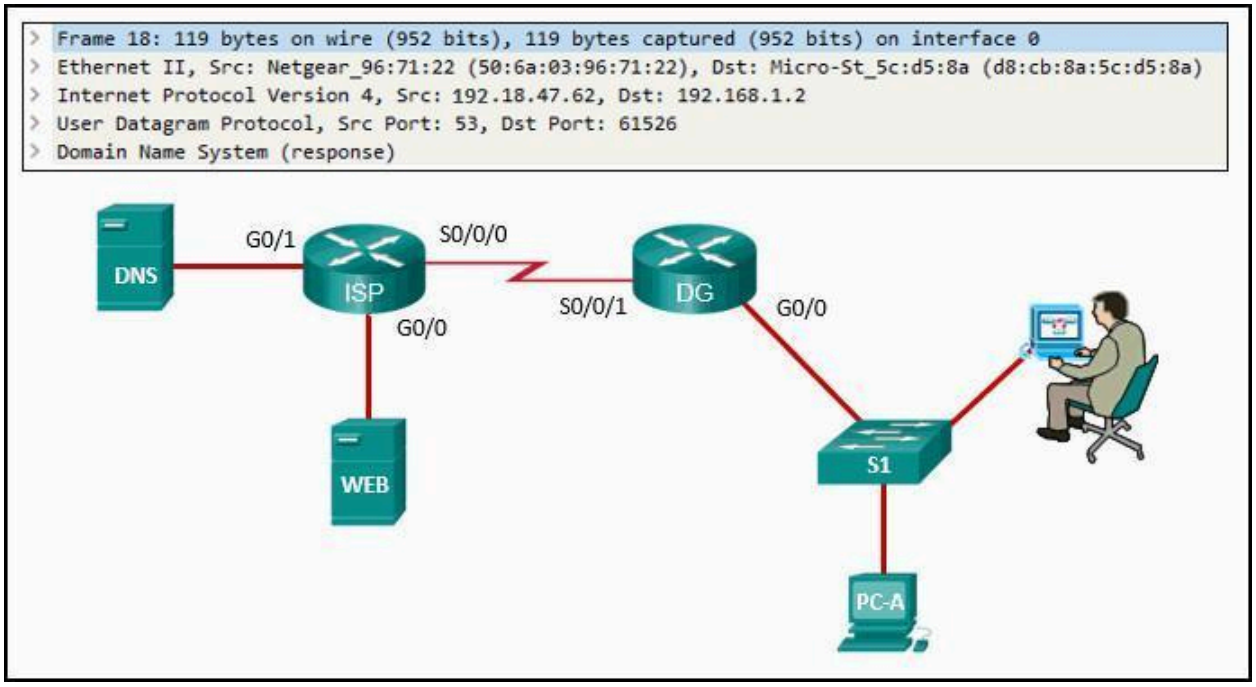
7. Which section of a security policy is used to specify that only authorized individuals should have access to enterprise data?

- statement of authority
- **identification and authentication policy**
- campus access policy
- Internet access policy
- statement of scope
- acceptable use policy

Explanation: The identification and authentication policy section of the security policy typically specifies authorized persons that can have access to network resources and identity verification procedures.

8. Refer to the exhibit. A cybersecurity analyst is viewing captured packets forwarded on switch S1. Which device has the MAC address

d8:cb:8a:5c:d5:8a?



- **PC-A**
- DNS server
- web server
- router DG
- router ISP

Explanation: The Wireshark capture is a DNS response from the DNS server to PC-A. Because the packet was captured on the LAN that the PC is on, router DG would have encapsulated the response packet from the ISP router into an Ethernet frame addressed to PC-A and forwarded the frame with the MAC address of PC-A as the destination.

9. What kind of message is sent by a DHCPv4 client requesting an IP address?

- **DHCPDISCOVER broadcast message**
- DHCPDISCOVER unicast message
- DHCPOFFER unicast message
- DHCPACK unicast message

Explanation: When the DHCPv4 client requests an IP address, it sends a DHCPDISCOVER broadcast message seeking a DHCPv4 server on the network.

10. Place the evidence collection priority from most volatile to least volatile as defined by the IETF guidelines.

11. Which two protocols are associated with the transport layer? (Choose two.)

- ICMP
- IP

- **UDP**
- PPP
- **TCP**

Explanation: TCP and UDP reside at the transport layer in both the OSI and TCP/IP models.

12. A network administrator is creating a network profile to generate a network baseline. What is included in the critical asset address space element?

- the time between the establishment of a data flow and its termination
- the TCP and UDP daemons and ports that are allowed to be open on the server
- **the IP addresses or the logical location of essential systems or data**
- the list of TCP or UDP processes that are available to accept data

Explanation: A network profile should include some important elements, such as the following:
Total throughput – the amount of data passing from a given source to a given destination in a given period of time
Session duratio n – the time between the establishment of a data flow and its termination
Ports used – a list of TCP or UDP processes that are available to accept data
Critical asset address space – the IP addresses or the logical location of essential systems or data

13. What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)

- **confidentiality**
- remediation level
- **integrity**
- attack vector
- exploit
- **availability**

Explanation:
The Common Vulnerability Scoring System (CVSS) is a vendor-neutral,

industry standard, open framework for weighing the risks of a vulnerability using a variety of metrics. CVSS uses three groups of metrics to assess vulnerability, the Base Metric Group, Temporal Metric Group, and Environmental Metric Group. The Base Metric Group has two classes of metrics (exploitability and impact). The impact metrics are rooted in the following areas: confidentiality, integrity, and availability.

14. What is a characteristic of DNS?

- **DNS servers can cache recent queries to reduce DNS query traffic.**
- All DNS servers must maintain mappings for the entire DNS structure.
- DNS servers are programmed to drop requests for name translations that are not within their zone.
- DNS relies on a hub-and-spoke topology with centralized servers.

Explanation: DNS uses a hierarchy for decentralized servers to perform name resolution. DNS servers only maintain records for their zone and can cache recent queries so that future queries do not produce excessive DNS traffic.

15. What are two differences between HTTP and HTTP/2? (Choose two.)

- **HTTP/2 uses a compressed header to reduce bandwidth requirements.**
- **HTTP/2 uses multiplexing to support multiple streams and enhance efficiency.**
- HTTP/2 uses different status codes than HTTP does to improve performance.
- HTTP/2 issues requests using a text format whereas HTTP uses binary commands.
- HTTP has a different header format than HTTP/2 has.

Explanation: The purpose of HTTP/2 is to improve HTTP performance by addressing the latency issues of HTTP. This is accomplished using features such as multiplexing, server push, binary code, and header compression.

16. Match the steps with the actions that are involved when an internal host with IP address 192.168.10.10 attempts to send a packet to an external server at the IP address 209.165.200.254 across a router R1

that is running dynamic NAT. (Not all options are used.)

step 1

step 2

step 3

step 4

step 5

R1 translates the IP address in the packets from 209.65.200.254 to 192.168.10.10.

R1 replaces the address 192.168.10.10 with a translated inside global address.

step 5

R1 checks the NAT configuration to determine if this packet should be translated.

step 2

R1 selects an available global address from the dynamic address pool.

step 4

The host sends packets that request a connection to the server at the address 209.165.200.254.

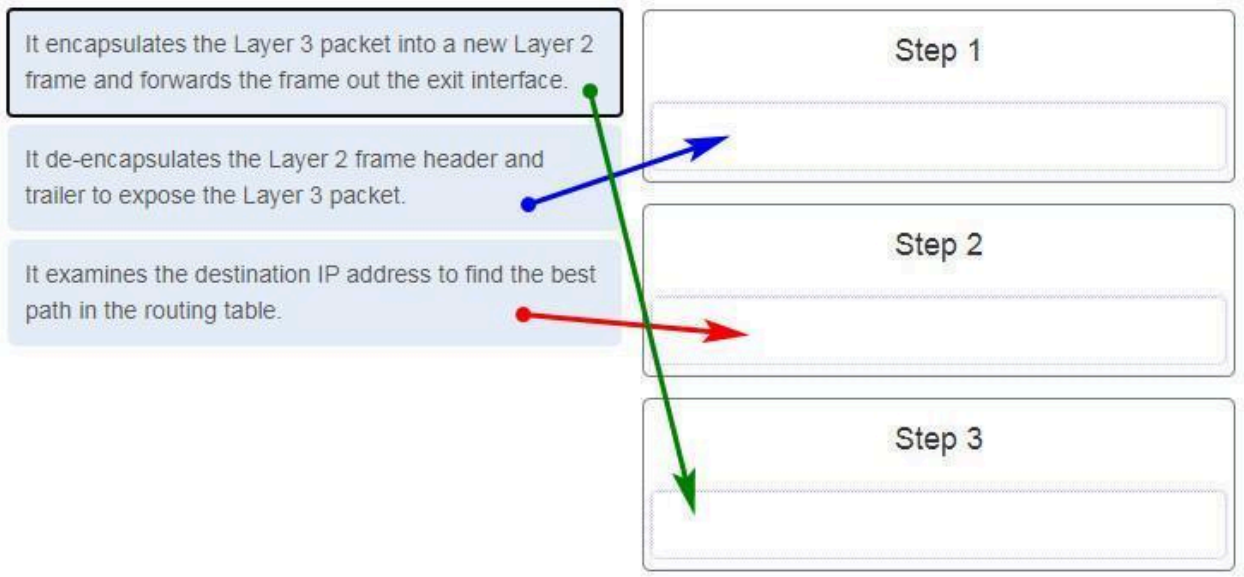
step 1

If there is no translation entry for this IP address, R1 determines that the source address 192.168.10.10 must be translated.

step 3

Explanation: The translation of the IP addresses from 209.65.200.254 to 192.168.10.10 will take place when the reply comes back from the server.

17. A router has received a packet destined for a network that is in the routing table. What steps does the router perform to send this packet on its way? Match the step to the task performed by the router.



18. What are two shared characteristics of the IDS and the IPS? (Choose two.)

- Both have minimal impact on network performance.
- **Both are deployed as sensors.**
- Both analyze copies of network traffic.
- **Both use signatures to detect malicious traffic.**
- Both rely on an additional network device to respond to malicious traffic.

Explanation: Both the IDS and the IPS are deployed as sensors and use signatures to detect malicious traffic. The IDS analyzes copies of network traffic, which results in minimal impact on network performance. The IDS also relies on an IPS to stop malicious traffic.

19. Which statement describes a typical security policy for a DMZ firewall configuration?

- **Traffic that originates from the DMZ interface is selectively permitted to the outside interface.**

- Return traffic from the inside that is associated with traffic originating from the outside is permitted to traverse from the inside interface to the outside interface.
- Return traffic from the outside that is associated with traffic originating from the inside is permitted to traverse from the outside interface to the DMZ interface.
- Traffic that originates from the inside interface is generally blocked entirely or very selectively permitted to the outside interface.
- Traffic that originates from the outside interface is permitted to traverse the firewall to the inside interface with few or no restrictions.

Explanation:
With a three interface firewall design that has internal, external, and DMZ connections, typical configurations include the following:
Traffic originating from DMZ destined for the internal network is normally blocked.
Traffic originating from the DMZ destined for external networks is typically permitted based on what services are being used in the DMZ.
Traffic originating from the internal network destined from the DMZ is normally inspected and allowed to return.
Traffic originating from external networks (the public network) is typically allowed in the DMZ only for specific services.

20. After complaints from users, a technician identifies that the college web server is running very slowly. A check of the server reveals that there are an unusually large number of TCP requests coming from multiple locations on the Internet. What is the source of the problem?

- The server is infected with a virus.
- **A DDoS attack is in progress.**
- There is insufficient bandwidth to connect to the server.
- There is a replay attack in progress.

Explanation: The source of the problem cannot be a virus because in this situation the server is passive and at the receiving end of the attack. A replay attack uses intercepted and recorded data in an attempt to gain access to an unauthorized server. This type of attack does not involve multiple computers. The issue is not the bandwidth available, but the number of TCP connections taking place. Receiving a

large number of connections from multiple locations is the main symptom of a distributed denial of service attack which use botnets or zombie computers.

21. Which two statements describe access attacks? (Choose two.)

- **Password attacks can be implemented by the use of brute-force attack methods, Trojan horses, or packet sniffers.**
- To detect listening services, port scanning attacks scan a range of TCP or UDP port numbers on a host.
- Port redirection attacks use a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.
- Trust exploitation attacks often involve the use of a laptop to act as a rogue access point to capture and copy all network traffic in a public location, such as a wireless hotspot.
- **Buffer overflow attacks write data beyond the allocated buffer memory to overwrite valid data or to exploit systems to execute malicious code.**

Explanation: An access attack tries to gain access to a resource using a hijacked account or other means. The five types of access attacks include the following:
password – a dictionary is used for repeated login attempts
trust exploitation – uses granted privileges to access unauthorized material
port redirection – uses a compromised internal host to pass traffic through a firewall
man-in-the-middle – an unauthorized device positioned between two legitimate devices in order to redirect or capture traffic
buffer overflow – too much data sent to a memory location that already contains data

22. Which two actions can be taken when configuring Windows Firewall? (Choose two.)

- Turn on port screening.
- **Manually open ports that are required for specific applications.**
- **Allow a different software firewall to control access.**
- Enable MAC address authentication.
- Perform a rollback.

Explanation: When a different software firewall is installed, Windows Firewall must be disabled through the Windows Firewall control panel. When Windows Firewall is enabled, specific ports can be enabled that are needed by specific applications.

23. Which statement describes the state of the administrator and guest accounts after a user installs Windows desktop version to a new computer?

- By default, the guest account is enabled but the administrator account is disabled.
- By default, both the administrator and guest accounts are enabled.
- **By default, both the administrator and guest accounts are disabled.**
- By default, the administrator account is enabled but the guest account is disabled.

Explanation: When a user installs Windows desktop version, two local user accounts are created automatically during the process, administrator and guest. Both accounts are disabled by default.

24. What is a purpose of entering the nslookup cisco.com command on a Windows PC?

- **to check if the DNS service is running**
- to connect to the Cisco server
- to test if the Cisco server is reachable
- to discover the transmission time needed to reach the Cisco server

Explanation: The `nslookup` command queries DNS servers to find out the IP address or addresses associated with the domain name cisco.com. A successful result indicates that the DNS configuration on the PC is functional, and also indicates the IP address for the domain name being displayed. The command does not try connect to the actual Cisco host directly.

25. How is the event ID assigned in Sguil?

- All events in the series of correlated events are assigned the same event ID.

- Only the first event in the series of correlated events is assigned a unique ID.
- All events in the series of correlated events are assigned the same event group ID.
- **Each event in the series of correlated events is assigned a unique ID.**

Explanation: In Sguil, each event receives a unique event ID, but only the first event ID in the series of correlated events is displayed in the RealTime tab.

26. Which two types of network traffic are from protocols that generate a lot of routine traffic? (Choose two.)

- **routing updates traffic**
- Windows security auditing alert traffic
- IPsec traffic
- **STP traffic**
- SSL traffic

Explanation: To reduce the huge amount of data collected so that cybersecurity analysts can focus on critical threats, some less important or less relevant data could be eliminated from the datasets. For example, routing network management traffic, such as routing updates and STP traffic, could be eliminated.

27. What are two elements that form the PRI value in a syslog message? (Choose two.)

- **facility**
- timestamp
- **severity**
- header
- hostname

Explanation: The PRI in a syslog message consists of two elements, the facility and severity of the message.

28. Which three pieces of information are found in session data? (Choose three.)

- default gateway IP address
- **source and destination port numbers**

- **Layer 4 transport protocol**
- source and destination MAC addresses
- user name
- **source and destination IP addresses**

Explanation: Session data includes identifying information such as source and destination IP addresses, source and destination port numbers, and the Layer 4 protocol in use. Session data does not include user name, source and destination MAC addresses, and a default gateway IP address.

29. What kind of ICMP message can be used by threat actors to perform network reconnaissance and scanning attacks?

- ICMP mask reply
- ICMP router discovery
- **ICMP unreachable**
- ICMP redirects

Explanation: Common ICMP messages of interest to threat actors include the these:
ICMP echo request and echo reply: used to perform host verification and DoS attacks
ICMP unreachable: used to perform network reconnaissance and scanning attacks
ICMP mask reply: used to map an internal IP network
ICMP redirects: used to lure a target host into sending all traffic through a compromised device and create a man-in-the-middle attack
ICMP router discovery: used to inject bogus route entries into the routing table of a target host

30. A flood of packets with invalid source IP addresses requests a connection on the network. The server busily tries to respond, resulting in valid requests being ignored. What type of attack has occurred?

- TCP session hijacking
- **TCP SYN flood**
- TCP reset
- UDP flood

Explanation: The TCP SYN Flood attack exploits the TCP three-way handshake. The threat actor continually sends TCP SYN session request packets with a randomly spoofed source IP address to an intended target. The target device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections and denies TCP services.

31. An attacker is redirecting traffic to a false default gateway in an attempt to intercept the data traffic of a switched network. What type of attack could achieve this?

- DNS tunneling
- TCP SYN flood
- **DHCP spoofing**
- ARP cache poisoning

Explanation: In DHCP spoofing attacks, a threat actor configures a fake DHCP server on the network to issue DHCP addresses to clients with the aim of forcing the clients to use a false or invalid default gateway. A man-in-the-middle attack can be created by setting the default gateway address to the IP address of the threat actor.

32. What is the most common goal of search engine optimization (SEO) poisoning?

- **to increase web traffic to malicious sites**
- to build a botnet of zombies
- to trick someone into installing malware or divulging personal information
- to overwhelm a network device with maliciously formed packets

Explanation: A malicious user could create a SEO so that a malicious website appears higher in search results. The malicious website commonly contains malware or is used to obtain information via social engineering techniques.

33. Users report that a database file on the main server cannot be accessed. A database administrator verifies the issue and notices that the database file is now encrypted. The organization receives a threatening email demanding payment for the decryption of the database file. What type of attack has the organization experienced?

- man-in-the-middle attack
- DoS attack
- **ransomware**
- Trojan horse

Explanation: A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

34. When dealing with a security threat and using the Cyber Kill Chain model, which two approaches can an organization use to help block potential exploitations on a system? (Choose two.)

- Collect email and web logs for forensic reconstruction.
- Conduct full malware analysis.
- **Train web developers for securing code.**
- Build detections for the behavior of known weaponizers.
- **Perform regular vulnerability scanning and penetration testing.**

Explanation: The most common exploit targets, once a weapon is delivered, are applications, operating system vulnerabilities, and user accounts. Among other measures, such as regular vulnerability scanning and penetration testing, training web developers in securing code can help block potential exploitations on systems.

35. How might corporate IT professionals deal with DNS-based cyber threats?

- Limit the number of simultaneously opened browsers or browser tabs.
- **Monitor DNS proxy server logs and look for unusual DNS queries.**
- Use IPS/IDS devices to scan internal corporate traffic.
- Limit the number of DNS queries permitted within the organization.

Explanation: DNS queries for randomly generated domain names or extremely long random-appearing DNS subdomains should be considered suspicious. Cyberanalysts could do the following for DNS-based attacks:
Analyze DNS logs.
Use a passive DNS service to block requests to suspected CnC and exploit domains.

36. How does using HTTPS complicate network security monitoring?

- **HTTPS adds complexity to captured packets.**
- HTTPS cannot protect visitors to a company-provided web site.
- Web browser traffic is directed to infected servers.
- HTTPS can be used to infiltrate DNS queries.

Explanation:
HTTPS adds extra overhead to the HTTP-formed packet. HTTPS encrypts using secure socket layer (SSL). Even though some devices can perform SSL decryption and inspection, this can present processing and privacy issues. HTTPS adds complexity to packet captures due to the additional message involved in establishing an encrypted data connection.

37. What is the responsibility of the human resources department when handling a security incident?

- Coordinate the incident response with other stakeholders and minimize the damage of the incident.
- Perform actions to minimize the effectiveness of the attack and preserve evidence.
- **Apply disciplinary measures if an incident is caused by an employee.**
- Review the incident policies, plans, and procedures for local or federal guideline violations.

Explanation: The human resources department may be called upon to perform disciplinary measures if an incident is caused by an employee.

38. How does a security information and event management system (SIEM) in a SOC help the personnel fight against security threats?

- by integrating all security devices and appliances in an organization
- by analyzing logging data in real time
- **by combining data from multiple technologies**
- by dynamically implementing firewall rules

Explanation: A security information and event management system (SIEM) combines data from multiple sources to help SOC personnel collect and filter data, detect and classify threats, analyze and

investigate threats, and manage resources to implement preventive measures.

39. At which OSI layer is a source IP address added to a PDU during the encapsulation process?

- **network layer**
- transport layer
- data link layer
- application layer

40. What is the purpose of CSMA/CA?

- to prevent loops
- to isolate traffic
- to filter traffic
- **to prevent collisions**

Explanation: CSMA/CA stands for carrier sense multiple access with collision avoidance. It is a mechanism used in wireless networks to prevent packet collisions from occurring.

41. Why is DHCP preferred for use on large networks?

- Hosts on large networks require more IP addressing configuration settings than hosts on small networks.
- It prevents sharing of files that are copyrighted.
- **It is a more efficient way to manage IP addresses than static address assignment.**
- Large networks send more requests for domain to IP address resolution than do smaller networks.
- DHCP uses a reliable transport layer protocol.

Explanation: Static IP address assignment requires personnel to configure each network host with addresses manually. Large networks can change frequently and have many more hosts to configure than do small networks. DHCP provides a much more efficient means of configuring and managing IP addresses on large networks than does static address assignment.

42. Which NIST incident response life cycle phase includes continuous monitoring by the CSIRT to quickly identify and validate an incident?

- postincident activities
- **detection and analysis**
- containment, eradication, and recovery
- preparation

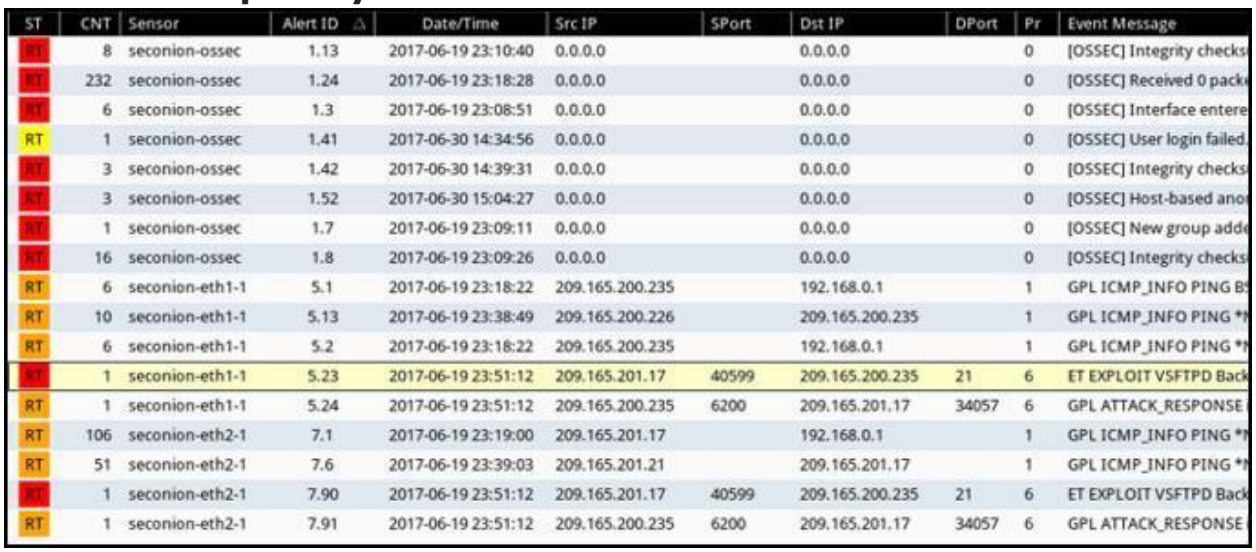
Explanation: It is in the detection and analysis phase of the NIST incident response life cycle that the CSIRT identifies and validates incidents through continuous monitoring. The NIST defines four stages of the incident response life cycle.

43. What are two problems that can be caused by a large number of ARP request and reply messages? (Choose two.)

- **All ARP request messages must be processed by all nodes on the local network.**
- A large number of ARP request and reply messages may slow down the switching process, leading the switch to make many changes in its MAC table.
- The network may become overloaded because ARP reply messages have a very large payload due to the 48-bit MAC address and 32-bit IP address that they contain.
- **The ARP request is sent as a broadcast, and will flood the entire subnet.**
- Switches become overloaded because they concentrate all the traffic from the attached subnets.

Explanation: ARP requests are sent as broadcasts:
(1) All nodes will receive them, and they will be processed by software, interrupting the CPU.
(2) The switch forwards (floods) Layer 2 broadcasts to all ports.
A switch does not change its MAC table based on ARP request or reply messages. The switch populates the MAC table using the source MAC address of all frames. The ARP payload is very small and does not overload the switch.

44. Refer to the exhibit. Which field in the Sguil application window indicates the priority of an event or set of correlated events?

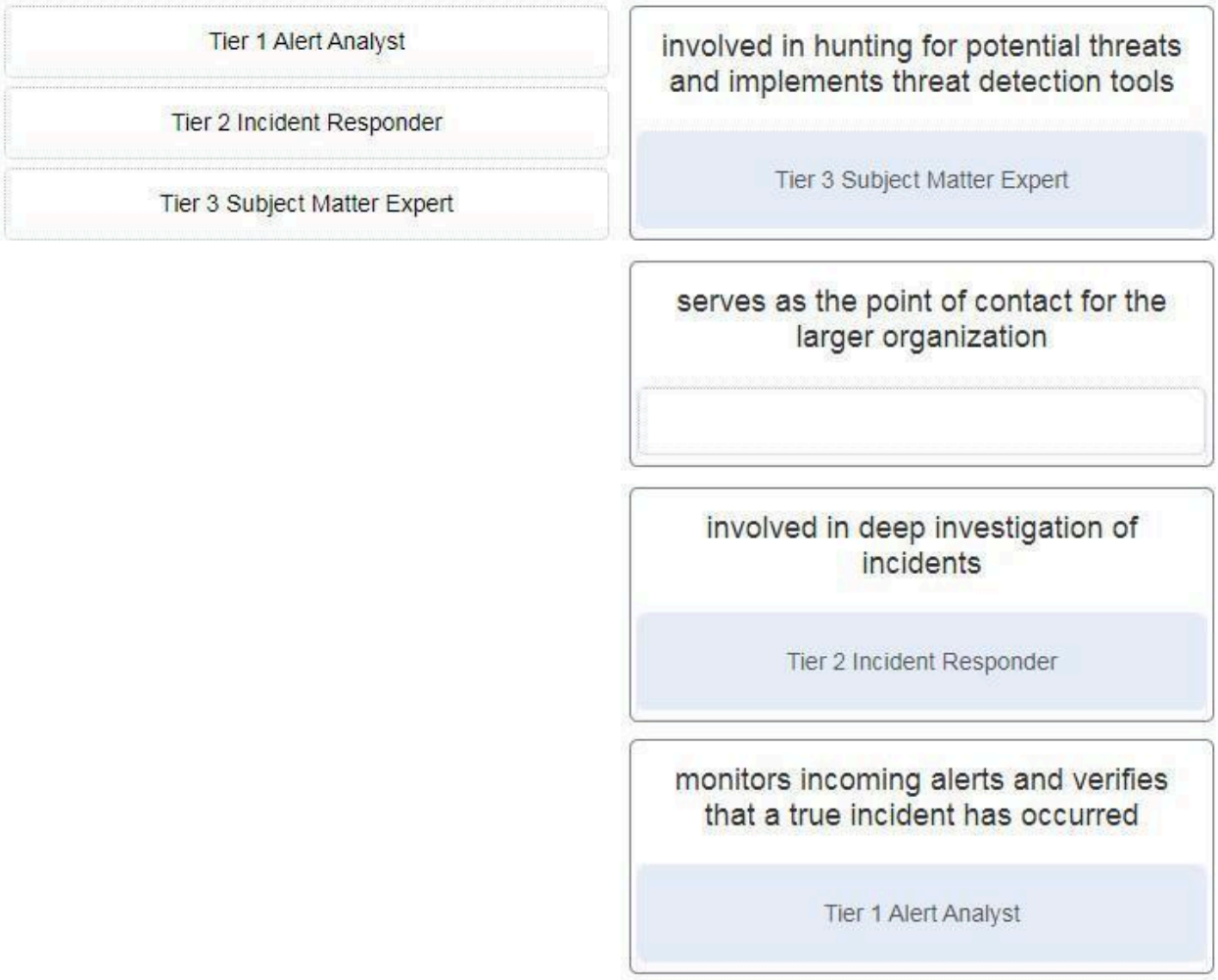


ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	8	seconion-ossec	1.13	2017-06-19 23:10:40	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks
RT	232	seconion-ossec	1.24	2017-06-19 23:18:28	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packe
RT	6	seconion-ossec	1.3	2017-06-19 23:08:51	0.0.0.0		0.0.0.0		0	[OSSEC] Interface entere
RT	1	seconion-ossec	1.41	2017-06-30 14:34:56	0.0.0.0		0.0.0.0		0	[OSSEC] User login failed.
RT	3	seconion-ossec	1.42	2017-06-30 14:39:31	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks
RT	3	seconion-ossec	1.52	2017-06-30 15:04:27	0.0.0.0		0.0.0.0		0	[OSSEC] Host-based ano
RT	1	seconion-ossec	1.7	2017-06-19 23:09:11	0.0.0.0		0.0.0.0		0	[OSSEC] New group adde
RT	16	seconion-ossec	1.8	2017-06-19 23:09:26	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks
RT	6	seconion-eth1-1	5.1	2017-06-19 23:18:22	209.165.200.235		192.168.0.1		1	GPL ICMP_INFO PING B
RT	10	seconion-eth1-1	5.13	2017-06-19 23:38:49	209.165.200.226		209.165.200.235		1	GPL ICMP_INFO PING *N
RT	6	seconion-eth1-1	5.2	2017-06-19 23:18:22	209.165.200.235		192.168.0.1		1	GPL ICMP_INFO PING *N
RT	1	seconion-eth1-1	5.23	2017-06-19 23:51:12	209.165.201.17	40599	209.165.200.235	21	6	ET EXPLOIT VSFTPD Back
RT	1	seconion-eth1-1	5.24	2017-06-19 23:51:12	209.165.200.235	6200	209.165.201.17	34057	6	GPL ATTACK_RESPONSE
RT	106	seconion-eth2-1	7.1	2017-06-19 23:19:00	209.165.201.17		192.168.0.1		1	GPL ICMP_INFO PING *N
RT	51	seconion-eth2-1	7.6	2017-06-19 23:39:03	209.165.201.21		209.165.201.17		1	GPL ICMP_INFO PING *N
RT	1	seconion-eth2-1	7.90	2017-06-19 23:51:12	209.165.201.17	40599	209.165.200.235	21	6	ET EXPLOIT VSFTPD Back
RT	1	seconion-eth2-1	7.91	2017-06-19 23:51:12	209.165.200.235	6200	209.165.201.17	34057	6	GPL ATTACK_RESPONSE

- **ST**
- AlertID
- Pr
- CNT

Explanation: The Sguil application window has several fields available that give information about an event. The ST field gives the status of an event that includes a color-coded priority from light yellow to red to indicate four levels of priority.

45. Match the job titles to SOC personnel positions. (Not all options are used.)



- Tier 1 Alert Analyst —› monitors incoming alerts & verifies that a true incident has occured
- Tier 2 Incident Responder –› involved in deep investigation of incident
- Tier 3 Subject Matter Expert –› involved in hunting for potential threads & implements thread detection tools
- (not use) –› serve as the point of contact for the large organitazion

46. If the default gateway is configured incorrectly on the host, what is the impact on communications?

- The host is unable to communicate on the local network.

- **The host can communicate with other hosts on the local network, but is unable to communicate with hosts on remote networks.**
- The host can communicate with other hosts on remote networks, but is unable to communicate with hosts on the local network.
- There is no impact on communications.

Explanation: A default gateway is only required to communicate with devices onanother network. The absence of a default gateway does not affect connectivity between devices on the same local network

47. When a connectionless protocol is in use at a lower layer of the OSI model, how is missing data detected and retransmitted if necessary?

- Connectionless acknowledgements are used to request retransmission.
- **Upper-layer connection-oriented protocols keep track of the data received and can request retransmission from the upper-level protocols on the sending host.**
- Network layer IP protocols manage the communication sessions if connection-oriented transport services are not available.
- The best-effort delivery process guarantees that all packets that are sent are received.

Explanation: When connectionless protocols are in use at a lower layer of the OSI model, upper-level protocols may need to work together on the sending and receiving hosts to account for and retransmit lost data. In some cases, this is not necessary, because for some applications a certain amount of data loss is tolerable.

48. What is the prefix length notation for the subnet mask 255.255.255.224?

- /25
- /26
- ***/27***
- /28

Explanation: The binary format for 255.255.255.224 is 11111111.11111111.11111111.11100000. The prefix length is the number of consecutive 1s in the subnet mask. Therefore, the prefix length is /27.

49. Which network monitoring tool saves captured network frames in PCAP files?

- NetFlow
- **Wireshark**
- SNMP
- SIEM

Explanation: Wireshark is a network protocol analyzer used to capture network traffic. The traffic captured by Wireshark is saved in PCAP files and includes interface information and timestamps.

50. What is the TCP mechanism used in congestion avoidance?

- three-way handshake
- socket pair
- two-way handshake
- **sliding window**

Explanation: TCP uses windows to attempt to manage the rate of transmission to the maximum flow that the network and destination device can support while minimizing loss and retransmissions. When overwhelmed with data, the destination can send a request to reduce the of the window. This congestion avoidance is called sliding windows.

51. What is the Internet?

- It is a network based on Ethernet technology.
- It provides network access for mobile devices.
- **It provides connections through interconnected global networks.**
- It is a private network for an organization with LAN and WAN connections.

Explanation: The Internet provides global connections that enable networked devices (workstations and mobile devices) with different network technologies, such as Ethernet, DSL/cable, and serial connections, to communicate. A private network for an organization with LAN and WAN connections is an intranet.

52. Which protocol is used by the traceroute command to send and receive echo-requests and echo-replies?

- SNMP
- **ICMP**
- Telnet
- TCP

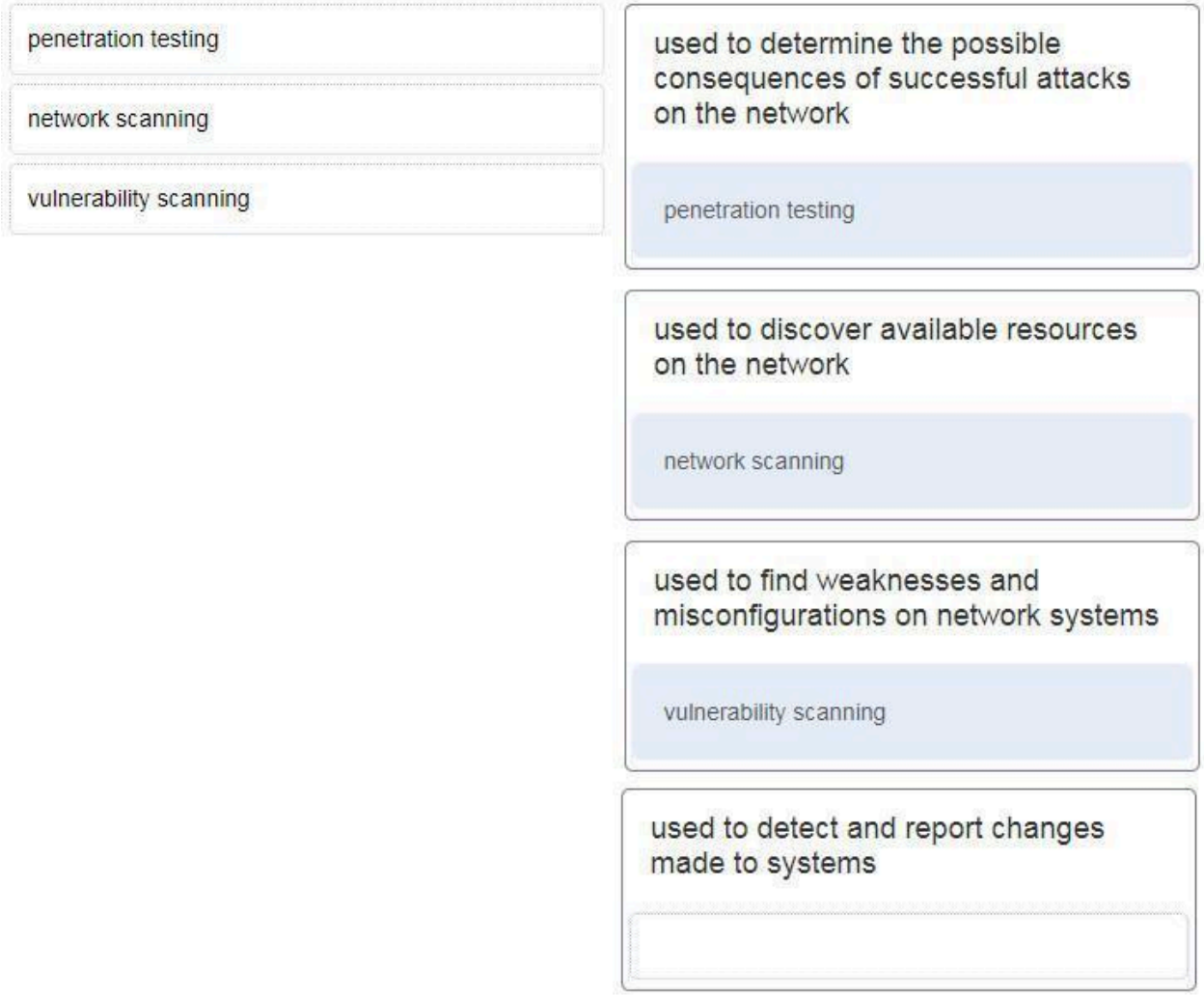
Explanation: Traceroute uses the ICMP (Internet Control Message Protocol) to send and receive echo-request and echo-reply messages.

53. What are two ICMPv6 messages that are not present in ICMP for IPv4? (Choose two.)

- **Neighbor Solicitation**
- Destination Unreachable
- Host Confirmation
- Time Exceeded
- **Router Advertisement**
- Route Redirection

Explanation: ICMPv6 includes four new message types: Router Advertisement, Neighbor Advertisement, Router Solicitation, and Neighbor Solicitation.

54. Match the network security testing technique with how it is used to test network security. (Not all options are used.)



55. What are two monitoring tools that capture network traffic and forward it to network monitoring devices? (Choose two.)

- **SPAN**
- **network tap**
- SNMP
- SIEM
- Wireshark

Explanation: A network tap is used to capture traffic for monitoring the network. The tap is typically a passive splitting device implemented inline on the network and forwards all traffic including physical layer errors to an analysis device. SPAN is a port mirroring technology

supported on Cisco switches that enables the switch to copy frames and forward them to an analysis device.

56. Which network monitoring tool is in the category of network protocol analyzers?

- SNMP
- SPAN
- **Wireshark**
- SIEM

Explanation: Wireshark is a network protocol analyzer used to capture network traffic. The traffic captured by Wireshark is saved in PCAP files and includes interface information and timestamps.

57. Based on the command output shown, which file permission or permissions have been assigned to the other user group for the data.txt file?

```
ls -l data.txt
-rwxrw-r-- sales staff 1028 May 28 15:50 data.txt
```

- full access
- read, write
- **read**
- read, write, execute

Explanation: The file permissions are always displayed in the user, group and other order. In the example displayed, the file has the following permissions:
The dash (–) means that this is a file. For directories, the first dash would be replaced with a “d”.
The first set of characters is for user permission (rwx). The user, sales, who owns the file can read, write and execute the file.
The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.
The third set of characters is for any other user or group permissions (r–). Any other user or group on the computer can only read the file.

58. What are three benefits of using symbolic links over hard links in Linux? (Choose three.)

- **They can link to a directory.**
- They can be compressed.
- Symbolic links can be exported.
- They can be encrypted.
- **They can link to a file in a different file system.**
- **They can show the location of the original file.**

Explanation: In Linux, a hard link is another file that points to the same location as the original file. A soft link (also called a symbolic link or a symlink) is a link to another file system name. Hard links are limited to the file system in which they are created and they cannot link to a directory; soft links are not limited to the same file system and they can link to a directory. To see the location of the original file for a symbolic link use the ls –l command.

59. What two kinds of personal information can be sold on the dark web by cybercriminals? (Choose two.)

- city of residence
- **Facebook photos**
- name of a bank
- name of a pet
- **street address**

Explanation: Personally identifiable information (PII) is any information that can be used to positively identify an individual. Examples of PII include the following:
Name
Social security number
Birthdate
Credit card numbers
Bank account numbers
Facebook information
Address information (street, email, phone numbers).

60. What three services are offered by FireEye? (Choose three.)

- **blocks attacks across the web**
- creates firewall rules dynamically
- **identifies and stops latent malware on files**
- subjects all traffic to deep packet inspection analysis
- deploys incident detection rule sets to network security tools

- **identifies and stops email threat vectors**

Explanation: FireEye is a security company that uses a three-pronged approach combining security intelligence, security expertise, and technology. FireEye offers SIEM and SOAR with the Helix Security Platform, which use behavioral analysis and advanced threat detection.

61. After containment, what is the first step of eradicating an attack?

- Change all passwords.
- Patch all vulnerabilities.
- Hold meetings on lessons learned.
- **Identify all hosts that need remediation.**

Explanation: Once an attack is contained, the next step is to identify all hosts that will need remediation so that the effects of the attack can be eliminated.

62. Which activity is typically performed by a threat actor in the installation phase of the Cyber Kill Chain?

- **Install a web shell on the target web server for persistent access.**
- Harvest email addresses of user accounts.
- Open a two-way communication channel to the CnC infrastructure.
- Obtain an automated tool to deliver the malware payload.

Explanation: In the installation phase of the Cyber Kill Chain, the threat actor establishes a back door into the system to allow for continued access to the target.

63. A network security specialist is tasked to implement a security measure that monitors the status of critical files in the data center and sends an immediate alert if any file is modified. Which aspect of secure communications is addressed by this security measure?

- origin authentication
- **data integrity**
- nonrepudiation
- data confidentiality

Explanation: Secure communications consists of four elements:
Data confidentiality – guarantees that only authorized users can read

the message
Data integrity – guarantees that the message was not altered
Origin authentication – guarantees that the message is not a forgery and does actually come from whom it states
Data nonrepudiation – guarantees that the sender cannot repudiate, or refute, the validity of a message sent

64. A network administrator is configuring an AAA server to manage TACACS+ authentication. What are two attributes of TACACS+ authentication? (Choose two.)

- TCP port 40
- **encryption for all communication**
- single process for authentication and authorization
- UDP port 1645
- encryption for only the password of a user
- **separate processes for authentication and authorization**

Explanation: TACACS+ authentication includes the following attributes:
Separates authentication and authorization processes
Encrypts all communication, not just passwords
Utilizes TCP port 49

65. In an attempt to prevent network attacks, cyber analysts share unique identifiable attributes of known attacks with colleagues. What three types of attributes or indicators of compromise are helpful to share? (Choose three.)

- **IP addresses of attack servers**
- **changes made to end system software**
- netbios names of compromised firewalls
- **features of malware files**
- BIOS of attacking systems
- system ID of compromised systems

Explanation: Many network attacks can be prevented by sharing information about indicators of compromise (IOC). Each attack has unique identifiable attributes. Indicators of compromise are the evidence that an attack has occurred. IOCs can be identifying features of malware files, IP addresses of servers that are used in the attack, filenames, and characteristic changes made to end system software.

66. Which two types of messages are used in place of ARP for address resolution in IPv6? (Choose two.)

- anycast
- broadcast
- **neighbor solicitation**
- echo reply
- echo request
- **neighbor advertisement**

Explanation: IPv6 does not use ARP. Instead, ICMPv6 neighbor discovery is used by sending neighbor solicitation and neighbor advertisement messages.

67. What is indicated by a true negative security alert classification?

- An alert is verified to be an actual security incident.
- An alert is incorrectly issued and does not indicate an actual security incident.
- **Normal traffic is correctly ignored and erroneous alerts are not being issued.**
- Exploits are not being detected by the security systems that are in place.

Explanation: True negative classifications are desirable because they indicate that normal traffic is correctly not being identified as malicious traffic by security measures.

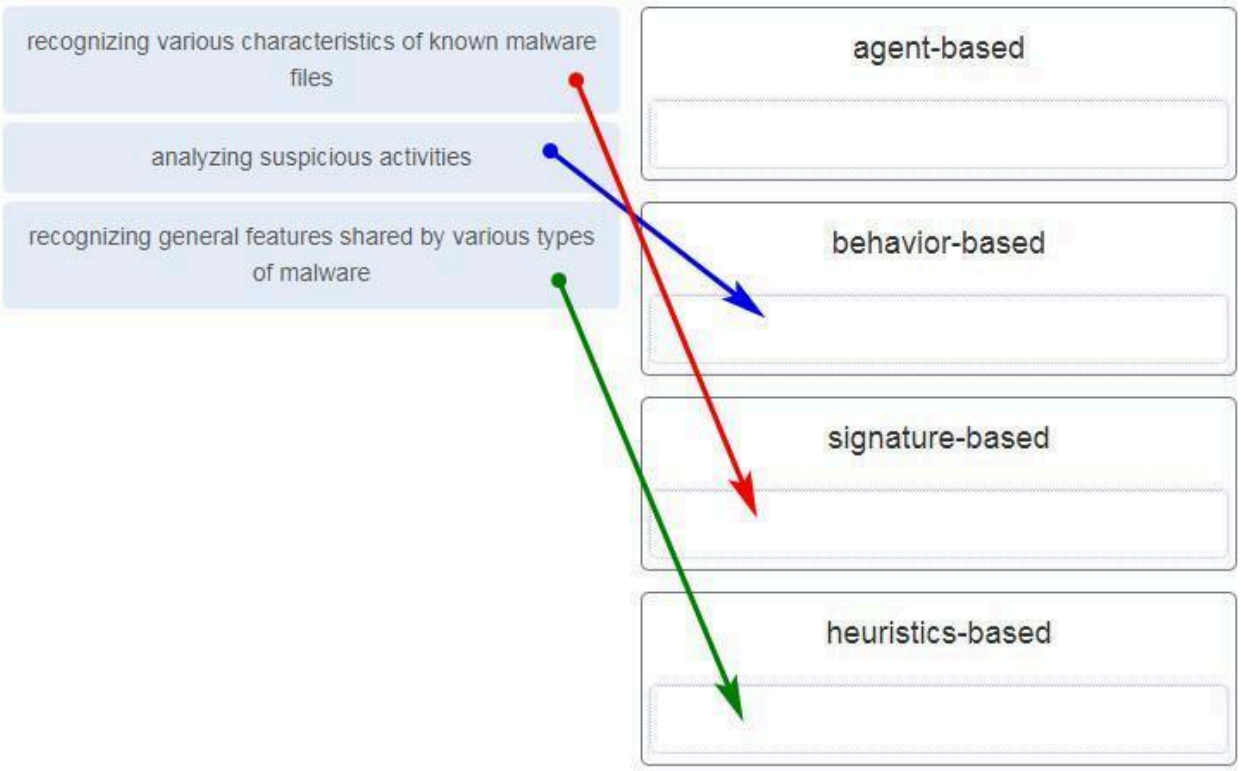
68. Which statement describes the anomaly-based intrusion detection approach?

- It compares the antivirus definition file to a cloud based repository for latest updates.
- **It compares the behavior of a host to an established baseline to identify potential intrusions.**
- It compares the signatures of incoming traffic to a known intrusion database.
- It compares the operations of a host against a well-defined security policy.

Explanation: With an anomaly-based intrusion detection approach, a baseline of host behaviors is established first. The host behavior is

checked against the baseline to detect significant deviations, which might indicate potential intrusions.

69. Match the description to the antimalware approach. (Not all options are used.)



Explanation: Antimalware programs may detect viruses using three different approaches:

- **signature-based** – by recognizing various characteristics of known malware files
- **heuristics-based** – by recognizing general features shared by various types of malware
- **behavior-based** – through analysis of suspicious activities

CyberOps Associate (Version 1.0) – CyberOps Associate 1.0 Final Exam Answers

1. The definition of computer security incidents and related terms element is in which part of the incident response plan?

- **policy**
- plan

- procedure

2. The strategy and goals element is in which part of the incident response plan?

- **plan**
- procedure
- policy

3. The organizational structure and definition of roles, responsibilities, and levels of authority element is in which part of the incident response plan?

- **policy**
- plan
- procedure

4. The prioritization and severity ratings of incidents element is in which part of the incident response plan?

- **policy**
- plan
- procedure

5. Which two `net` commands are associated with network resource sharing? (Choose two.)

- net start
- net accounts
- net share
- net use
- net stop

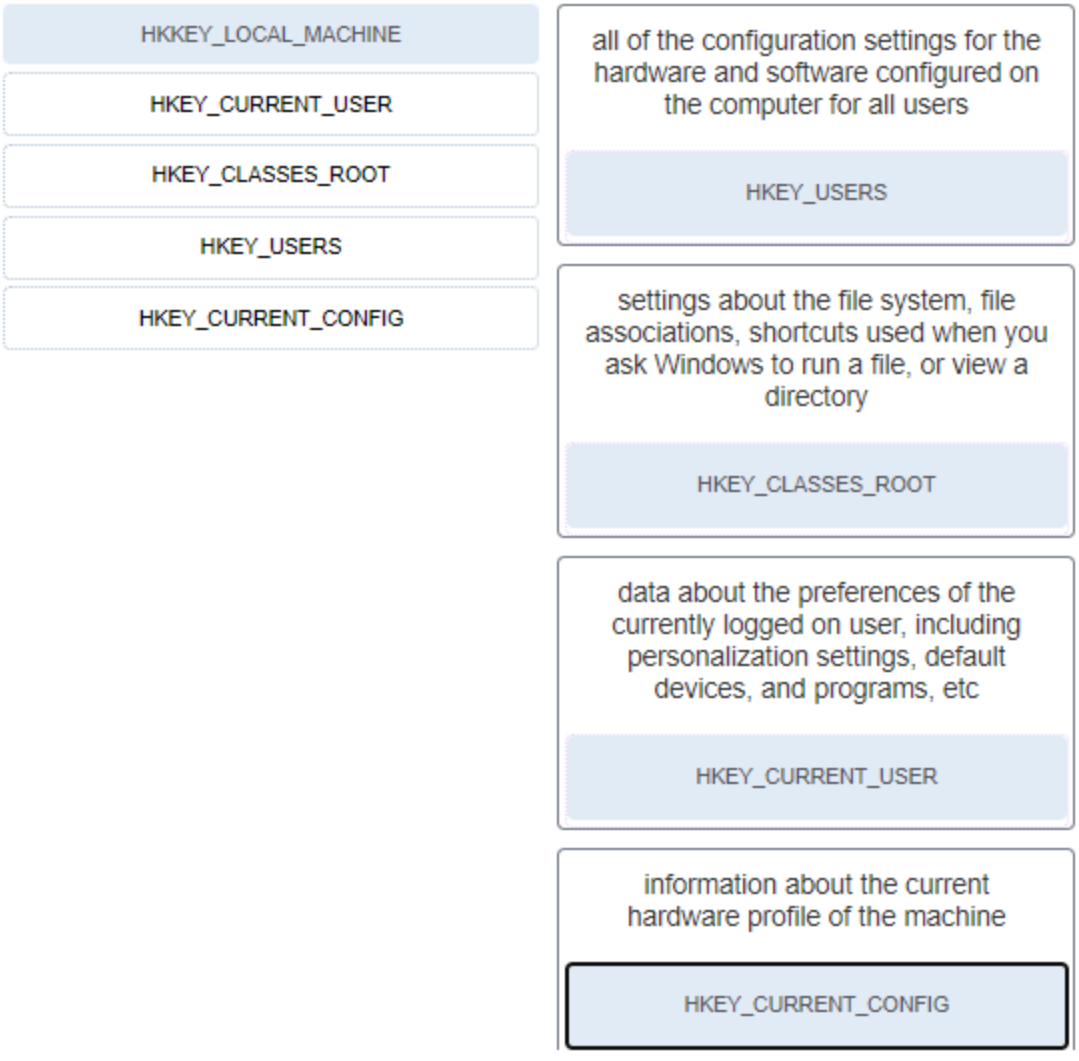
Explanation:

The `net` command is a very important command. Some common `net` commands include these:

- `net accounts` – sets password and logon requirements for users
- `net session` – lists or disconnects sessions between a computer and other computers on the network
- `net share` – creates, removes, or manages shared resources

- `net start` – starts a network service or lists running network services
- `net stop` – stops a network service
- `net use` – connects, disconnects, and displays information about shared network resources
- `net view` – shows a list of computers and network devices on the network

6. Match the Windows 10 Registry key with its description. (Not all options are used)



7. Which PDU format is used when bits are received from the network medium by the NIC of a host?

- segment

- file
- packet
- frame

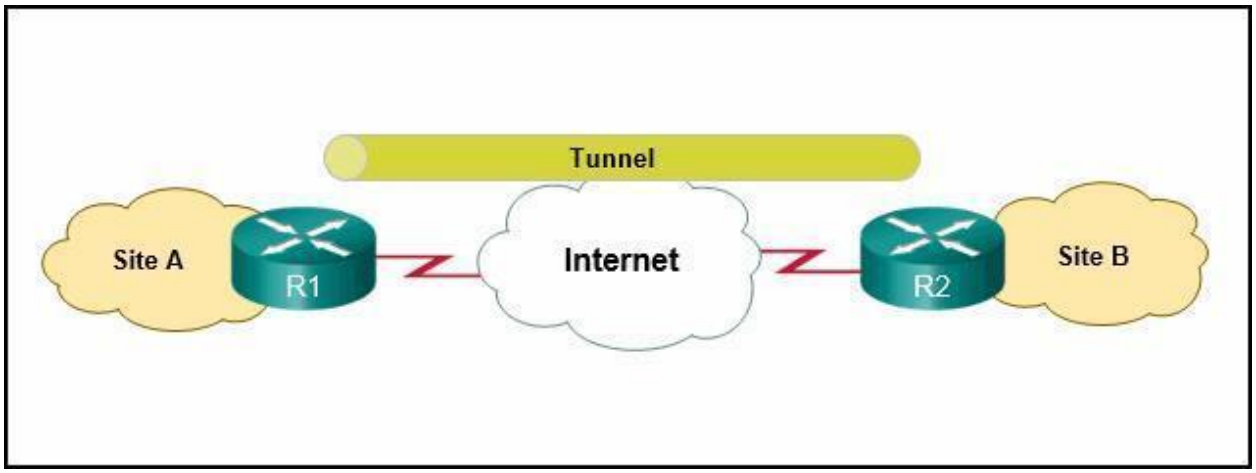
Explanation: When received at the physical layer of a host, the bits are formatted into a frame at the data link layer. A packet is the PDU at the network layer. A segment is the PDU at the transport layer. A file is a data structure that may be used at the application layer.

8. A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?

- when the router receives an ICMP Time Exceeded message
- when the values of both the Echo Request and Echo Reply messages reach zero
- when the RTT value reaches zero
- when the value in the TTL field reaches zero
- when the host responds with an ICMP Echo Reply message

Explanation: When a router receives a traceroute packet, the value in the TTL field is decremented by 1. When the value in the field reaches zero, the receiving router will not forward the packet, and will send an ICMP Time Exceeded message back to the source.

9. Refer to the exhibit. What solution can provide a VPN between site A and site B to support encapsulation of any Layer 3 protocol between the internal networks at each site?



- an IPsec tunnel

- Cisco SSL VPN
- a GRE tunnel
- a remote access tunnel

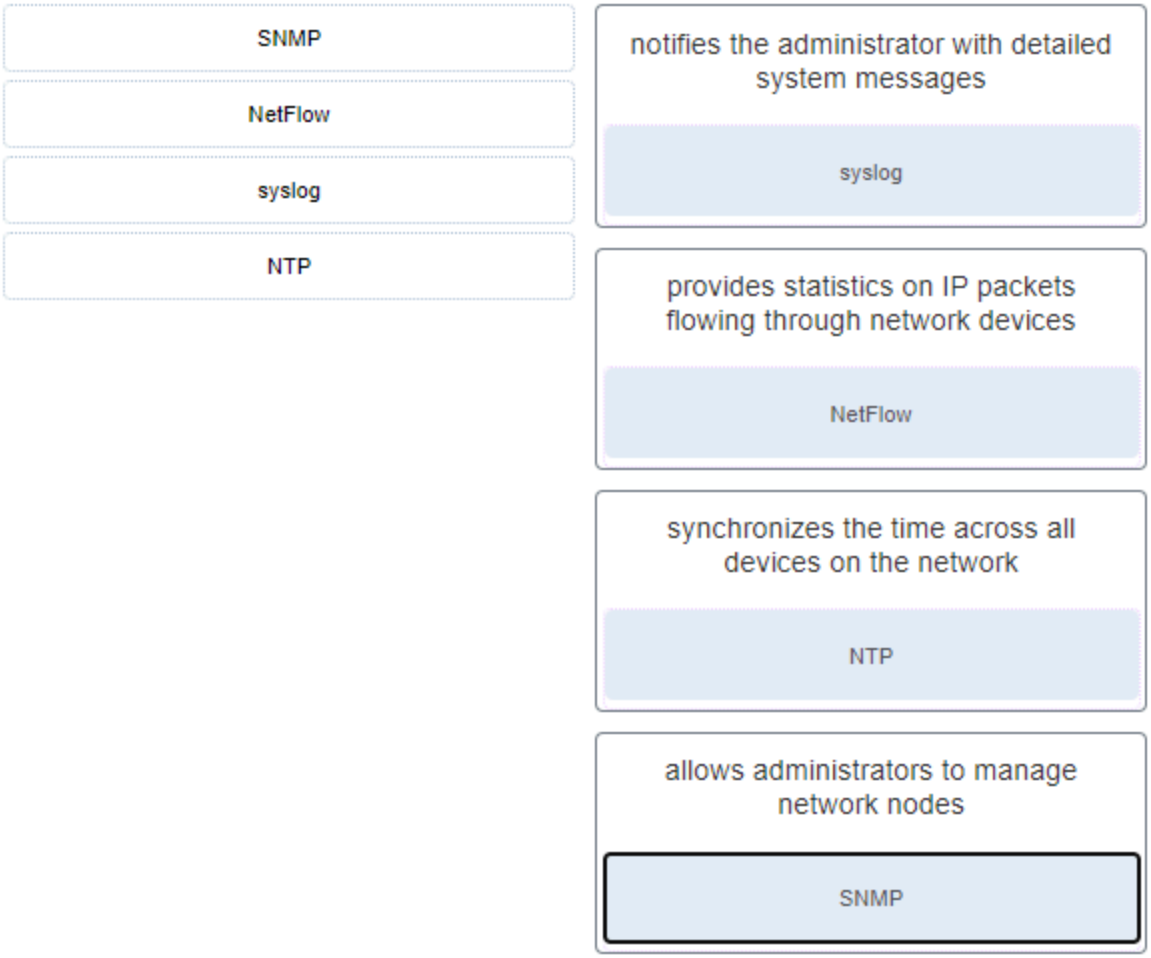
Explanation: A Generic Routing Encapsulation (GRE) tunnel is a non-secure, site-to-site VPN tunneling solution that is capable of encapsulating any Layer 3 protocol between multiple sites across over an IP internetwork.

10. For what purpose would a network administrator use the Nmap tool?

- protection of the private IP addresses of internal hosts
- identification of specific network anomalies
- collection and analysis of security alerts and logs
- detection and identification of open ports

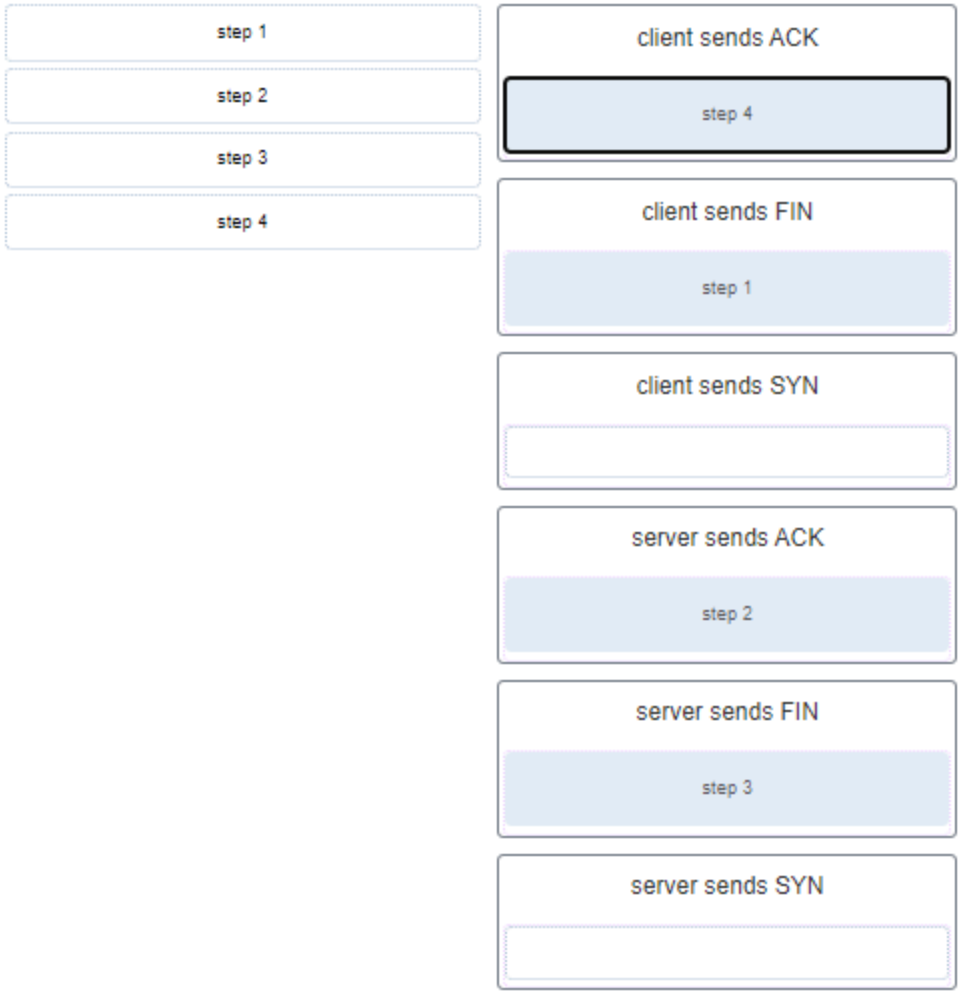
11. Match the network service with the description.

Match the network service with the description.

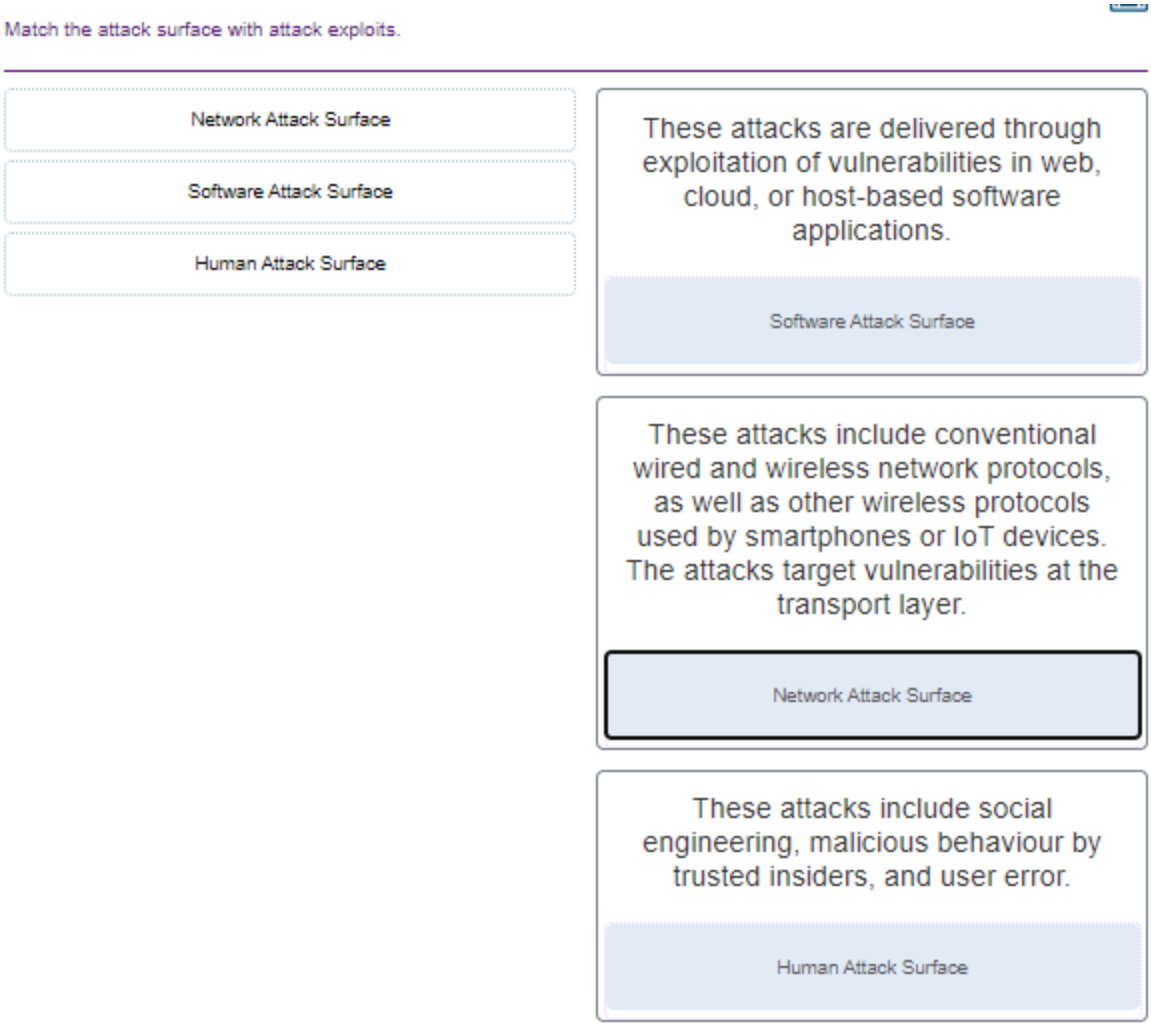


12. A client application needs to terminate a TCP communication session with a server. Place the termination process steps in the order that they will occur. (Nat all options are used.)

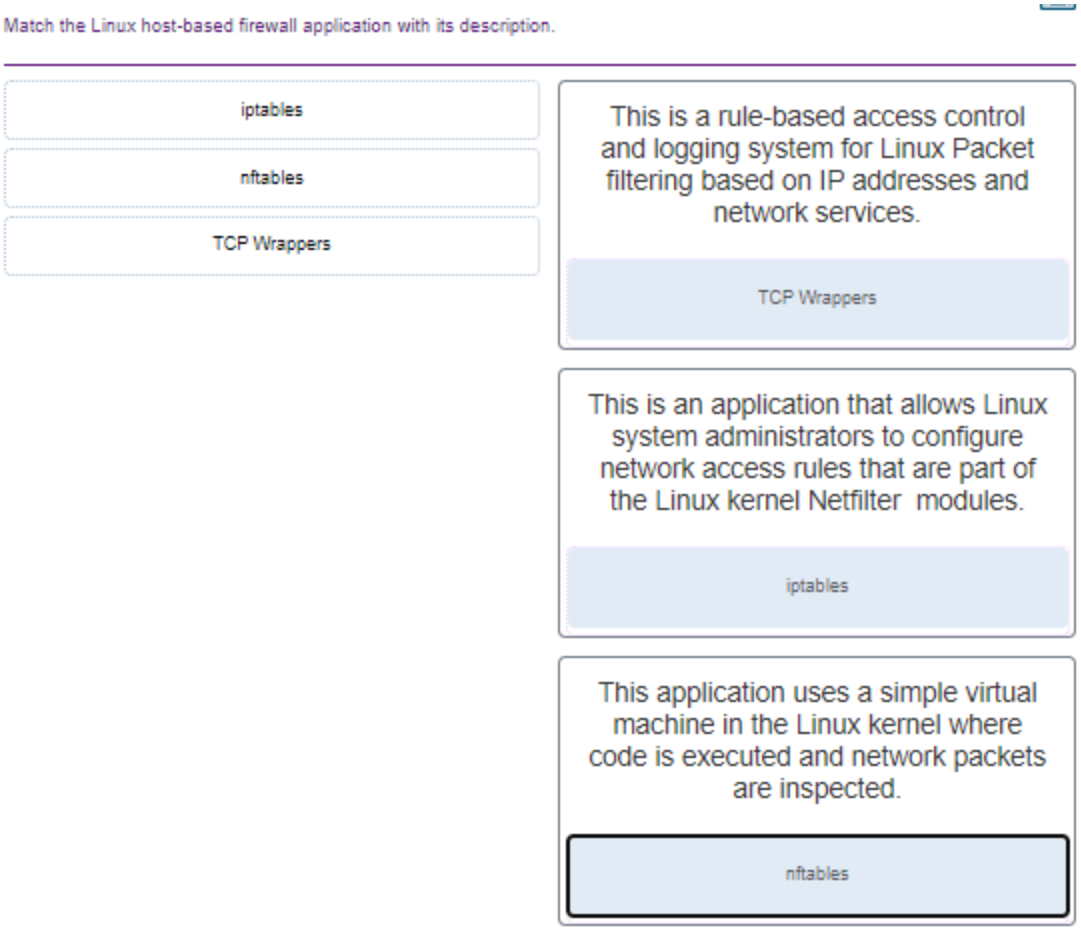
A client application needs to terminate a TCP communication session with a server. Place the termination process steps in the order that they will occur. (Not all options are used.)



13. Match the attack surface with attack exploits.



14. Match the Linux host-based firewall application with its description.

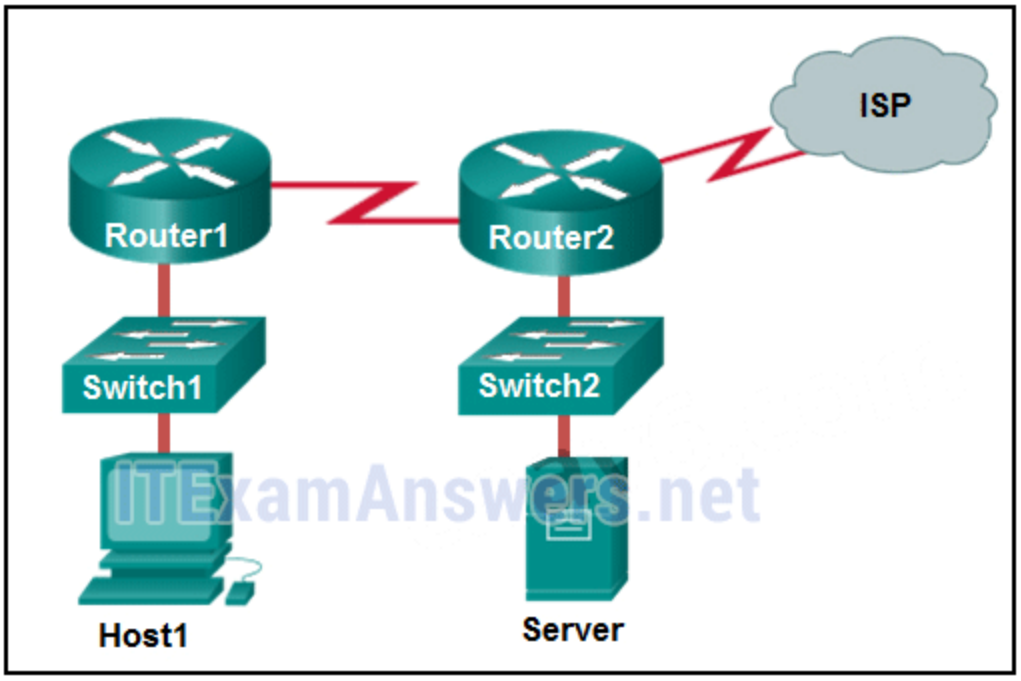


15. What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?

- **DHCP starvation**
- IP address spoofing
- DHCP spoofing
- CAM table attack

Explanation: DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages in order to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

16. Refer to the exhibit. If Host1 were to transfer a file to the server, what layers of the TCP/IP model would be used?



- only application and Internet layers
- **application, transport, Internet, and network access layers**
- only Internet and network access layers
- only application, transport, network, data link, and physical layers
- only application, Internet, and network access layers
- application, session, transport, network, data link, and physical layers

Explanation: The TCP/IP model contains the application, transport, internet, and network access layers. A file transfer uses the FTP application layer protocol. The data would move from the application layer through all of the layers of the model and across the network to the file server.

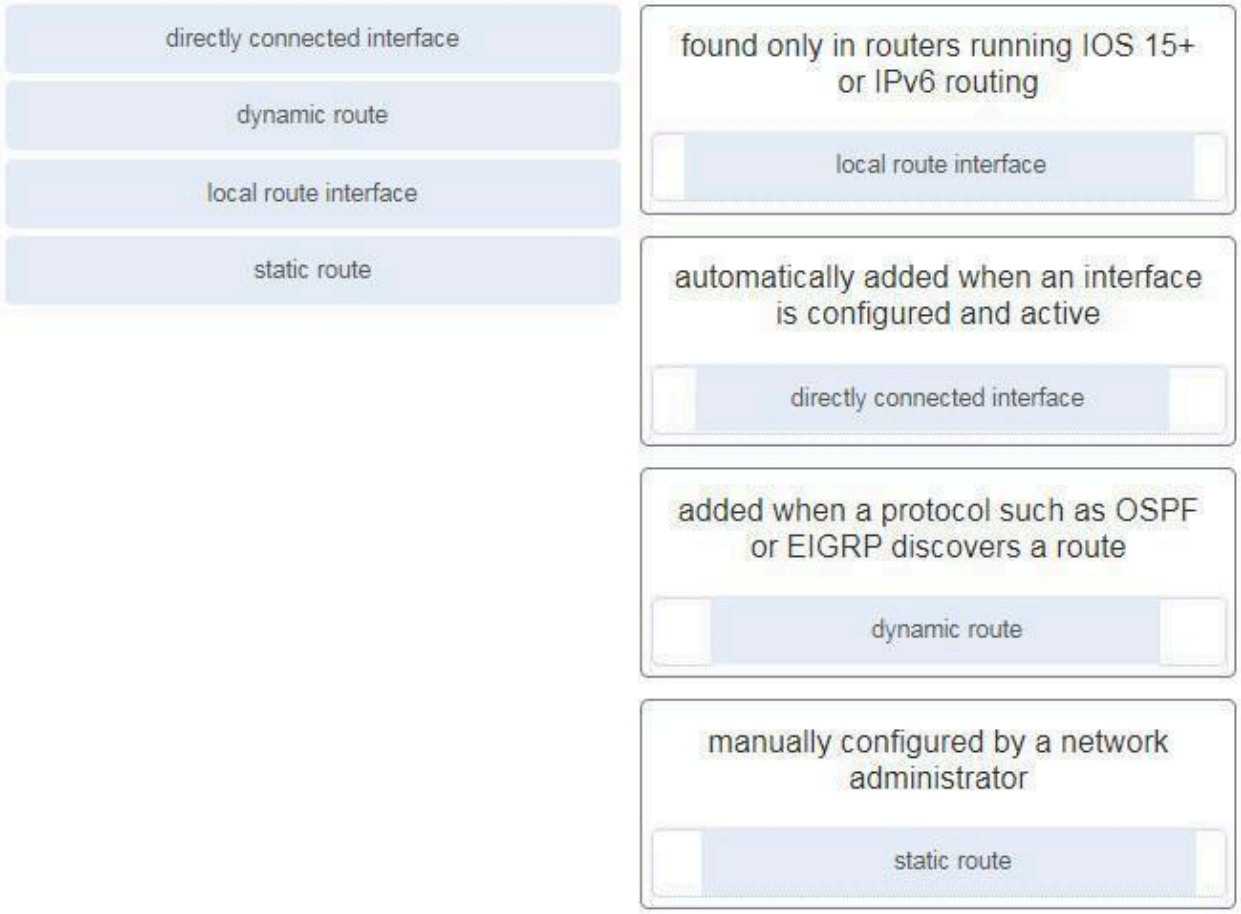
17. A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?

- automation

- authentication
- **authorization**
- accounting

Explanation: After a user is successfully authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform.

18. Match the destination network routing table entry type with a defintion.



19. A person coming to a cafe for the first time wants to gain wireless access to the Internet using a laptop. What is the first step the wireless client will do in order to communicate over the network using a wireless management frame?

- associate with the AP
- authenticate to the AP

- **discover the AP**
- agree with the AP on the payload

Explanation: In order for wireless devices to communicate on a wireless network, management frames are used to complete a three-stage process:

Discover the AP
Authenticate with the AP
Associate with the AP

20. A device has been assigned the IPv6 address of 2001:0db8:cafe:4500:1000:00d8:0058:00ab/64. Which is the network identifier of the device?

- 2001:0db8:cafe:4500:1000
- 2001:0db8:cafe:4500:1000:00d8:0058:00ab
- 1000:00d8:0058:00ab
- **2001:0db8:cafe:4500**
- 2001

Explanation: The address has a prefix length of /64. Thus the first 64 bits represent the network portion, whereas the last 64 bits represent the host portion of the IPv6 address.

21. An administrator wants to create four subnetworks from the network address 192.168.1.0/24. What is the network address and subnet mask of the second useable subnet?

subnetwork 192.168.1.64
subnet mask 255.255.255.192

subnetwork 192.168.1.64
subnet mask 255.255.255.240

subnetwork 192.168.1.32
subnet mask 255.255.255.240

subnetwork 192.168.1.128
subnet mask 255.255.255.192

subnetwork 192.168.1.8
subnet mask 255.255.255.224

22. What term describes a set of software tools designed to increase the privileges of a user or to grant access to the user to portions of the operating system that should not normally be allowed?

- compiler
- **rootkit**
- package manager
- penetration testing

Explanation: A rootkit is used by an attacker to secure a backdoor to a compromised computer, grant access to portions of the operating system normally not permitted, or increase the privileges of a user.

23. The IT security personnel of an organization notice that the web server deployed in the DMZ is frequently targeted by threat actors. The decision is made to implement a patch management system to manage the server. Which risk management strategy method is being used to respond to the identified risk?

- risk sharing
- risk avoidance
- **risk reduction**
- risk retention

Explanation: There are four potential strategies for responding to risks that have been identified:

Risk avoidance – Stop performing the activities that create risk.

Risk reduction – Decrease the risk by taking measures to reduce vulnerability.

Risk sharing – Shift some of the risk to other parties.

Risk retention – Accept the risk and its consequences.

24. What are two characteristics of the SLAAC method for IPv6 address configuration? (Choose two.)

- **The default gateway of an IPv6 client on a LAN will be the link-local address of the router interface attached to the LAN.**
- This stateful method of acquiring an IPv6 address requires at least one DHCPv6 server.

- Clients send router advertisement messages to routers to request IPv6 addressing.
- **IPv6 addressing is dynamically assigned to clients through the use of ICMPv6.**
- Router solicitation messages are sent by the router to offer IPv6 addressing to clients.

25. A technician notices that an application is not responding to commands and that the computer seems to respond slowly when applications are opened. What is the best administrative tool to force the release of system resources from the unresponsive application?

- Event Viewer
- System Restore
- Add or Remove Programs
- **Task Manager**

Explanation: Use the Task Manager Performance tab to see a visual representation of CPU and RAM utilization. This is helpful in determining if more memory is needed. Use the Applications tab to halt an application that is not responding.

26. How can statistical data be used to describe or predict network behavior?

- **by comparing normal network behavior to current network behavior**
- by recording conversations between network endpoints
- by listing results of user web surfing activities
- by displaying alert messages that are generated by Snort

Explanation: Statistical data is created through the analysis of other forms of network data. Statistical characteristics of normal network behavior can be compared to current network traffic in an effort to detect anomalies. Conclusions resulting from analysis can be used to describe or predict network behavior.

27. Which metric in the CVSS Base Metric Group is used with an attack vector?

- **the proximity of the threat actor to the vulnerability**
- the presence or absence of the requirement for user interaction in order for an exploit to be successful

- the determination whether the initial authority changes to a second authority during the exploit
- the number of components, software, hardware, or networks, that are beyond the control of the attacker and that must be present in order for a vulnerability to be successfully exploited

Explanation: This is a metric that reflects the proximity of the threat actor to the vulnerable component. The more remote the threat actor is to the component, the higher the severity. Threat actors close to your network or inside your network are easier to detect and mitigate.

28. Which NIST Cybersecurity Framework core function is concerned with the development and implementation of safeguards that ensure the delivery of critical infrastructure services?

- respond
- detect
- identify
- recover
- **protect**

29. What is one difference between the client-server and peer-to-peer network models?

- Only in the client-server model can file transfers occur.
- A data transfer that uses a device serving in a client role requires that a dedicated server be present.
- A peer-to-peer network transfers data faster than a transfer using a client-server network.
- **Every device in a peer-to-peer network can function as a client or a server.**

30. Which statement is correct about network protocols?

- **They define how messages are exchanged between the source and the destination.**
- They all function in the network access layer of TCP/IP.
- They are only required for exchange of messages between devices on remote networks.
- Network protocols define the type of hardware that is used and how it is mounted in racks.

31. Which approach can help block potential malware delivery methods, as described in the Cyber Kill Chain model, on an Internet-faced web server?

- Build detections for the behavior of known malware.
- Collect malware files and metadata for future analysis.
- Audit the web server to forensically determine the origin of exploit.
- **Analyze the infrastructure storage path used for files.**

Explanation: A threat actor may send the weapon through web interfaces to the target server, either in file uploads or coded web requests. By analyzing the infrastructure storage path used for files, security measures can be implemented to monitor and detect malware deliveries through these methods.

32. Which meta-feature element in the Diamond Model classifies the general type of intrusion event?

- phase
- **results**
- methodology
- direction

33. Which Linux command is used to manage processes?

- chrootkit
- ls
- grep
- **kill**

Explanation: The kill command is used to stop, restart, or pause a process. The chrootkit command is used to check the computer for rootkits, a set of software tools that can increase the privilege level of a user or grant access to portions of software normally not allowed. The grep command is used to look for a file or text within a file. The ls command is used to list files, directories, and file information.

34. Which tool can be used in a Cisco AVC system to analyze and present the application analysis data into dashboard reports?

- NetFlow
- NBAR2
- **Prime**

- IPFIX

Explanation: A management and reporting system, such as Cisco Prime, can be used to analyze and present the application analysis data into dashboard reports for use by network monitoring personnel.

35. Which Windows Event Viewer log includes events regarding the operation of drivers, processes, and hardware?

- **system logs**
- application logs
- security logs
- setup logs

By default Windows keeps four types of host logs:

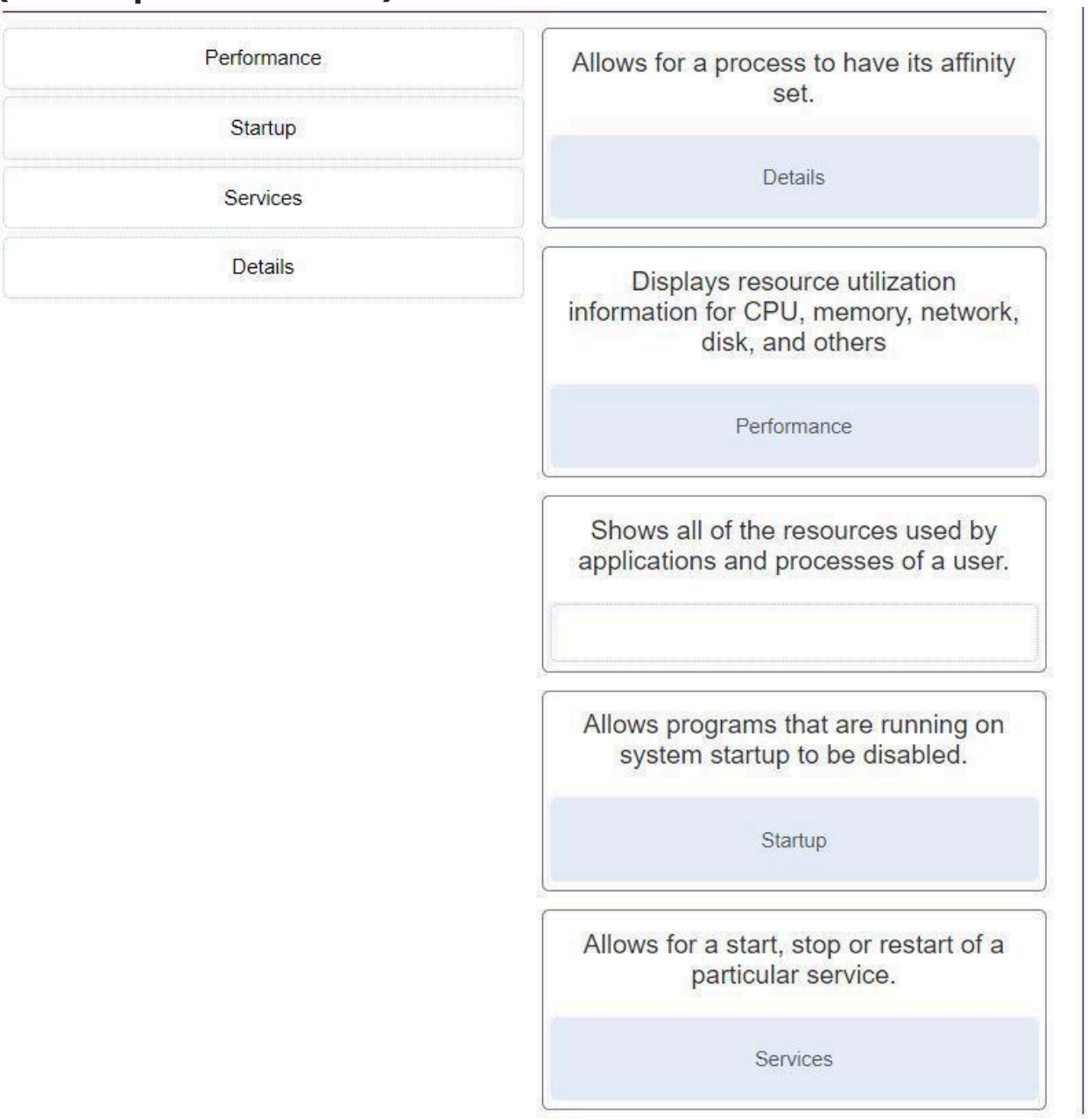
- **Application logs –** events logged by various applications
- **System logs –** events about the operation of drivers, processes, and hardware
- **Setup logs –** information about the installation of software, including Windows updates
- **Security logs –** events related to security, such as logon attempts and operations related to file or object management and access

36. Which method is used to make data unreadable to unauthorized users?

- **Encrypt the data.**
- Fragment the data.
- Add a checksum to the end of the data.
- Assign it a username and password.

Explanation: Network data can be encrypted using various cryptography applications so that the data is made unreadable to unauthorized users. Authorized users have the cryptography application so the data can be unencrypted.

37. Match the tabs of the Windows 10 Task Manager to their functions. (Not all options are used.)



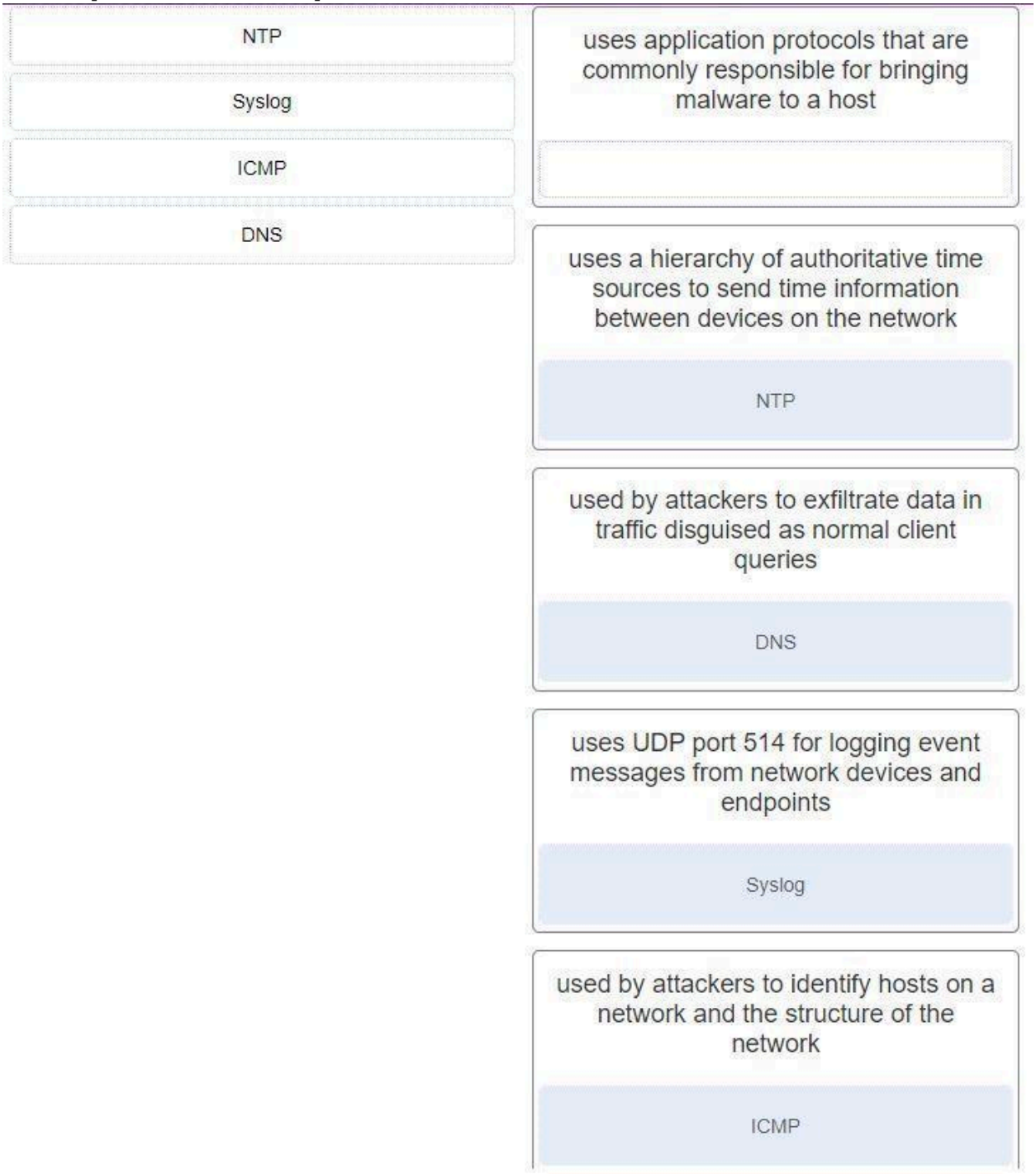
38. For network systems, which management system addresses the inventory and control of hardware and software configurations?

- asset management
- vulnerability management
- risk management

- **configuration management**

Explanation: Configuration management addresses the inventory and control of hardware and software configurations of network systems.

38. Match the common network technology or protocol with the description. (Not all options are used.)



40. What are the three core functions provided by the Security Onion? (Choose three.)

- business continuity planning

- **full packet capture**
- **alert analysis**
- **intrusion detection**
- security device management
- threat containment

Explanation: Security Onion is an open source suite of Network Security Monitoring (NSM) tools for evaluating cybersecurity alerts. For cybersecurity analysts the Security Onion provides full packet capture, network-based and host-based intrusion detection systems, and alert analysis tools.

41. In NAT terms, what address type refers to the globally routable IPv4 address of a destination host on the Internet?

- **outside global**
- inside global
- outside local
- inside local

Explanation: From the perspective of a NAT device, inside global addresses are used by external users to reach internal hosts. Inside local addresses are the addresses assigned to internal hosts. Outside global addresses are the addresses of destinations on the external network. Outside local addresses are the actual private addresses of destination hosts behind other NAT devices.

42. Which two fields or features does Ethernet examine to determine if a received frame is passed to the data link layer or discarded by the NIC? (Choose two.)

- CEF
- source MAC address
- **minimum frame size**
- auto-MDIX
- **Frame Check Sequence**

43. Which type of data would be considered an example of volatile data?

- web browser cache
- **memory registers**
- log files

- temp files

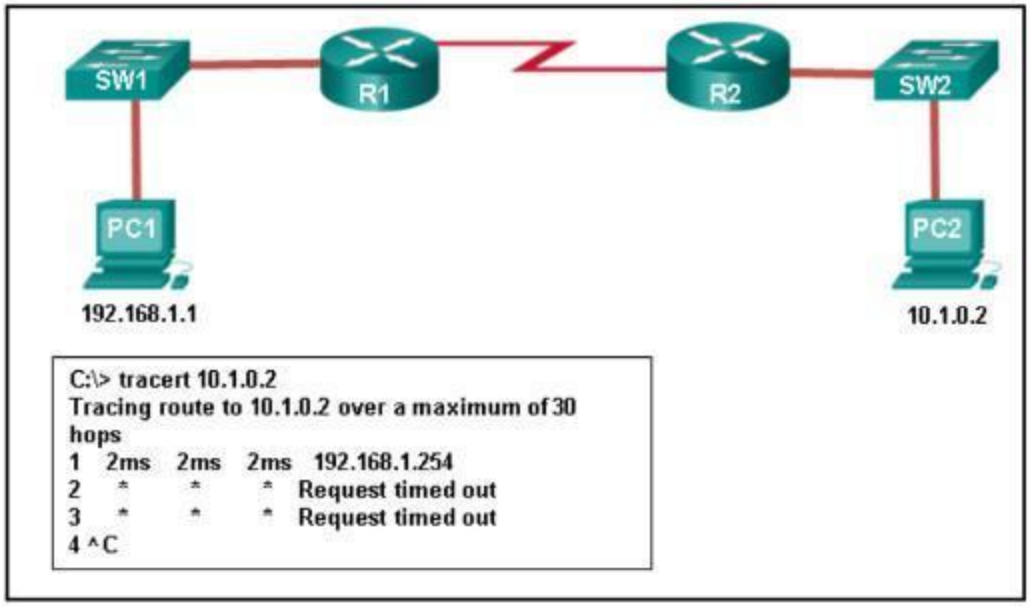
Explanation: Volatile data is data stored in memory such as registers, cache, and RAM, or it is data that exists in transit. Volatile memory is lost when the computer loses power.

44. What is the main purpose of exploitations by a threat actor through the weapon delivered to a target during the Cyber Kill Chain exploitation phase?

- Launch a DoS attack.
- Send a message back to a CnC controlled by the threat actor.
- **Break the vulnerability and gain control of the target.**
- Establish a back door into the system.

Explanation: After the weapon has been delivered, the threat actor uses it to break the vulnerability and gain control of the target. The threat actor will use an exploit that gains the effect desired, does it quietly, and avoids detections. Establishing a back door in the target system is the phase of installation.

45. Refer to the exhibit. An administrator is trying to troubleshoot connectivity between PC1 and PC2 and uses the tracert command from PC1 to do it. Based on the displayed output, where should the administrator begin troubleshooting?



- **R1**
- PC2
- SW2
- R2
- SW1

Explanation: Tracert is used to trace the path a packet takes. The only successful response was from the first device along the path on the same LAN as the sending host. The first device is the default gateway on router R1. The administrator should therefore start troubleshooting at R1.

46. What three security tools does Cisco Talos maintain security incident detection rule sets for? (Choose three.)

- **Snort**
- NetStumbler
- Socat
- **SpamCop**
- **ClamAV**

47. Which host-based firewall uses a three-profile approach to configure the firewall functionality?

- **Windows Firewall**
- iptables
- TCP Wrapper
- nftables

Explanation: Windows Firewall uses a profile-based approach to configuring firewall functionality. It uses three profiles, Public, Private, and Domain, to define firewall functions.

48. When a user visits an online store website that uses HTTPS, the user browser queries the CA for a CRL. What is the purpose of this query?

- **to verify the validity of the digital certificate**
- to request the CA self-signed digital certificate
- to check the length of key used for the digital certificate
- to negotiate the best encryption to use

Explanation: A digital certificate must be revoked if it is invalid. CAs maintain a certificate revocation list (CRL), a list of revoked certificate serial numbers that have been invalidated. The user browser will query the CRL to verify the validity of a certificate.

49. Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

- discover
- **assess**
- prioritize assets
- verify

Explanation: The steps in the Vulnerability Management Life Cycle include these:

- Discover – inventory all assets across the network and identify host details, including operating systems and open services, to identify vulnerabilities
- Prioritize assets – categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to business operations
- Assess – determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability threats, and asset classification
- Report – measure the level of business risk associated with assets according to security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
- Remediate – prioritize according to business risk and fix vulnerabilities in order of risk
- Verify – verify that threats have been eliminated through follow-up audits

50. Which management system implements systems that track the location and configuration of networked devices and software across an enterprise?

- **asset management**
- vulnerability management
- risk management
- configuration management

Explanation: Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.

51. A network administrator is reviewing server alerts because of reports of network slowness. The administrator confirms that an alert was an actual security incident. What is the security alert classification of this type of scenario?

- false negative
- **true positive**
- true negative
- false positive

52. Which application layer protocol is used to provide file-sharing and print services to Microsoft applications?

- SMTP
- HTTP
- **SMB**
- DHCP

Explanation: SMB is used in Microsoft networking for file-sharing and print services. The Linux operating system provides a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA.

53. Which device in a layered defense-in-depth approach denies connections initiated from untrusted networks to internal networks, but allows internal users within an organization to connect to untrusted networks?

- access layer switch
- **firewall**
- internal router
- IPS

Explanation: A firewall is typically a second line of defense in a layered defense-in-depth approach to network security. The firewall typically connects to an edge router that connects to the service provider. The firewall tracks connections initiated within the company going out of

the company and denies initiation of connections from external untrusted networks going to internal trusted networks.

54. What are two potential network problems that can result from ARP operation? (Choose two.)

- Large numbers of ARP request broadcasts could cause the host MAC address table to overflow and prevent the host from communicating on the network.
- On large networks with low bandwidth, multiple ARP broadcasts could cause data communication delays.
- **Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent of intercepting network traffic.**
- Multiple ARP replies result in the switch MAC address table containing entries that match the MAC addresses of hosts that are connected to the relevant switch port.
- Manually configuring static ARP associations could facilitate ARP poisoning or MAC address spoofing.

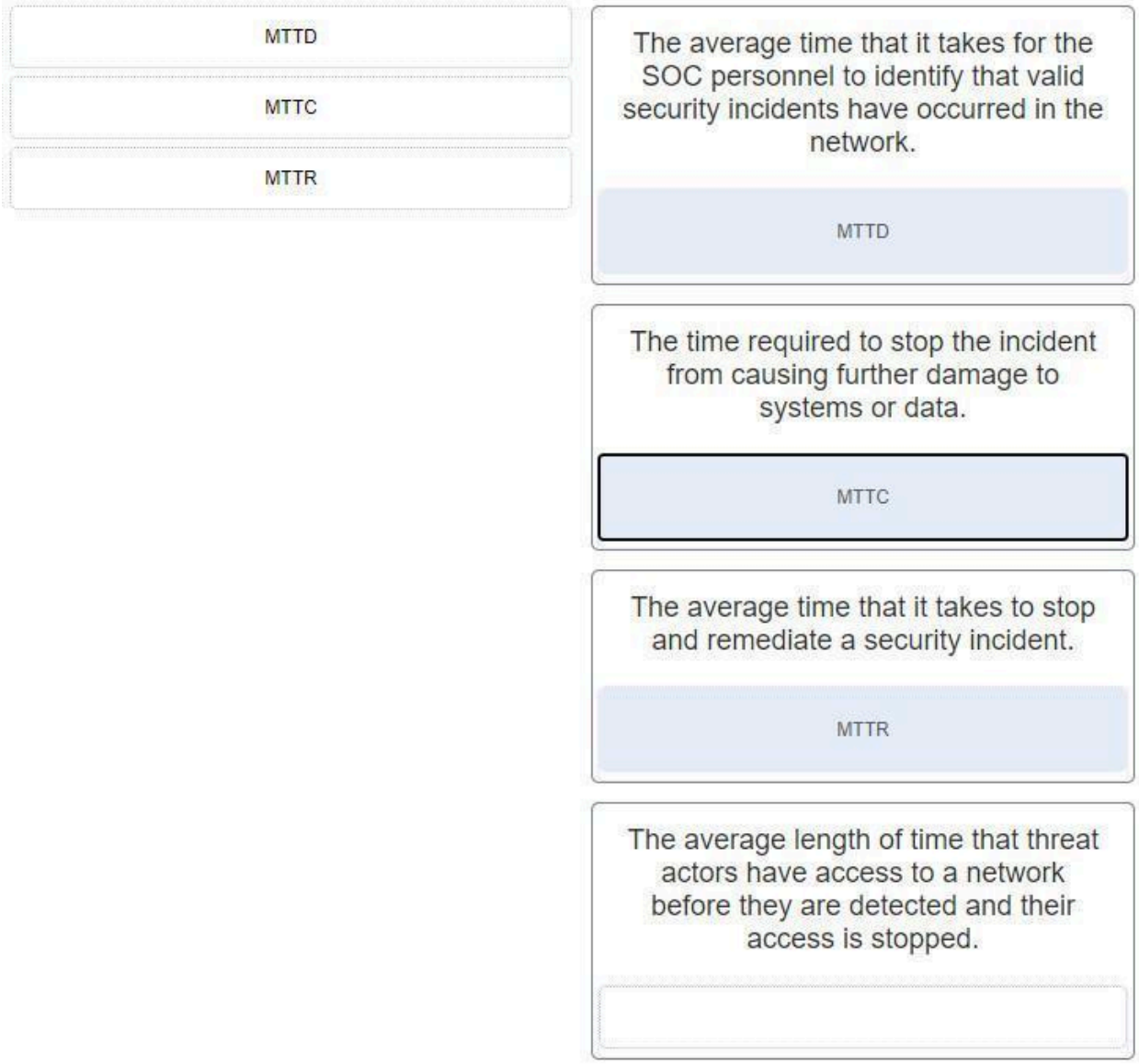
55. Which three procedures in Sguil are provided to security analysts to address alerts? (Choose three.)

- **Escalate an uncertain alert.**
- Correlate similar alerts into a single line.
- **Categorize true positives.**
- Pivot to other information sources and tools.
- Construct queries using Query Builder.
- **Expire false positives.**

Explanation: Sguil is a tool for addressing alerts. Three tasks can be completed in Sguil to manage alerts:

- Alerts that have been found to be false positives can be expired.
- An alert can be escalated if the cybersecurity analyst is uncertain how to handle it.
- Events that have been identified as true positives can be categorized.

56. Match the SOC metric with the description. (Not all options apply.)



57. Which two services are provided by the NetFlow tool? (Choose two.)

- QoS configuration
- **usage-based network billing**
- log analysis
- access list monitoring
- **network monitoring**

Explanation: NetFlow efficiently provides an important set of services for IP applications including network traffic accounting, usage-based

network billing, network planning, security, denial of service monitoring capabilities, and network monitoring.

58. Which two statements are characteristics of a virus? (Choose two.)

- A virus typically requires end-user activation.
- A virus can be dormant and then activate at a specific time or date.
- A virus replicates itself by independently exploiting vulnerabilities in networks.
- A virus has an enabling vulnerability, a propagation mechanism, and a payload.
- A virus provides the attacker with sensitive data, such as passwords

Explanation: The type of end user interaction required to launch a virus is typically opening an application, opening a web page, or powering on the computer. Once activated, a virus may infect other files located on the computer or other computers on the same network.

59. What is a characteristic of a Trojan horse as it relates to network security?

- Too much information is destined for a particular memory block, causing additional memory areas to be affected.
- Extreme quantities of data are sent to a particular network device interface.
- An electronic dictionary is used to obtain a password to be used to infiltrate a key network device.
- Malware is contained in a seemingly legitimate executable program.

Explanation: A Trojan horse carries out malicious operations under the guise of a legitimate program. Denial of service attacks send extreme quantities of data to a particular host or network device interface. Password attacks use electronic dictionaries in an attempt to learn passwords. Buffer overflow attacks exploit memory buffers by sending too much information to a host to render the system inoperable.

60. What technique is used in social engineering attacks?

- sending junk email

- buffer overflow
- phishing
- man-in-the-middle

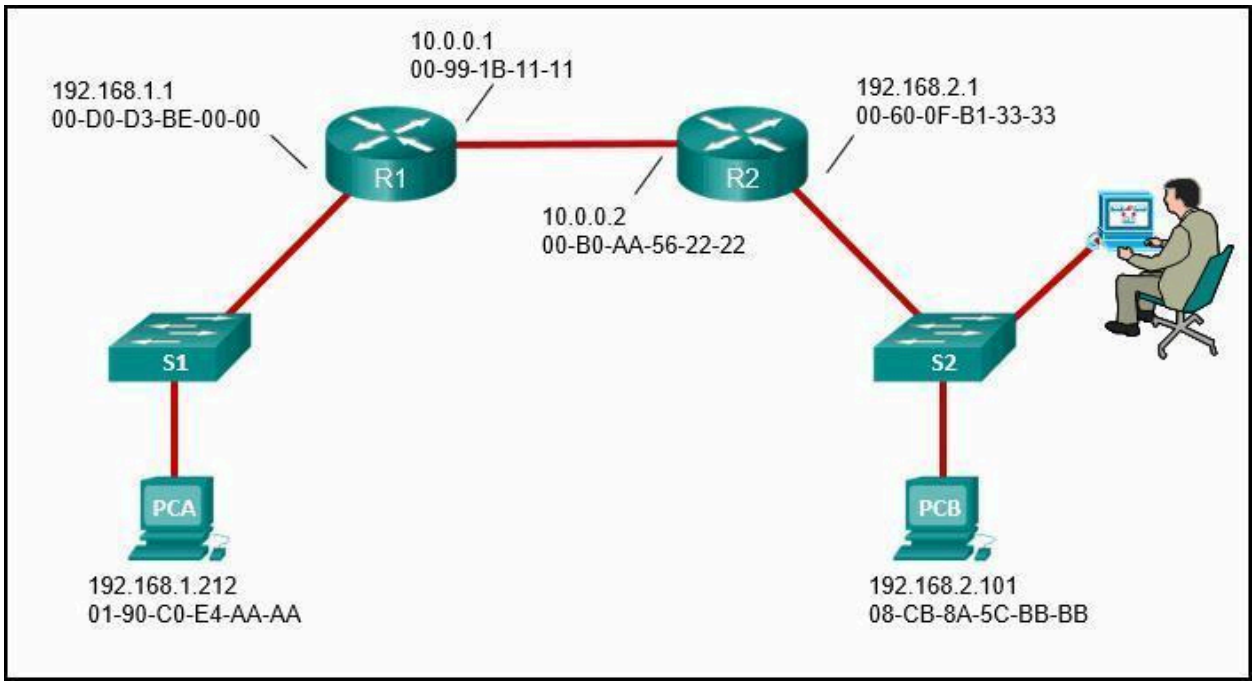
Explanation: A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.

61. What is a purpose of implementing VLANs on a network?

- They can separate user traffic.
- They prevent Layer 2 loops.
- They eliminate network collisions.
- They allow switches to forward Layer 3 packets without a router.

Explanation: VLANs are used on a network to separate user traffic based on factors such as function, project team, or application, without regard for the physical location of the user or device.

62. Refer to the exhibit. A cybersecurity analyst is viewing packets forwarded by switch S2. What addresses will identify frames containing data sent from PCA to PCB?



Src IP: 192.168.2.1
Src MAC: 00-60-0F-B1-33-33
Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212
Src MAC: 01-90-C0-E4-AA-AA
Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

Src IP: 192.168.1.212
Src MAC: 00-60-0F-B1-33-33
Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

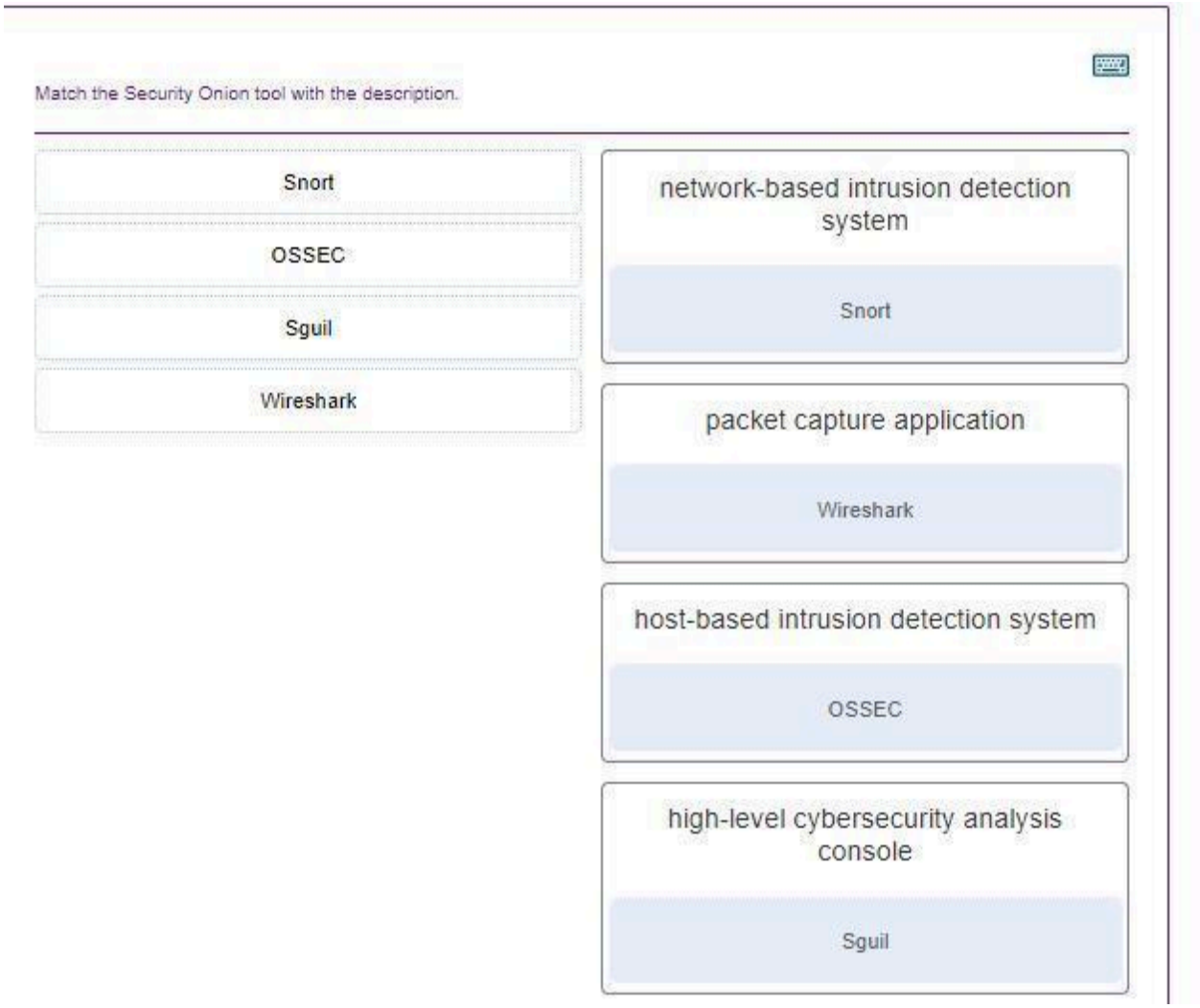
Src IP: 192.168.1.212
Src MAC: 00-60-0F-B1-33-33
Dst IP: 192.168.2.101
Dst MAC: 00-D0-D3-BE-00-00

Explanation: When a message sent from PCA to PCB reaches router R2, some frame header fields will be rewritten by R2 before forwarding to switch S2. The frames will contain the source MAC address of router R2 and the destination MAC address of PCB. The frames will retain the original IPv4 addressing applied by PCA which is the IPv4 address of PCA as the source address and the IPv4 address of PCB as the destination.

63. A cybersecurity analyst needs to collect alert data. What are three detection tools to perform this task in the Security Onion architecture? (Choose three.)

- CapME
- Wazuh
- Kibana
- Zeek
- Sguil
- Wireshark

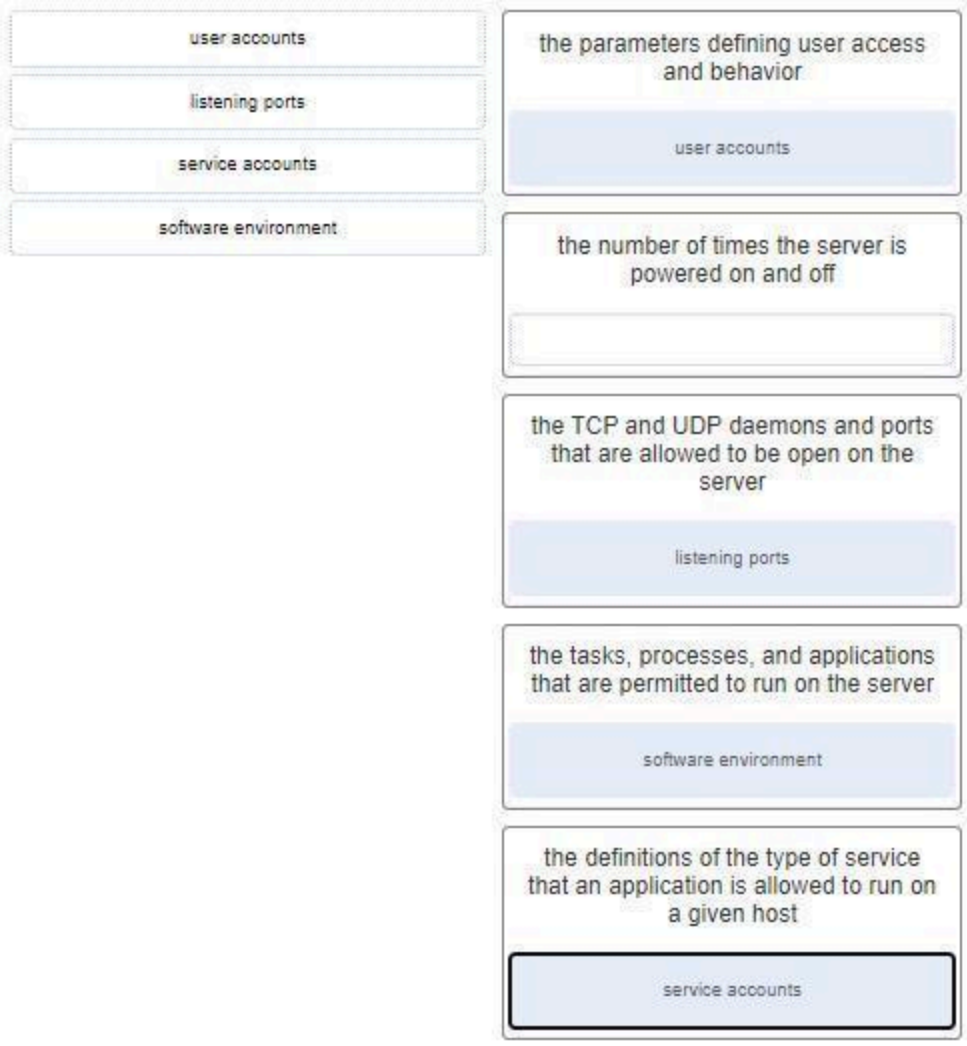
64. Match the Security Onion tool with the description.



65. In network security assessments, which type of test is used to evaluate the risk posed by vulnerabilities to a specific organization including assessment of the likelihood of attacks and the impact of successful exploits on the organization?

- port scanning
- risk analysis
- penetration testing
- vulnerability assessment

66. Match the server profile element to the description. (Not all options are used.)



Explanation: The elements of a server profile include the following:Listening ports – the TCP and UDP daemons and ports that are allowed to be open on the server
User accounts – the parameters defining user access and behavior
Service accounts – the definitions of the type of service that an application is allowed to run on a given host
Software environment – the tasks, processes, and applications that are permitted to run on the server

67. In addressing an identified risk, which strategy aims to shift some of the risk to other parties?

- risk avoidance
- risk sharing
- risk retention

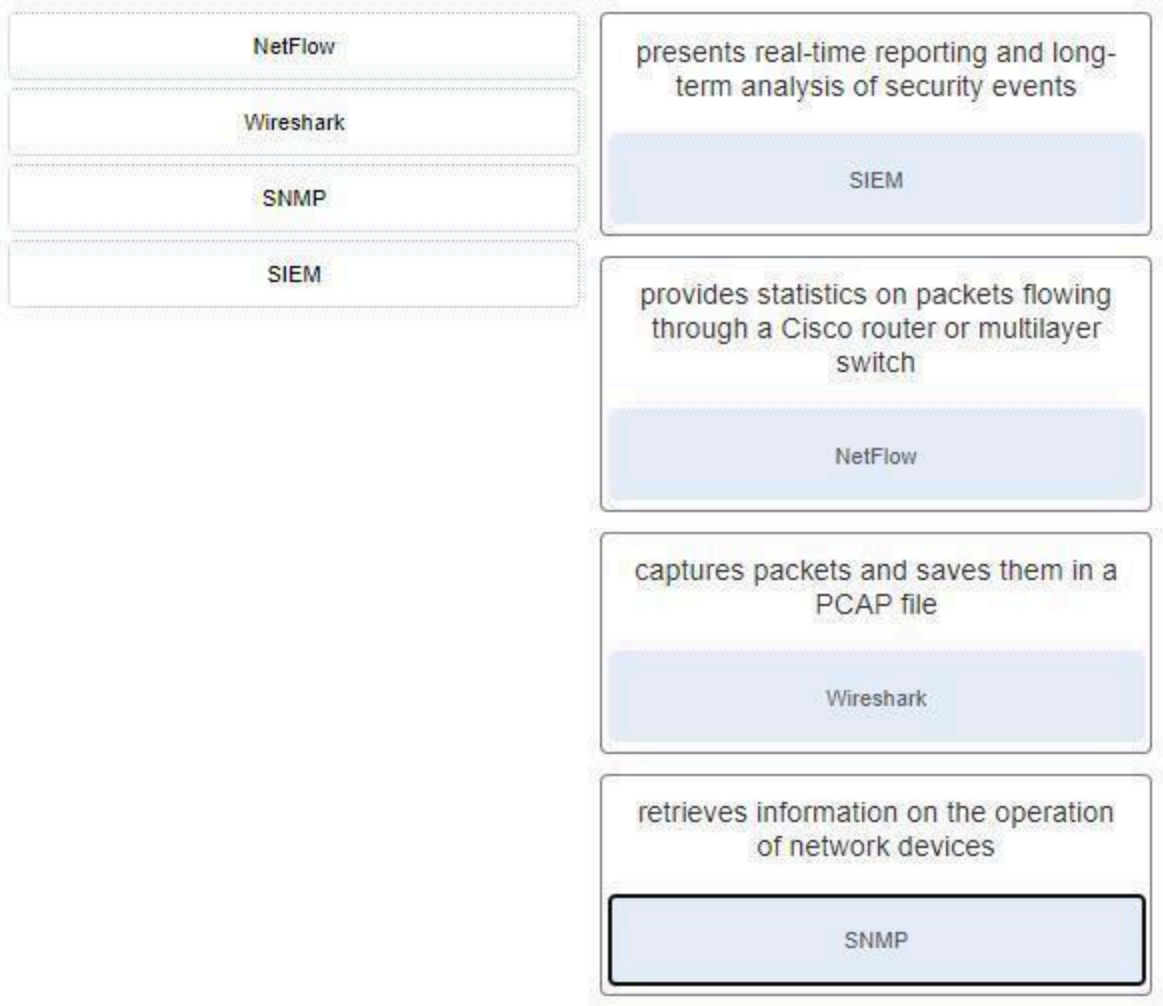
- risk reduction

68. What is a network tap?

- a technology used to provide real-time reporting and long-term analysis of security events
- a Cisco technology that provides statistics on packets flowing through a router or multilayer switch
- a feature supported on Cisco switches that enables the switch to copy frames and forward them to an analysis device
- a passive device that forwards all traffic and physical layer errors to an analysis device

Explanation: A network tap is used to capture traffic for monitoring the network. The tap is typically a passive splitting device implemented inline on the network and forwards all traffic, including physical layer errors, to an analysis device.

69. Match the monitoring tool to the definition.



70. If a SOC has a goal of 99.999% uptime, how many minutes of downtime a year would be considered within its goal?

- Approximately 5 minutes per year.
- Approximately 10 minutes per year
- Approximately 20 minutes per year.
- Approximately 30 minutes per year.

Explanation: Within a year, there are 365 days x 24 hours a day x 60 minutes per hour = 525,600 minutes. With the goal of uptime 99.999% of time, the downtime needs to be controlled under 525,600 x (1-0.99999) = 5.256 minutes a year.

71. The HTTP server has responded to a client request with a 200 status code. What does this status code indicate?

- The request is understood by the server, but the resource will not be fulfilled.
- The request was completed successfully.
- The server could not find the requested resource, possibly because of an incorrect URL.
- The request has been accepted for processing, but processing is not completed.

72. What is an advantage for small organizations of adopting IMAP instead of POP?

- POP only allows the client to store messages in a centralized way, while IMAP allows distributed storage.
- IMAP sends and retrieves email, but POP only retrieves email.
- When the user connects to a POP server, copies of the messages are kept in the mail server for a short time, but IMAP keeps them for a long time.
- Messages are kept in the mail servers until they are manually deleted from the email client.

Explanation: IMAP and POP are protocols that are used to retrieve email messages. The advantage of using IMAP instead of POP is that when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. IMAP then stores the email messages on the server until the user manually deletes those messages.

73. What debugging security tool can be used by black hats to reverse engineer binary files when writing exploits?

- WinDbg
- Firesheep
- Skipfish
- AIDE

74. What are three characteristics of an information security management system? (Choose three.)

- It involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.
- **It is a systematic and multilayered approach to cybersecurity.**

- It addresses the inventory and control of hardware and software configurations of systems.
- **It consists of a set of practices that are systematically applied to ensure continuous improvement in information security.**
- **It consists of a management framework through which an organization identifies, analyzes, and addresses information security risks.**
- It is based on the application of servers and security devices.

Explanation: An Information Security Management System (ISMS) consists of a management framework through which an organization identifies, analyzes, and addresses information security risks. ISMSs are not based in servers or security devices. Instead, an ISMS consists of a set of practices that are systematically applied by an organization to ensure continuous improvement in information security. ISMSs provide conceptual models that guide organizations in planning, implementing, governing, and evaluating information security programs.

ISMSs are a natural extension of the use of popular business models, such as Total Quality Management (TQM) and Control Objectives for Information and Related Technologies (COBIT), into the realm of cybersecurity.

An ISMS is a systematic, multi-layered approach to cybersecurity. The approach includes people, processes, technologies, and the cultures in which they interact in a process of risk management.

75. Which three technologies should be included in a SOC security information and event management system? (Choose three.)

- **event collection, correlation, and analysis**
- **security monitoring**
- user authentication
- proxy service
- intrusion prevention
- **threat intelligence**

Explanation: Technologies in a SOC should include the following:
• Event collection, correlation, and analysis
• Security monitoring
• Security control
• Log management
• Vulnerability assessment

• Vulnerability tracking
• Threat intelligence
Proxy server, VPN, and IPS are security devices deployed in the network infrastructure.

76. What part of the URL, http://www.cisco.com/index.html, represents the top-level DNS domain?

- http
- www
- **.com**
- index

Explanation: The components of the URL http://www.cisco.com/index.htm are as follows:
http = protocol
www = part of the server name
cisco = part of the domain name
index = file name
com = the top-level domain

77. What best describes the security threat of spoofing?

- sending bulk email to individuals, lists, or domains with the intention to prevent users from accessing email
- **sending abnormally large amounts of data to a remote server to prevent user access to the server services**
- intercepting traffic between two hosts or inserting false information into traffic between two hosts
- making data appear to come from a source that is not the actual source

78. A newly created company has fifteen Windows 10 computers that need to be installed before the company can open for business. What is a best practice that the technician should implement when configuring the Windows Firewall?

- The technician should remove all default firewall rules and selectively deny traffic from reaching the company network.
- **After implementing third party security software for the company, the technician should verify that the Windows Firewall is disabled.**

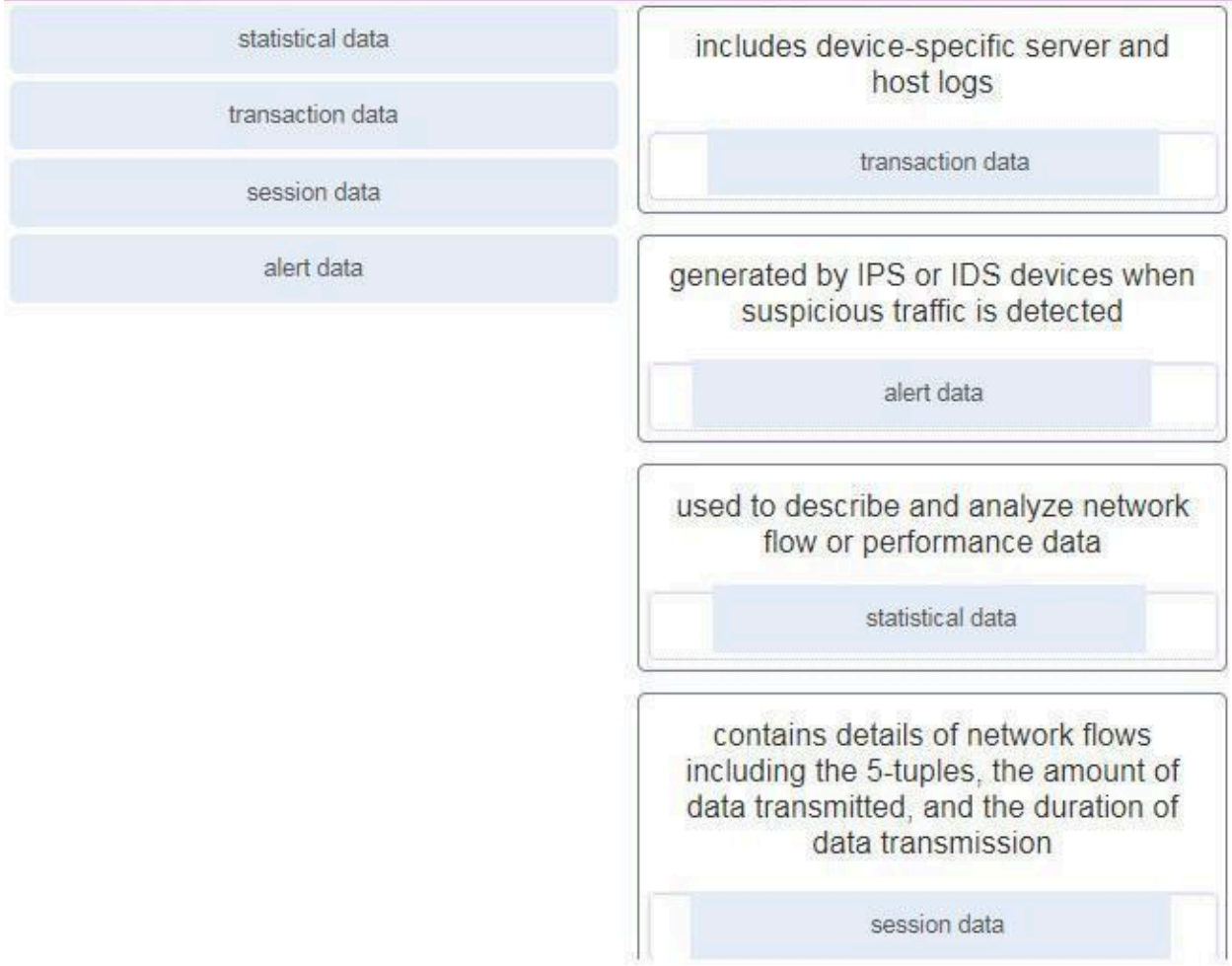
- The technician should create instructions for corporate users on how to allow an app through the WIndows Firewall using the Administrator account.
- The technician should enable the Windows Firewall for inbound traffic and install other firewall software for outbound traffic control.

Explanation: Only disable Windows Firewall if other firewall software is installed. Use the Windows Firewall (Windows 7 or 8) or the Windows Defender Firewall (Windows 10) Control Panel to enable or disable the Windows Firewall.

79. Which statement defines the difference between session data and transaction data in logs?

- Session data analyzes network traffic and predicts network behavior, whereas transaction data records network sessions.
- Session data is used to make predictions on network behaviors, whereas transaction data is used to detect network anomalies.
- **Session data records a conversation between hosts, whereas transaction data focuses on the result of network sessions.**
- Session data shows the result of a network session, whereas transaction data is in response to network threat traffic.

80. Match the network monitoring data type with the description.



81. Which device supports the use of SPAN to enable monitoring of malicious activity?

- **Cisco Catalyst switch**
- Cisco IronPort
- Cisco NAC
- Cisco Security Agent

82. Which term is used for describing automated queries that are useful for adding efficiency to the cyberoperations workflow?

- cyber kill chain
- **playbook**
- chain of custody
- rootkit

Explanation: A playbook is an automated query that can add efficiency to the cyberoperations workflow.

83. When ACLs are configured to block IP address spoofing and DoS flood attacks, which ICMP message should be allowed both inbound and outbound?

- echo reply
- unreachable
- source quench
- **echo**

84. After a security monitoring tool identifies a malware attachment entering the network, what is the benefit of performing a retrospective analysis?

- It can identify how the malware originally entered the network.
- **A retrospective analysis can help in tracking the behavior of the malware from the identification point forward.**
- It can calculate the probability of a future incident.
- It can determine which network host was first affected.

Explanation: General security monitoring can identify when a malware attachment enters a network and which host is first infected. Retrospective analysis takes the next step and is the tracking of the behavior of the malware from that point forward.

85. Which two data types would be classified as personally identifiable information (PII)? (Choose two.)

- house thermostat reading
- average number of cattle per region
- **vehicle identification number**
- hospital emergency use per region
- **Facebook photographs**

86. A help desk technician notices an increased number of calls relating to the performance of computers located at the manufacturing plant. The technician believes that botnets are causing the issue. What are two purposes of botnets? (Choose two.)

- **to transmit viruses or spam to computers on the same network**
- to record any and all keystrokes

- **to attack other computers**
- to withhold access to a computer or files until money has been paid
- to gain access to the restricted part of the operating system

Explanation: Botnets can be used to perform DDoS attacks, obtain data, or transmit malware to other devices on the network.

87. Which two statements describe the use of asymmetric algorithms? (Choose two.)

- Public and private keys may be used interchangeably.
- **If a public key is used to encrypt the data, a private key must be used to decrypt the data.**
- If a public key is used to encrypt the data, a public key must be used to decrypt the data.
- **If a private key is used to encrypt the data, a public key must be used to decrypt the data.**
- If a private key is used to encrypt the data, a private key must be used to decrypt the data.

Explanation: Asymmetric algorithms use two keys: a public key and a private key. Both keys are capable of the encryption process, but the complementary matched key is required for decryption. If a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

88. Which three security services are provided by digital signatures? (Choose three.)

- **provides confidentiality of digitally signed data**
- guarantees data has not changed in transit
- provides nonrepudiation using HMAC functions
- **provides data encryption**
- **authenticates the source**
- authenticates the destination

89. What are two methods to maintain certificate revocation status? (Choose two.)

- **CRL**
- DNS

- subordinate CA
- **OCSP**
- LDAP

Explanation: A digital certificate might need to be revoked if its key is compromised or it is no longer needed. The certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP), are two common methods to check a certificate revocation status.

90. What are two uses of an access control list? (Choose two.)

- **ACLs provide a basic level of security for network access.**
- **ACLs can control which areas a host can access on a network.**
- Standard ACLs can restrict access to specific applications and ports.
- ACLs assist the router in determining the best path to a destination.
- ACLs can permit or deny traffic based upon the MAC address originating on the router.

Explanation: ACLs can be used for the following:Limit network traffic in order to provide adequate network performance
Restrict the delivery of routing updates
Provide a basic level of security
Filter traffic based on the type of traffic being sent
Filter traffic based on IP addressing

91. A client is using SLAAC to obtain an IPv6 address for the interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

- It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.
- It must send an ICMPv6 Router Solicitation message to request the address of the DNS server.
- **It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.**
- It must wait for an ICMPv6 Router Advertisement message giving permission to use this address.

Explanation: Stateless DHCPv6 or stateful DHCPv6 uses a DHCP server, but Stateless Address Autoconfiguration (SLAAC) does not. A SLAAC

client can automatically generate an address that is based on information from local routers via Router Advertisement (RA) messages. Once an address has been assigned to an interface via SLAAC, the client must ensure via Duplicate Address Detection (DAD) that the address is not already in use. It does this by sending out an ICMPv6 Neighbor Solicitation message and listening for a response. If a response is received, then it means that another device is already using this address.

92. A technician is troubleshooting a network connectivity problem. Pings to the local wireless router are successful but pings to a server on the Internet are unsuccessful. Which CLI command could assist the technician to find the location of the networking problem?

- **tracert**
- ipconfig
- msconfig
- ipconfig/renew

Explanation: The tracert utlility (also known as the tracert command or tracert tool) will enable the technician to locate the link to the server that is down. The ipconfig command displays the computer network configuration details. The ipconfig/renew command requests an IP address from a DHCP server. Msconfig is not a network troubleshooting command.

93. What are two evasion techniques that are used by hackers? (Choose two.)

- Trojan horse
- **pivot**
- **rootkit**
- reconnaissance
- phishing

Explanation: The following methods are used by hackers to avoid detection:Encryption and tunneling – hide or scramble the malware content
Resource exhaustion – keeps the host device too busy to detect the invasion
Traffic fragmentation – splits the malware into multiple packets
Protocol-level misinterpretation – sneaks by the firewall

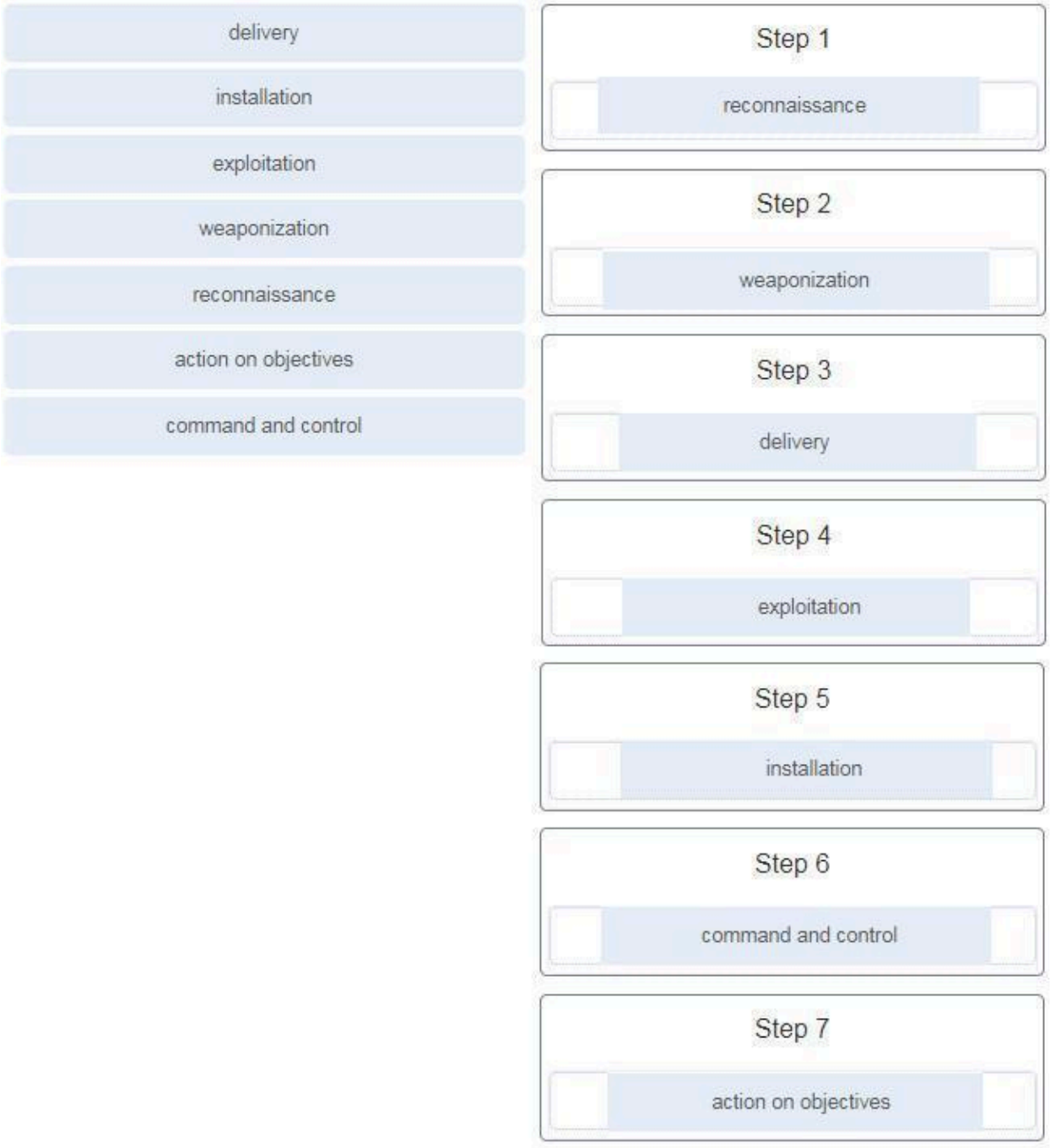
Pivot – uses a compromised network device to attempt access to another device
Rootkit – allows the hacker to be undetected and hides software installed by the hacker

94. When a security attack has occurred, which two approaches should security professionals take to mitigate a compromised system during the Actions on Objectives step as defined by the Cyber Kill Chain model? (Choose two.)

- **Perform forensic analysis of endpoints for rapid triage.**
- Train web developers for securing code.
- Build detections for the behavior of known malware.
- Collect malware files and metadata for future analysis.
- **Detect data exfiltration, lateral movement, and unauthorized credential usage.**

Explanation: When security professionals are alerted about the system compromises, forensic analysis of endpoints should be performed immediately for rapid triage. In addition, detection efforts for further attacking activities such as data exfiltration, lateral movement, and unauthorized credential usage should be enhanced to reduce damage to the minimum.

95. Place the seven steps defined in the Cyber Kill Chain in the correct order.



96. What are three goals of a port scan attack? (Choose three.)

- to identify peripheral configurations
- **to determine potential vulnerabilities**
- to disable used ports and services

- **to identify operating systems**
- **to identify active services**
- to discover system passwords

97. Which field in the TCP header indicates the status of the three-way handshake process?

- **control bits**
- window
- reserved
- checksum

Explanation: The value in the control bits field of theTCP header indicates the progress and status of the connection.

98. A user opens three browsers on the same PC to access www.cisco.com to search for certification course information. The Cisco web server sends a datagram as a reply to the request from one of the web browsers. Which information is used by the TCP/IP protocol stack in the PC to identify which of the three web browsers should receive the reply?

- the source IP address
- **the destination port number**
- the destination IP address
- the source port number

Explanation: Each web browser client application opens a randomly generated port number in the range of the registered ports and uses this number as the source port number in the datagram that it sends to a server. The server then uses this port number as the destination port number in the reply datagram that it sends to the web browser. The PC that is running the web browser application receives the datagram and uses the destination port number that is contained in this datagram to identify the client application.

99. What are two scenarios where probabilistic security analysis is best suited? (Choose two.)

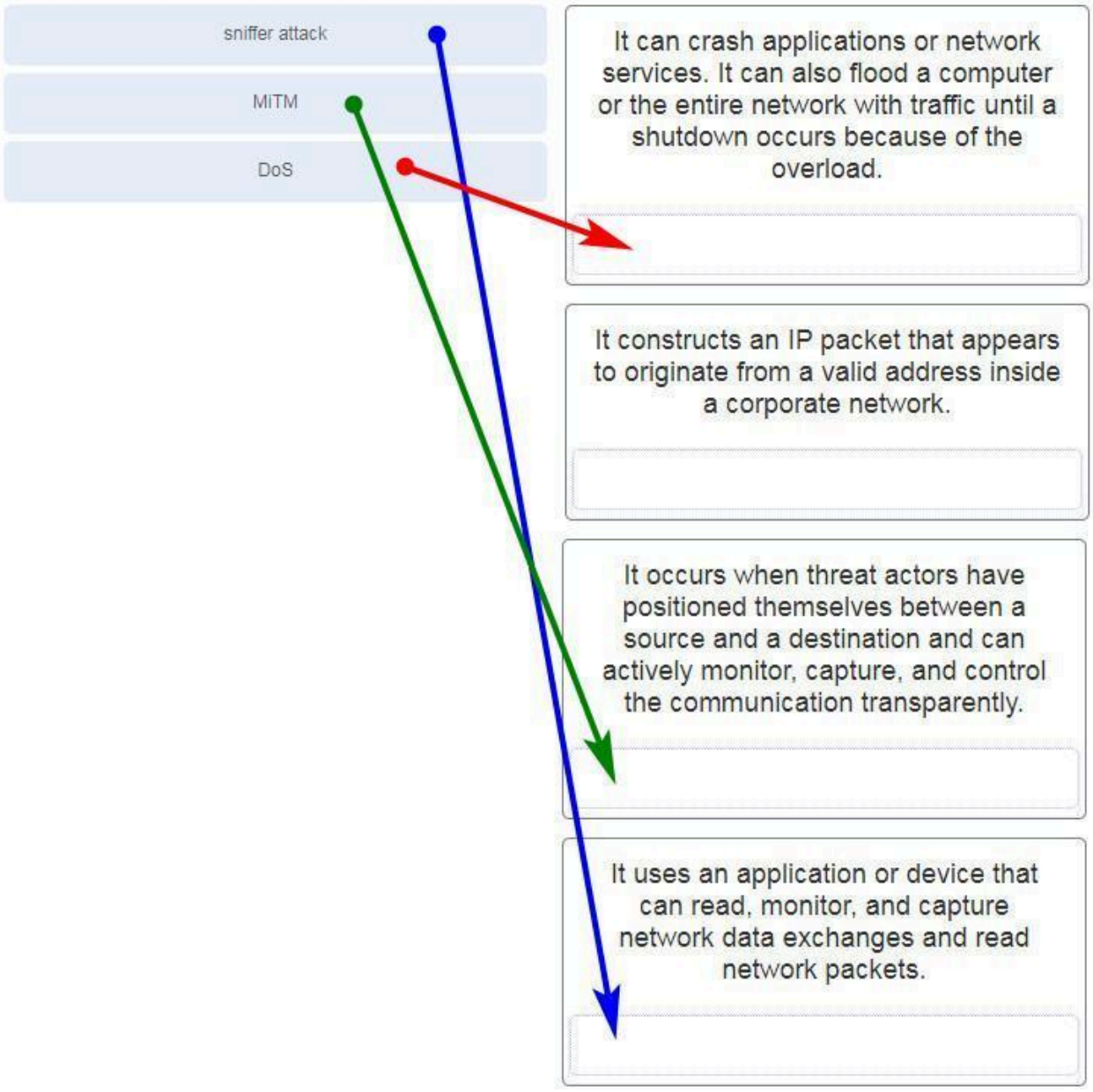
- when applications that conform to application/networking standards are analyzed
- **when analyzing events with the assumption that they follow predefined steps**

- when random variables create difficulty in knowing with certainty the outcome of any given event
- **when analyzing applications designed to circumvent firewalls**
- when each event is the inevitable result of antecedent causes

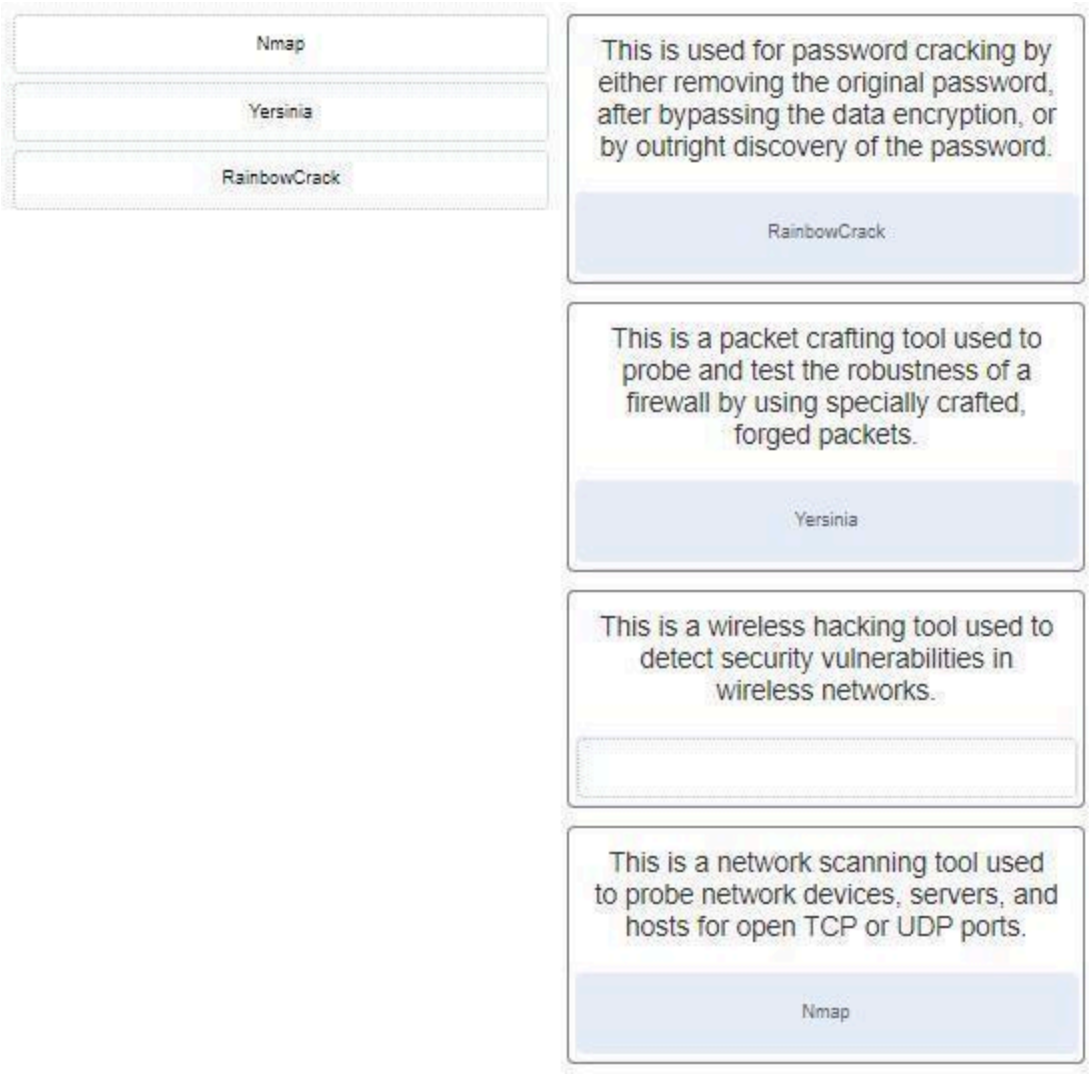
100. Which tool is a web application that provides the cybersecurity analyst an easy-to-read means of viewing an entire Layer 4 session?

- Snort
- Zeek
- **CapME**
- OSSEC

101. Match the category of attacks with the description. (Not all options are used.)



102. Match the attack tools with the description. (Not all options are used.)



103. What are two features of ARP? (Choose two.)

- When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses.
- If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address of the destination, it generates an ARP broadcast.
- If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.
- If no device responds to the ARP request, then the originating node will broadcast the data packet to all devices on the network segment.

- An ARP request is sent to all devices on the Ethernet LAN and contains the IP address of the destination host and the multicast MAC address.

Explanation: When a node encapsulates a data packet into a frame, it needs the destination MAC address. First it determines if the destination device is on the local network or on a remote network. Then it checks the ARP table (not the MAC table) to see if a pair of IP address and MAC address exists for either the destination IP address (if the destination host is on the local network) or the default gateway IP address (if the destination host is on a remote network). If the match does not exist, it generates an ARP broadcast to seek the IP address to MAC address resolution. Because the destination MAC address is unknown, the ARP request is broadcast with the MAC address FFFF.FFFF.FFFF. Either the destination device or the default gateway will respond with its MAC address, which enables the sending node to assemble the frame. If no device responds to the ARP request, then the originating node will discard the packet because a frame cannot be created.

104. What is a property of the ARP table on a device?

- Entries in an ARP table are time-stamped and are purged after the timeout expires.
- Every operating system uses the same timer to remove old entries from the ARP cache.
- Static IP-to-MAC address entries are removed dynamically from the ARP table.
- Windows operating systems store ARP cache entries for 3 minutes.

105. What is the purpose of Tor?

- to allow users to browse the Internet anonymously
- to securely connect to a remote network over an unsecure link such as an Internet connection
- to donate processor cycles to distributed computational tasks in a processor sharing P2P network
- to inspect incoming traffic and look for any that violates a rule or matches the signature of a known exploit

Explanation: Tor is a software platform and network of peer-to-peer (P2P) hosts that function as routers. Users access the Tor network by using a special browserthat allows them to browse anonymously.

106. Which two techniques are used in a smurf attack? (Choose two.)

- session hijacking
- resource exhaustion
- botnets
- **amplification**
- **reflection**

107. What is the primary objective of a threat intelligence platform (TIP)?

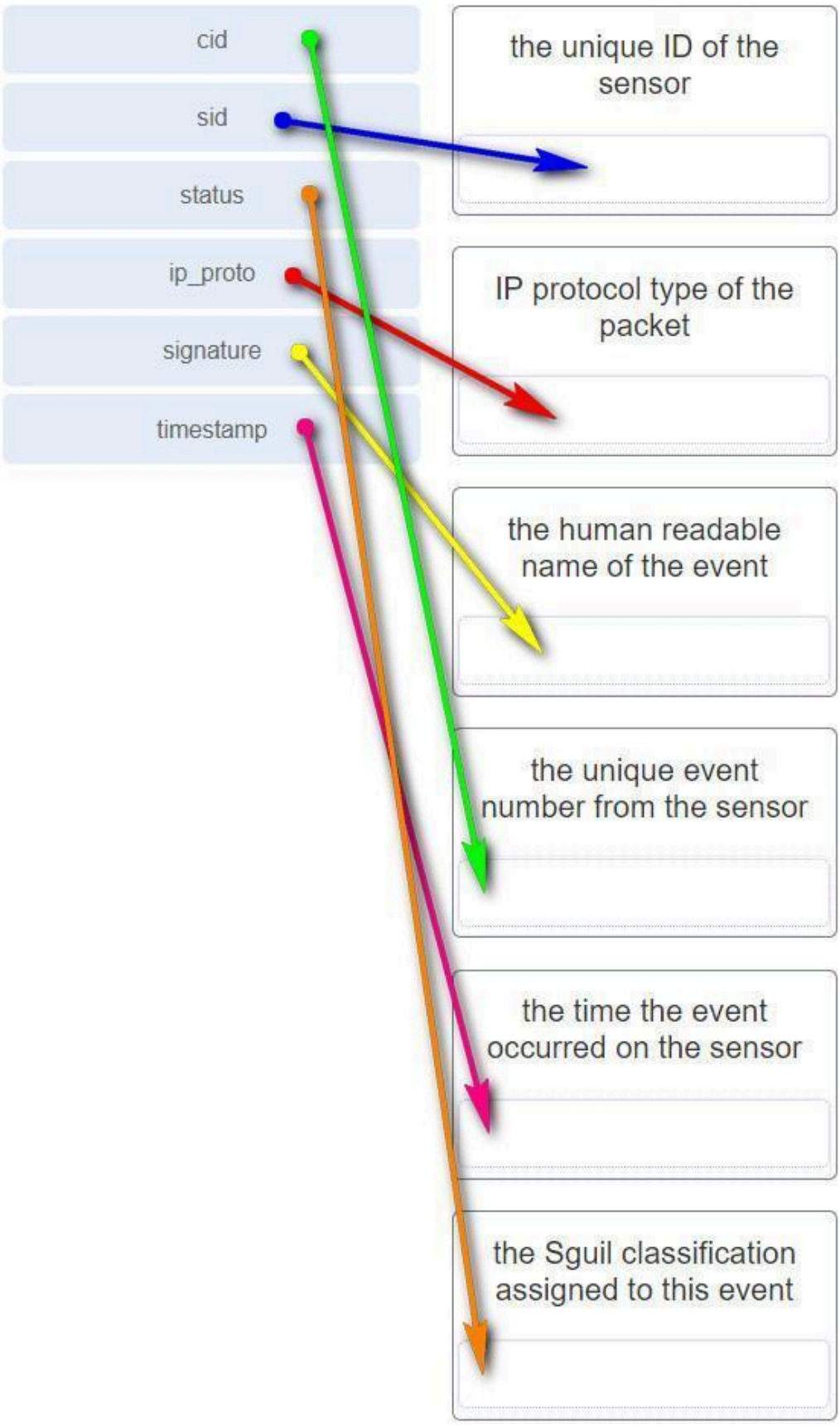
- to aggregate the data in one place and present it in a comprehensible and usable format
- to provide a specification for an application layer protocol that allows the communication of CTI over HTTPS
- to provide a standardized schema for specifying, capturing, characterizing, and communicating events and properties of network operations
- **to provide a security operations platform that integrates and enhances diverse security tools and threat intelligence**

108. Which wireless parameter is used by an access point to broadcast frames that include the SSID?

- security mode
- active mode
- **passive mode**
- channel setting

Explanation: The two scanning or probing modes an access point can be placed into are passive or active. In passive mode, the AP advertises the SSID, supported standards, and security settings in broadcast beacon frames. In active mode, the wireless client must be manually configured for the same wireless parameters as the AP has configured.

109. Match the field in the Event table of Sguil to the description.



Match the field

in the Event table of Sguil to the description

110. An employee connects wirelessly to the company network using a cell phone. The employee then configures the cell phone to act as a wireless access point that will allow new employees to connect to the company network. Which type of security threat best describes this situation?

- **rogue access point**
- cracking
- denial of service
- spoofing

111. What information is required for a WHOIS query?

- outside global address of the client
- ICANN lookup server address
- link-local address of the domain owner
- **FQDN of the domain**

112. Which two statements describe the characteristics of symmetric algorithms? (Choose two.)

- **They are referred to as a pre-shared key or secret key.**
- They use a pair of a public key and a private key.
- **They are commonly used with VPN traffic.**
- They provide confidentiality, integrity, and availability.

Explanation: Symmetric encryption algorithms use the same key (also called shared secret) to encrypt and decrypt the data. In contrast, asymmetric encryption algorithms use a pair of keys, one for encryption and another for decryption.

113. What are two drawbacks to using HIPS? (Choose two.)

- With HIPS, the success or failure of an attack cannot be readily determined.
- **With HIPS, the network administrator must verify support for all the different operating systems used inthe network.**
- **HIPS has difficulty constructing an accurate network picture or coordinating events that occur across the entire network.**
- If the network traffic stream is encrypted, HIPS is unable to access unencrypted forms of the traffic.

- HIPS installations are vulnerable to fragmentation attacks or variable TTL attacks

114. What are three functions provided by the syslog service? (Choose three.)

- **to select the type of logging information that is captured**
- to periodically poll agents for data
- to provide statistics on packets that are flowing through a Cisco device
- to provide traffic analysis
- **to gather logging information for monitoring and troubleshooting**
- **to specify the destinations of captured messages**

Explanation: There are three primary functions provided by the syslog service:

1. gathering logging information
2. selection of the type of information to be logged
3. selection of the destination of the logged information

115. Which consideration is important when implementing syslog in a network?

- Enable the highest level of syslog available to ensure logging of all possible event messages.
- **Synchronize clocks on all network devices with a protocol such as Network Time Protocol.**
- Log all messages to the system buffer so that they can be displayed when accessing the router.
- Use SSH to access syslog information

116. What are the two ways threat actors use NTP? (Choose two.)

- They place an attachment inside an email message.
- **They attack the NTP infrastructure in order to corrupt the information used to log the attack.**
- They place iFrames on a frequently used corporate web page.
- They encode stolen data as the subdomain portion where the nameserver is under control of an attacker.

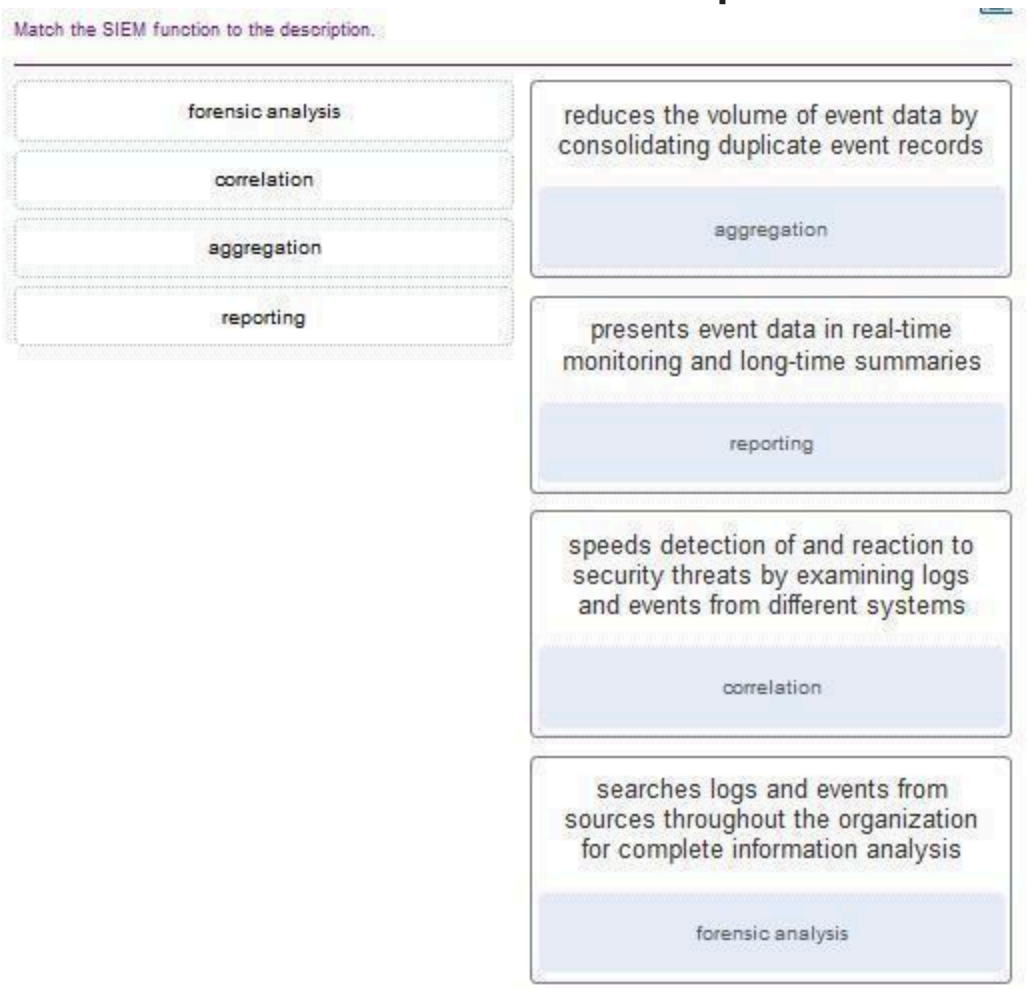
- **Threat actors use NTP systems to direct DDoS attacks.**

117. Which two features are included by both TACACS+ and RADIUS protocols? (Choose two.)

- password encryption
- **separate authentication and authorization processes**
- SIP support
- **utilization of transport layer protocols**
- 802.1X support

Explanation: Both TACACS+ and RADIUS support password encryption (TACACS+ encrypts all communication) and use Layer 4 protocol (TACACS+ uses TCP and RADIUS uses UDP). TACACS+ supports separation of authentication and authorization processes, while RADIUS combines authentication and authorization as one process. RADIUS supports remote access technology, such as 802.1x and SIP; TACACS+ does not.

118. Match the SIEM function to the description.



119. What are two types of attacks used on DNS open resolvers? (Choose two.)

- **amplification and reflection**
- fast flux
- ARP poisoning
- **resource utilization**
- cushioning

Explanation: Three types of attacks used on DNS open resolvers are as follows:DNS cache poisoning – attacker sends spoofed falsified information to redirect users from legitimate sites to malicious sites DNS amplification and reflection attacks – attacker sends an increased volume of attacks to mask the true source of the attack

DNS resource utilization attacks – a denial of service (DoS) attack that consumes server resources

120. Which host-based firewall uses a three-profile approach to configure the firewall functionality?

- iptables
- Windows Firewall
- **nftables**
- TCP Wrapper

121. Which protocol or service uses UDP for a client-to-server communication and TCP for server-to-server communication?

- HTTP
- FTP
- **DNS**
- SMTP

Explanation: Some applications may use both TCP and UDP. DNS uses UDP when clients send requests to a DNS server, and TCP when two DNS serves directly communicate.

122. Which two network protocols can be used by a threat actor to exfiltrate data in traffic that is disguised as normal network traffic? (Choose two.)

- NTP
- DNS
- HTTP
- syslog
- SMTP

123. What is a key difference between the data captured by NetFlow and data captured by Wireshark?

- NetFlow data shows network flow contents whereas Wireshark data shows network flow statistics.
- NetFlow data is analyzed by tcpdump whereas Wireshark data is analyzed by nfdump.
- NetFlow provides transaction data whereas Wireshark provides session data.

- NetFlow collects metadata from a network flow whereas Wireshark captures full data packets.

Explanation: Wireshark captures the entire contents of a packet. NetFlow does not. Instead, NetFlow collects metadata, or data about the flow.

124. Which tool captures full data packets with a command-line interface only?

- nfdump
- Wireshark
- NBAR2
- tcpdump

Explanation: The command-line tool tcpdump is a packet analyzer. Wireshark is a packet analyzer with a GUI interface.

125. Which method can be used to harden a device?

- maintain use of the same passwords
- allow default services to remain enabled
- allow USB auto-detection
- use SSH and disable the root account access over SSH

Explanation: The basic best practices for device hardening are as follows:
Ensure physical security.
Minimize installed packages.
Disable unused services.
Use SSH and disable the root account login over SSH.
Keep the system updated.
Disable USB auto-detection.
Enforce strong passwords.
Force periodic password changes.
Keep users from re-using old passwords.
Review logs regularly.

126. In a Linux operating system, which component interprets user commands and attempts to execute them?

- GUI
- daemon

- kernel
- shell

127. A network administrator is configuring an AAA server to manage RADIUS authentication. Which two features are included in RADIUS authentication? (Choose two.)

- encryption for all communication
- encryption for only the data
- single process for authentication and authorization
- separate processes for authentication and authorization
- hidden passwords during transmission

128. What is privilege escalation?

- Vulnerabilities in systems are exploited to grant higher levels of privilege than someone or some process should have.
- Everyone is given full rights by default to everything and rights are taken away only when someone abuses privileges.
- Someone is given rights because she or he has received a promotion.
- A security problem occurs when high ranking corporate officials demand rights to systems or files that they should not have.

Explanation: With privilege escalation, vulnerabilities are exploited to grant higher levels of privilege. After the privilege is granted, the threat actor can access sensitive information or take control of the system.

129. What two assurances does digital signing provide about code that is downloaded from the Internet? (Choose two.)

- The code contains no viruses.
- The code has not been modified since it left the software publisher.
- The code is authentic and is actually sourced by the publisher.
- The code contains no errors.
- The code was encrypted with both a private and public key.

Explanation: Digitally signing code provides several assurances about the code:
The code is authentic and is actually sourced by the publisher.
The code has not been modified since it left the software publisher.

The publisher undeniably published the code. This provides nonrepudiation of the act of publishing.

130. An IT enterprise is recommending the use of PKI applications to securely exchange information between the employees. In which two cases might an organization use PKI applications to securely exchange information between users? (Choose two.)

- HTTPS web service
- 802.1x authentication
- local NTP server
- FTP transfers
- file and directory access permission

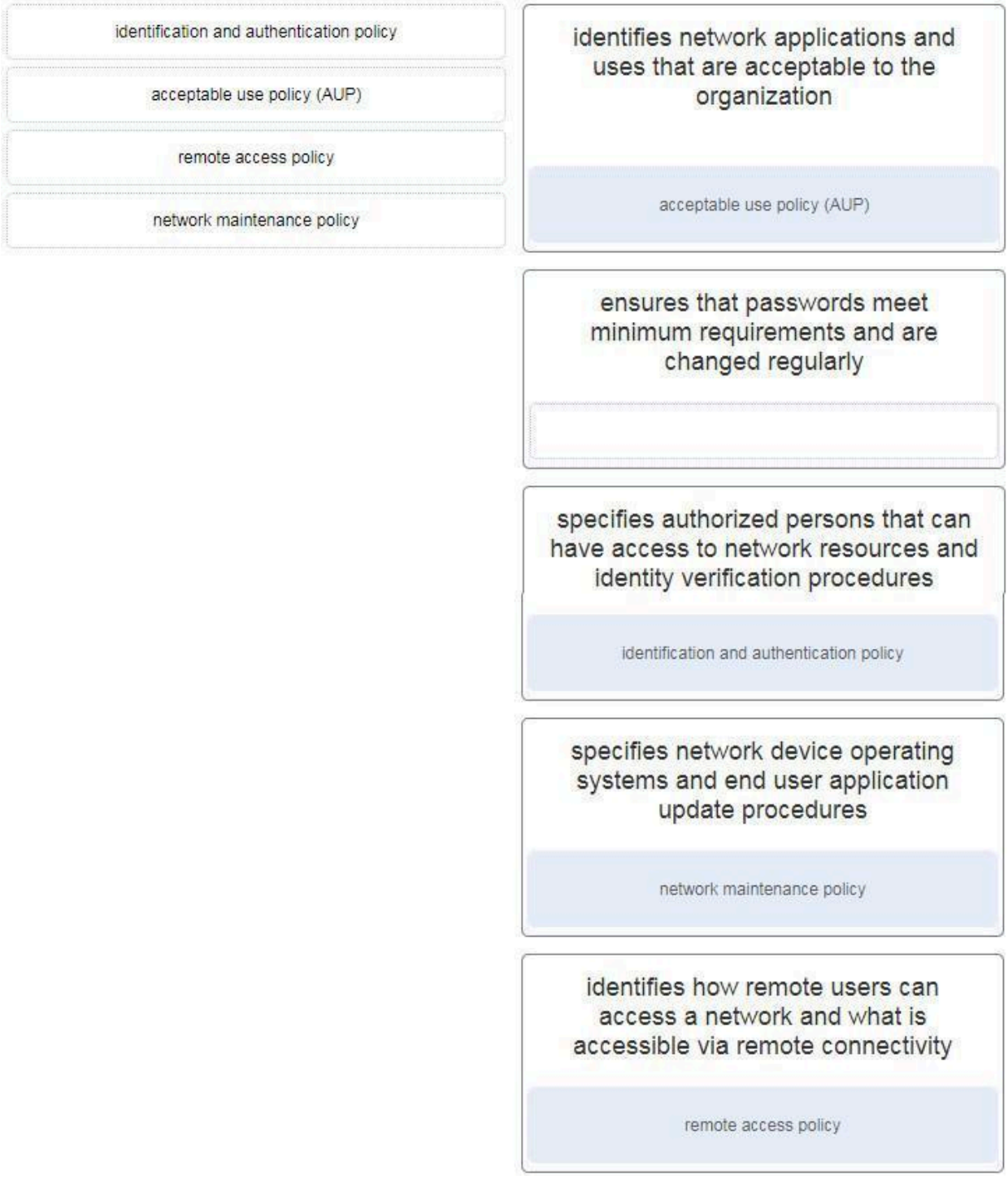
131. Which measure can a security analyst take to perform effective security monitoring against network traffic encrypted by SSL technology?

- Use a Syslog server to capture network traffic.
- Deploy a Cisco SSL Appliance.
- Require remote access connections through IPsec VPN.
- Deploy a Cisco ASA.

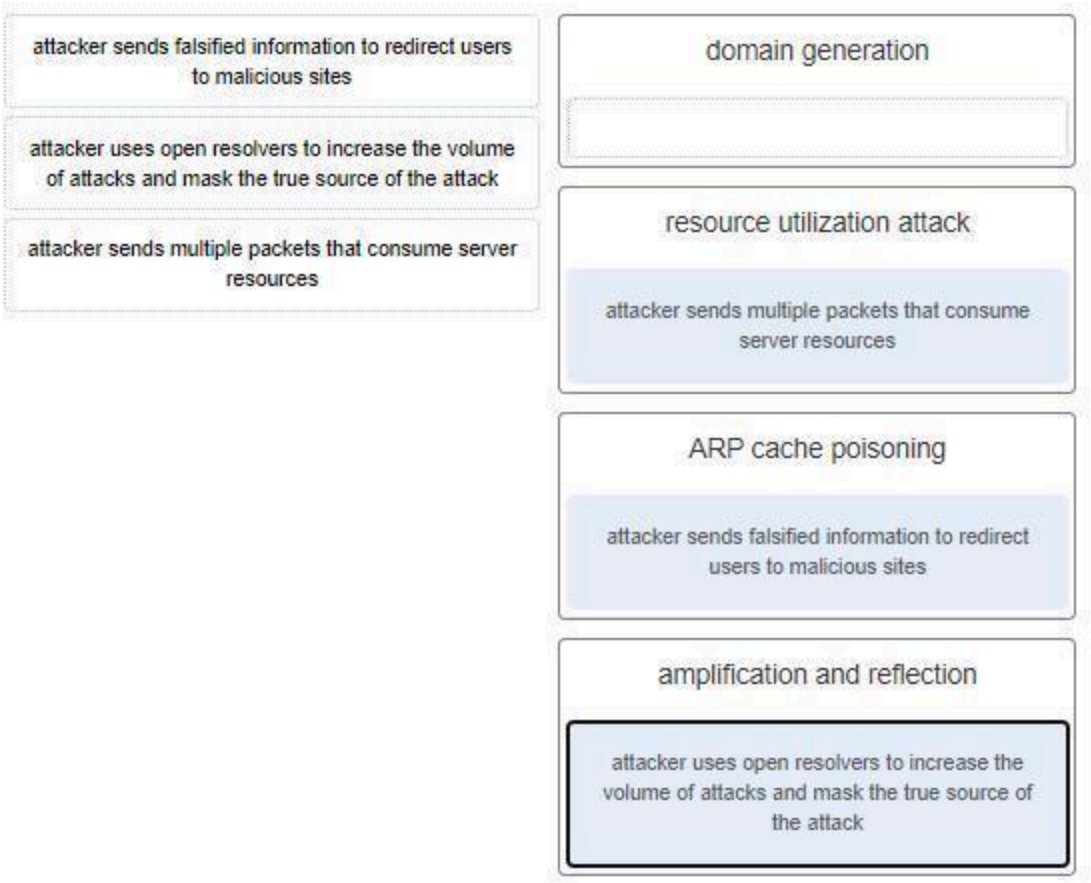
132. An administrator is trying to develop a BYOD security policy for employees that are bringing a wide range of devices to connect to the company network. Which three objectives must the BYOD security policy address? (Choose three.)

- All devices must be insured against liability if used to compromise the corporate network.
- All devices must have open authentication with the corporate network.
- Rights and activities permitted on the corporate network must be defined.
- Safeguards must be put in place for any personal device being compromised.
- The level of access of employees when connecting to the corporate network must be defined.
- All devices should be allowed to attach to the corporate network flawlessly.

133. Match the security policy with the description. (Not all options are used.)



134. Match the attack to the definition. (Not all options are used.)



135. What type of attack targets an SQL database using the input field of a user?

- XML injection
- buffer overflow
- Cross-site scripting
- SQL injection

Explanation: A criminal can insert a malicious SQL statement in an entry field on a website where the system does not filter the user input correctly.

136. What are two characteristics of Ethernet MAC addresses? (Choose two.)

- MAC addresses use a flexible hierarchical structure.
- They are expressed as 12 hexadecimal digits.
- They are globally unique.
- They are routable on the Internet.

- MAC addresses must be unique for both Ethernet and serial interfaces on a device.

137. A user calls to report that a PC cannot access the internet. The network technician asks the user to issue the command `ping 127.0.0.1` in a command prompt window. The user reports that the result is four positive replies. What conclusion can be drawn based on this connectivity test?

- The IP address obtained from the DHCP server is correct.
- The PC can access the network. The problem exists beyond the local network.
- The PC can access the Internet. However, the web browser may not work.
- The TCP/IP implementation is functional.

138. What characterizes a threat actor?

- They are all highly-skilled individuals.
- They always use advanced tools to launch attacks.
- They always try to cause some harm to an individual or organization.
- They all belong to organized crime.

139. A computer is presenting a user with a screen requesting payment before the user data is allowed to be accessed by the same user. What type of malware is this?

- a type of logic bomb
- a type of virus
- a type of worm
- a type of ransomware

Explanation: Ransomware commonly encrypts data on a computer and makes the data unavailable until the computer user pays a specific sum of money

140. Which ICMPv6 message type provides network addressing information to hosts that use SLAAC?

- router solicitation
- neighbor advertisement

- neighbor solicitation
- router advertisement

141. A client is using SLAAC to obtain an IPv6 address for the interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

- It must wait for an ICMPv6 Router Advertisement message giving permission to use this address.
- It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.
- It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.
- It must send an ICMPv6 Router Solicitation message to request the address of the DNS server.

142. Which two types of unreadable network traffic could be eliminated from data collected by NSM? (Choose two.)

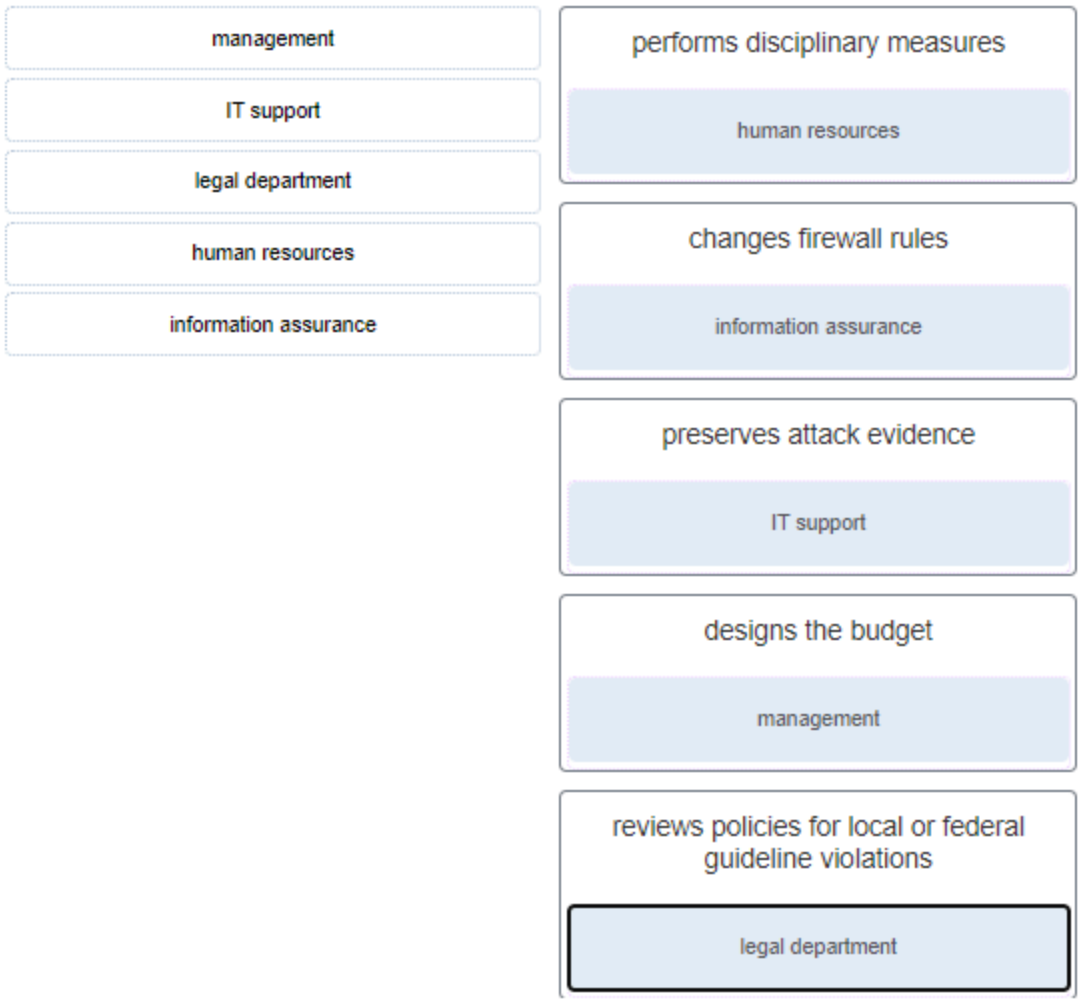
- STP traffic
- IPsec traffic
- routing updates traffic
- SSL traffic
- broadcast traffic

Explanation: To reduce the huge amount of data collected so that cybersecurity analysts can focus on critical threats, some less important or unusable data could be eliminated from the datasets. For example, encrypted data, such as IPsec and SSL traffic, could be eliminated because it is unreadable in a reasonable time frame.

143. Which core open source component of the Elastic-stack is responsible for accepting the data in its native format and making elements of the data consistent across all sources?

- Logstash
- Kibana
- Beats
- Elasticsearch

144. Match the security incident stakeholder with the role.

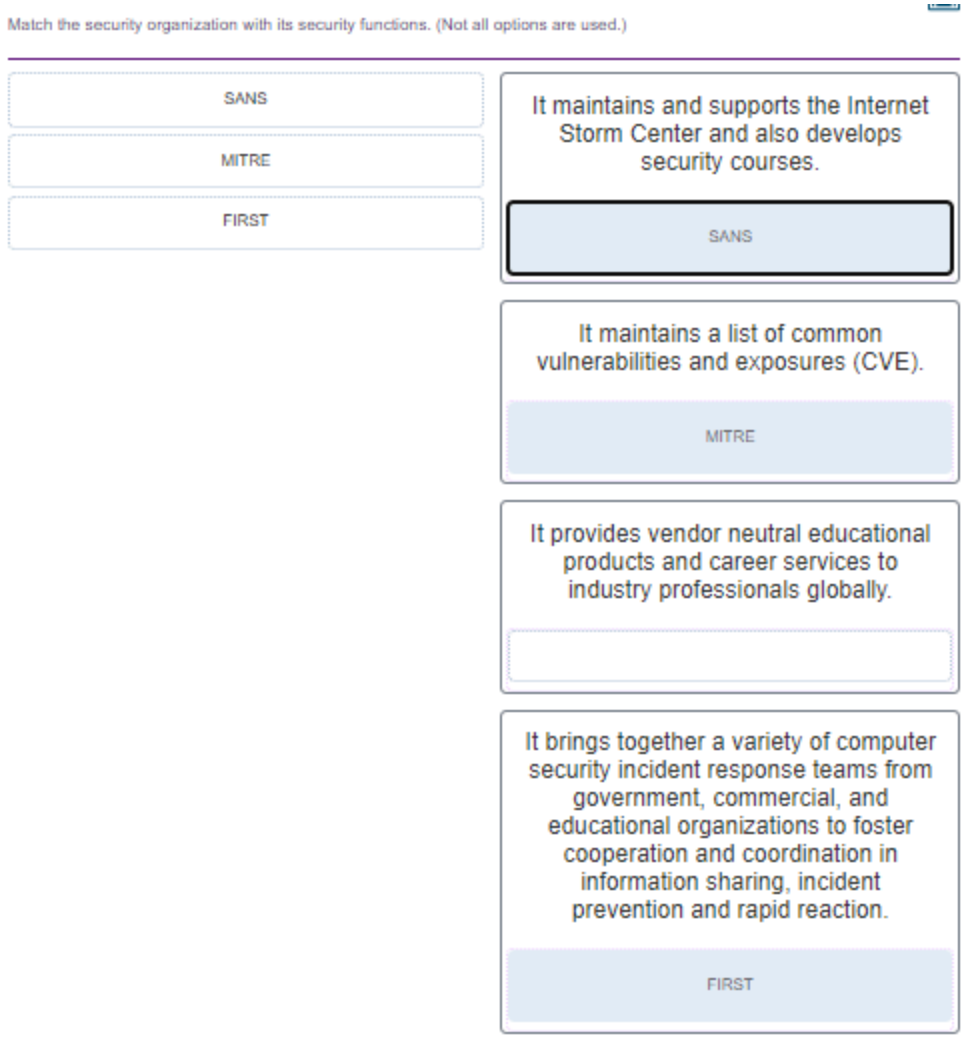


145. In the NIST incident response process life cycle, which type of attack vector involves the use of brute force against devices, networks, or services?

- media
- impersonation
- attrition
- loss or theft

Explanation: Common attack vectors include media, attrition, impersonation, and loss or theft. Attrition attacks are any attacks that use brute force. Media attacks are those initiated from storage devices. Impersonation attacks occur when something or someone is replaced for the purpose of the attack, and loss or theft attacks are initiated by equipment inside the organization.

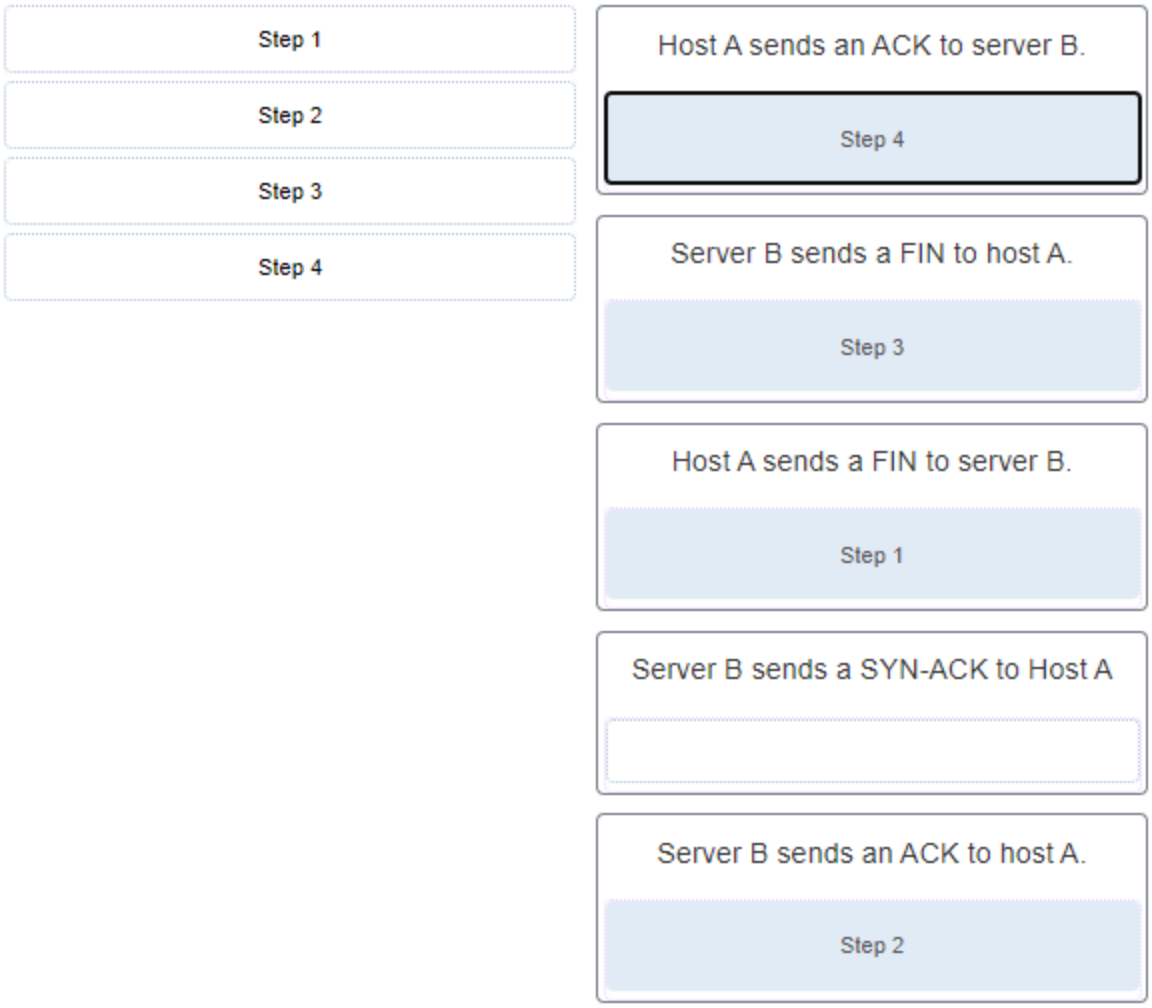
146. Match the security organization with its security functions. (Not all options are used.)



147. What is a characteristic of CybOX?

- It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations.
- It enables the real-time exchange of cyberthreat indicators between the U.S. Federal Government and the private sector.
- It is a set of specifications for exchanging cyberthreat information between organizations.
- It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.

148. After host A receives a web page from server B, host A terminates the connection with server B. Match each step to its correct option in the normal termination process for a TCP connection. (Not all options are used.)



149. What are two ways that ICMP can be a security threat to a company? (Choose two.)

- by collecting information about a network
- by corrupting data between email servers and email recipients
- by the infiltration of web pages
- by corrupting network IP data packets
- by providing a conduit for DoS attacks

Explanation: ICMP can be used as a conduit for DoS attacks. It can be used to collect information about a network such as the identification of

hosts and network structure, and by determining the operating systems being used on the network.

150. Which three IPv4 header fields have no equivalent in an IPv6 header? (Choose three.)

- fragment offset
- protocol
- flag
- TTL
- identification
- version

Explanation: Unlike IPv4, IPv6 routers do not perform fragmentation. Therefore, all three fields supporting fragmentation in the IPv4 header are removed and have no equivalent in the IPv6 header. These three fields are fragment offset, flag, and identification. IPv6 does support host packet fragmentation through the use of extension headers, which are not part of the IPv6 header.

151. An administrator discovers that a user is accessing a newly established website that may be detrimental to company security. What action should the administrator take first in terms of the security policy?

- Ask the user to stop immediately and inform the user that this constitutes grounds for dismissal.
- Create a firewall rule blocking the respective website.
- **Revise the AUP immediately and get all users to sign the updated AUP.**
- Immediately suspend the network privileges of the user.

1. Which tool is included with Security Onion that is used by Snort to automatically download new rules?

- **PulledPork**
- ELK
- Wireshark
- Sguil

2. Which tool included in Security Onion is an interactive dashboard interface to Elasticsearch data?

- Zeek
- Wireshark
- **Kibana**
- Sguil

3. A NIDS/NIPS has identified a threat. Which type of security data will be generated and sent to a logging device?

- alert
- session
- **statistical**
- transaction

4. Which statement describes an operational characteristic of NetFlow?

- NetFlow captures the entire contents of a packet.
- NetFlow can provide services for user access control.
- **NetFlow collects basic information about the packet flow, not the flow data itself.**
- NetFlow flow records can be viewed by the tcpdump tool.

5. Which regular expression would match any string that contains 4 consecutive zeros?

- {0-4}
- [0-4]
- **0{4}**
- ^0000

Explanation: The regular expression 0{4} matches any string that contains 4 repetitions of zero or 4 consecutive zeros.

6. Refer to the exhibit. Which technology generated the event log?

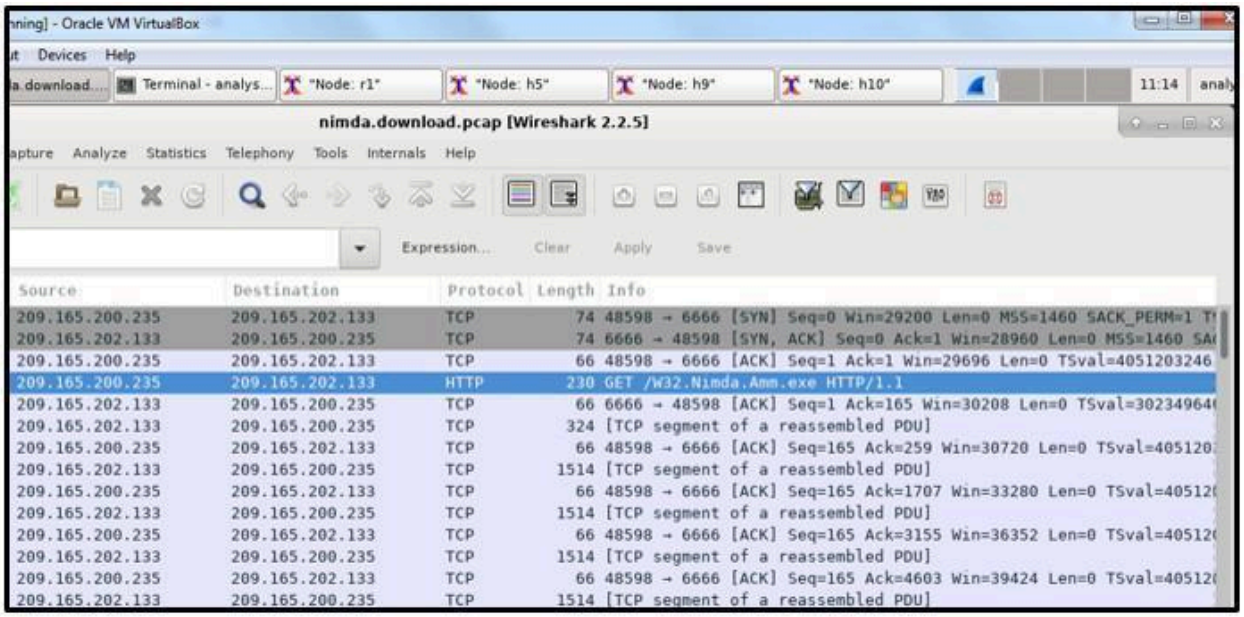
```
Traffic Contribution: 8% (3/37)

Flow information:
IPV4 SOURCE ADDRESS:            10.1.1.2
IPV4 DESTINATION ADDRESS:       13.1.1.2
INTERFACE INPUT:      Se0/0/1
TRNS SOURCE PORT:     8974
TRNS DESTINATION PORT:          80
IP TOS:               0x00
IP PROTOCOL:                    6
FLOW SAMPLER ID:      0
FLOW DIRECTION:       Input
ipv4 source mask:     /0
ipv4 destination mask:          /8
counter bytes:                  205
ipv4 next hop address:          13.1.1.2
tcp flags:                      0x1b
interface output:     Fa0/0
counter packets:      5
timestamp first:                00:09:12.596
timestamp last:                 00:09:12.606
ip source as:                   0
```

- Wireshark
- **Netflow**
- web proxy
- syslog

Explanation: The source of the output is Netflow.

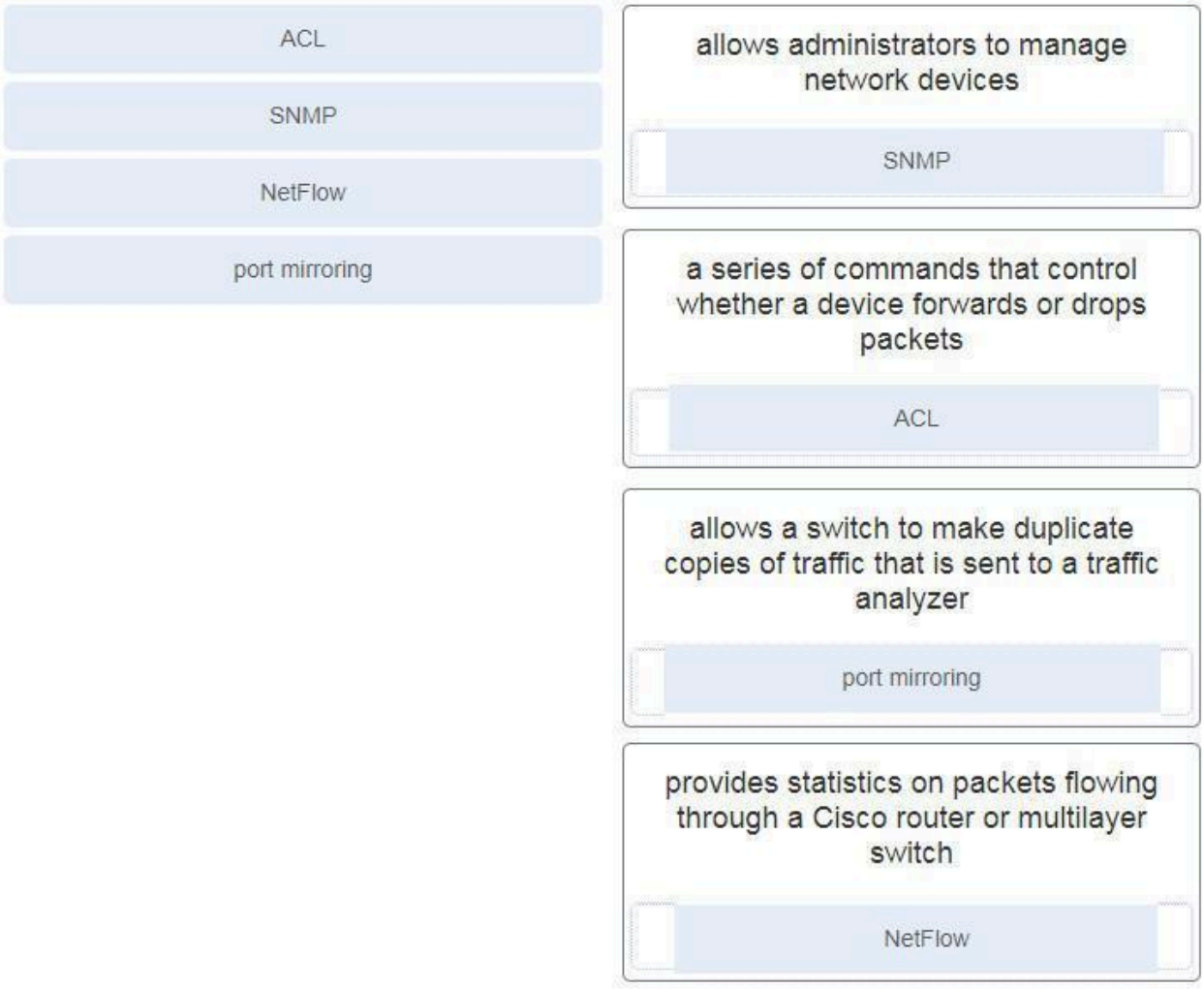
7. Refer to the exhibit. A security specialist is using Wireshark to review a PCAP file generated by tcpdump. When the client initiated a file download request, which source socket pair was used?



- 209.165.202.133:48598
- 209.165.202.133:6666
- 209.165.200.235:6666
- **209.165.200.235:48598**

Explanation: The combination of the source IP address and source port number, or the destination IP address and destination port number, is known as a socket. A socket is shown as the IP address and associated port number with a colon in between the two (IP_address:port_number).

8. Match the security service with the description.

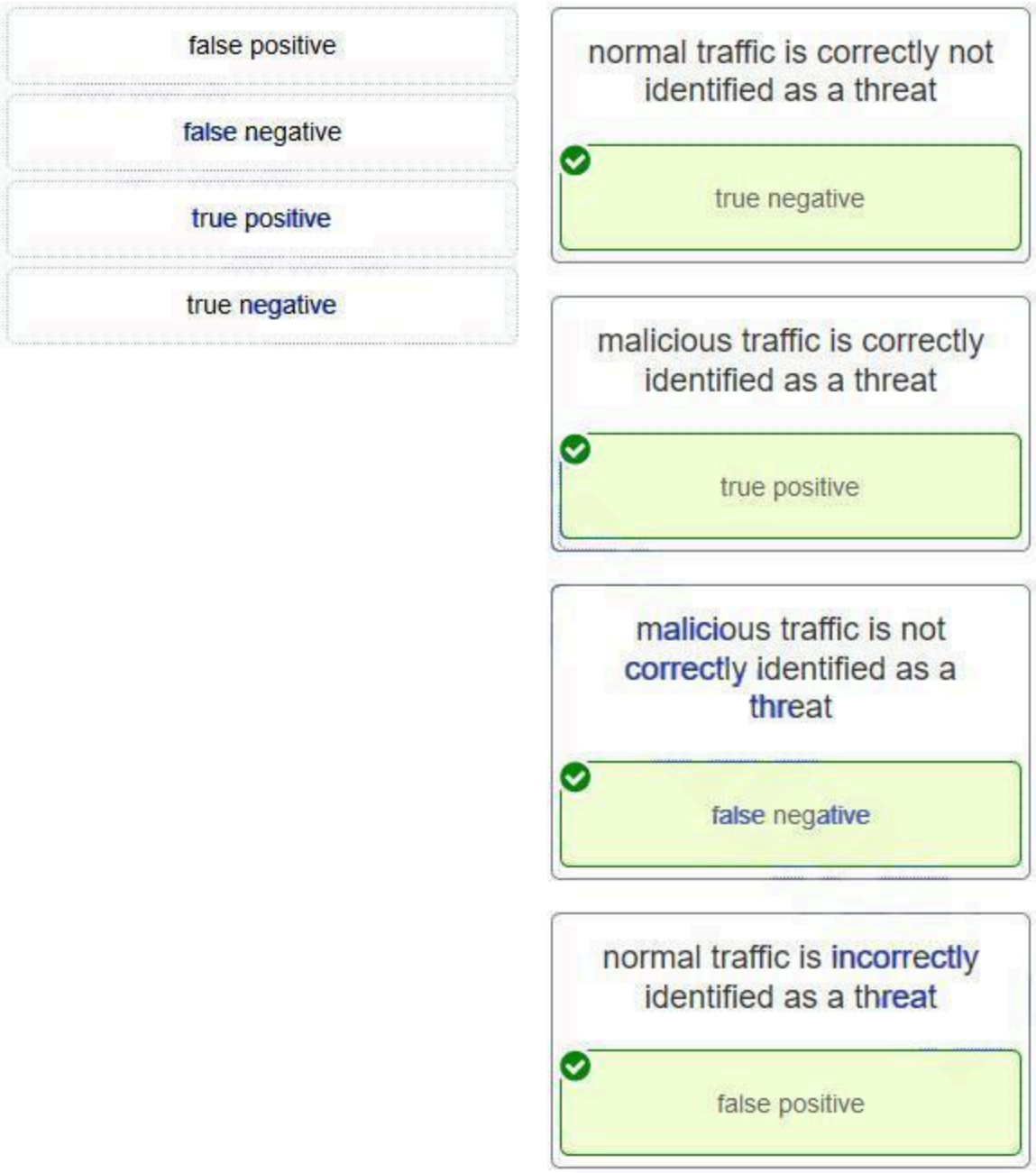


9. Using Tcpdump and Wireshark, a security analyst extracts a downloaded file from a pcap file. The analyst suspects that the file is a virus and wants to know the file type for further examination. Which Linux command can be used to determine the file type?

- **file**
- tail
- nano
- ls -l

Explanation: The Linux file command can be used to determine a file type, such as whether it is executable, ASCII text, or zip.

10. Match the IPS alarm with the description.



11. What is a feature of an IPS?

- **It can stop malicious packets.**
- It is deployed in offline mode.
- It has no impact on latency.
- It is primarily focused on identifying possible incidents.

Explanation: An advantage of an intrusion prevention systems (IPS) is that it can identify and stop malicious packets. However, because an IPS is deployed inline, it can add latency to the network.

12. Which three fields are found in both the TCP and UDP headers? (Choose three.)

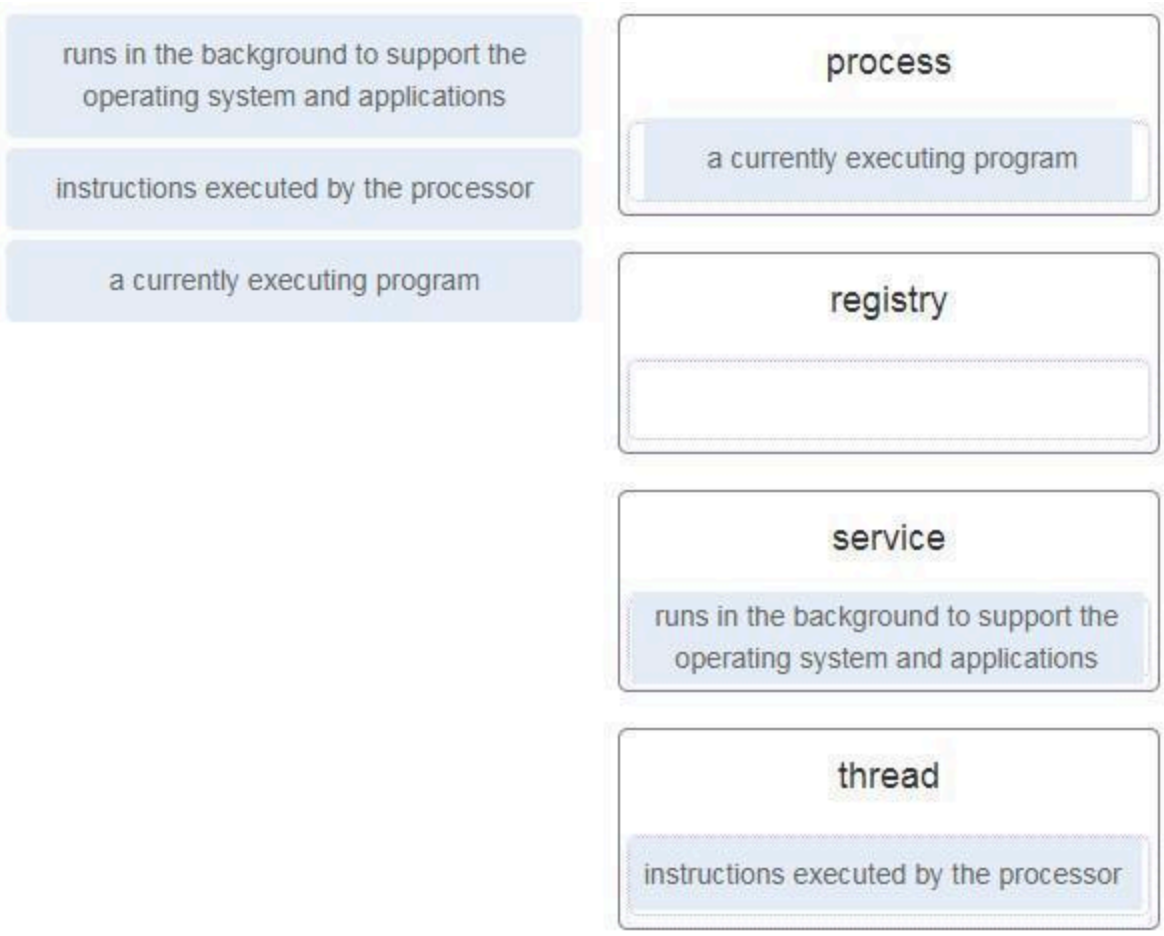
- window
- **checksum**
- options
- sequence number
- **destination port**
- **source port**

Explanation: The UPD header has four fields. Three of these fields are in common with the TCP header. These three fields are the source port, destination port, and checksum.

13. Match the definition to the Microsoft Windows term. (Not all options are used.)


database of hardware, software, users, and settings
used to manage remote computers
provides access needed by the user space process
handle
provides access needed by the user space process
registry
database of hardware, software, users, and settings
thread
WMI
used to manage remote computers

Case 2



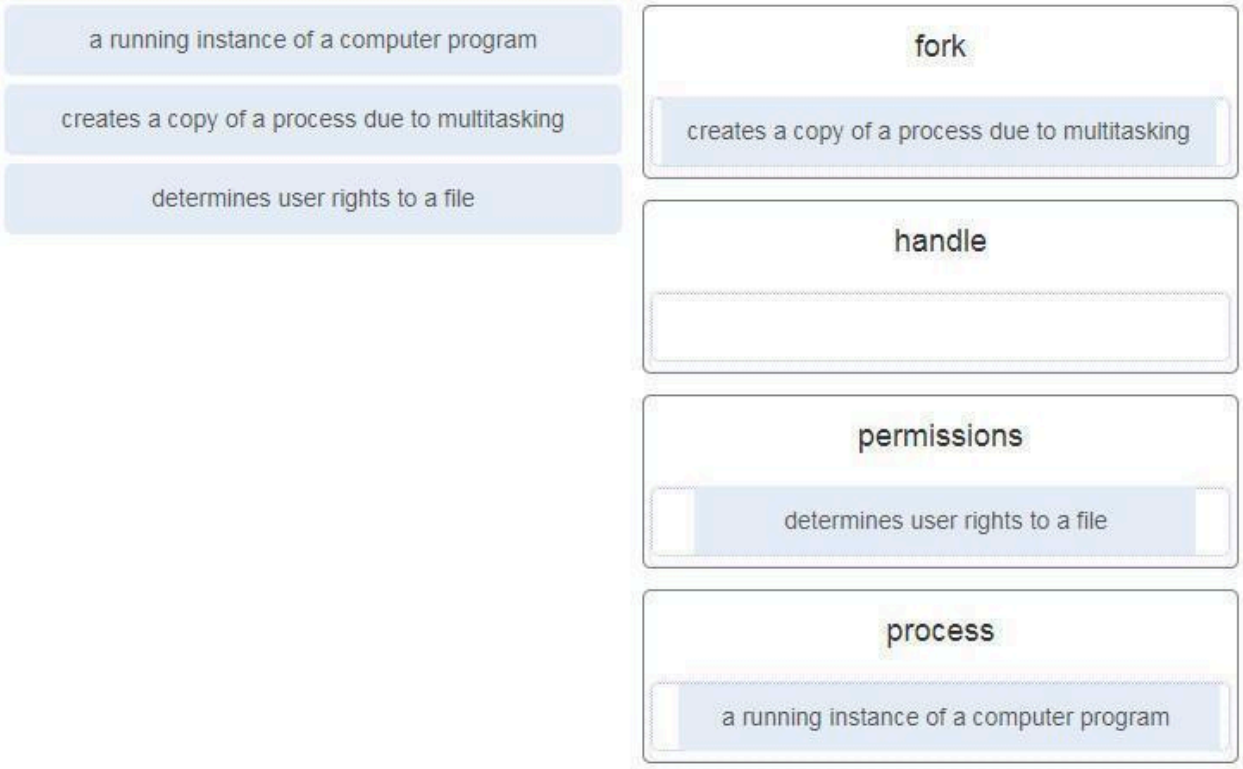
Match the definition to the Microsoft Windows term. (Not all options are used.)

14. What are two motivating factors for nation-state sponsored threat actors? (Choose two.)

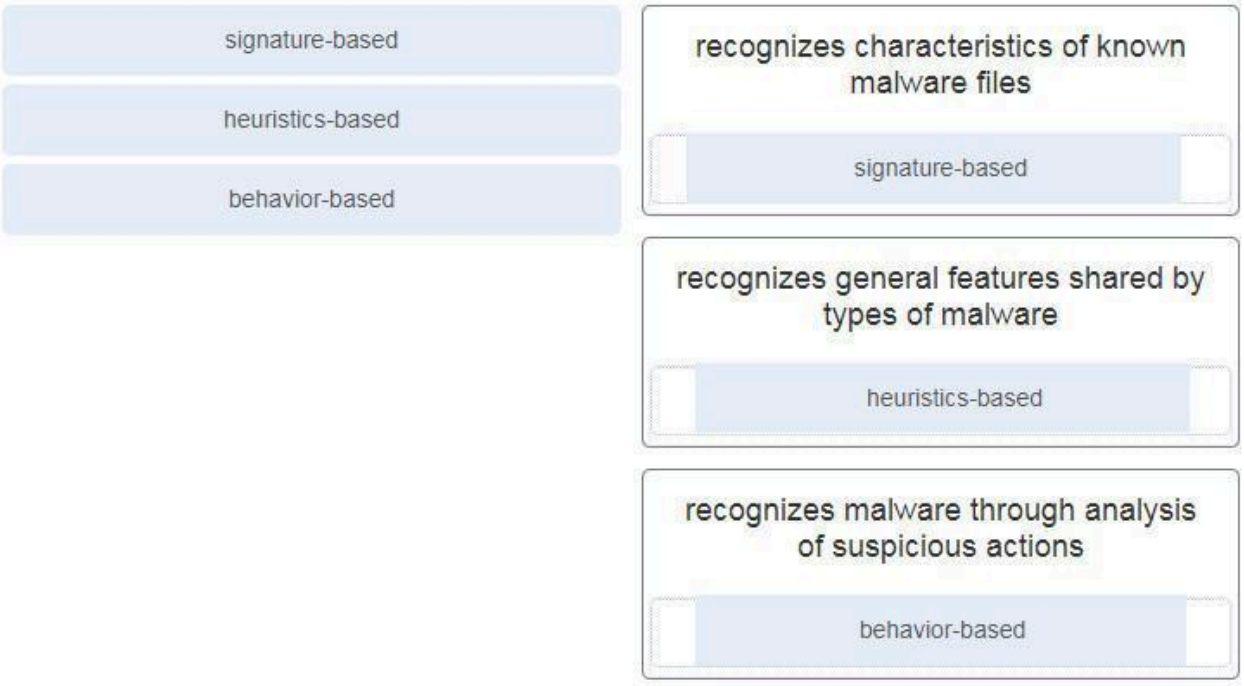
- **industrial espionage**
- showing off their hacking skill
- **disruption of trade or infrastructure**
- social or personal causes
- financial gain

Explanation: Nation-state threat actors are not typically interested or motivated by financial gain. They are primarily involved in corporate espionage or disrupting international trade or critical infrastructure.

15. Match the description to the Linux term. (Not all options are used.)



16. Match the antimalware approach to the description.



17. Which type of data is used by Cisco Cognitive Intelligence to find malicious activity that has bypassed security controls, or entered

through unmonitored channels, and is operating inside an enterprise network?

- **statistical**
- session
- alert
- transaction

Explanation: Cisco Cognitive Intelligence utilizes statistical data for statistical analysis in order to find malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside the network of an organization.

18. Which type of evasion technique splits malicious payloads into smaller packets in order to bypass security sensors that do not reassemble the payloads before scanning them?

- pivoting
- **traffic fragmentation**
- protocol-level misinterpretation
- traffic insertion

Explanation: In order to keep the malicious payload from being recognized by security sensors, such as IPS or IDS, perpetrators fragment the data into smaller packets.These fragments can be passed by sensors that do not reassemble the data before scanning.

19. Which type of cyber attack is a form of MiTM in which the perpetrator copies IP packets off the network without modifying them?

- compromised key
- **eavesdropping**
- denial-of-service
- IP spoofing

Explanation: An eavesdropping attack is a form of man-in-the-middle in which the perpetrator just reads or copies IP packets off the network but does not alter them.

20. Which is an example of social engineering?

- an anonymous programmer directing a DDoS attack on a data center
- **an unidentified person claiming to be a technician collecting user information from employees**
- a computer displaying unauthorized pop-ups and adware
- the infection of a computer by a virus carried by a Trojan

Explanation: A social engineer attempts to gain the confidence of an employee and convince that person to divulge confidential and sensitive information, such as usernames and passwords. DDoS attacks, pop-ups, and viruses are all examples of software based security threats, not social engineering.

21. Which type of analysis relies on different methods to establish the likelihood that a security event has happened or will happen?

- deterministic
- statistical
- log
- **probabilistic**

Explanation: Probabilistic methods use powerful tools to create a probabilistic answer as a result of analyzing applications.

22. Which access control model allows users to control access to data as an owner of that data?

- mandatory access control
- nondiscretionary access control
- **discretionary access control**
- attribute-based access control

Explanation: In the discretionary access control (DAC) model, users can control access to data as owners of the data.

23. What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)

- **confidentiality**
- remediation level
- **integrity**
- attack vector
- exploit

- **availability**

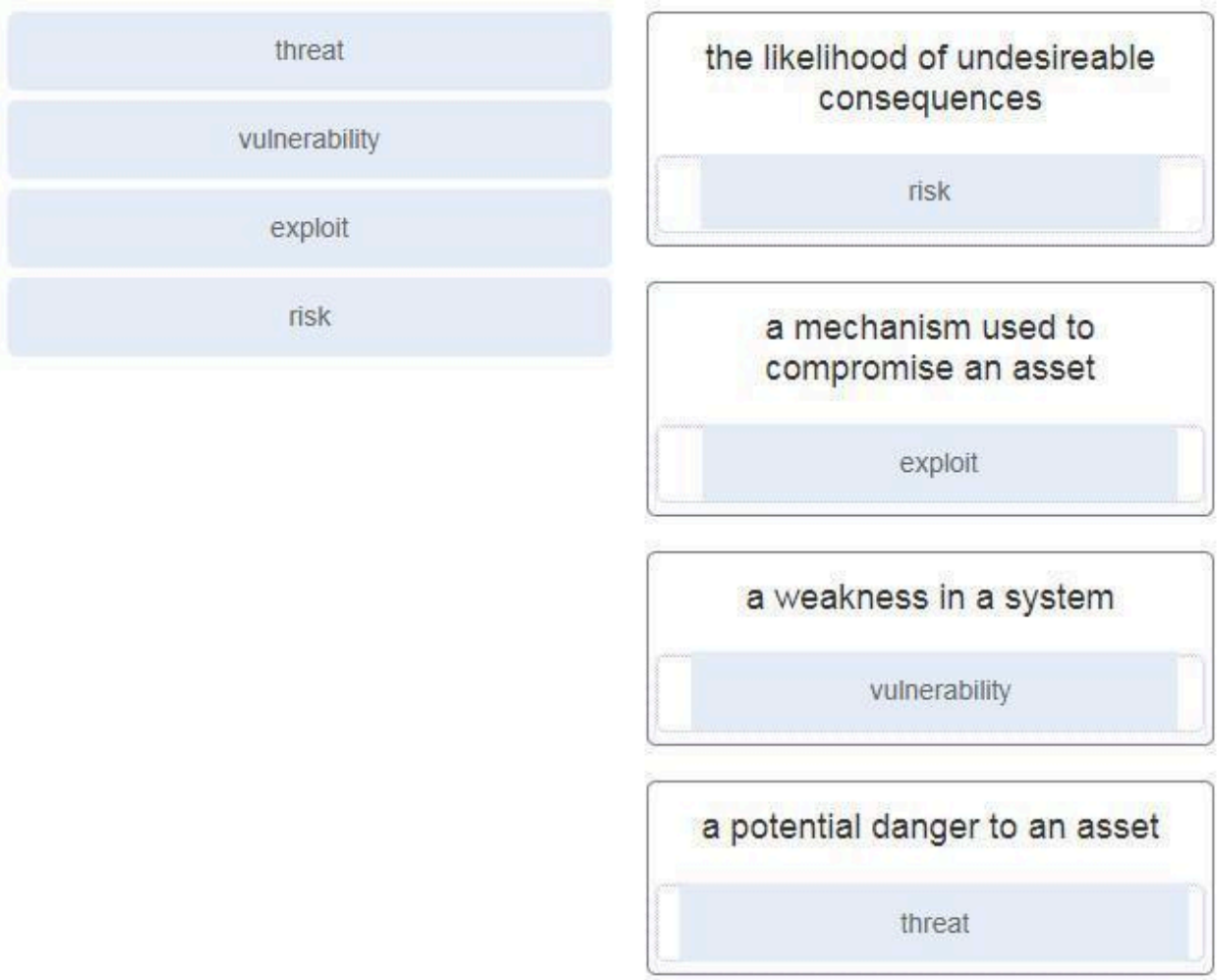
Explanation: The Common Vulnerability Scoring System (CVSS) is a vendor-neutral, industry standard, open framework for weighing the risks of a vulnerability using a variety of metrics. CVSS uses three groups of metrics to assess vulnerability, the Base Metric Group, Temporal Metric Group, and Environmental Metric Group. The Base Metric Group has two classes of metrics (exploitability and impact). The impact metrics are rooted in the following areas: confidentiality, integrity, and availability.

24. Which access control model applies the strictest access control and is often used in military and mission critical applications?

- discretionary
- **mandatory**
- nondiscretionary
- attribute-based

Explanation: Military and mission critical applications typically use mandatory access control which applies the strictest access control to protect network resources.

25. Match the security concept to the description.

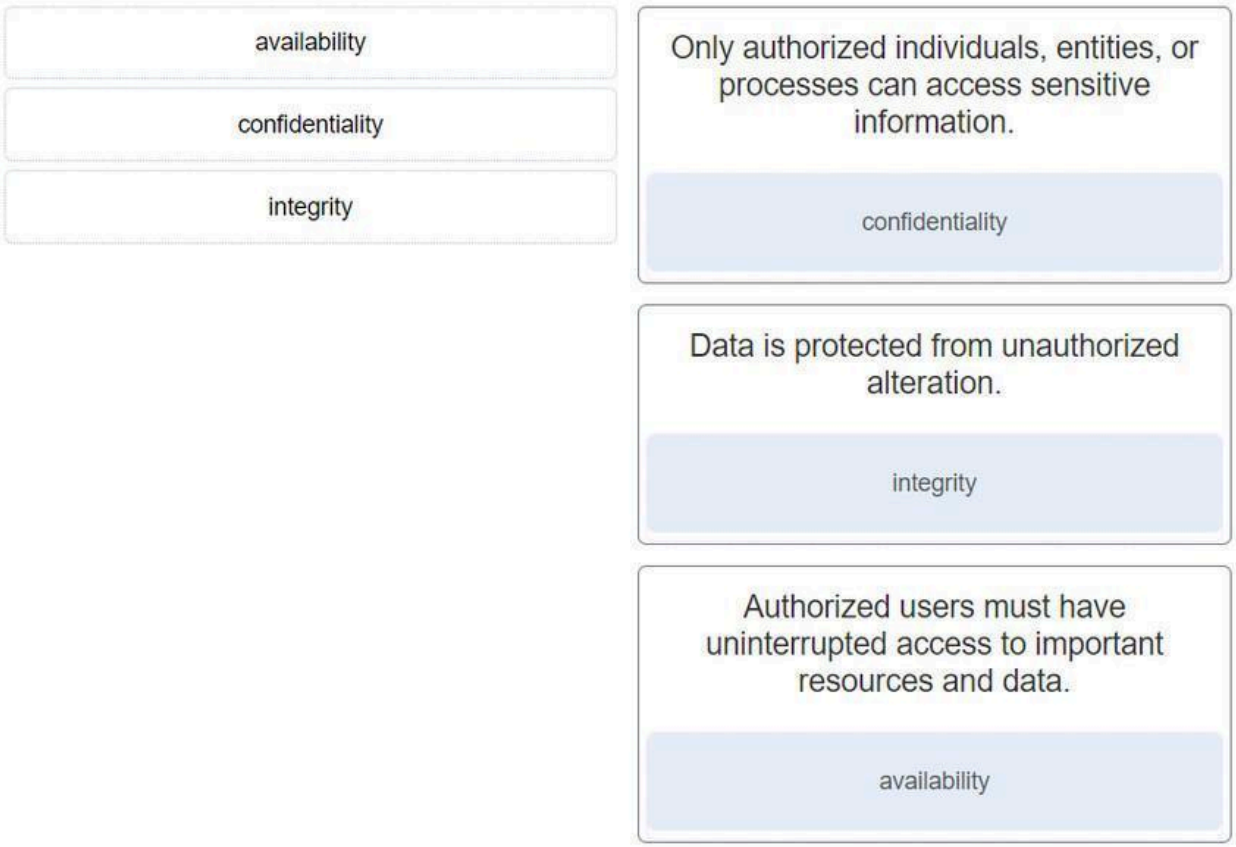


26. What is the principle behind the nondiscretionary access control model?

- It applies the strictest access control possible.
- **It allows access decisions to be based on roles and responsibilities of a user within the organization.**
- It allows users to control access to their data as owners of that data.
- It allows access based on attributes of the object be to accessed.

Explanation: The nondiscretionary access control model used the roles and responsibilities of the user as the basis for access decisions.

27. Match the information security component with the description.



28. Which attack is integrated with the lowest levels of the operating system of a host and attempts to completely hide the activities of the threat actor on the local system?

- **rootkit**
- traffic insertion
- traffic substitution
- encryption and tunneling

Explanation: A rootkit is a complex attack tool and it integrates with the lowest levels of the operating system. The goal of the rootkit is to completely hide the activities of the threat actor on the local system.

29. Which tool captures full data packets with a command-line interface only?

- nfdump
- NBAR2
- **tcpdump**

- Wireshark

Explanation: The command-line tool tcpdump is a packet analyzer. Wireshark is a packet analyzer with a GUI interface.

30. To which category of security attacks does man-in-the-middle belong?

- DoS
- **access**
- reconnaissance
- social engineering

Explanation: With a man-in-the-middle attack, a threat actor is positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.

31. What is an example of a local exploit?

- Port scanning is used to determine if the Telnet service is running on a remote server.
- A threat actor performs a brute force attack on an enterprise edge router to gain illegal access.
- A buffer overflow attack is launched against an online shopping website and causes the server crash.
- **A threat actor tries to gain the user password of a remote host by using a keyboard capture software installed on it by a Trojan.**

Explanation: Vulnerability exploits may be remote or local. In a local exploit, the threat actor has some type of user access to the end system, either physically or through remote access. The exploitation activity is within the local network.

32. Which Cisco appliance can be used to filter network traffic contents to report and deny traffic based on the web server reputation?

- **WSA**
- AVC
- ASA
- ESA

Explanation: The Cisco Web Security Appliance (WSA) acts as a web proxy for an enterprise network. WSA can provide many types of logs related to web traffic security including ACL decision logs, malware scan logs, and web reputation filtering logs. The Cisco Email Security Appliance (ESA) is a tool to monitor most aspects of email delivery, system functioning, antivirus, antispam operations, and blacklist and whitelist decisions. The Cisco ASA is a firewall appliance. The Cisco Application Visibility and Control (AVC) system combines multiple technologies to recognize, analyze, and control over 1000 applications.

33. Which evasion method describes the situation that after gaining access to the administrator password on a compromised host, a threat actor is attempting to login to another host using the same credentials?

- **pivoting**
- traffic substitution
- resource exhaustion
- protocol-level misinterpretation

Explanation: Pivoting is an evasion method that assumes the threat actor has compromised an inside host and the actor wants to expand the access further into the compromised network.

34. What are two examples of DoS attacks? (Choose two.)

- port scanning
- SQL injection
- **ping of death**
- phishing
- **buffer overflow**

Explanation: The buffer overflow and ping of death DoS attacks exploit system memory-related flaws on a server by sending an unexpected amount of data or malformed data to the server.

35. Which type of attack is carried out by threat actors against a network to determine which IP addresses, protocols, and ports are allowed by ACLs?

- social engineering
- denial of service
- phishing

- **reconnaissance**

Explanation: Packet filtering ACLs use rules to filter incoming and outgoing traffic. These rules are defined by specifying IP addresses, port numbers, and protocols to be matched. Threat actors can use a reconnaissance attack involving port scanning or penetration testing to determine which IP addresses, protocols, and ports are allowed by ACLs.

36. Refer to the exhibit. A security analyst is reviewing an alert message generated by Snort. What does the number 2100498 in the message indicate?

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown;
sid:2100498; rev:8;)
```

- the id of the user that triggers the alert
- the message length in bits
- **the Snort rule that is triggered**
- the session number of the message

Explanation: The sid field in a Snort alert message indicates the Snort security rule that is triggered.

37. Which two attacks target web servers through exploiting possible vulnerabilities of input functions used by an application? (Choose two.)

- **SQL injection**
- port scanning
- port redirection
- trust exploitation
- **cross-site scripting**

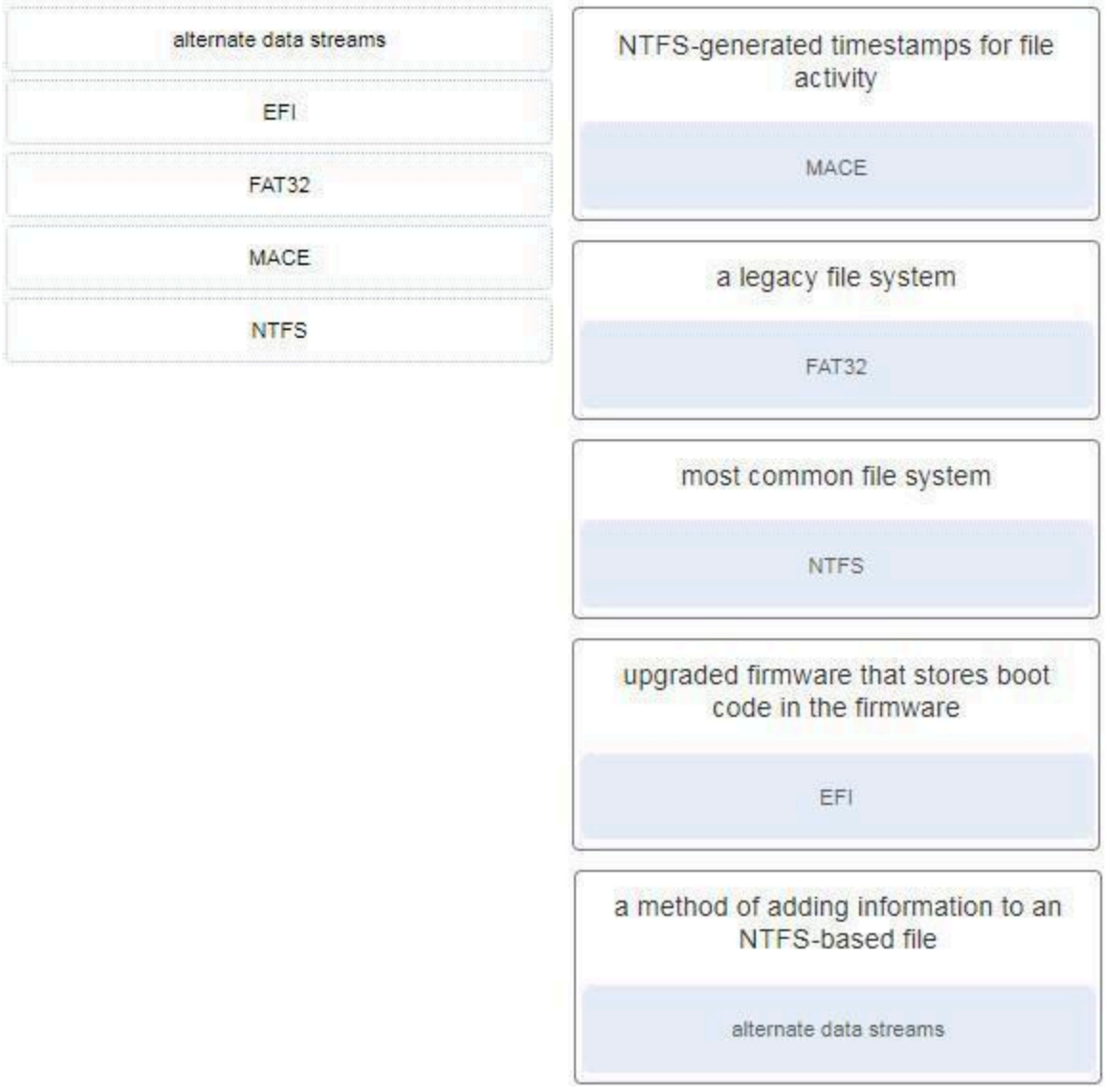
Explanation: When a web application uses input fields to collect data from clients, threat actors may exploit possible vulnerabilities for entering malicious commands. The malicious commands that are executed through the web application might affect the OS on the web server. SQL injection and cross-site scripting are two different types of command injection attacks.

38. Which security function is provided by encryption algorithms?

- key management
- authorization
- integrity
- **confidentiality**

Explanation: Encryption algorithms are used to provide data confidentiality, which ensures that if data is intercepted in transit, it cannot be read.

39. Match the Windows term to the description.

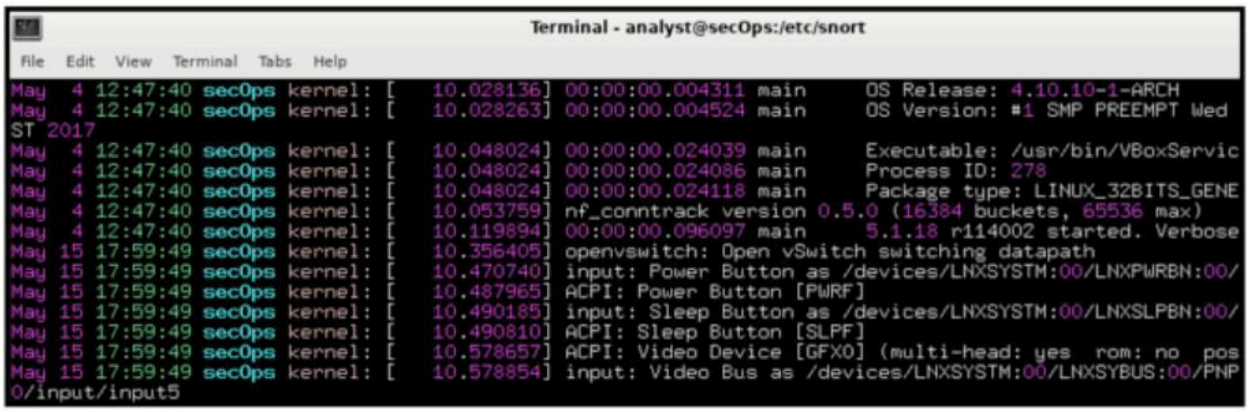


40. Which security endpoint setting would be used by a security analyst to determine if a computer has been configured to prevent a particular application from running?

- baselining
- **blacklisting**
- services
- whitelisting

Explanation: Blacklisting can be used on a local system or updated on security devices such as a firewall. Blacklists can be manually entered or obtained from a centralized security system. Blacklists are applications that are prevented from executing because they pose a security risk to the individual system and potentially the company.

41. Refer to the exhibit. Which technology would contain information similar to the data shown for infrastructure devices within a company?



- Apache server
- firewall
- HIDS
- **syslog server**

Explanation: A syslog server consolidates and maintains messages from infrastructure devices that have been configured to send logging information. Data from the syslog server can be analyzed to detect anomalies.

42. At the request of investors, a company is proceeding with cyber attribution with a particular attack that was conducted from an

external source. Which security term is used to describe the person or device responsible for the attack?

- **threat actor**
- fragmenter
- tunneler
- skeleton

Explanation: Some people may use the common word of "hacker" to describe a threat actor. A threat actor is an entity that is involved with an incident that impacts or has the potential to impact an organization in such a way that it is considered a security risk or threat.

43. Which Windows application is commonly used by a cybersecurity analyst to view Microsoft IIS access logs?

- **Event Viewer**
- Notepad
- SIEM
- Word

Explanation: Event Viewer is an application on a Windows-based device used to view event logs including IIS access logs.

44. Which two algorithms use a hashing function to ensure message integrity? (Choose two.)

- SEAL
- AES
- 3DES
- **MD5**
- **SHA**

Explanation: Hashing algorithms are used to provide data integrity, which ensures that the data has not changed during transmission. MD5 and SHA are commonly used hashing algorithms.

45. Which type of evidence cannot prove an IT security fact on its own?

- best
- corroborative
- **indirect**

- hearsay

Explanation: Indirect evidence cannot prove a fact on its own, but direct evidence can. Corroborative evidence is supporting information. Best evidence is most reliable because it is something concrete such as a signed contract.

46. What is an example of privilege escalation attack?

- A DDoS attack is launched against a government server and causes the server to crash.
- A port scanning attack finds that the FTP service is running on a server that allows anonymous access.
- **A threat actor performs an access attack and gains the administrator password.**
- A threat actor sends an email to an IT manager to request the root access.

Explanation: With the privilege escalation exploit, vulnerabilities in servers or access control systems are exploited to grant an unauthorized user, or software process, higher levels of privilege than either should have. After the higher privilege is granted, the threat actor can access sensitive information or take control of a system.

47. A threat hunter is concerned about a significant increase in TCP traffic sourced from port 53. It is suspected that malicious file transfer traffic is being tunneled out using the TCP DNS port. Which deep packet inspection tool can detect the type of application originating the suspicious traffic?

- syslog analyzer
- **NBAR2**
- NetFlow
- IDS/IPS
- Wireshark

Explanation: NBAR2 is used to discover the applications that are responsible for network traffic. NBAR is a classification engine that can recognize a wide variety of applications, including web-based applications and client/server applications.

48. Which type of evaluation includes the assessment of the likelihood of an attack, the type of threat actor likely to perpetrate

such an attack, and what the consequences could be to the organization if the exploit is successful?

- penetration testing
- **risk analysis**
- vulnerability identification
- server profiling

49. When establishing a network profile for an organization, which element describes the time between the establishment of a data flow and its termination?

- **session duration**
- total throughput
- routing protocol convergence
- bandwidth of the Internet connection

Explanation: A network profile should include some important elements, such as the following:

- **Total throughput** – the amount of data passing from a given source to a given destination in a given period of time
- **Session duration** – the time between the establishment of a data flow and its termination
- **Ports used** – a list of TCP or UDP processes that are available to accept data
- **Critical asset address space** – the IP addresses or the logical location of essential systems or data

50. Which term describes a threat actor who has advanced skills and pursues a social agenda?

- organized crime
- script kiddie
- corporate/industrial spies
- **hacktivist**

51. Refer to the exhibit. A security specialist is checking if files in the directory contain ADS data. Which switch should be used to show that

a file has ADS attached?

```
Microsoft Windows [Version 10.0.16299.19]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\User\Public> dir <switch>
```

- /a
- **/r**
- /d
- /s

Explanation: By using NTFS, Alternate Data Streams (ADSs) can be connected to a file as an attribute called $DATA. The command dir /r can be used to see if a file contains ADS data.

52. The SOC manager is reviewing the metrics for the previous calendar quarter and discovers that the MTTD for a breach of password security perpetrated through the Internet was forty days. What does the MTTD metric represent within the SOC?

- window of time required to stop the spread of malware in the network
- **the average time that it takes to identify valid security incidents that have occurred**
- the time required to stop the incident from causing further damage to systems or data
- the average time that it takes to stop and remediate a security incident

Explanation: Cisco defines MTTD as the average time that it takes for the SOC personnel to identify that valid security incidents have occurred in the network.

53. A cybersecurity analyst is performing a CVSS assessment on an attack where a web link was sent to several employees. Once clicked, an internal attack was launched. Which CVSS Base Metric Group Exploitability metric is used to document that the user had to click on the link in order for the attack to occur?

- scope
- integrity requirement

- availability requirement
- **user interaction**

Explanation: The CVSS Base Metric Group has the following metrics: attack vector, attack complexity, privileges required, user interaction, and scope. The user interaction metric expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful.

54. When a server profile for an organization is being established, which element describes the TCP and UDP daemons and ports that are allowed to be open on the server?

- critical asset address space
- service accounts
- software environment
- **listening ports**

Explanation: A server profile will often contain the following:

- Listening ports – the TCP and UDP daemons and ports that are allowed to be open on the server
- User accounts – the parameters defining user access and behavior
- Service accounts – the definitions of the type of service that an application is allowed to run on a server
- Software environment – the tasks, processes, and applications that are permitted to run on the server

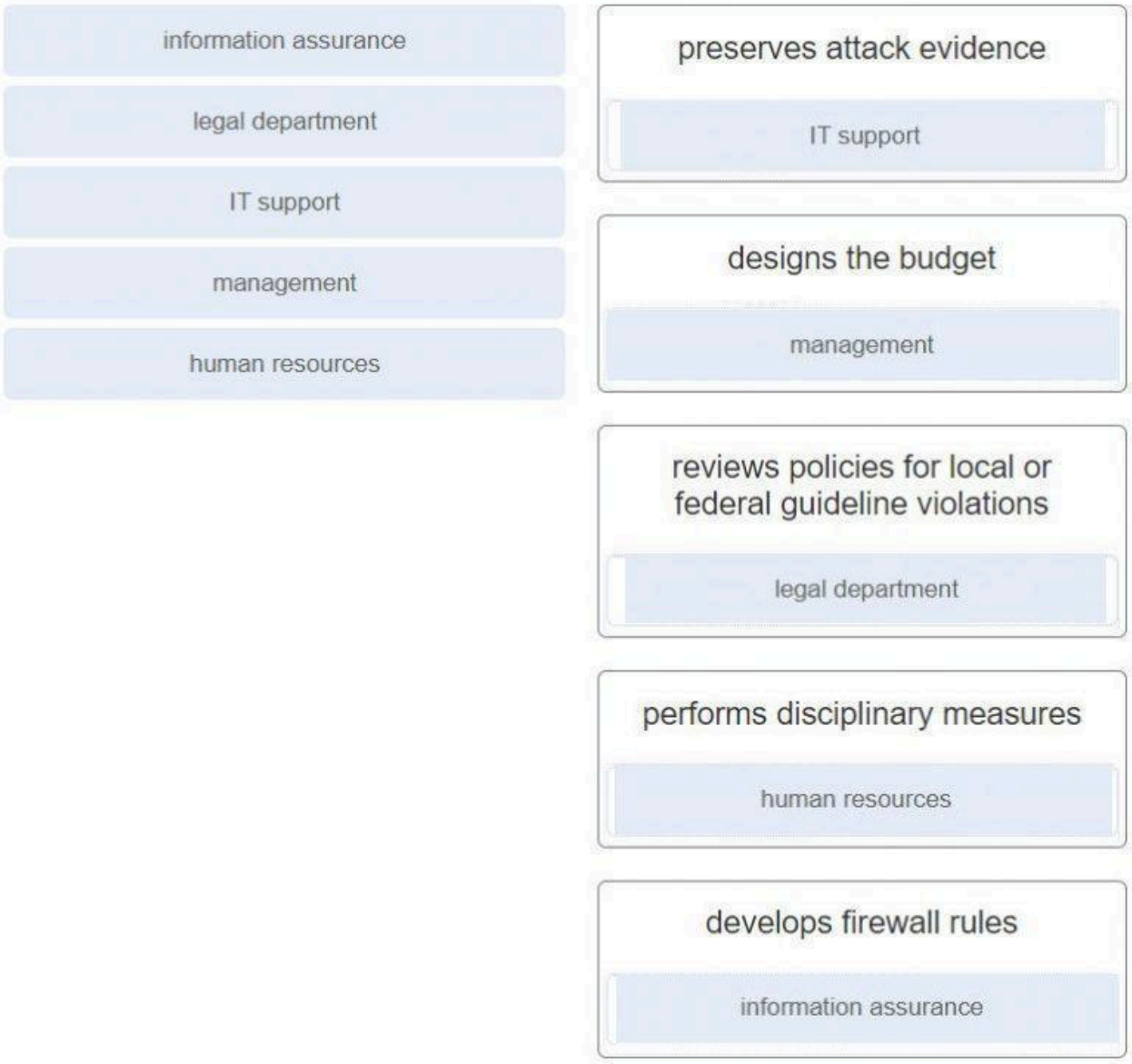
55. Which two actions should be taken during the preparation phase of the incident response life cycle defined by NIST? (Choose two.)

- Fully analyze the incident.
- Meet with all involved parties to discuss the incident that took place.
- Detect all the incidents that occurred.
- **Acquire and deploy the tools that are needed to investigate incidents.**
- **Create and train the CSIRT**

Explanation: According to the guideline defined in the NIST Incident Response Life Cycle, several actions should be taken during the

preparation phase including (1) creating and training the CSIRT and (2) acquiring and deploying the tools needed by the team to investigate incidents.

56. Match the NIST incident response stakeholder with the role.



57. Which component is a pillar of the zero trust security approach that focuses on the secure access of devices, such as servers, printers, and other endpoints, including devices attached to IoT?

- workflows
- workloads

- **workplace**
- workforce

Explanation: The workplace pillar focuses on secure access for any and all devices, including devices on the internet of things (IoT), which connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras, HVAC systems, kiosks, infusion pumps, industrial control systems, and more.

58. A security analyst is reviewing information contained in a Wireshark capture created during an attempted intrusion. The analyst wants to correlate the Wireshark information with the log files from two servers that may have been compromised. What type of information can be used to correlate the events found in these multiple data sets?

- ISP geolocation data
- **IP five-tuples**
- logged-in user account
- ownership metadata

Explanation: The source and destination IP address, ports, and protocol (the IP five-tuples) can be used to correlate different data sets when analyzing an intrusion.

59. A security analyst is investigating a cyber attack that began by compromising one file system through a vulnerability in a custom software application. The attack now appears to be affecting additional file systems under the control of another security authority. Which CVSS v3.0 base exploitability metric score is increased by this attack characteristic?

- privileges required
- **scope**
- attack complexity
- user interaction

Explanation: The scope metric is impacted by an exploited vulnerability that can affect resources beyond the authorized privileges of the vulnerable component or that are managed by a different security authority.

60. What will match the regular expression ^83?

- any string that includes 83
- **any string that begins with 83**
- any string with values greater than 83
- any string that ends with 83

Explanation: The expression ^83 indicates any string that begins with 83 will be matched.

61. What is a key difference between the data captured by NetFlow and data captured by Wireshark?

- NetFlow provides transaction data whereas Wireshark provides session data.
- NetFlow data is analyzed by tcpdump whereas Wireshark data is analyzed by nfdump.
- **NetFlow collects metadata from a network flow whereas Wireshark captures full data packets.**
- NetFlow data shows network flow contents whereas Wireshark data shows network flow statistics.

Explanation: Wireshark captures the entire contents of a packet. NetFlow does not. Instead, NetFlow collects metadata, or data about the flow.

62. Which three IPv4 header fields have no equivalent in an IPv6 header? (Choose three.)

- **flag**
- **identification**
- TTL
- **fragment offset**
- version
- protocol

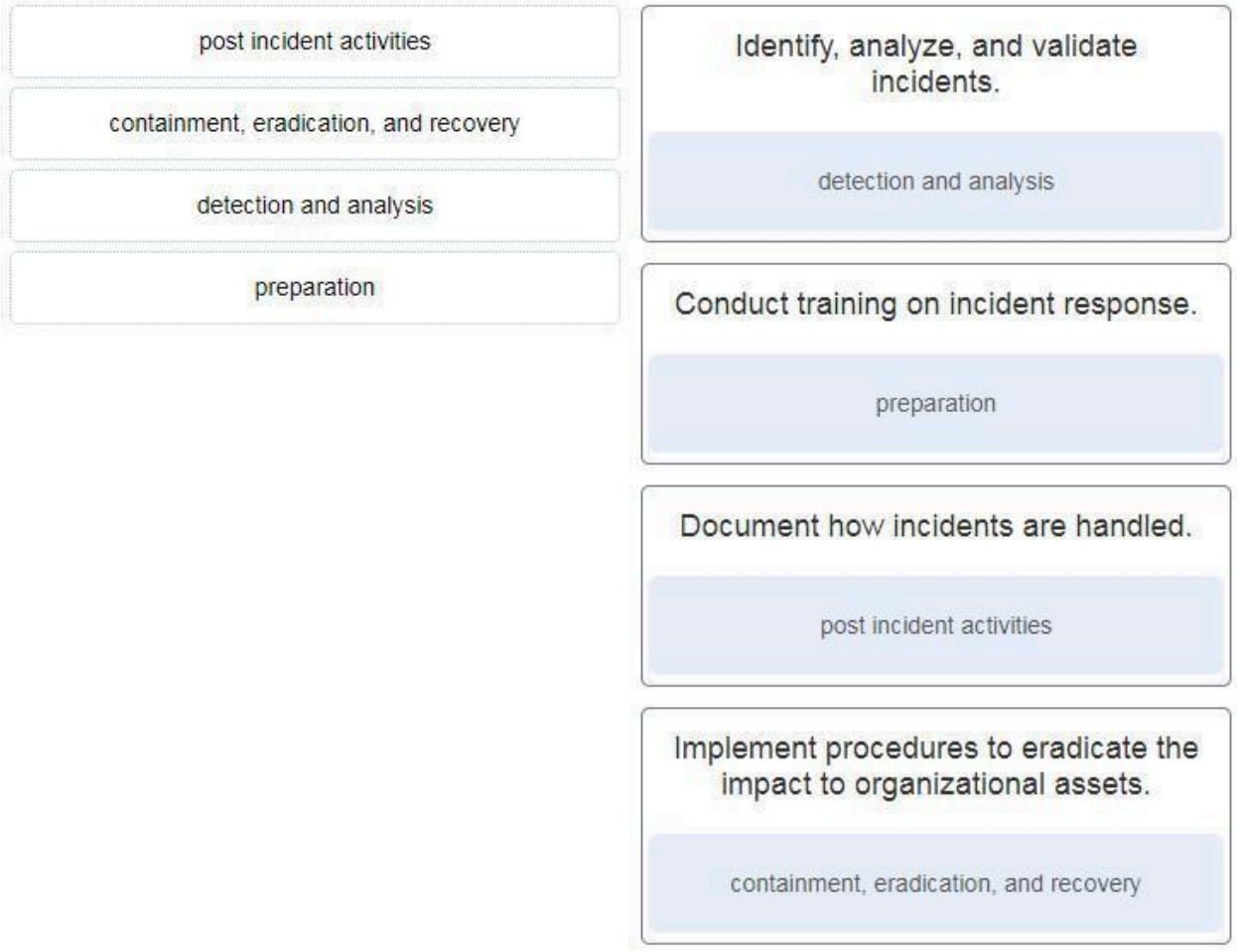
Explanation: Unlike IPv4, IPv6 routers do not perform fragmentation. Therefore, all three fields supporting fragmentation in the IPv4 header are removed and have no equivalent in the IPv6 header. These three fields are fragment offset, flag, and identification. IPv6 does support host packet fragmentation through the use of extension headers, which are not part of the IPv6 header.

63. What classification is used for an alert that correctly identifies that an exploit has occurred?

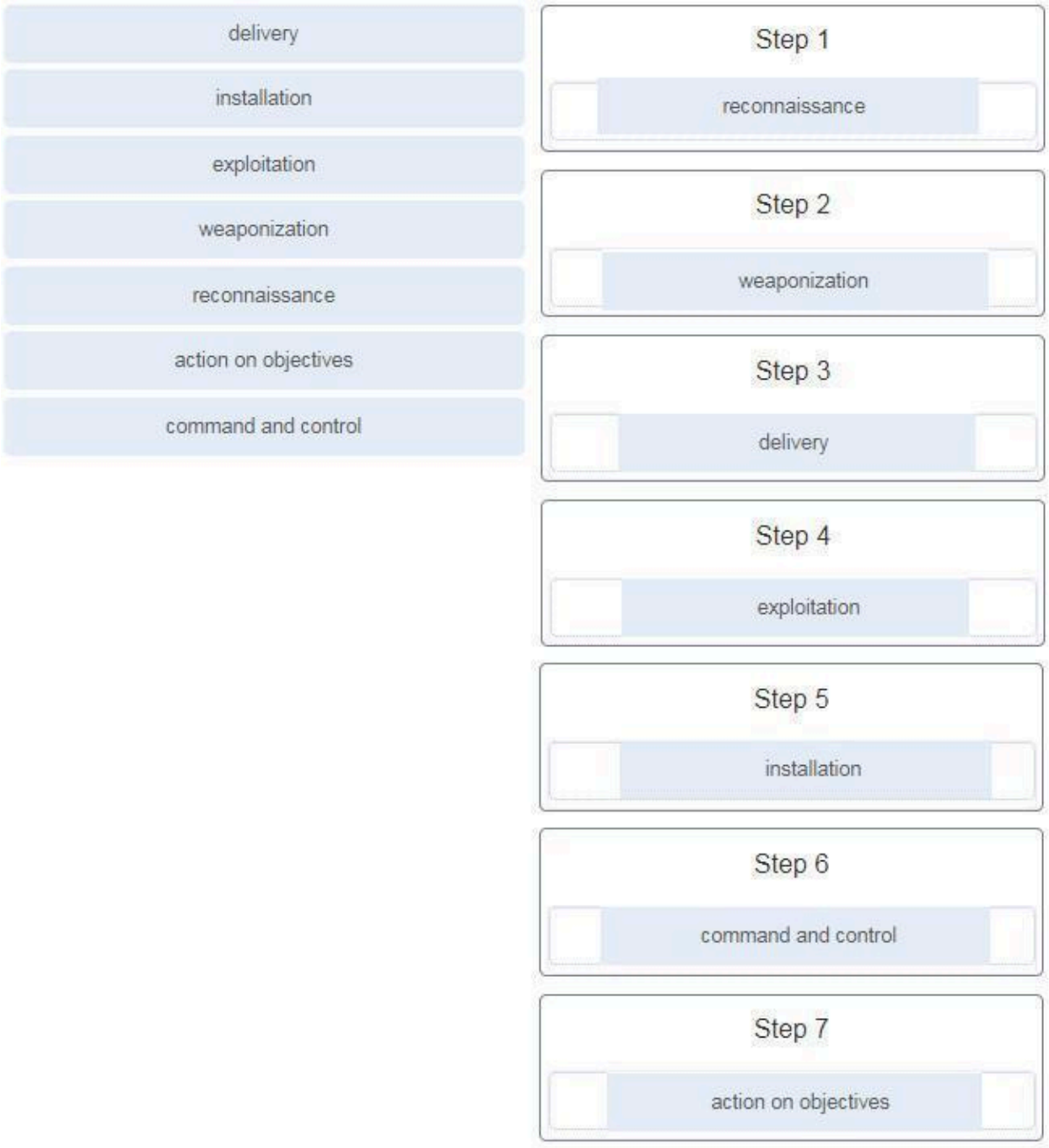
- false negative
- false positive
- **true positive**
- true negative

Explanation: A true positive occurs when an IDS and IPS signature is correctly fired and an alarm is generated when offending traffic is detected.

64. Match the NIST incident response life cycle phase with the description.



65. Place the seven steps defined in the Cyber Kill Chain in the correct order.



66. During the detection and analysis phase of the NIST incident response process life cycle, which sign category is used to describe that an incident might occur in the future?

- attrition
- impersonation
- **precursor**

- indicator

Explanation: There are two categories for the signs of an incident:

- **Precursor** – a sign that an incident might occur in the future
- **Indicator** – a sign that an incident might already have occurred or is currently occurring

67. According to the Cyber Kill Chain model, after a weapon is delivered to a targeted system, what is the next step that a threat actor would take?

- action on objectives
- **exploitation**
- weaponization
- installation

Explanation: The Cyber Kill Chain specifies seven steps (or phases) and sequences that a threat actor must complete to accomplish an attack:

- **Reconnaissance** – The threat actor performs research, gathers intelligence, and selects targets.
- **Weaponization** – The threat actor uses the information from the reconnaissance phase to develop a weapon against specific targeted systems.
- **Delivery** – The weapon is transmitted to the target using a delivery vector.
- **Exploitation** – The threat actor uses the weapon delivered to break the vulnerability and gain control of the target.
- **Installation** – The threat actor establishes a back door into the system to allow for continued access to the target.
- **Command and Control (CnC)** – The threat actor establishes command and control (CnC) with the target system.
- **Action on Objectives** – The threat actor is able to take action on the target system, thus achieving the original objective.

68. A company is applying the NIST.SP800-61 r2 incident handling process to security events. What are two examples of incidents that are in the category of precursor? (Choose two.)

- multiple failed logins from an unknown source
- **log entries that show a response to a port scan**

- an IDS alert message being sent
- **a newly-discovered vulnerability in Apache web servers**
- a host that has been verified as infected with malware

Explanation: As an incident category, the precursor is a sign that an incident might occur in the future. Examples of precursors are log entries that show a response to a port scan or a newly-discovered vulnerability in web servers using Apache.

69. A network administrator is creating a network profile to generate a network baseline. What is included in the critical asset address space element?

- the time between the establishment of a data flow and its termination
- the TCP and UDP daemons and ports that are allowed to be open on the server
- **the IP addresses or the logical location of essential systems or data**
- the list of TCP or UDP processes that are available to accept data

Explanation: A network profile should include some important elements, such as the following:
Total throughput – the amount of data passing from a given source to a given destination in a given period of time
Session duratio n – the time between the establishment of a data flow and its termination
Ports used – a list of TCP or UDP processes that are available to accept data
Critical asset address space – the IP addresses or the logical location of essential systems or data

70. Which NIST-defined incident response stakeholder is responsible for coordinating incident response with other stakeholders and minimizing the damage of an incident?

- human resources
- IT support
- the legal department
- **management**

Explanation: The management team creates the policies, designs the budget, and is in charge of staffing all departments. Management is also responsible for coordinating the incident response with other stakeholders and minimizing the damage of an incident.

71. What is defined in the policy element of the NIST incident response plan?

- **how to handle incidents based on the mission and functions of an organization**
- a roadmap for updating the incident response capability
- the metrics used for measuring incident response capability in an organization
- how the incident response team of an organization will communicate with organization stakeholders

Explanation: The policy element of the NIST incident response plan details how incidents should be handled based on the mission and function of the organization.

72. What is the responsibility of the human resources department when handing a security incident as defined by NIST?

- Review the incident policies, plans, and procedures for local or federal guideline violations.
- **Perform disciplinary actions if an incident is caused by an employee.**
- Coordinate the incident response with other stakeholders and minimize the damage of an incident.
- Perform actions to minimize the effectiveness of the attack and preserve evidence.

Explanation: The human resources department may be called upon to perform disciplinary measures if an incident is caused by an employee.

73. What is the benefit of a defense-in-depth approach?

- All network vulnerabilities are mitigated.
- The need for firewalls is eliminated.
- Only a single layer of security at the network core is required.
- **The effectiveness of other security measures is not impacted when a security mechanism fails.**

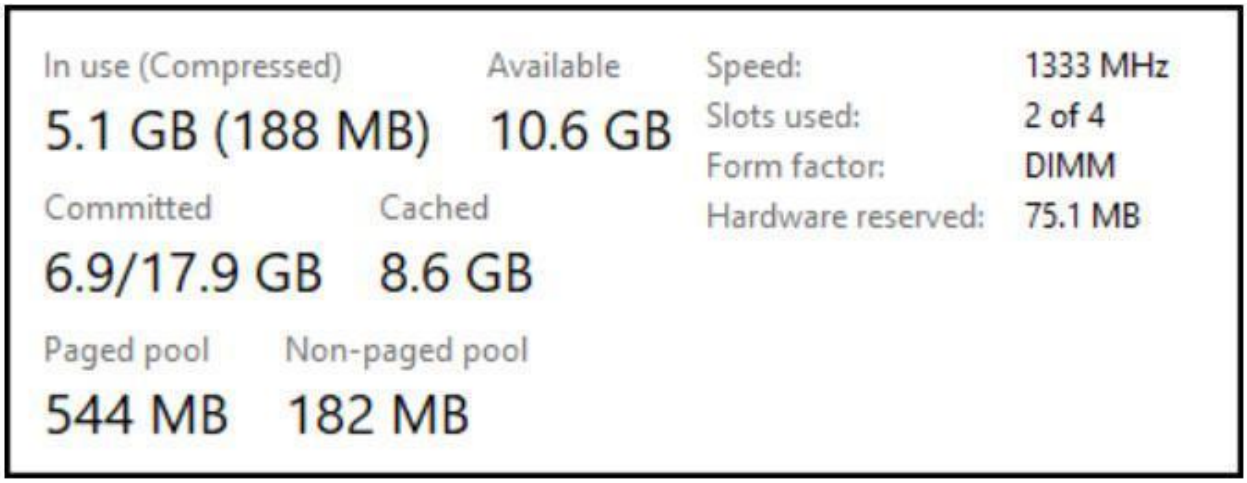
Explanation: The benefit of the defense-in-depth approach is that network defenses are implemented in layers so that failure of any single security mechanism does not impact other secuirty measures.

74. Which type of analysis relies on predefined conditions and can analyze applications that only use well-known fixed ports?

- statistical
- **deterministic**
- log
- probabilistic

Explanation: Deterministic analysis uses predefined conditions to analyze applications that conform to specification standards, such as performing a port-based analysis.

75. Refer to the exhibit. Approximately what percentage of the physical memory is still available on this Windows system?



- 32%
- 53%
- **68%**
- 90%

Explanation: The graphic shows that there is 5.1 GB (187 MB) of memory in use with 10.6 GB still available. Together this adds up to 16 GB of total physical memory. 5 GB is approximately 32% of 16 GB leaving 68% still available.

76. Which Windows tool can be used by a cybersecurity administrator to secure stand-alone computers that are not part of an active directory domain?

- PowerShell
- Windows Defender
- **Local Security Policy**
- Windows Firewall

Explanation: Windows systems that are not part of an Active Directory Domain can use the Windows Local Security Policy to enforce security settings on each stand-alone system.

77. What are three benefits of using symbolic links over hard links in Linux? (Choose three.)

- **They can show the location of the original file.**
- Symbolic links can be exported.
- They can be compressed.
- They can be encrypted.
- **They can link to a directory.**
- **They can link to a file in a different file system.**

Explanation: In Linux, a hard link is another file that points to the same location as the original file. A soft link (also called a symbolic link or a symlink) is a link to another file system name. Hard links are limited to the file system in which they are created and they cannot link to a directory; soft links are not limited to the same file system and they can link to a directory. To see the location of the original file for a symbolic link use the ls –l command.

78. When attempting to improve system performance for Linux computers with a limited amount of memory, why is increasing the size of the swap file system not considered the best solution?

- **A swap file system uses hard disk space to store inactive RAM content.**
- A swap file system cannot be mounted on an MBR partition.
- A swap file system only supports the ex2 file system.
- A swap file system does not have a specific file system.

Explanation: The swap file system is used by Linux when it runs out of physical memory. When needed, the kernel moves inactive RAM content

to the swap partition on the hard disk. Storing and retrieving content in the swap partition is much slower than RAM is, and therefore using the swap partition should not be considered the best solution to improving system performance.

79. Refer to the exhibit. A security analyst is reviewing the logs of an Apache web server. Which action should the analyst take based on the output shown?

```
HTTP/1.1 503 Service Temporarily Unavailable
Date: Sat, Jul 2017 14:36:45 GMT
Server: Apache
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age-3600,public,proxy-revalidate
Retry-After: 60
Content-Length: 4296
Connection: close
Content-Type: text/html
```

- Notify the appropriate security administration for the country.
- Restart the server.
- **Notify the server administrator.**
- Ignore the message.

Explanation: An Apache web server is an open source server that delivers web pages. Security access logs for an Apache web server include a 3-digit HTTP code that represents the status of the web request. A code that begins with 2 indicates access success. A code that begins with 3 represents redirection. A code that begins with 4 represents a client error and a code that begins with 5 represents a server error. The server administrator should be alerted if a server error such as the 503 code occurs.

80. A security professional is making recommendations to a company for enhancing endpoint security. Which security endpoint technology would be recommended as an agent-based system to protect hosts against malware?

- IPS
- **HIDS**
- baselining

- blacklisting

Explanation: A host-based intrusion detection systems (HIDS) is a comprehensive security application that provides antimalware applications, a firewall, and monitoring and reporting.

81. Which technique could be used by security personnel to analyze a suspicious file in a safe environment?

- whitelisting
- baselining
- **sandboxing**
- blacklisting

Explanation: Sandboxing allows suspicious files to be executed and analyzed in a safe environment. There are free public sandboxes that allow for malware samples to be uploaded or submitted and analyzed.

82. A cybersecurity analyst has been called to a crime scene that contains several technology items including a computer. Which technique will be used so that the information found on the computer can be used in court?

- rootkit
- log collection
- Tor
- **unaltered disk image**

Explanation: A normal file copy does not recover all data on a storage device so an unaltered disk image is commonly made. An unaltered disk image preserves the original evidence, thus preventing inadvertent alteration during the discovery phase. It also allows recreation of the original evidence.

83. Which SOC technology automates security responses by using predefined playbooks which require a minimum amount of human intervention?

- **SOAR**
- Wireshark
- NetFlow
- SIEM

- syslog

Explanation: SOAR technology goes a step further than SIEM by integrating threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team.

84. What is the first line of defense when an organization is using a defense-in-depth approach to network security?

- proxy server
- firewall
- IPS
- **edge router**

Explanation: A defense-in-depth approach uses layers of security measures starting at the network edge, working through the network, and finally ending at the network endpoints. Routers at the network edge are the first line of defense and forward traffic intended for the internal network to the firewall.

85. Which access control model assigns security privileges based on the position, responsibilities, or job classification of an individual or group within an organization?

- rule-based
- **role-based**
- discretionary
- mandatory

Explanation: Role-based access control models assign privileges based on position, responsibilities, or job classification. Users and groups with the same responsibilities or job classification share the same assigned privileges. This type of access control is also referred to as nondiscretionary access control.

86. Which metric in the CVSS Base Metric Group is used with an attack vector?

- the presence or absence of the requirement for user interaction in order for an exploit to be successful

- the number of components, software, hardware, or networks, that are beyond the control of the attacker and that must be present in order for a vulnerability to be successfully exploited
- the determination whether the initial authority changes to a second authority during the exploit
- **the proximity of the threat actor to the vulnerability**

Explanation: The attack vector is one of several metrics defined in the Common Vulnerability Scoring System (CVSS) Base Metric Group Exploitability metrics. The attack vector is how close the threat actor is to the vulnerable component. The farther away the threat actor is to the component, the higher the severity because threat actors close to the network are easier to detect and mitigate.

87. Which field in the IPv6 header points to optional network layer information that is carried in the IPv6 packet?

- traffic class
- flow label
- **next header**
- version

Explanation: Optional Layer 3 information about fragmentation, security, and mobility is carried inside of extension headers in an IPv6 packet. The next header field of the IPv6 header acts as a pointer to these optional extension headers if they are present.

88. Which data security component is provided by hashing algorithms?

- **integrity**
- confidentiality
- key exchange
- authentication

Explanation: Hashing algorithms are used to provide message integrity, which ensures that data in transit has not changed or been altered.

89. Which attack surface, defined by the SANS Institute, is delivered through the exploitation of vulnerabilities in web, cloud, or host-based applications?

- human

- network
- host
- **software**

Explanation: The SANS Institute describes three components of the attack surface:

- Network Attack Surface – exploits vulnerabilities in networks
- Software Attack Surface – delivered through the exploitation of vulnerabilities in web, cloud, or host-based software applications
- Human Attack Surface – exploits weaknesses in user behavior

90. What is the main goal of using different evasion techniques by threat actors?

- to launch DDoS attacks on targets
- to identify vulnerabilities of target systems
- **to prevent detection by network and host defenses**
- to gain the trust of a corporate employee in an effort to obtain credentials

Explanation: Many threat actors use stealthy evasion techniques to disguise an attack payload because the malware and attack methods are most effective if they are undetected. The goal is to prevent detection by network and host defenses.

91. How can NAT/PAT complicate network security monitoring if NetFlow is being used?

- It disguises the application initiated by a user by manipulating port numbers.
- It changes the source and destination MAC addresses.
- It conceals the contents of a packet by encrypting the data payload.
- **It hides internal IP addresses by allowing them to share one or a few outside IP addresses.**

Explanation: NAT/PAT maps multiple internal IP addresses with only a single or a few outside IP addresses breaking end-to-end flows. The result makes it difficult to log the inside device that is requesting and receiving the traffic. This is especially a problem with a NetFlow

application because NetFlow flows are unidirectional and are defined by the addresses and ports that they share.

92. Which statement describes the function provided by the Tor network?

- It conceals packet contents by establishing end-to-end tunnels.
- It distributes user packets through load balancing.
- **It allows users to browse the Internet anonymously.**
- It manipulates packets by mapping IP addresses between two networks.

Explanation: Tor is a software platform and network of P2P hosts that function as Internet routers on the Tor network. The Tor network allows users to browse the Internet anonymously.

93. When establishing a server profile for an organization, which element describes the type of service that an application is allowed to run on the server?

- user account
- listening port
- **service account**
- software environment

Explanation: A server profile should contain some important elements including these:

- Listening ports – the TCP and UDP daemons and ports that are allowed to be open on the server
- User accounts – the parameters defining user access and behavior
- Service accounts – the definitions of the type of service that an application is allowed to run on a server
- Software environment – the tasks, processes, and applications that are permitted to run on the server

94. What will a threat actor do to create a back door on a compromised target according to the Cyber Kill Chain model?

- **Add services and autorun keys.**
- Collect and exfiltrate data.

- Open a two-way communications channel to the CnC infrastructure.
- Obtain an automated tool to deliver the malware payload.

Explanation: Once a target system is compromised, the threat actor will establish a back door into the system to allow for continued access to the target. Adding services and autorun keys is a way to create a point of persistent access.

95. Which three things will a threat actor do to prepare a DDoS attack against a target system on the Internet? (Choose three.)

- Install a black door on the target system.
- Obtain an automated tool to deliver the malware payload.
- **Establish two-way communications channels to the CnC infrastructure with zombies.**
- Collect and exfiltrate data.
- **Compromise many hosts on the Internet.**
- **Install attack software on zombies.**

Explanation: To prepare for launching a DDoS attack, a threat actor will compromise many hosts on the Internet, called zombies. The threat actor will then install attack software on zombies and establish a two-way communications channel to CnC infrastructure with zombies. The threat actor will issue the command to zombies through the CnC to launch a DDoS attack against a target system.

96. What is specified in the plan element of the NIST incident response plan?

- organizational structure and the definition of roles, responsibilities, and levels of authority
- **metrics for measuring the incident response capability and effectiveness**
- priority and severity ratings of incidents
- incident handling based on the mission of the organization

Explanation: NIST recommends creating policies, plans, and procedures for establishing and maintaining a CSIRC. One component of the plan element is to develop metrics for measuring the incident response capability and its effectiveness.

97. What is the responsibility of the IT support group when handing an incident as defined by NIST?

- coordinates the incident response with other stakeholders and minimizes the damage of an incident
- performs disciplinary measures if an incident is caused by an employee
- **performs actions to minimize the effectiveness of the attack and preserve evidence**
- reviews the incident policies, plans, and procedures for local or federal guideline violations