What was on the OA:

Fundamentals of Information Security

CIA Triad
Parkerian Hexad
Attack Types
Threat
Vulnerability
Authentication
Mutual Authentication
Risk Management Process
Incident Response Process

Key Concepts, Identification, and Authorization

Authorization
Least Privilege
Access Control
Access Control Models
Network ACL
Accountability
Intrusion Detection (IDS)
Intrusion Prevention (IPS)
Auditing

Auditing, Cryptography, and Legal Issues

Symmetric and Asymmetric Encryption
Symmetric and Assymetric Key Algorithms
Hash Functions
Keyless Cryptography
Digital Signature
Certificates
Secure Socket Layer (SSL)
Transport Layer Security (TLS)
IPsec and SSL VPN

Protecting data at rest/motion/use
DDos
Man-in-the-middle attacks
FISMA, FERPA, HIPPA, HITECH, SOX, GLBA, PCI DSS, COPPA
Compliance

Operations and Human Element Study

Phishing
Tailgating
Brute Force

Physical and Network Security

Physical Threats
Defense-in-depth
Raid
NIDS/HIDS
Network Segmentation
Firewalls
VPN
Packet Filtering
Stateful Firewall
Deep Packet Inspection
Proxy Servers
DMZ
Port Scanners
- Nmap

Packet Sniffers
- Wireshark
- Tcpdump

Honeypots
Burp Suite

Operating System and Application Security

OS Hardening
Nessus
Buffer Overflows

Race Conditions
SQL Injections
Cross-Site Scripting
Fuzzers

Tips/Advice:

When you're applying CIA to situations, remember:

Confidentiality - WHO can access the data

Integrity - keeping data UNALTERED

Availability - for ones AUTHORIZED to ACCESS data when needed

Attack types and their effect:

Interception is the ONLY attack that affects on confidentiality. Interruption, modification, and fabrication affects integrity and availability because most of the time they're impacting data.

An easy trick to memorize the laws and regulations:

FISMA - the **FI** stands for "federal information"
F**E**RPA - the **E** stands for "educational"
HIPPA - the **HI** stands for "health insurance"
HI**TECH** - **TECH** means "technology"
P**C**I DSS - the **C** stands for "credit card"
COPPA - the **CO** stands for "children online"
SOX - rhymes with "stocks", so think of finance
GLBA - this is the only one you would have to memorize

- There's gonna be questions where they give you a scenario and you have to identify what type of security it is (application, network, physical, or operating systems).

- Understand the difference between each network tools and their functions (Nessus, WireShark, Burp Suite, Fuzzers, Honeypots, NMAP).

- Know your definitions, but the OA heavily relies on applying the concepts to real-life situations.

When you're taking the OA, analyze and break down the question. Understand what they're really trying to ask you.

Notes

Fundamentals of Info Security

CIA Triad

Confidential - allowing only those authorized to access the data requested
Integrity - keeping data unaltered in an unauthorized manner and reliable
Availability - the ability for those authorized to access data when needed

Parkerian Hexad

Confidentiality - allowing only those authorized to access the data requested
Integrity - keeping data unaltered without detection
Availability - the ability to access data when needed
Possession - physical deposition of the media on which the data is stored
Authenticity - allows us to talk about the proper attribution as to the owner or creator of the data in question
Utility - how useful the data is to us

Attack Types

Interception - an attacker has access to data, applications, or environment
Interruption - attacks cause our assets to become unusable or unavailable
Modification - attacks involve tampering with our asset
Fabrication - attacks that create false information

Threat - something that has potential to cause harm

Vulnerability - weaknesses that can be used to harm us

Authentication - verifying that a person is who they claim to be

Something you know: username, password, PIN
Something you have: ID badge, swipe card, OTP
Something you are: fingerprint, Iris, Retina scan
Somewhere you are: geolocation
Something you do: handwriting, typing, walking

Mutual authentication - both parties in a transaction to authenticate each other

- Has digital certificates
- Prevents man in the middle attacks
- The man in the middle is where the attacker inserts themselves into the traffic flow
- **Ex.** Both the PC and server authenticate each other before data is sent in either direction

Risk management process

1. **Identify Asset** - identifying and categorizing assets that we're protecting
2. **Identify Threats** - identify threats
3. **Assess Vulnerabilities** - look for impacts
4. **Assess Risk** - asses the risk overall
5. **Mitigate Risk** - ensure that a given type of threat is accounted for

Incident response process

1. **Preparation** - the activities that we can perform, in advance of the incident itself, in order to better enable us to handle it.
2. **Detection and Analysis (Identification)** - detect the occurrence of an issue and decide whether or not it is actually an incident, so that we can respond appropriately to it.
3. **Containment** - involves taking steps to ensure that the situation does not cause any more damage than it already has, or to at least lessen any ongoing harm.
4. **Eradication** - attempt to remove the effects of the issue from our environment.
5. **Recovery** - restoring devices or data to pre-incident state (rebuilding systems, reloading applications, backup media, etc.)
6. **Post-incident activity** - determine specifically what happened, why it happened, and what we can do to keep it from happening again. (postmortem).

Key Concepts, Identification, Authorization

Authorization - what the user can access, modify, and delete

Least Privilege - giving the bare minimum level of access it needs to perform its job/functionality

Acess Control

- **Allowing** - lets us give a particular party access to a given source
- **Denying** - opposite of gaining access
- **Limiting** - allowing some access to our resource, only up to a certain point
- **Revoking** - takes access away from former user

Access Control LIst - info about what kind of access certain parties are allowed to have to a given system.

- Read, write, execute

Network ACL - filter access rules for incoming and outgoing network transactions, such as Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, and ports.

Access Control Models

Discretionary (DAC) - owner of resources determines who gets access and what level

Mandatory (MAC) - separate group or individual (from owner) has the authority to set access to resources
Rule-based - allows access according to a set of rules defined by the system administrator

Role-based (RBAC) - functions access controls set by an authority responsible for doing so, rather than by the owner of the resource

Attribute-based (ABAC) - based on attributes, such as of a person, resource, or an environment

Accountability - refers to making sure that a person is responsible for their actions. It provides us with the means to trace activities in our environment back to their source.

- Depends on identification, authentication, and access control being present so that we can know who a given transaction is associated with, and what permissions were used to allow them to carry it out.

Nonrepudiation - a situation in which sufficient evidence exists as to prevent an individual from successfully denying that he or she has made a statement, or taken an action

Intrusion detection (IDSes) - monitors and reports malicious events

Intrusion prevention (IPSes) - takes actions when malicious events occur

Auditing - the examination and review of an organization's records to ensure accountability through technical means.

Penetration testing - mimicking, as closely as possible, the techniques an actual attack would use

Auditing, Cyrptography, and Legal Issues

Cryptography - the practice of keeping information secure through the use of codes and ciphers

Symmetric cryptography - encryption that uses a single key to encrypt and decrypt a message (aka the private key cryptography)

Block Cipher - takes a predetermined number of bits, known as a block, in the plaintext message and encrypts that block

Stream Cipher - encrypts each bit in the plaintext message, 1 bit at a time

Symmetric Key Algorithms

DES - a block cipher based on symmetric key cryptography and uses a 56-bit key. Not that secured any more.

3DES - DES used to encrypt each block three times, each with a different key

AES - uses three different ciphers: one with a 128-bit key, one with a 192-bit key, and one with a 256-bit key, all having a block length of 128 bits

Asymmetric cyrptography - a public key and a private key. The public key is used to encrypt data sent from the sender to the receiver and is shared with everyone. Private keys are used to decrypt data that arrives at the receiving end and are very carefully guarded by the receive (aka the public key cryptography)

Asymmetric Key Algorithms

- **Secure Sockets Layer (RSA)** - SSL, to secure transactions like web and e-mail traffic

- **Elliptic Curve Cryptography (ECC)** - can secure all browser connections to the Web servers
- **Pretty Good Privacy (PGP)** - securing messages and files
- **Transport Layer Security (TLS)**

SSL (Secure Socket Layer) and TLS (Transport Layer Security) - encryption protocols that are used to secure the transmission of data over a network. They provide secure communications by allowing two applications to authenticate each other and by negotiating a secure, encrypted connection.

Hash Functions - create a largely unique and fixed-length hash value based on the original message (input/output)

- Hashes provide integrity, but not confidentiality. It can't un-hash a message.
- Hashes are very useful when distributing files or sending communications, as the hash can be sent with the message so that the receiver can verify its integrity

Keyless cryptography - a method of encrypting data that does not use a key. Instead, it uses mathematical algorithms to secure the information (hash functions)

Digital Signatures - ensure that the message was legitimately sent by the expected party, and to prevent the sender from denying that he or she sent the message, known as nonrepudiation

Certificates - link a public key to a particular individual and are often used as a form of electronic identification for that particular person

IPsec (Internet Protocol Security) and SSL VPN (Secure Sockets Layer Virtual Private Network) - technologies that can be used to secure the connection between two devices. They can be used to establish a secure, encrypted tunnel between devices, which can be used to protect data in motion.

Protecting data at rest - data is at rest when it is on a storage device

- Data protection is done by encryption

Protecting data in motion - data is in motion when it is on a actively transporting over a network

- SSL VPN and TLS are often used to protect information sent over networks and over the Internet

Protecting data in use - data is in use when a user is accessing the data

- Hardest to protect, encryption is limited

DDOS - a type of cyber attack where an attacker floods a website or network with so much traffic that it becomes unavailable to legitimate users.

Man-in-the-middle attacks - a type of cyber attack where an attacker intercepts a communication between two parties and can read, alter, or inject new information into the communication

Laws and Regulations

Federal Information Security Modernization Act (FISMA) - protects the information, operations, and assets in the federal government

Family Educational Rights and Priacy Act (FERPA) - protects the privacy of students and their parents, regulating educational records, including educational information, personally identifiable information, and directory information.

Health Insurance Rights and Priacy Act (HIPAA) - health care organizations to protect the confidentiality and integrity of personal health information

HITECH (Health Information Technology for Economic and Clinical Health) - to promote and expand the adoption of health information technology, especially the ues of electronic health records by healthcare providers

Sarbanes-Oxley Act (SOX) - for trade companies to maintain accurate financial records and disclose financial information in a timely manner

Gramm-Leach-Biley Act (GLBA) - protects the privacy of their customers' non-public personal information

Payment Card Industry Data Security Standard (PCI DSS) - companies that process credit card payments must protect its information

Childrens' Online Privacy Protection Act (COPPA) - sets rules on data collection for children under 13 to protect their online privacy.

Compliance - conforming to a rule, such as specification, policy, standard or law

- **Regulatory compliance** - organizational goal to comply with relevant laws and regulations
- **Industry compliance** - regulations or standards usually not mandated by law, it is designed for specific industries (e.g. PCI DSS)

Operations and Human Element Study

Pretexting - when we assume the guise of a manager, customer reporter, or even a co-worker's family member

Phishing - an attack by convincing the potential victim to click on a link in an e-mail, which steals the victim's personal information and installs viruses

Tailgating - an unauthorized person attempts to enter a secure area by following someone who is authorized

Brute Force - an attack by submitting password attempts until eventually guessed correctly

Physical and Network Security

Physical Threats

- Extreme temperature
- Gases
- Liquids
- Living organism
- Projectiles
- Movement
- Energy anomalies
- People
- Toxins
- Smoke and fire

Defense in-depth - using a variety of security measures that will still achieve a successful defense should one or more of the defensive measures fail

RAID - data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both

Intrusive detection system (IDS) - monitor the networks, hosts, or applications to which they are connected for unauthorized activity

Network intrusion detection system (NIDS) - a type of IDS that attempts to detect malicious network activities—for example, port scans and DoS attacks—by constantly monitoring network traffic.

- Anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.

Host Intrusion detection system (HIDS) - A software-based application that runs on a local host computer that can detect an attack as it occurs.

- Anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside environment such as the Internet

Network segmentation - dividing a network into multiple smaller networks (subnet)

Firewalls - controls access to a network and the traffic that flows into and out of our networks, naturally creating network segmentation when installed

Virtual Private Network (VPN) - the use of private networks to provide a solution for sending sensitive traffic over unsecure networks

Firewalls and DMZs

Packet filtering - a technique by firewall to allow/block certain types of network traffic based on the IP, port, and protocol being used.

Stateful firewall - keeps track of the connection state and will only allow traffic that is part of a new or already established connection

- A firewall that can watch packets and monitor the traffic from a given connection

Deep packet inspection - analyzing the actual content of the traffic that is flowing through them.

Proxy servers - provides a layer of security serving as a choke point, allowing us to filter and inspect traffic for attacks or undesirable content

DMZ - a layer of protection that separates a device from the rest of a network and used to host public facing services such as websites.

Network Tools

Port Scanners - Port scanners are a software-based utility. They are a security tool designed to search a network host for open ports on a TCP/IP-based network.

- **Nmap** - network mapper, used to scan ports, search for hosts on the network, and other operations

Packet Sniffers - a technique used by attackers to intercept and read network traffic. Essentially, it allows an attacker to see the data that is being sent over a network.

- **Wireshark** - graphical interface tool for packet analyzer capable of capturing and analyzing network traffic
- **Tcpdump** - this command-line packet sniffing tool runs on Linux and UNIX operating systems

Honeypots - detects, monitor, amd sometimes tamper with the activities and vulnerabilities of an attacker

Operating System and Application Security

OS Hardening

1. Remove unnecessary software
2. Removing or turning off unessential services
3. Making alternations to common accounts
4. Applying the principle of least privilege
5. Applying software updates in a timely manner
6. Making use of logging and auditing functions

Nessus - Vulnerability Assessment Tools, a tool that can be used for port scanning, which is a way to check for open ports on a system. It helps identify any potential vulnerabilities that could be exploited by an attacker.

Buffer overflows - a vulnerability that occurs when we do not properly store the size of the data input into our applications, causing the program to crash and an attacker to take advantage

Race conditions - a vulnerability that occurs when multiple processes or multiple threads are accessing and modifying shared resources

- Can be very difficult to detect in existing software, as they are hard to reproduce

SQL injections - a type of cyber attack where an attacker injects malicious code into a website's database through a web form.

- Server-side attack
- OS hardening is the process of making an operating system more secure by removing unnecessary features and tightening security settings.
- Nessus is a tool that can be used for port scanning, which is a way to check for open ports on a system.

Cross-Site Scripting (XSS) - an attack carried out by placing code in the form of a scripting language into a Web page, or other media, that is interpreted by a client browser, including Adobe Flash animation and some types of video files

Web Application Analysis Tools - perform the same general set of tasks and will search for common flaws such as XSS or SQL injection flaws, as well as improperly set permissions, extraneous files, outdated software versions, and many more such items

- **Ex:** Nikto and Wikto and Burp Suite

Fuzzers - a tool that can be used to test the security of a system by sending it unexpected input. The goal of using a fuzzer is to find vulnerabilities or weaknesses in a system by causing it to crash or behave in unexpected ways.

BinScope Binary Analyzer - a tool developed by Microsoft to examine source code for general good practices

Nikto/Wikto - checks for many common server-side vulnerabilities, and creates an index of all the files and directories it can see on the target Web server