Computer Forensics Mid1Exam 2May2022 4/4-SemII

Answer any two questions.Each question carries 5 marks.

1.(a)Draw the Figure 4-1 that illustrates the Initial Response steps.

(b)Draw the Figure 2-1 that depicts the seven components of incident response methodology.

2.(a)Draw the Figure 2-3 depicting the possible investigation phase steps

(b)Draw the Figure 2-4 depicting the major steps in performing forensic analysis

3.(a)Depict the Table 2-1 that shows some common situations with possible response strategies and potential outcomes and as to how to get from an incident to an outcome.

(b)Depict the Table 2-2 that shows several common scenarios and some potential/possible actions that may lead to law enforcement involvement

4.(a)(i)Draw the Figure 3-1 that identifies the role of pre-incident preparation within the overall response process.

(ii)Draw the Table 5-3 consisting the tools used for an In-Depth response w.r.t. live data collection from windows systems

(b)(i)Enumerate the approaches for validating forensic data

(ii)Enumerate the data-hiding techniques

Computer Forensics Mid1Exam 2May2022 4/4-SemII

PART-II=QUIZ paper **20x1/2=10m**

1.Network security actions include which of the following.

(a)Install firewalls and intrusion detection systems (b) Use access control lists on routers (c) Create a network topology conducive to monitoring (d) Encrypt network traffic (e)Require authentication (f)all of these

2.Which of the following is a step that you can take to help any investigator respond effectively.

(a) Record cryptographic checksums of critical files. (b) Increase or enable secure audit logging. (c) Build up your host's defenses. (d) Back up critical data and store media securely. (e) Educate users about host-based security (f)all of these

3.Which of the following, basically a digital signature is synonymous with each other

(a) cryptographic checksum (b) message digest (c) fingerprint (d)all of these

4. What are the substeps under Increasing or Enabling Secure Audit Logging?

(a)Configuring Unix Logging (b)Configuring Windows Logging (c)Configuring Application Logging (d)all of these

5.Which one of the following is a organization step/CSIRT preparation step.

(a) Identify your corporate risk. (b) Prepare your hosts for incident response and recovery. (c) Prepare your network by implementing network security measures. (d) Establish policies and procedures that allow you to meet your incident response objectives.(Developing Acceptable Use Policies) (e) Create a response toolkit for use by the CSIRT. (f) Create a CSIRT that can assemble to handle incidents (g)all of these

6.Which of the following can be the response stance of a computer crime victim organization?

(a)Ignore the incident altogether. (b)Defend against further attacks. (c) Defend against further attacks by identifying and disabling the initiators (by criminal arrest or civil action). (d) Perform surveillance and counterintelligence data gathering. (e)all of these

7.Which of the following is an influential factor for determining your response stance to CSI?

(a) The effect the incident has on your business (b) Legal issues and constraints (c) Political influence or corporate politics (c)Technical capabilities of the response team (d) Funding and available resources (e)all of these

8.Which of the following may be in the CSIRT mission?

(a)Respond to all security incidents or suspected incidents using an organized, formal investigative process. (b) Conduct a complete investigation free from bias (well, as much as possible). (c)Quickly confirm or dispel whether an intrusion or security incident actually occurred. (d)Assess the damage and scope of an incident. (e) Establish a 24*7 hotline for clients during the duration of the investigation. (f) Control and contain the incident. (g)Collect and document all evidence related to an incident. (h) Maintain a chain of custody (protect the evidence after collection). (i) Select additional support when needed. (j)Protect privacy rights established by law and/or corporate policy. (k) Provide liaison to proper law enforcement and legal authorities. (l)Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure. (m)Provide expert testimony. (n) Provide management with incident-handling recommendations that are fully supported by facts. (o)all of these

9.Which of the following should be in an organization's initial response activities w.r.t. a CSI?

(a) Receiving the initial notification of an incident (b) Recording the details after the initial notification, including an incident declaration, if appropriate (c) Assembling the CSIRT (d)Performing traditional investigative steps (e) Conducting interviews (f)Determining whether the incident is escalated or not (g)all of these

10._____ (forensic duplication?) of the target media provides the mirror image of the target system.

11.W.r.t. live data collection from Unix systems, _____(unlinked files?) are files marked for deletion when processes that access it terminate.

12.W.r.t. live data collection from Unix systems _____(loadable kernel modules (LKMs), also called kernel loadable modules?) are programs that can be dynamically linked into the kernel after the system has booted up.

13._____(Rootkits?) are collections of commonly trojaned system processes and scripts that automate many of the actions attackers take when they compromise a system.

14._____(Data collection?) is the accumulation of facts and clues that should be considered during your forensic analysis.

15._____(Forensic analysis?) includes reviewing all the data collected. This includes reviewing log files, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files, … …

16-20.Match the following by filling with appropriate digits in the blanks. a-_____, b-_____, c_____, d-_____, e-_____

(a)Collections of commonly trojaned system processes and scripts that automate many of the actions attackers take when they compromise a system. (1)Rootkits

(b)file-transfer tools (2)netcat, cryptcat

(c)3 factors are used to determine risk (3) assets, vulnerabilities, and threats.

(d)Advantages of cryptographic checksums (4) provide nonrepudiation for data.

(e)a command that shows open files, including those that have opened sockets, a command that can be used to display all open sockets and, in some cases, the files that opened those sockets. (5)lsof, netstat