Implementing Cisco Cybersecurity Operations

1. Employees are allowed access to internal websites. An employee connects to an internal website and IDS reports it as malicious behavior. What is this example of?

A. false negative

B. false positive

C. true positive

D. true negative

Answer(s): B

---

2. What mechanism does the Linux operating system provide to control access to files?

A. access complexity

B. user interaction

C. file permissions

D. privileges required

Answer(s): C

---

3. Which statement about the collected evidence data when performing digital forensics is true?

A. It must be deleted as soon as possible due to PCI compliance.

B. It must be stored in a forensics lab only by the data custodian.

C. It must be copied to external storage media and immediately distributed to the CISO.

D. it must be preserved and its integrity verified.

Answer(s): D

---

4. You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attach and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. action on objectives

B. delivery

C. weaponization

D. reconnaissance

Answer(s): A

---

5. Refer to the exhibit. We have performed a malware detection on the Cisco website. Which statement about the result is true?

A. The website has been marked benign on all 68 checks.

B. The website has 68 open threats.

C. The website has been marked benign on 0 checks.

D. The threat detection needs to run again.

Answer(s): A

---

6. Which type of analysis allows you to see how likely an exploit could affect your network?

A. probabilistic

B. descriptive

C. inferential

D. casual

Answer(s): A

---

7. Which function does an internal CSIRT provide?

A. incident handling services for a country's government

B. incident handling services for a parent organization

C. incident handling services as a service for other organization

D. incident handling services across various CSIRTs

Answer(s): B

---

8. What is accomplished in the identification phase of incident handling?

A. determining the responsible user

B. identifying source and destination IP addresses

C. defining the limits of your authority related to a security event

D. determining that a security event has occurred

Answer(s): D

---

9. What are the metric values for confidentiality impact in the CVSS v3.0 framework?

A. open, closed, obsolete

B. high, medium, none

C. high, low, none

D. high, low

Answer(s): C

---

10. What can be addressed when using retrospective security techniques?

A. if the affected host needs a software update

B. why the malware is still in our network

C. if the affected system needs replacement

D. what system are affected

Answer(s): D

---

11. Which statement about threat actors is true?

A. They are perpetrators of attacks.

B. They are any assets that are threatened.

C. They are victims of attacks.

D. They are any company assets that are threatened.

Answer(s): A

---

12. Which option allows a file to be extracted from a TCP stream within Wireshark?

A. Analyze > Extract

B. View > Extract

C. Tools > Export > TCP

D. File > Export Objects

Answer(s): D

---

13. Which of the following is one of the main goals of the CSIRT?

A. To monitor the organization's IPS devices

B. To minimize and control the damage associated with incidents, provide guidance for mitigation, and work to prevent future incidents

C. To configure the organization's firewalls

D. To hire security professionals who will be part of the InfoSec team of the organization.

Answer(s): B

---

14. Refer to the exhibit. Which type of log is this an example of?

A. IDS log

B. NetFlow log

C. syslog

D. proxy log

Answer(s): A

---

15. What is a listening port?

A. A port that remains open and waiting for incoming connections

Answer(s): A

---

16. Refer to the exhibit. Which host is likely connecting to a malicious site?

A. 10.0.1.1

B. 10.0.1.10

C. 10.0.1.20

D. 10.0.12

Answer(s): A

---

17. Which option is the common artifact used to uniquely identify a detected file?

A. file extension

B. file size

C. file hash

D. file timestamp

Answer(s): C

---

18. Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

A. detection and analysis

B. post-incident analysis

C. preparation

D. containment, eradication, and recovery

Answer(s): B

---

19. Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?

A. evidence collection

B. data analytics

C. threat actor attribution

D. asset attribution

Answer(s): C

---

20. Which command can be used to find open ports on a system?

A. netstat -v

B. netstat -r

C. netstat -I

D. netstat-g

Answer(s): C
