[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 13 Exam Answers

1. When dealing with security threats and using the Cyber Kill Chain model, which two approaches can an organization use to help block potential exploitations of a system? (Choose two.)

- Collect email and web logs for forensic reconstruction.
- Analyze the infrastructure path used for delivery.
- **Audit endpoints to forensically determine origin of exploit.**
- Conduct full malware analysis.
- **Conduct employee awareness training and email testing.**

2. Which action should be included in a plan element that is part of a computer security incident response capability (CSIRC)?

- Detail how incidents should be handled based on the mission and functions of an organization.
- **Develop metrics for measuring the incident response capability and its effectiveness.**
- Create an organizational structure and definition of roles, responsibilities, and levels of authority.
- Prioritize severity ratings of security incidents.

3. What is the objective the threat actor in establishing a two-way communication channel between the target system and a CnC infrastructure?

- **to allow the threat actor to issue commands to the software that is installed on the target**
- to steal network bandwidth from the network where the target is located
- to launch a buffer overflow attack
- to send user data stored on the target to the threat actor

4. After containment, what is the first step of eradicating an attack?

- Hold meetings on lessons learned.
- Change all passwords.
- Patch all vulnerabilities.
- **Identify all hosts that need remediation.**

5. What is defined in the SOP of a computer security incident response capability (CSIRC)?

- **the procedures that are followed during an incident response**
- the metrics for measuring incident response capabilities
- the roadmap for increasing incident response capabilities
- the details on how an incident is handled

6. A school has a web server mainly used for parents to view school events, access student performance indicators, and communicate with teachers. The network administrator suspects a security-related event has occurred and is reviewing what steps should be taken.

7. The threat actor has already placed malware on the server causing its performance to slow. The network administrator has found and removed the malware as well as patched the security

hole where the threat actor gained access. The network administrator can find no other security issue. What stage of the Cyber Kill Chain did the threat actor achieve?

- actions on objectives
- command and control
- delivery
- **exploitation**
- installation

8. If the web server runs Microsoft IIS, which Windows tool would the network administrator use to view the access logs?

- **Event Viewer**
- net command
- PowerShell
- Task Manager

9. Reports of network slowness lead the network administrator to review server alerts. The administrator confirms that an alert was an actual security incident. Which type of security alert classification would this be?

- false negative
- false positive
- true negative
- **true positive**

10. The network administrator believes that the threat actor used a commonly available tool to slow the server down. The administrator concludes that based on the source IP address identified in the alert, the threat actor was probably one of the students. What type of hacker would the student be classified as?

- black hat
- **gray hat**
- red hat
- white hat

11. What is the goal of an attack in the installation phase of the Cyber Kill Chain?

- **Create a back door in the target system to allow for future access.**
- Establish command and control (CnC) with the target system.
- Use the information from the reconnaissance phase to develop a weapon against the target.
- Break the vulnerability and gain control of the target.

12. Which meta-feature element in the Diamond Model describes information gained by the adversary?

- resources
- methodology
- direction
- **results**

13. What is a benefit of using the VERIS community database?

- **It can be used to discover how other organizations dealt with a particular type of security incident.**
- Companies who pay to contribute and access the database are protected from security threats.
- It can be used to discover the name of known threat actors.
- The database can be easily compressed.

14. 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.)

- Build detections for the behavior of known malware.
- Train web developers for securing code.
- **Detect data exfiltration, lateral movement, and unauthorized credential usage.**
- **Perform forensic analysis of endpoints for rapid triage.**
- Collect malware files and metadata for future analysis.

15. A threat actor has identified the potential vulnerability of the web server of an organization and is building an attack. What will the threat actor possibly do to build an attack weapon?

- **Obtain an automated tool in order to deliver the malware payload through the vulnerability.**
- Install a webshell on the web server for persistent access.
- Create a point of persistence by adding services.
- Collect credentials of the web server developers and administrators.

16. Which action is taken in the postincident phase of the NIST incident response life cycle?

- **Document the handling of the incident.**
- identify and validate incidents.
- Conduct CSIRT response training.
- Implement procedures to contain threats.

17. Which top-level element of the VERIS schema would allow a company to log who the actors were, what actions affected the asset, which assets were affected, and how the asset was affected?

- **incident description**
- incident tracking
- discovery and response
- victim demographics

18. What is the role of vendor teams as they relate to CSIRT?

- Coordinate incident handling across multiple CSIRTs.
- **Handle customer reports concerning security vulnerabilities.**
- Use data from many sources to determine incident activity trends.
- Provide incident handling to other organizations as a fee-based service.

19. According to information outlined by the Cyber Kill Chain, which two approaches can help identify reconnaissance threats? (Choose two.)

- **Analyze web log alerts and historical search data.**
- Audit endpoints to forensically determine origin of exploit.
- **Build playbooks for detecting browser behavior.**
- Conduct full malware analysis.
- Understand targeted servers, people, and data available to attack.

20. To ensure that the chain of custody is maintained, what three items should be logged about evidence that is collected and analyzed after a security incident has occurred? (Choose three.)

- measures used to prevent an incident
- **time and date the evidence was collected**
- extent of the damage to resources and assets
- vulnerabilities that were exploited in an attack
- **serial numbers and hostnames of devices used as evidence**

- **location of all evidence**

21. Which schema or model was created to anonymously share quality information about security events to the security community?

- **VERIS**
- Diamond
- CSIRT
- Cyber Kill Chain

22. What is the purpose of the policy element in a computer security incident response capability of an organization, as recommended by NIST?

- It provides a roadmap for maturing the incident response capability.
- It provides metrics for measuring the incident response capability and effectiveness.
- It defines how the incident response teams will communicate with the rest of the organization and with other organizations.
- **It details how incidents should be handled based on the organizational mission and functions.**

23. What information is gathered by the CSIRT when determining the scope of a security incident?

- the processes used to preserve evidence
- the strategies and procedures used for incident containment
- **the networks, systems, and applications affected by an incident**
- the amount of time and resources needed to handle an incident

24. 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.

25. Which term is used in the Diamond Model of intrusion to describe a tool that a threat actor uses toward a target system?

- infrastructure
- **capability**
- weaponization
- adversary

26. What is the role of a Computer Emergency Response Team?

- Receive, review, and respond to security incidents in an organization.
- Provide national standards as a fee-based service.
- Coordinate security incident handling across multiple CSIRTs.
- **Provide security awareness, best practices, and security vulnerability information to a specific population.**