

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

1. Which event is user interaction?

A. gaining root access

B. executing remote code

C. reading and writing file permission

D. opening a malicious file

Answer(s): D

2. Which security principle requires more than one person is required to perform a critical task?

A. least privilege

B. need to know

C. separation of duties

D. due diligence

Answer(s): C

3. How is attacking a vulnerability categorized?

A. action on objectives

B. delivery

C. exploitation

D. installation

Answer(s): C

4. What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs

B. It provides a centralized platform

C. It collects and detects all traffic locally

D. It manages numerous devices simultaneously

Answer(s): C

5. Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making

B. rapid response

C. data mining

D. due diligence

Answer(s): B

6. One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization

B. confidentiality, integrity, and authorization

C. confidentiality, identity, and availability

D. confidentiality, integrity, and availability

Answer(s): D

7. What is rule-based detection when compared to statistical detection?

A. proof of a user's identity

B. proof of a user's action

C. likelihood of user's action

D. falsification of a user's identity

Answer(s): B

8. A user received a malicious attachment but did not run it. Which category classifies the intrusion?

A. weaponization

B. reconnaissance

C. installation

D. delivery

Answer(s): D

9. Which process is used when IPS events are removed to improve data integrity?

A. data availability

B. data normalization

C. data signature

D. data protection

Answer(s): B

10. An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

A. sequence numbers

B. IP identifier

C. 5-tuple

D. timestamps

Answer(s): C

11. What is a difference between SOAR and SIEM?

A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not

B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not

C. SOAR receives information from a single platform and delivers it to a SIEM

D. SIEM receives information from a single platform and delivers it to a SOAR

Answer(s): A

12. What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator

B. MAC is the strictest of all levels of control and DAC is object-based access

C. DAC is controlled by the operating system and MAC is controlled by an administrator

D. DAC is the strictest of all levels of control and MAC is object-based access

Answer(s): B

13. What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege

B. need to know

C. integrity validation

D. due diligence

Answer(s): A

14. What is the virtual address space for a Windows process?

A. physical location of an object in memory

B. set of pages that reside in the physical memory

C. system-level memory protection feature built into the operating system

D. set of virtual memory addresses that can be used

Answer(s): D

15. Which security principle is violated by running all processes as root or administrator?

A. principle of least privilege

B. role-based access control

C. separation of duties

D. trusted computing base

Answer(s): A

16. What is the function of a command and control server?

A. It enumerates open ports on a network device

B. It drops secondary payload into malware

C. It is used to regain control of the network after a compromise

D. It sends instruction to a compromised system

Answer(s): D

17. What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection is more secure than stateful inspection on Layer 4

B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7

C. Stateful inspection is more secure than deep packet inspection on Layer 7

D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer

Answer(s): D

18. Which evasion technique is a function of ransomware?

- A. extended sleep calls
- B. encryption
- C. resource exhaustion
- D. encoding

Answer(s): B

19. Refer to the exhibit.

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category
2018-03-07 13:42:01	2018-03-07 13:42:01	Sinkhole DNS Block		10.0.10.75		JERI LABORDE (DCLLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC
2018-03-07 13:42:01	2018-03-07 13:42:01	Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC
2018-03-07 13:42:01	2018-03-07 13:42:01	Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLLOUD-SOC, LDAP)	192.168.1.153		DNS Intelligence-CnC

Which two elements in the table are parts of the 5-tuple? (Choose two.)

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

Answer(s): D E

20. DRAG DROP (Drag and Drop is not supported)

Drag and drop the security concept on the left onto the example of that concept on the right.

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

- A. See Explanation section for answer.

Answer(s): A

