Understanding Cisco Cybersecurity Fundamentals

1. After a large influx of network traffic to externally facing devices, you begin investigating what appear to be a denial of service attack. When you review packets capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

A. Traffic fragmentation.

B. Host porfiling.

C. Port scanning.

D. SYN flood.

Answer(s): D

---

2. Which purpose of the certificate revocation list is true?

A. Provide a list of certificates that are trusted regardless of other validity makers.

B. Provide a list of certificates used in the chain of trust

C. Provide a list of certificates of certificates that are untrusted regardless of other validity makers.

D. Provide a list of alternate device identifiers.

Answer(s): C

---

3. What does the sum of the risks presented by an application represent for that application?

A. Application attack surface

B. Vulnerability

C. Security violation

D. HIPPA violation

Answer(s): A

---

4. In which context is it inappropriate to use a hash algorithm?

A. Verifying file integrity

B. Telnet logins

C. Digital signature verification

D. SSH logins

Answer(s): B

---

5. Which is considered a configuration item?

A. network switch

B. SNMP configuration on a router

C. policy-defining configuration management

D. software backup image of a server

Answer(s): C

---

6. As per RFC 1035 which transport layer protocol is used for DNS zone transfer?

A. RDP

B. UDP

C. TCP

D. HTTP

Answer(s): C

---

7. For which kind of attack does an attacker use known information in encrypted files to break the encryption scheme for the rest of the file ciphertext?

A. unknown key

B. known-ciphertext

C. known-plaintext

D. man in the middle

Answer(s): C

---

8. Which term describes reasonable effort that must be made to obtain relevant information to facilitate appropriate courses of action?

A. data mining.

B. ethical behavior

C. Due diligence

D. decision making

Answer(s): C

---

9. Which of the following are examples of system-based sandboxing implementations? (Select all that apply.)

A. Google Project Zero

B. Java JVM sandboxing

C. HTML5 "sandbox" attribute for use with iframes.

D. Threat Grid

E. Google Chromium sandboxing

Answer(s): B,C,E

---

10. Which evasion method may be in use when TLS is observed between two endpoints?

A. traffic insertion

B. tunneling

C. encryption

D. X.509 certificate authentication

Answer(s): B

---

11. What may an increase in IPv4 traffic carrying protocol 41 indicate?

A. deployment of a GRE network on top of an existing Layer 3 network

B. unauthorised peer to peer traffic

C. additional PPTP traffic due to Windows clients

D. attempts to tunnel IPv6 traffic through an IPv4 network

Answer(s): D

---

12. Which benefit does the Antivirus Engine within AMP for Endpoints provide?

A. It displays all files mat have been executed across your organization, ordered by prevalence from lowest to highest

B. It provides visibility into which command line arguments are used to launch executables

C. It performs offline and system based detections, including rootkit scanning

D. It continuously tracks file propagation over time throughout your environment.

Answer(s): C

---

13. Which tool is commonly used in a Security Operations center to aggregate logs sent by endpoint system, firewalls, intrusion prevention systems, and NetFlow?

A. Security Information Management System

B. Security Information and Event Management system

C. Cybersecurity Event Management

D. Firepower Management Center

Answer(s): B

---

14. A child process that's permitted to continue on its own after its parent process is terminated. What is that child process called?

A. Leaf.

B. Child tab.

C. Orphan

D. Zombie.

Answer(s): C

---

15. Which term represents a weakness in a system that could lead to the system being compromised?

A. exploit

B. vulnerability

C. threat

D. risk

Answer(s): B

---

16. which protocol helps to synchronizes and correlate events across multiple network devices:

A. NTP

B. CDP

C. SNMP

D. time zone

Answer(s): A

---

17. Which access control model does SELinux use?

A. RBAC

B. MAC

C. DAC

D. ABAC

Answer(s): B

---

18. Which encryption algorithm is the strongest?

A. 3DES

B. CES

C. AES

D. DES

Answer(s): C

---

19. Which definition of vulnerability is true?

A. software that does not have the most current patch applied

B. an exploitable unpatched and unmitigated weakness in software

C. an incompatible piece of software

D. software that was not approved for installation

Answer(s): B

---

20. Which data can be obtained using NetFlow?

A. network downtime

B. report full packet capture

C. application logs

D. session data

Answer(s): D