Implementing and Operating Cisco Security Core Technologies

1. In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. Smurf

B. distributed denial of service

C. cross-site scripting

D. rootkit exploit

Answer(s): C

---

2. Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application

B. Linux and Windows operating systems

C. database

D. web page images

Answer(s): A

---

3. Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)

☐ A. Check integer, float, or Boolean string parameters to ensure accurate values.

☐ B. Use prepared statements and parameterized queries.

□ C. Secure the connection between the web and the app tier.

□ D. Write SQL code instead of using object-relational mapping libraries.

□ E. Block SQL code execution in the web application database login.

Answer(s): A B

---

4. Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

□ A. Patch for cross-site scripting.

□ B. Perform backups to the private cloud.

□ C. Protect against input validation and character escapes in the endpoint.

□ D. Install a spam and virus email filter.

□ E. Protect systems with an up-to-date antimalware program

Answer(s): D E

---

5. Which two mechanisms are used to control phishing attacks? (Choose two)

□ A. Enable browser alerts for fraudulent websites.

□ B. Define security group memberships.

□ C. Revoke expired CRL of the websites.

□ D. Use antispyware software.

□ E. Implement email filtering techniques.

Answer(s): A E

---

6. Which two behavioral patterns characterize a ping of death attack? (Choose two)

- □ A. The attack is fragmented into groups of 16 octets before transmission.
- □ B. The attack is fragmented into groups of 8 octets before transmission.
- □ C. Short synchronized bursts of traffic are used to disrupt TCP connections.
- □ D. Malformed packets are used to crash systems.
- □ E. Publicly accessible DNS servers are typically used to execute the attack.

Answer(s): B D

---

7. Which two preventive measures are used to control cross-site scripting? (Choose two)

- □ A. Enable client-side scripts on a per-domain basis.
- □ B. Incorporate contextual output encoding/escaping.
- □ C. Disable cookie inspection in the HTML inspection engine.
- □ D. Run untrusted HTML input through an HTML sanitization engine.
- □ E. Same Site cookie attribute should not be used.

Answer(s): A B

---

8. What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.

B. A spear phishing campaign is aimed at a specific person versus a group of people.

C. Spear phishing is when the attack is aimed at the C-level executives of an organization.

D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer(s): B

---

9. Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Answer(s): D

---

10. What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

A. STIX

B. XMPP

C. pxGrid

D. SMTP

Answer(s): A

---

11. Which two capabilities does TAXII support? (Choose two)

□ A. Exchange

□ B. Pull messaging

□ C. Binding

□ D. Correlation

□ E. Mitigating

Answer(s): A B

---

12. Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

□ A. exploits

□ B. ARP spoofing

□ C. denial-of-service attacks

□ D. malware

□ E. eavesdropping

Answer(s): A D

---

13. Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

A. url

B. terminal

C. profile

D. selfsigned

Answer(s): C

---

14. What are two rootkit types? (Choose two)

□ A. registry

□ B. virtual

□ C. bootloader

□ D. user mode

□ E. buffer mode

Answer(s): C D

---

15. Which form of attack is launched using botnets?

A. EIDDOS

B. virus

C. DDOS

D. TCP flood

Answer(s): C

---

16. Which threat involves software being used to gain unauthorized access to a computer system?

A. virus

B. NTP amplification

C. ping of death

D. HTTP flood

Answer(s): A

---

17. Which type of attack is social engineering?

A. trojan

B. phishing

C. malware

D. MITM

Answer(s): B

---

18. Which two key and block sizes are valid for AES? (Choose two)

□ A. 64-bit block size, 112-bit key length

□ B. 64-bit block size, 168-bit key length

□ C. 128-bit block size, 192-bit key length

□ D. 128-bit block size, 256-bit key length

□ E. 192-bit block size, 256-bit key length

Answer(s): C D

---

19. Which two descriptions of AES encryption are true? (Choose two)

□ A. AES is less secure than 3DES.

□ B. AES is more secure than 3DES.

□ C. AES can use a 168-bit key for encryption.

□ D. AES can use a 256-bit key for encryption.

□ E. AES encrypts and decrypts a key three times in sequence.

Answer(s): B D

---

20. Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM

B. SHA-96

C. AES-256

D. SHA-384

Answer(s): A
