Comptia Academic/E2C Security+ Certification Exam Voucher Only

1. A company's Chief Information Officer realizes the company cannot continue to operate after a disaster. Which of the following describes the disaster?

A. Vulnerability

B. Risk

C. Threat

D. Asset

Answer(s): C

---

2. Which of the following is an application security coding problem?

A. Error and exception handling

B. Patch management

C. Application hardening

D. Application fuzzing

Answer(s): A

---

3. Which of the following should be used to authenticate and log connections from wireless users connecting with EAP-TLS?

A. LDAP

B. RADIUS

C. Kerberos

D. SAML

Answer(s): B

---

4. After a company has standardized to a single operating system, not all servers are immune to a well-known OS vulnerability. Which of the following solutions would mitigate this issue?

A. Host based firewall

B. Initial baseline configurations

C. Discretionary access control

D. Patch management system

Answer(s): D

---

5. Which of the following will help prevent smurf attacks?

A. Disabling unused services on the gateway firewall

B. Allowing necessary UDP packets in and out of the network

C. Flash the BIOS with the latest firmware

D. Disabling directed broadcast on border routers

Answer(s): D

---

6. The chief Risk officer is concerned about the new employee BYOD device policy and has requested the security department implement mobile security controls to protect corporate data in the event that a device is lost or stolen. The level of protection must not be compromised even if

the communication SIM is removed from the device. Which of the following BEST meets the requirements? (Select TWO)

A. Asset tracking

B. Screen-locks

C. GEO-Tracking

D. Device encryption

Answer(s): A,D

---

7. Which of the following would be MOST appropriate to secure an existing SCADA system by preventing connections from unauthorized networks?

A. Implement a NIDS to protect the SCADA system

B. Implement a firewall to protect the SCADA system

C. Implement a HIDS to protect the SCADA system

D. Implement a Layer 2 switch to access the SCADA system

Answer(s): B

---

8. Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years.

A. Accept the risk saving $10,000.

B. Ignore the risk saving $5,000.

C. Mitigate the risk saving $10,000.

D. Transfer the risk saving $5,000.

Answer(s): D

---

9. An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.

A. Use encryption for the credential fields and hash the credit card field

B. Encrypt the username and hash the password

C. Hash the credential fields and use encryption for the credit card field

D. Hash both the credential fields and the credit card field

Answer(s): C

---

10. After working on his doctoral dissertation for two years, Joe, a user, is unable to open his dissertation file. The screen shows a warning that the dissertation file is corrupted because it is infected with a backdoor, and can only be recovered by upgrading the antivirus software from the free version to the commercial version. Which of the following types of malware is the laptop MOST likely infected with?

A. Trojan

B. Ransomware

C. Backdoor

D. Armored virus

Answer(s): B

---

11. An administrator needs to secure a wireless network and restrict access based on the hardware address of the device. Which of the following solutions should be implemented?

A. Enable MAC filtering

B. Force the WAP to use channel 1

C. Upgrade to WPA2 encryption

D. Use a stateful firewall

Answer(s): A

---

12. A distributed denial of service attack can BEST be described as:

A. Invalid characters being entered into a field in a database application.

B. Users attempting to input random or invalid data into fields within a web browser application.

C. Multiple computers attacking a single target in an organized attempt to deplete its resources.

D. Multiple attackers attempting to gain elevated privileges on a target system.

Answer(s): C

---

13. Which the following flags are used to establish a TCP connection? (Select TWO).

A. PSH

B. ACK

C. SYN

D. URG

E. FIN

Answer(s): B,C

---

14. Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

A. Network based firewall

B. Anti-spam software

C. Host based firewall

D. Anti-spyware software

Answer(s): D

---

15. The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

A. Recovery

B. Follow-up

C. Validation

D. Identification

E. Eradication

F. Containment

Answer(s): D

---

16. A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of

A. Brute force password attack

B. Cross-site request forgery

C. Cross-site scripting

D. Fuzzing

Answer(s): B

---

17. A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

A. SNMP

B. SNMPv3

C. ICMP

D. SSH

Answer(s): B

---

18. An organization recently switched from a cloud-based email solution to an in-house email server. The firewall needs to be modified to allow for sending and receiving email. Which of the following ports should be open on the firewall to allow for email traffic? (Select THREE).

A. TCP 22

B. TCP 23

C. TCP 445

D. TCP 53

E. TCP 110

F. TCP 143

G. TCP 25

Answer(s): E,F,G

19. A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

A. IPsec

B. SFTP

C. BGP

D. PPTP

Answer(s): A

---

20. Which of the following should a security technician implement to identify untrusted certificates?

A. CA

B. PKI

C. CRL

D. Recovery agent

Answer(s): C
