Comptia Security+ Certification

1. An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up.

A. Rootkit

B. Ransomware

C. Spyware

D. Scareware

Answer(s): B

---

2. A group of users from multiple departments are working together on a project and will maintain their digital output in a single location. Which of the following is the BEST method to ensure access is restricted to use by only these users?

A. Group based privileges

B. User assigned privileges

C. Rule-based access

D. Mandatory access control

Answer(s): B

---

3. Which of the following is the GREATEST security risk of two or more companies working together under a Memorandum of Understanding?

A. Budgetary considerations may not have been written into the MOU, leaving an entity to absorb more cost than intended at signing.

B. MOUs have strict policies in place for services performed between the entities and the penalties for compromising a partner are high.

C. MOUs are generally loose agreements and therefore may not have strict guidelines in place to protect sensitive data between the two entities.

D. MOUs between two companies working together cannot be held to the same legal standards as SLAs.

Answer(s): C

---

4. In order for network monitoring to work properly, you need a PC and a network card running in what mode?

A. Launch

B. Exposed

C. Promiscuous

D. Sweep

Answer(s): C

---

5. Which of the following automated or semi-automated software testing techniques relies on inputting large amounts of random data to detect coding errors or application loopholes?

A. SQL injection

B. Fault injection

C. Black box

D. Fuzzing

Answer(s): D

---

6. A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

A. Create new email spam filters to delete all messages from that sender

B. Set the email program default to open messages in plain text

C. Install host-based firewalls on all computers that have an email client installed

D. Install end-point protection on all computers that access web email

Answer(s): D

---

7. A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?

A. ACL

B. IDS

C. UTM

D. Firewall

Answer(s): C

---

8. The Quality Assurance team is testing a third party application. They are primarily testing for defects and have some understanding of how the application works. Which of the following is the team performing?

A. Black box testing

B. Penetration testing

C. Grey box testing

D. White box testing

Answer(s): C

---

9. A network administrator has purchased two devices that will act as failovers for each other.

A. Authentication

B. Integrity

C. Confidentiality

D. Availability

Answer(s): D

---

10. A network technician at a company, Joe is working on a network device. He creates a rule to prevent users from connecting to a toy website during the holiday shopping season. This website is blacklisted and is known to have SQL injections and malware. Which of the following has been implemented?

A. Implicit Deny

B. Mandatory access

C. Firewall rules

D. Network separation

Answer(s): A

---

11. All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD.

B. RC4.

C. SHA-512.

D. MD4.

Answer(s): B

---

12. An administrator is investigating a system that may potentially be compromised, and sees the following log entries on the router.

A. It is running a rogue web server

B. It is being used in a man-in-the-middle attack

C. It is participating in a botnet

D. It is an ARP poisoning attack

Answer(s): C

---

13. A security administrator must implement a wireless security system, which will require users to enter a 30 character ASCII password on their accounts. Additionally the system must support 3DS wireless encryption.

A. WPA2-CCMP with 802.1X

B. WPA2-PSK

C. WPA2-CCMP

D. WPA2-Enterprise

Answer(s): D

---

14. A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

A. The CSP takes into account multinational privacy concerns

B. The financial review indicates the company is a startup

C. The CPS utilizes encryption for data at rest and in motion

D. SLA state service tickets will be resolved in less than 15 minutes

Answer(s): A

---

15. A network operations manager has added a second row of server racks in the datacenter.

A. To maximize fire suppression capabilities

B. To create environmental hot and cold isles

C. To eliminate the potential for electromagnetic interference

D. To lower energy consumption by sharing power outlets

Answer(s): B

---

16. Which of the following password attacks involves attempting all kinds of keystroke combinations on the keyboard with the intention to gain administrative access?

A. Watering hole

B. Brute Force

C. Hybrid

D. Dictionary

Answer(s): D

---

17. An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

A. Find a common hash between a specific message and a random message

B. Find two identical messages with different hashes

C. Find a common has between two specific messages

D. Find two identical messages with the same hash

Answer(s): B

---

18. Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?

A. Replay

B. Fraggle

C. Smurf

D. Xmas

Answer(s): D

---

19. When using PGP, which of the following should the end user protect from compromise?

A. Private key

B. CRL details

C. Public key

D. Key password

E. Key escrow

F. Recovery agent

Answer(s): A,D

---

20. A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing

B. Mantrap

C. A guard

D. Video surveillance

Answer(s): B
