UPGRADE YOUR SKILL

IT SECURITY PRACTICE TEST QUESTIONS

1. What is the term for a backup of an entire partition or computing system's hard drive? Select all that apply.

A. Incremental backup
B. Continuous backup
C. System image
D. System restore
E. Full backup
G. Differential backup

---

2. What valuable function do hashing algorithms provide? Choose the best answer.

A. Hashes encrypt messages, making them impossible to read without the decryption key.
B. Hashes mask packet header information, protecting the anonymity of the data's sender.
C. Hashes compute a unique value based on the message's content, verifying the integrity of the data.
D. None of the above.

---

3. Which of the following security mechanisms are used to identify an individual? Select all that apply.

A. Symmetric encryption key
B. Asymmetric encryption key
C. ID access card
D. PIN number
E. Message digest

---

4. Which of the following are valid functions of firewalls? Select all that apply.

A. To permit or deny traffic based on port numbers.
B. To permit or deny traffic based on the source address.
C. To permit or deny traffic based on the destination address.
D. To provide login authentication, similarly to a TACACS+ or RADIUS server.
E. To scan and identify malware threats that have invaded host systems.
F. To detect network intrusions.

5. Which of the following VPN connection protocols offers the weakest security, and is unfit for sensitive applications, such as the banking industry? Choose the best answer.

A. PPTP
B. L2TP/IPsed
C. OpenVPN
D. SSTP

---

6. Which of the following accurately describes a zero-day vulnerability?

A. A software error whereby improperly sanitized data accepts a zero or null value, which causes the system to crash.
B. A vulnerability caused by the access and manipulation of a computer system's internal clock using NTP (Network Time Protocol) that causes systems to revert to older system updates, thereby reintroducing past security flaws by removing software patches.
C. A vulnerability that has been known and present since the software released.
D. A vulnerability unknown to the software developers that has existed for a period of time, but only recently been discovered.

---

7. True or false? EMI shielding is a modern requirement necessary for the secure operation of wireless networks.

A. True
B. False

---

8. Which of the following describes the best way to manage heat in a server room? Select all that apply.

A. Alternate aisles with hot and cold designations to efficiently manage heat.
B. Place the front ends of the servers all in the same direction.
C. Blow cold air into the center of the room and face the back-ends of all servers and devices towards the outer walls.
D. Refrain from placing servers above 4 feet above the ground, since heat rises and can cause systems to overheat.

9. Which of the following tunneling options do **not** provide any encryption? Select all that apply:

A. L2TP
B. PPTP
C. IPSec
D. GRE
E. OpenVPN
F. All of these tunneling options provide encryption.
G. None of these tunneling options provide encryption.

---

10. Which of the following is/are traits of RAID level 10? Select all that apply.

A. Disk striping
B. Disk mirroring
C. Parity
D. None of the above

---

11. When considering backups, which of the following accurately describes the purpose and function of the archive bit?

A. The archive bit signals how much storage space is required to archive a file.
B. The archive bit signals whether or not a file has already been backed up.
C. The archive bit marks the sector of the hard drive where the first block of the backup data is stored.
D. The archive bit is only present on files stored on mirrored RAID drives, and marks the file as a redundant backup.

---

12. Which, if any, of the following protocols are used with HTTPS?

A. SSH
B. IPsec
C. TFTP
D. SSL

E. L2TP
F. PPTP
G. None of the above.

---

13. Which of the following matches protocols with the correct port numbers? Select all that apply.

A. HTTPS uses port 443, and SSL uses port 443.
B. HTTPS uses port 80, and SSL uses port 443.
C. HTTPS uses port 443, and SSL uses port 80.
D. IKE uses port 500, and PPTP uses port 1723.
E. IKE uses port 501, and PPTP uses port 1237.
F. IKE uses port 53, and PPTP uses port 123.
G. SSH uses port 21, and Telnet uses port 22.
H. SSH uses port 22, and Telnet uses port 23.
I. SSH uses port 23, and Telnet uses port 24.

---

14. Which of the following lists the layers of the OSI model in ascending order? Choose the correct answer.

A. Physical, Data-link, Network, Transport, Session, Application, Presentation
B. Network, Transport, Session, Application, Presentation, Physical, Data-link
C. Data-link, Network, Transport, Session, Presentation, Application, Physical
D. Data-link, Physical, Network, Transport, Session, Presentation, Application
E. Network, Data-link, Physical, Network, Transport, Session, Application
F. Physical, Data-link, Network, Transport, Session, Presentation, Application
G. Application, Session, Transport, Network, Physical, Data-link
H. Network,Physical, Network, Transport, Session, Application, Data-link

---

15. Which of the following should be avoided when drafting a password policy? Select all that apply.

A. Using personal information, such as addresses and birth dates, as your password.
B. Writing passwords down on post-it notes and other easily accessible
C. Using numerics, alpha-numerics, special symbols, and a mix of upper and lower-case symbols.
D. Creating passwords that are at least 7 characters in length.
E. Using random generators that create strings of text that are not easily remembered, even by the user in possession of the login credentials.

F. Creating a new password every 30 days.

---

16. True or false? It is, generally speaking, more secure to disable pings from external sources such as extranets and public IP addresses.

A. True.
B. False.

---

17. Which of the following mechanisms, if any, is used by ping operations?

A. ICMP echo request.
B. ICMP echo reply.
C. IKE
D. GRE
E. SMTP
F. SSH
G. None of the above.

---

18. Which TCP ports, if any, does ICMP use? Choose the correct answer(s).

A. Port 53.
B. Ports 21 and 22.
C. Port 443.
D. Port 80.
E. Port 8080.
F. Port 25.
G. All of the above.
H. None of the above.

---

19. True or false? Layer 2 switches commonly use ACLs to block or forward traffic.

A. True.
B. False.

---

20. True or false? An HTTP proxy server encrypts data and masks the IP address of incoming connections.

A. True.
B. False.

1.
Correct answer: C.

Explanation: Though counter intuitive, a full backup may not necessarily contain any system files. Instead, a full backup completely backs up a group of files, regardless of previous incremental backups. Incremental backups seek to only back up the changed files in a set of data. A differential backup works by copying all the files that have changed since the last full backup.

2.
Correct answer: C.

Explanation: Hashes do not provide encryption or anonymity. Rather, they verify that the data was not altered in transit by computing a hash value, which is sometimes called message digest. By using a string of text as input, the hashing algorithm computes a unique value. The algorithm is run again on the receiving system, and if the values match, the data's integrity is valid.

3.
Correct answer: C and D.

Explanation: Pin numbers and identity cards are frequently used to identify individuals for various security applications. Encryption keys are used to scramble data, and a message digest is used for hashing purposes.

4.
Correct answer: A, B, C.

Explanation: Firewalls don't typically provide authentication services or scan for malware (as antivirus software would). The last choice is incorrect because that is the function of an IPS and IDS device.

5.
Correct answer: A.

Explanation: PPTP is one of the weakest tunneling options in existence, and is on it's way towards becoming obsolete. In fact, it can easily be cracked due to security vulnerabilities and flaws in the algorithm using inexpensive software. As such, it is unfit for most real-world applications.

6.
Correct answer: D.

Explanation: A zero-day vulnerability is a massive threat because it requires the software developers to scramble in order to patch it as soon as possible. The anti-malware software industry responds to zero-day threats as fast as possible, and pushes updates to their clients to provide cutting-edge protection from the latest threats.

7.
Correct answer: B.

Explanation: EMI shielding protects physical cable mediums, such as Ethernet, from electro-magnetic interference. Electromagnetic interference can cause the weakening and attenuation of signals traversing a physical cable medium at layer 1 of the OSI model.

8.
Correct answer: A.

Explanation: Alternating hot and cold aisles prevents servers and networking devices from taking in heat from other systems.

9.
Correct answer: A and D.

Explanation: LT2P is strictly a transport protocol. By itself, it offers no encryption; that's why it is often paired with IPSec, which does provide encryption features. Furthermore, GRE does not provide encryption by itself, either, and can be paired with other protocols to secure data with encryption.

10.
Correct answer: A and B.

Explanation: RAID 0 works by striping data across multiple drives, while RAID 1 offers mirroring operations for redundancy. RAID 1 + 0 is often simply referred to as RAID 10.

11.
Correct answer: B.

Explanation: The archive bit's purpose is to include or exclude files in various backup operations. The archive bit is set when files have changed since the last full backup.

12.
Correct answer: D.

Explanation: SSL is used to secure HTTP connections, using port 443.

13.
Correct answer: A, D, and H.

Explanation: HTTPS is really just an HTTP connection secured by SSL. Both HTTPS and SSL use port 443. IKE, which is used to initiate VPN tunnel connections, uses port 500 while PPTP uses port 1723. SSH, which is a secured connection, uses port 22, but Telnet (which is not secured) uses port 23.

14.
Correct answer: F.

Explanation: If you want a good mnemonic device to help remember the OSI layers, remember the phrase “Please Do Not Throw Sausage Pizza Away.” The first letter of each word matches the first letter of each layers name: Physical, Data-link, Network, Transport, Session, Presentation, Application.

15.
Correct answer: A, B, and D.

Explanation: Answers A and B are just poor security practice. Answer D should be avoided as well, because the general rule-of-thumb is to create passwords *at least* 8 characters long, though

some corporate policies specify longer requirements.

16.
Correct answer: A.

Explanation: Pings are frequently used in scanners and reconnaissance tools to identify active hosts. As such, it's better to disable them from sources other than the local network to thwart potential scanning and network discovery attempts.

17.
Correct answer: A and B.

Explanation: The ping utility is contained within ICMP (Internet Control Message Protocol). For a ping to succeed, it needs to successfully send an ICMP echo request, and receive an ICMP echo reply.

18.
Correct answer: H.

Explanation: ICMP doesn't use a TCP or UDP port to facilitate connections. In fact, ICMP doesn't even belong in the same layer as TCP or UDP (they belong in the IP Transport layer). ICMP belongs in the next-lowest layer, the Internet layer. As such, it doesn't use port numbers, though firewalls can still identify and block this type of traffic.

19.

Correct answer: B.

Explanation: Layer two switches don't make advanced decisions on layer 3 addresses or TCP ports. ACLs are more typically found on routers, layer 3 switches, and firewalls.

20
Correct answer: B.

Explanation: Though proxy servers do have the ability to mask IP addresses, HTTP proxy connections are insecure because they don't provide encryption.