

1. Among the most frequent Internet attacks, which of the following is not true.

1 / 1 point

- ☐ DNS attacks result in changed domain names in order to hijack a communication session
- ☒ Brute force attacks result in stolen smartphones, laptops, etc.
- ☐ Browser attacks are the most frequent Internet attack type
- ☐ Browser attacks can be defended by updating the OS and application
- ☐ Scan attacks result in computer ports being used in security breaches to the network computing systems

✓ Correct

2. Among the following descriptions of 3G (3rd Generation) Firewalls, which is incorrect?

1 / 1 point

- ☐ HTTP and DNS operations are filtered in 3G firewalls
- ☐ 3G firewalls include IPS (Intrusion Prevention System) technology
- ☐ 3G firewalls use DPI (Deep Packet Inspection) and WAF (Web Application Firewall) technology
- ☐ User Identities and computer MAC addresses are monitored in 3G firewalls
- ☒ 3G firewalls track state changes in IPv4 and IPv6, but does not track TCP or UDP changes

✓ Correct

3. Among the following descriptions of how to prevent an attack, which is incorrect?

1 / 1 point

- ☒ Backdoor attacks can be defended by frequent replacing of Internet switches and routers
- ☐ Brute force attacks can be defended by frequent and well-selected password changes
- ☐ DoS (Denial of Service) attacks can be defended by anti-virus software and firewall updating
- ☐ DNS spoofing and hijacking can be defended by using a random source port and updating server security patches
- ☐ DNS attacks can be defended by using a random source port and updating server security patches

✓ Correct

4. Among the following, which is not a type of IDS (Intrusion Detection System)?

1 / 1 point

- ☐ Anomaly-based IDS
- ☐ HIDS (Host IDS)
- ☒ Location-based IDS
- ☐ Signature-based IDS
- ☐ NIDS (Network IDS)

✓ Correct

5. Among the following listed,
which is not a Phishing type?

1 / 1 point

- ☐ Clone Phishing
- ☐ Social Engineering
- ☐ Whaling
- ☐ Link Manipulation
- ☐ Filter Evasion
- ☒ Fishing Phishing

✓ Correct

6. Among the following descriptions of Buffer Overflow, which is incorrect?

1 / 1 point

- ☐ Buffer overflow is used in DoS (Denial of Service) and DDoS (Distributed DoS) attacks
- ☐ Buffer overflow can occur when malware overruns the buffer's boundary and overwrites into adjacent memory locations
- ☐ Buffer overflow defense schemes include randomizing the layout of memory and monitoring actions that write into adjacent memory spaces
- ☐ Stack overflow is a type of buffer overflow that the attacker manipulates a local variable, the return address, or a function pointer to create a malfunction on the stack's buffer
- ☒ USB overflow is a type of buffer overflow that the attacker fills up one's portable USB such that no more files can be saved on the USB memory device

✓ Correct

7. Among the following Internet security and threat issues, which is not true?

1 / 1 point

- ☐ Zero-day attacks commonly result in disabled web services
- ☐ A zombie computer is a hacker compromised computer that is connected to the Internet
- ☒ Companies that receive a cyber attack are seldom attacked again
- ☐ Users of zombie computers are commonly unaware
- ☐ New zero-day vulnerabilities are discovered almost every day

✓ Correct

8. Among the following Internet security and protection schemes, which is not true?

1 / 1 point

- ☐ Botnets are used to conduct various Internet attacks, which include DDoS, spam, and intrusions
- ☐ Backdoors are used by developers or administrators to fix the system, but if a hacker gets access to a backdoor, then the amount of damage to the system or network can be significant
- ☐ DNS spoofing is commonly used in DNS hijacking attacks
- ☒ Botnets are used as a countermeasure to defend against zombie computers
- ☐ MITM (Man-in-the-Middle) attackers secretly relay packets in conducting eavesdropping and manipulation of information

✓ Correct

9. Which of the following statements on Internet security and protection is incorrect?

1 / 1 point

- ☐ TLS (Transport Layer Security)
is a symmetric cryptography technology that is used with encryption keys generated uniquely for each connection in order to provide privacy and data integrity between networked applications
- ☐ WPA2 (Wi-Fi Protected Access 2)
includes all mandatory elements of the IEEE 802.11i standard and requires Wi-Fi Alliance testing and certification
- ☐ SSH (Secure Shell)
cryptography enable secure services over unsecured networks
- ☒ WPA2 certified Wi-Fi devices
are rare to find in new Wi-Fi AP (Access Point) products
- ☐ TLS replaces SSL (Secure Sockets Layer) technology as it provides a higher level of protection

✓ Correct

10. Which of the following statements on Internet security and protection is incorrect?

1 / 1 point

- ☐ Attackers use SQL code injection to attack SQL databases and data-driven applications
- ☒ Due to the vulnerabilities of WPA (Wi-Fi Protected Access), it was replaced with the new WEP (Wired Equivalent Privacy) protocol
- ☐ DoS (Denial of Service) is a cyber attack that disables a device or network by making operational resources unavailable
- ☐ One of the best known defense mechanisms against MITM (Man-in-the-Middle) attacks is to enhance the authentication process using a CA (Certificate Authority)
- ☐ DDoS (Distributed DoS) attacks commonly occur using multiple distributed botnets and zombie computers

✓ Correct