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

1 / 1 point

○ DoS (Denial of Service) attacks can be defended by anti-virus software and firewall updating

○ DNS (Domain Name System) attacks
result in changed domain names in order to hijack a communication session,
which can be prevented by using random source port selections and updating
server security patches

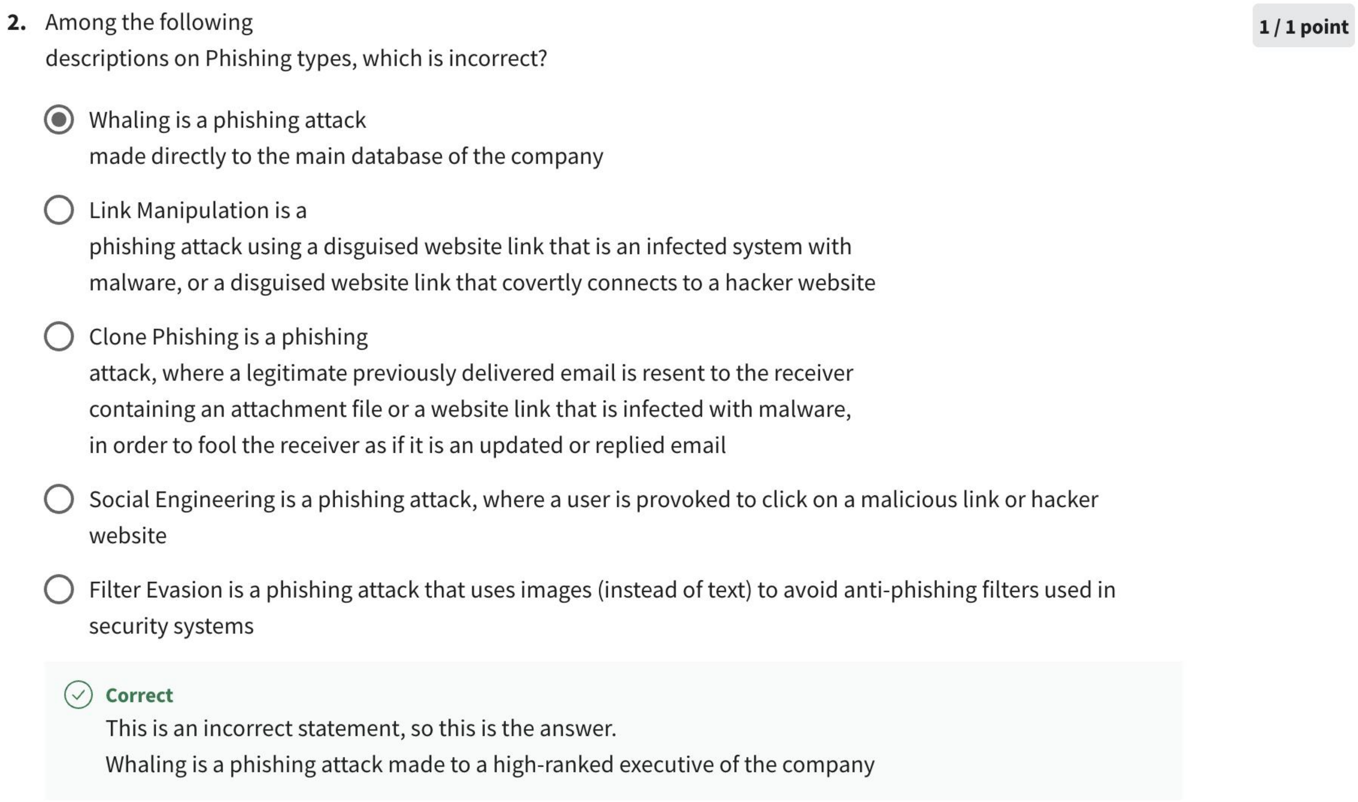
○ Brute force attacks occur when an attacker (repeatedly) tries to decode a password or pin number to gain illegal access of a website or account, and can be defended by frequent and well-selected password and pin number changes

● Browser attacks rarely occur but can be defended by multiple website servers to support the different browser types

○ Scan attacks occur when computer
ports are used to breach the security system of network gateways and servers

○ Backdoor attacks can be defended
by updating security patches and application updates, which are all software
updates

✓ **Correct**
This is the answer. This is not true. Browser attacks are the most frequent Internet attack type and can be defended by updating the browser, OS, and application



2. Among the following
descriptions on Phishing types, which is incorrect?

1 / 1 point

● Whaling is a phishing attack
made directly to the main database of the company

○ Link Manipulation is a
phishing attack using a disguised website link that is an infected system with
malware, or a disguised website link that covertly connects to a hacker website

○ Clone Phishing is a phishing
attack, where a legitimate previously delivered email is resent to the receiver
containing an attachment file or a website link that is infected with malware,
in order to fool the receiver as if it is an updated or replied email

○ Social Engineering is a phishing attack, where a user is provoked to click on a malicious link or hacker website

○ Filter Evasion is a phishing attack that uses images (instead of text) to avoid anti-phishing filters used in security systems

✓ **Correct**
This is an incorrect statement, so this is the answer.
Whaling is a phishing attack made to a high-ranked executive of the company

3. Among the following
descriptions on security technologies, which is incorrect?

1 / 1 point

○ IDS (Intrusion Detection System) types include HIDS (Host IDS), Signature-based IDS, NIDS (Network IDS), and Anomaly-based IDS

○ TLS (Transport Layer Security) is a symmetric cryptography technology that provides privacy and data integrity between networked applications by using uniquely generated encryption keys for each connection

○ 3G firewalls use DPI (Deep
Packet Inspection) and WAF (Web Application Firewall) functions and include IPS
(Intrusion Prevention System) technology

● Stateful filtering of IP
packets and transport layer (TCP, UDP) protocols were conducted by 1G
firewalls, for protection of IP, TCP, and UDP functions

✓ **Correct**

This is an incorrect statement, so this is the answer. 1G firewalls were not capable of conducting stateful filtering. Stateful filtering of IP packets and transport layer (TCP, UDP) protocols were first conducted by 2G firewalls, and because all 2G firewall functions are included in 3G firewalls, 3G firewalls also include the stateful filtering capability

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

1 / 1 point

○ Buffer overflow can be defended
by including a randomized layout of memory and monitoring actions that write
into adjacent memory spaces

● MITM (Man-in-the-Middle)
attacks are due to espionage activity, and therefore, the human spy needs to be
found and removed

○ 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

✓ **Correct**
This is an incorrect statement, so this is the answer. MITM attacks are cyber attacks that can be prevented by using a CA (Certificate Authority) to enhance the authentication process

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

1 / 1 point

○ In 2003, the Wi-Fi Alliance announced that due to the security vulnerabilities of WEP (Wired Equivalent Privacy), WEP was to be replaced with WPA (Wi-Fi Protected Access)

○ WPA was replaced with the more secure WPA2, where currently WPA2 certification is a mandatory requirement for all Wi-Fi devices, including all new APs (Access Points)

● In order to overcome DoS (Denial of Service) cyber attacks, DDoS (Distributed DoS) was created as a security mechanism against DoS attacks by diluting the attacks (making it easier to defend) through intentionally distributing the attack resources

○ SSL (Secure Sockets Layer) was replaced with TLS (Transport Layer Security) due to improved protection

○ SSH (Secure Shell) cryptography can provide secure services over unsecured networks

✓ **Correct**

This is an incorrect statement, so this is the answer. DoS (Denial of Service) cyber attacks disable devices or networks by making operational resources unavailable, and DDoS (Distributed DoS) attacks use multiple distributed botnets and zombie computers in executing more powerful DoS cyber attacks