# Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 7:55:02 pm • Time spent: 00:09

Score: 0%

Passing Score: 80%

## Question 1:

✕ Incorrect

You are the security analyst for your organization and have discovered evidence that someone is attempting to brute-force the root password on the web server. Which classification of attack type is this?

○ Inside

➡ ○ Active

○ External

○ Passive

EXPLANATION

Active attacks are when perpetrators attempt to compromise or affect the operations of a system in some way. For example, trying to brute-force the root password on a web server is considered an active attack. A distributed denial-of-service (DDoS) attack is also an active attack.

Passive attacks occur when perpetrators attempt to gather information without affecting the flow of that information on the network. Packet sniffing and port scanning are passive attacks.

External attacks are when unauthorized individuals try to breach a network from off-site. Remember that perpetrators of external attacks are unauthorized for any level of access to the network.

Inside attacks are initiated by authorized individuals inside the network's security perimeter who attempt to access systems or resources to which they're not authorized. For example, an inside attack could be a disgruntled employee accessing unauthorized company documents and leaking them to the public.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_active_secp7.question.fex

**Question 2:** ✕ Incorrect

Drag the network attack technique on the left to the appropriate description or example on the right. (Each technique may be used once, more than once, or not at all.)

Perpetrators attempt to compromise or affect the operations of a system.

Active attack

Unauthorized individuals try to breach a network from off-site.

External attack

Attempting to find the root password on a web server by brute force.

Active attack

Attempting to gather information without affecting the flow of information on the network.

Passive attack

Sniffing network packets or performing a port scan.

Passive attack

EXPLANATION

Network attacks are classified as follows:

- Active attacks are when perpetrators attempt to compromise or affect the operations of a system in some way. For example, trying to brute-force the root password on a web server is considered an active attack. A distributed denial-of-service (DDoS) attack is also an active attack.
- Passive attacks occur when perpetrators attempt to gather information without affecting the flow of that information on the network. Packet sniffing and port scanning are passive attacks.
- External attacks are when unauthorized individuals try to breach a network from off-site. Remember that perpetrators of external attacks are unauthorized for any level of access to the network.
- Inside attacks are initiated by authorized individuals inside the network's security perimeter who attempt to access systems or resources to which they're not authorized. For example, an inside attack could be a disgruntled employee accessing unauthorized company documents and leaking them to the public.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_attacks_secp7.question.fex

### Question 3: ✕ Incorrect

An attacker sets up 100 drone computers that flood a DNS server with invalid requests. This is an example of which kind of attack?

- ○ Replay
- ○ Backdoor
- ➡ ○ DDoS
- ○ Spamming

EXPLANATION

A denial-of-service (DoS) attack generates excessive traffic to overload communication channels or exploit software flaws. A distributed denial-of-service (DDoS) attack employs multiple attackers.

Spamming is just a traffic generation form of attack where unrequested messages are sent to a victim. Replay and backdoor attacks are both flaw-exploitation attack forms. Replay attacks exploit software flaws by capturing traffic, possibly editing it, and then replaying the traffic in an attempt to gain access to a system. Backdoor attacks exploit software flaws by obtaining access codes or account credentials to bypass security. Backdoors can also be planted by hackers to allow easy re-access to a compromised system.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_ddos_secp7.question.fex

### Question 4: ✕ Incorrect

In which of the following zones would a web server most likely be placed?

➡ ○ Low-trust zone

○ High-trust zone

○ No-trust zone

○ Medium-trust zone

EXPLANATION

A low-trust zone is where publicly available information resides. You do have control over the security of this zone, but it is still exposed to the internet. For example, a web server might reside in this zone. It is also referred to as a DMZ, or demilitarized zone.

A web server would not be housed in any trust zone higher than a low-trust zone. Since the web server is open to the internet, not much trust can be placed in it.

A no-trust zone is a zone that you have no control over, such as the internet.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_dmz_secp7.question.fex

**Question 5:** ✗ Incorrect

Which area of focus helps to identify weak network architecture or design?

- ○ Entry points
- ➡ ○ Documentation
- ○ Network baseline
- ○ Inherent vulnerabilities

EXPLANATION

Documentation is one of the most important components of knowing a network. Proper network documentation and diagrams not only help identify a weak network architecture or design, but they also protect against system sprawl and unknown systems.

Entry points are any possible way into the network. Identifying entry points do not identify weak network architecture or design.

Inherent vulnerabilities are any system that lacks proper security controls. Identifying inherent vulnerabilities does not identify weak network architecture or design.

A network baseline tells you the normal activity level on a network. This does not help in identifying weak network architecture or design.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_docs_secp7.question.fex

**Question 6:** ✕ Incorrect

Which classification of attack type does packet sniffing fall under?

○ Inside

○ Active

○ External

➡ ○ Passive

EXPLANATION

Passive attacks occur when perpetrators attempt to gather information without affecting the flow of that information on the network. Packet sniffing and port scanning are passive attacks.

Active attacks are when perpetrators attempt to compromise or affect the operations of a system in some way. For example, trying to brute-force the root password on a web server is considered an active attack. A distributed denial-of-service (DDoS) attack is also an active attack.

External attacks are when unauthorized individuals try to breach a network from off-site. Remember that perpetrators of external attacks are unauthorized for any level of access to the network.

Inside attacks are initiated by authorized individuals inside the network's security perimeter who attempt to access systems or resources to which they're not authorized. For example, an inside attack could be a disgruntled employee accessing unauthorized company documents and leaking them to the public.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_passive_secp7.question.fex

**Question 7:** ✕ Incorrect

Which area of focus do public-facing servers, workstations, Wi-Fi networks, and personal devices fall under?

○ Network baseline

○ Inherent vulnerabilities

○ Network segmentation

➡ ○ Entry points

EXPLANATION

Public-facing servers, workstations, Wi-Fi networks, and personal devices are all examples of entry points for possible attacks. You must account for anything that connects to the network as a possible entry point.

Inherent vulnerabilities are any system that lacks proper security controls.

Network segmentation is the process of splitting the network into different sections.

A network baseline tells you the normal activity level on a network.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_public_secp7.question.fex

▼ **Question 8:** ✕ Incorrect

Your network devices are categorized into the following zone types:

- No-trust zone
- Low-trust zone
- Medium-trust zone
- High-trust zone

Your network architecture employs multiple VLANs for each of these network zones. Each zone is separated by a firewall that ensures only specific traffic is allowed.

Which of the following is the secure architecture concept that is being used on this network?

○ Virtual local area networking

○ Trust-zone networking

➡ ○ Network segmentation

○ Network firewalling

EXPLANATION

The secure network architecture concept that is being used in this example is network segmentation. The most common way to segment networks is to create multiple VLANs for each network zone. These zones can also be separated by firewalls to ensure only specific traffic is allowed. One way to segment a network is to categorize systems into different zones (for example, a no-trust zone, low-trust zone, medium-trust zone, high-trust zone, and highest-trust zone).

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_segment_secp7.question.fex

### ▼ Question 9: ✕ Incorrect

Your organization has started receiving phishing emails. You suspect that an attacker is attempting to find an employee workstation they can compromise. You know that a workstation can be used as a pivot point to gain access to more sensitive systems.

Which of the following is the MOST important aspect of maintaining network security against this type of attack?

➡ ○ User education and training

○ Network segmentation

○ Documenting all network assets in your organization

○ Identifying inherent vulnerabilities

○ Identifying a network baseline

EXPLANATION

User education and training is the most important aspect of maintaining network security against an email phishing attack.

REFERENCES

☰ 5.8.2 Network Threats Facts

q_net_threat_users_secp7.question.fex

**Question 10:** ✕ Incorrect

Which of the following is commonly created to segment a network into different zones?

○ DNS

○ DMZ

➡ ○ VLANs

○ VPNs

EXPLANATION

The most common way to segment networks is to create multiple virtual local area networks (VLANs) for each network zone.

VPNs are used to create a remote secure connection to a network resource.

A DMZ is a type of zone that is exposed to the internet.

The Domain Name System (DNS) is used to match IP addresses to their corresponding URLs.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_vlan_secp7.question.fex