Chp 11 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/13/2022 8:34:37 pm • Time spent: 12:34

Score: 93%

Passing Score: 80%

Question 1: ✓ Correct

You have run a vulnerability scanning tool and identified several patches that need to be applied to a system. What should you do next after applying the patches?

○ Document your actions.

➡ ● Run the vulnerability assessment again.

○ Use a port scanner to check for open ports.

○ Update the vulnerability scanner definition files.

EXPLANATION

After fixing an identified vulnerability, you should re-run the vulnerability scan to verify that everything has been fixed and that additional issues are not present.

You should update definition files before you run the first scan. Using a port scanner is unnecessary because most vulnerability scanners include a check of open ports. Documenting your actions should occur after you have finished all necessary actions.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_vuln_02_secp7.question.fex

Question 2: ✓ Correct

Which type of denial-of-service (DoS) attack occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses?

○ SYN flood

○ Spam

➡ ● DNS poisoning

○ ARP poisoning

EXPLANATION

DNS poisoning occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. In a DNS poisoning attack:

- Incorrect DNS data is introduced into a primary DNS server.
- The incorrect mapping is made available to client applications through the resolver.
- Traffic is directed to incorrect sites.

ARP poisoning corrupts the ARP cache or sends incorrect ARP data that spoofs MAC addresses, causing devices to send frames to the wrong host or an unreachable host.

Spam sent in such great amounts can consume bandwidth or fill a mailbox, leaving no room for legitimate traffic.

A SYN flood exploits the TCP three-way handshake.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_dns_pois_01_secp7.question.fex

Question 3: ✓ Correct

Which of the following strategies can protect against a rainbow table password attack?

- ○ Encrypt the password file with one-way encryption
- ○ Educate users to resist social engineering attacks
- ➡ ● Add random bits to the password before hashing takes place
- ○ Enforce strict password restrictions

EXPLANATION

Some authentication protocols send password hashes between systems during the authentication process. Rainbow table attacks apply hashing algorithms to every word in a dictionary (sometimes including hybrids or passwords accumulated in brute force techniques) in an attempt to match hashed passwords. To protect against this type of attack, you can salt the hash by adding random bits to the password before hashing takes place, thereby producing an entirely different hash value for the password. Because the hacker does not know the extra random bits, the rainbow table is of no value.

The password file should be encrypted. But rainbow attacks do not work by accessing the password file, but by capturing hashed passwords being transmitted on the network. Users should be educated about social engineering attacks, but there is no connection between social engineering and rainbow table attacks. Enforcing strict password restrictions might actually weaken network security if you do not educate users about proper procedures that protect login credentials.

REFERENCES

11.7.2 Password Attack Facts

q_pwd_attacks_rainbow_02_secp7.question.fex

Question 4: ✓ Correct

Which SIEM component is responsible for gathering all event logs from configured devices and securely sending them to the SIEM system?

- ○ SIEM alerts
- ○ Security automation
- ○ Data handling
- ➡ ● Collectors

EXPLANATION

Collectors are responsible for gathering all event logs from configured devices and securely sending them to the Security Information and Event Management (SIEM) system. Collectors are basically the middleman between devices and the SIEM system.

The data handling component receives the data from the collectors and then reads, analyzes, and separates the data into different categories.

SIEM alerts are responsible for triggering alerts if any data exceeds the established thresholds.

Security automation is a feature of a SOAR system.

REFERENCES

11.4.4 SIEM and SOAR Facts

q_siem_soar_collector_secp7.question.fex

Question 5: ✓ Correct

You have been hired to perform a penetration test for an organization. You are given full knowledge of the network before the test begins.

Which type of penetration test are you performing?

➡ ● White box

○ Black box

○ Bug bounty

○ Gray box

EXPLANATION

In a white box test, the ethical hacker is given full knowledge of the target or network. This test allows for a comprehensive and thorough test, but it is not very realistic.

In a black box test, the ethical hacker has no information regarding the target or network. This type of test best simulates an outside attack and ignores insider threats.

In a gray box test, the ethical hacker is given partial information about the target or network, such as IP configurations, email and lists. This test simulates an insider threat.

Bug bounties are unique tests that are set up by organizations such as Google and Facebook. The organization sets strict guidelines and boundaries for ethical hackers to operate within. Any discovered vulnerabilities are reported, and the ethical hacker is paid based on the severity of the vulnerability.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_white_box_secp7.question.fex

Question 6: ✓ Correct

Which of the following describes a man-in-the-middle attack?

○ Malicious code is planted on a system, where it waits for a triggering event before activating.

○ A person convinces an employee to reveal his or her login credentials over the phone.

○ An IP packet is constructed that is larger than the valid size.

➡ ● A false server intercepts communications from a client by impersonating the intended server.

EXPLANATION

A false server intercepting communications from a client by impersonating the intended server is a form of a man-in-the-middle attack.

Convincing an employee to reveal his or her logon credentials over the phone is an example of a social engineering attack. Constructing an IP packet that is larger than the valid size is a land attack (a form of DoS). Planted malicious code that waits for a triggering event before activating is a logic bomb.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_mtm_01_secp7.question.fex

Question 7: ✓ Correct

Which of the following describes a false positive when using an IPS device?

➡ ● Legitimate traffic being flagged as malicious

○ Malicious traffic masquerading as legitimate traffic

○ Malicious traffic not being identified

○ The source address identifying a non-existent host

○ The source address matching the destination address

EXPLANATION

On an intrusion prevention system (IPS), a positive match occurs when traffic matches the signature that identifies malicious traffic. A false positive occurs when legitimate traffic is identified as malicious traffic. This situation is undesirable, as it often results in legitimate traffic being rejected. Good IPS signature files result in low false positive rates.

A false negative occurs when malicious traffic is not identified and is, therefore, allowed.

Spoofing is the technique of falsifying the source address in a packet.

REFERENCES

☰ 11.3.2 IDS Facts

q_ids_false_pos_02_secp7.question.fex

Question 8: ✓ Correct

You are concerned about attacks directed at your network firewall. You want to be able to identify and be notified of any attacks. In addition, you want the system to take immediate action to stop or prevent the attack, if possible.

Which tool should you use?

- ○ IDS
- ➡ ● IPS
- ○ Port scanner
- ○ Packet sniffer

EXPLANATION

Use an intrusion prevention system (IPS) to both detect and respond to attacks.

An intrusion detection system (IDS) can detect attacks and send notifications, but it cannot respond to attacks.

Use a port scanner to check for open ports on a system or a firewall. Use a packet sniffer to examine packets on the network.

REFERENCES

11.3.2 IDS Facts

q_ids_ips_01_secp7.question.fex

Question 9: ✓ Correct

In a variation of the brute force attack, an attacker may use a predefined list of common usernames and passwords to gain access to existing user accounts. Which countermeasure best addresses this issue?

○ 3DES encryption

○ AES encryption

○ VLANs

➡ ● A strong password policy

EXPLANATION

A strong password policy is the best defense against dictionary attacks. The policy must be enforced, and all users must be trained to properly construct and protect strong passwords.

3DES and AES encryption alone do not protect against dictionary attacks. Encryption technologies are useless if weak passwords permit easy access to encrypted channels.

VLANs allow logical segmentation of a physical network and do not prevent dictionary attacks or weak passwords.

REFERENCES

11.7.2 Password Attack Facts

q_pwd_attacks_dictionary_secp7.question.fex

Question 10: ✓ Correct

Which of the following activities are typically associated with a penetration test?

- ○ Run a vulnerability scanner on network servers.
- ➡ ● Attempt social engineering.
- ○ Create a performance baseline.
- ○ Interview employees to verify that the security policy is being followed.

EXPLANATION

Penetration testing typically uses tools and methods that are available to attackers. Penetration testing might start with attempts at social engineering or other reconnaissance activities. This may be followed by more active scans of systems and actual attempts to access secure systems.

A vulnerability scanner checks a system for weaknesses. Vulnerability scanners typically require administrative access to a system and are performed internally. They are not done to test system security. Typically, penetration testers cannot run a vulnerability scanner unless they have gained authorized access to a system.

A performance baseline is created by an administrator to identify normal network and system performance. Auditing might include interviewing employees to make sure that security policies are being followed.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_social_secp7.question.fex

Question 11: ✓ Correct

Which type of reconnaissance is dumpster diving?

- ○ OSINT
- ○ Packet sniffing
- ○ Active
- ➡ ● Passive

EXPLANATION

Dumpster diving is when an attacker goes through the trash to find important information that may have accidentally been thrown away. Because there is no direct interaction with the target, dumpster diving is a form of passive reconnaissance.

Active reconnaissance is the process of gathering information by interacting with the target in some manner. Dumpster diving does not fall under this category.

Open-source intelligence (OSINT) is any data that is collected from publicly available sources. Dumpster diving does not fall under this category.

Packet sniffing is the process of capturing data packets that are flowing across a network and analyzing them for important information. Dumpster diving does not fall under this category.

REFERENCES

11.2.8 Reconnaissance Facts

q_recon_passive_01_secp7.question.fex

Question 12: ✓ Correct

You are using a password attack that tests every possible keystroke for each single key in a password until the correct one is found. Which of the following technical password attacks are you using?

- ➡ ● Brute force attack
- ○ Password sniffing
- ○ Keylogger
- ○ Pass-the-hash attack

EXPLANATION

In a brute force attack, every password is eventually found because the technique is to test every possible keystroke for each single key in a password until the correct one is found.

Keyloggers log or record every keystroke on the computer keyboard to obtain passwords and other important data.

A pass-the-hash attack is a hacking technique where an attacker uses an underlying NTLM or hash of a user's password to gain access to a server without ever using the actual plaintext password.

Password sniffing is a passive way for attackers to gain access to an account. The sniffer collects data that is in transit in a LAN. If access is gained on one system in a LAN, data can be gathered from data being sent from any other system in the network. The sniffer runs in the background, making it undetectable.

REFERENCES

11.7.2 Password Attack Facts

q_pwd_attacks_brute_02_secp7.question.fex

Question 13: ✓ Correct

You need to check network connectivity from your computer to a remote computer.

Which of the following tools would be the BEST option to use?

➡ ● **ping**

○ **tracert**

○ **nmap**

○ **route**

EXPLANATION

The **ping** command is used to perform a connection test between two network devices. It works by sending ICMP packets to a specified device on a network and waiting for a response. This shows if there is a connection issue or not.

The **tracert** command shows the path a packet takes to reach its destination. This is not the best tool to check for connectivity between two network devices.

The **nmap** utility is a network security scanner. Use **nmap** to scan an entire network or specific IP addresses to discover all sorts of information. This is not the best tool to check for connectivity between two network devices.

The **route** command is used in both Windows and Linux to show the routing table and to make manual changes to it.

REFERENCES

11.2.2 Network Monitoring Facts

q_netmon_ping_secp7.question.fex

Question 14: ✓ Correct

You are cleaning your desk at work. You toss several stacks of paper in the trash, including a sticky note with your password written on it. Which of the following types of non-technical password attacks have you enabled?

○ Shoulder surfing

○ Social engineering

○ Password guessing

➡ ● Dumpster diving

EXPLANATION

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Social engineering relies on human error. It works by feigning trustworthiness to convince someone to give the attacker access.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like a pet's name or a hobby.

REFERENCES

2.3.1 Social Engineering Overview

2.3.2 Social Engineering Overview Facts

2.3.3 Social Engineering Motivation

2.3.4 Social Engineering Motivation Facts

2.3.5 Social Engineering Techniques

2.3.6 Social Engineering Techniques Facts

2.3.7 Phishing and Internet-Based Techniques

2.3.8 Phishing and Internet-Based Techniques Facts

2.3.9 Use the Social Engineer Toolkit

2.3.10 Investigating a Social Engineering Attack

2.3.11 Identify Social Engineering

11.7.2 Password Attack Facts

q_pwd_attacks_dumpster_secp7.question.fex

Question 15: ✓ Correct

What is the most common form of host-based IDS that employs signature or pattern-matching detection methods?

➡ ● Antivirus software

○ Firewalls

○ Honeypots

○ Motion detectors

EXPLANATION

Antivirus software using signatures is the most commonly deployed form of a host-based IDS.

REFERENCES

11.3.2 IDS Facts

q_ids_host_03_secp7.question.fex

Question 16: ✓ Correct

Which phase or step of a security assessment is a passive activity?

- ○ Vulnerability mapping
- ○ Privilege escalation
- ➡ ● Reconnaissance
- ○ Enumeration

EXPLANATION

Reconnaissance is the only step of a security assessment (penetration test) that is passive.

Enumeration, vulnerability mapping, and privilege escalation are all active events in a security assessment.

REFERENCES

☰ 11.1.2 Penetration Testing Facts

q_pene_test_recon_secp7.question.fex

Question 17: ✓ Correct

You need to enumerate the devices on your network and display the network's configuration details.

Which of the following utilities should you use?

○ **scanless**

○ **dnsenum**

○ **nslookup**

➡ ● **nmap**

EXPLANATION

The **nmap** utility is an open-source security scanner used for network enumeration and the creation of network maps. Use **nmap** to send specially crafted packets to a target host and then analyze the responses to create a map.

The **scanless** utility is used for port scanning.

The **dnsenum** utility is a program that performs DNS enumeration and can find the DNS servers and entries for an organization.

Use **nslookup** to submit name resolution requests to identify DNS name servers and IP addresses for hosts.

REFERENCES

11.2.8 Reconnaissance Facts

q_recon_nmap_secp7.question.fex

Question 18: ✓ Correct

Which type of activity changes or falsifies information in order to mislead or re-direct traffic?

- ○ Spamming
- ○ Snooping
- ➡ ● Spoofing
- ○ Sniffing

EXPLANATION

Spoofing changes or falsifies information in order to mislead or re-direct traffic.

Snooping is the act of spying into private information or communications.

One type of snooping is sniffing. Sniffing captures network packets to examine the contents of communications.

Spamming is sending a victim unwanted and unrequested email messages.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_spoof_01_secp7.question.fex

Question 19: ✓ Correct

Which of the following are network-sniffing tools?

○ WinDump, KFSensor, and Wireshark

○ Ufasoft snif, TCPDump, and Shark

➡ ● Cain and Abel, Ettercap, and TCPDump

○ Ettercap, Ufasoft snif, and Shark

EXPLANATION

Cain and Abel is a collection of tools that includes ARP poisoning. Cain and Abel redirects packets from a target by forging ARP replies.

Ettercap is a sniffing tool with multiple functions that can be used for ARP poisoning, passive sniffing, packet grabbing, and protocol decoding.

TCPDump is a command line sniffer designed for the Linux environment.

Ufasoft snif is a sniffing tool that has capture, analysis, and decryption features.

WinDump is the Windows version of TCPdump.

Wireshark is a network packet analyzer that tries to capture network packets and display the data they carry in as much detail as possible.

Shark is a tool that is used to create botnets.

KFSensor is a Windows host-based intrusion detection system. It acts as a vulnerable server to attract hackers and record their activities.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_tcpdump_secp7.question.fex

Question 20: ✓ Correct

You have been hired as part of the team that manages an organization's network defense.

Which security team are you working on?

○ Red

○ Purple

➡ ● Blue

○ White

EXPLANATION

Blue team members are the defense of the system. This team is responsible for stopping the red team's advances.

Members of the purple team work on both offense and defense. This team is a combination of the red and blue teams.

The red team members are the ethical hackers. This team is responsible for performing the penetration tests.

The white team members are the referees of cybersecurity. This team is responsible for managing the engagement between the red and blue teams. This group typically consists of the managers or team leads.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_blue_secp7.question.fex

Question 21: ✓ Correct

Which step in the penetration testing life cycle is accomplished using rootkits or Trojan horse programs?

- ○ Enumeration
- ○ Reconnaissance
- ○ Gain access
- ➡ ● Maintain access

EXPLANATION

Once a penetration tester has gained access, maintaining that access becomes the next priority. This can be done by installing backdoors, rootkits, or Trojans.

Gain access is the third phase of the penetration test life cycle and uses the information gathered in earlier phases to exploit discovered vulnerabilities.

Reconnaissance is the first phase in the penetration testing process. This is when the penetration tester begins gathering information.

Enumeration is the second phase in the penetration testing process. The penetration tester uses scanning techniques to extract information such as usernames and computer names.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_access_secp7.question.fex

Question 22: ✓ Correct

You want to identify traffic that is generated and sent through a network by a specific application running on a device.

Which tool should you use?

○ Multimeter

○ Toner probe

○ TDR

○ Certifier

➡ ● Protocol analyzer

EXPLANATION

Use a protocol analyzer (also called a packet sniffer) to examine network traffic. You can capture or filter packets from a specific device or packets that use a specific protocol.

Use a time-domain reflector (TDR) to measure the length of a cable or to identify the location of a fault in the cable. A toner probe is two devices used together to trace the end of a wire from a known endpoint into the termination point in the wiring closet. A cable certifier is a multi-function tool that verifies that a cable or an installation meets the requirements for a specific architectural implementation. A multimeter is a device that tests various electrical properties, such as voltage, amps, and ohms.

REFERENCES

▷ 11.5.1 Protocol Analyzers

☰ 11.5.2 Protocol Analyzer Facts

🖥 11.5.3 Analyzing Network Traffic

q_prot_analyzers_output_03_secp7.question.fex

Question 23: ✓ Correct

You decide to use a packet sniffer to identify the type of traffic sent to a router. You run the packet sniffing software on a device that is connected to a hub with three other computers. The hub is connected to a switch that is connected to the router.

When you run the software, you see frames addressed to the four workstations, but not to the router.

Which feature should you configure on the switch?

- ○ Promiscuous mode
- ○ Bonding
- ○ Spanning Tree Protocol
- ➡ ● Port mirroring

EXPLANATION

A switch only forwards packets to the switch port that holds a destination device. This means that when your packet sniffer is connected to a switch port, it does not see traffic sent to other switch ports. To configure the switch to send all frames to the packet sniffing device, configure port mirroring on the switch. With port mirroring, all frames sent to all other switch ports are forwarded on the mirrored port.

Promiscuous mode configures a network adapter to process every frame it sees, not just the frames addressed to that network adapter. In this scenario, you know that the packet sniffer is running in promiscuous mode because it can already see frames sent to other devices.

Bonding logically groups two or more network adapters together to be used at the same time for a single logical network connection.

Spanning Tree Protocol (STP) runs on a switch and ensures that there is only one active path between switches, allowing for backup-redundant paths.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_mirroring_secp7.question.fex

Question 24: ✓ Correct

You are concerned about protecting your network from network-based attacks on the internet. Specifically, you are concerned about attacks that have not yet been identified or that do not have prescribed protections.

Which type of device should you use?

➡ ● Anomaly-based IDS

○ Host-based firewall

○ Network-based firewall

○ Antivirus scanner

○ Signature-based IDS

EXPLANATION

An anomaly-based intrusion detection system (IDS) can recognize and respond to some unknown attacks. Signature recognition, also referred to as pattern matching or dictionary recognition, looks for patterns in network traffic and compares them to known attack patterns called signatures. Signature-based recognition cannot detect unknown attacks. This system can only detect attacks identified by published signature files.

Antivirus software is a form of signature-based IDS. A network-based firewall filters packets for a network, while a host-based firewall filters packets for a host. Firewalls are typically configured using access control lists that identify specific traffic as allowed or denied.

REFERENCES

11.3.2 IDS Facts

q_ids_anomaly_secp7.question.fex

Question 25: ✓ Correct

You want to check a server for user accounts that have weak passwords. Which tool should you use?

- ➡ ● John the Ripper
- ○ Retina
- ○ OVAL
- ○ Nessus

EXPLANATION

John the Ripper is a password cracking tool. Password crackers perform cryptographic attacks on passwords. Use a password cracker to identify weak passwords or passwords protected with weak encryption.

Nessus and Retina are vulnerability scanners. While vulnerability scanners check for default user accounts and often check for accounts with blank passwords, they typically do not include password cracking features to test for weak passwords.

The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

REFERENCES

5.9.2 Device Vulnerability Facts

11.7.2 Password Attack Facts

11.7.5 Crack Passwords

11.7.6 Crack Password Protected Files

11.7.7 Crack a Password with John the Ripper

q_pwd_attacks_pass_crack_secp7.question.fex

Question 26: ✓ Correct

In your role as a security analyst, you ran a vulnerability scan, and several vulnerabilities were reported. Upon further inspection, none of the vulnerabilities actually existed.

Which type of result is this?

➡ ● False positive

○ False negative

○ True negative

○ True positive

EXPLANATION

False positives occur when a scan says there is a vulnerability, but there is none. They happen as a matter of course and should be discovered during the follow-up to the scan.

False negatives occur when the scanner misses a vulnerability.

True negatives occur when the scanner says there are no vulnerabilities and there are none.

True positives occur when the scanner shows a vulnerability that does exist.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_false_secp7.question.fex

Question 27: ✓ Correct

Which passive reconnaissance tool is used to gather information from a variety of public sources?

- ○ Shodan
- ➡ ● theHarvester
- ○ Packet sniffing
- ○ scanless

EXPLANATION

theHarvester is a passive reconnaissance tool that is used to gather information from a variety of public sources. This tool gathers emails, names, subdomains, IPs, and URLs using multiple public data sources. These include search engines, social media sites, and Shodan.

Packet sniffing is the process of capturing data packets that are flowing across a network and analyzing them for important information.

Shodan is a popular search engine for internet-connected devices. Users can search for specific types of devices and locations.

Use **scanless** for port scanning. Instead of an attacker scanning ports from their own machine, **scanless** uses exploitation websites to perform port scans on their behalf.

REFERENCES

11.2.8 Reconnaissance Facts

q_recon_passive_02_secp7.question.fex

Question 28: ✓ Correct

You are concerned about attacks directed against the firewall on your network. You would like to examine the content of individual frames sent to the firewall.

Which tool should you use?

○ System log

➡ ● Packet sniffer

○ Throughput tester

○ Event log

○ Load tester

EXPLANATION

A packet sniffer is special software that captures frames transmitted on the network. Use a packet sniffer to:

- View packet contents.
- Identify the types of traffic on a network.
- View the exchange of packets between communicating devices. For example, you can capture frames related to the domain name system and view the exact exchange of packets for a specific name resolution request.
- Analyze packets sent to and from a specific device.

A load tester simulates a load on a server or service.

A throughput tester measures the amount of data that can be transferred through a network or processed by a device (such as the amount of data that can be retrieved from a disk in a specific period of time).

System and event logs record what has happened on a device. They do not record individual frames or packets.

REFERENCES

11.5.1 Protocol Analyzers

11.5.2 Protocol Analyzer Facts

11.5.3 Analyzing Network Traffic

q_prot_analyzers_sniffer_02_secp7.question.fex

Question 29: ✓ Correct

Which of the following tools can be used to view and modify DNS server information in Linux?

- ○ **route**
- ➡ ● **dig**
- ○ **tracert**
- ○ **netstat**

EXPLANATION

The **dig** command is used to view and modify DNS settings. These tools can be used to look up DNS server information and give IP addresses and domain names for a network server.

The **tracert** command shows the path a packet takes to reach its destination. This is not the best tool for checking connectivity between two network devices.

The **route** command is used in both Windows and Linux to show the routing table and to make manual changes to it.

The **netstat** command is used to display a variety of network statistics in both Windows and Linux. This command is not used to look up DNS server information.

REFERENCES

☰ 11.2.2 Network Monitoring Facts

q_netmon_dig_secp7.question.fex

Question 30: ✓ Correct

In your role as a security analyst, you need to stay up to date on the latest threats. You are currently reviewing the latest real-time updates on cyberthreats from across the world.

Which of the following resources are you MOST likely using?

- ○ Advisories and bulletins
- ○ Intelligence fusion
- ○ Threat hunting
- ➡ ● Threat feeds

EXPLANATION

Threat feeds provide real-time updates on cyberthreats across the world. They can provide information such as suspicious domains, known malware, known malicious IP addresses, and more. The **tracert** command shows the path a packet takes to reach its destination. This is not the best tool to check for connectivity between two network devices.

Advisories and bulletins are usually updated weekly and provide much more detailed information on the newest threats.

Intelligence fusion is the sharing of information between multiple government agencies and private security firms.

Threat hunting is the human-based, proactive and methodical monitoring of a network, systems, and software. This is done in order to detect any suspicious activity that may have evaded the automated tools.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_threat_secp7.question.fex

Question 31: ✓ Correct

Which of the following processes identifies an operating system based on its response to different types of network traffic?

○ Port scanning

○ Social engineering

○ Firewalking

➡ ● Fingerprinting

EXPLANATION

A hacker can use an analyzer to perform system fingerprinting. System fingerprinting identifies which operating system the system is running based on how it responds to different types of network traffic.

Port scanning pings every port on an external interface or attempts a connection in order to discover which ports are open and active, and which ones are not.

Firewalking uses the **traceroute** command to discover which services can pass through a firewall or router.

Social engineering exploits human nature to obtain information. A hacker often impersonates someone of authority and requests data.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_finger_secp7.question.fex

Question 32: ✓ Correct

The process of walking around an office building with an 802.11 signal detector is known as:

- ○ War dialing
- ○ Driver signing
- ○ Daemon dialing
- ➡ ◉ War driving

EXPLANATION

War driving is the act of searching for wireless networks (802.11) using a signal detector or a network client (such as a PDA or notebook). While the phrase war driving originated from the action of driving around a city searching for wireless networks, the name currently applies to any method of searching for wireless networks, including walking around.

War dialing and daemon dialing are both the act of dialing phone numbers in search of an answering modem. Often, war/daemon dialing calls all of the phone numbers in an area code or a prefix range in search of active modems.

Driver signing is a method of signing device drivers in an attempt to verify the source and quality of installed drivers. However, signing a device driver only indicates its source. Signing does not guarantee the reliability, stability, quality, or compatibility of a device driver.

REFERENCES

☰ 11.2.8 Reconnaissance Facts

q_recon_war_driving_secp7.question.fex

Question 33: ✓ Correct

While using the internet, you type the URL of one of your favorite sites in the browser. Instead of going to the correct site, the browser displays a completely different website. When you use the IP address of the web server, the correct site is displayed.

Which type of attack has likely occurred?

○ Man-in-the-middle

➡ ● DNS poisoning

○ Hijacking

○ Spoofing

EXPLANATION

Because the correct site shows when you use the IP address, you know that the main website is still functional and that the problem is likely caused by an incorrect domain name mapping. DNS poisoning occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. In a DNS poisoning attack:

- Incorrect DNS data is introduced into the cache of a primary DNS server.
- The incorrect mapping is made available to client applications through the resolver.

Spoofing is used to hide the true source of packets or redirect traffic to another location. Spoofing attacks use modified source and/or destination addresses in packets and can include site spoofing that tricks users into revealing information. A man-in-the-middle attack is used to intercept information passing between two communication partners. TCP/IP hijacking is an extension of a man-in-the-middle attack in which the attacker steals an open and active communication session from a legitimate user. With spoofing, man-in-the-middle, and hijacking, the attack would be successful regardless of whether the DNS name or the IP address were used.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_dns_pois_02_secp7.question.fex

Question 34: ✕ Incorrect

Which of the following is the term used to describe what happens when an attacker sends falsified messages to link their MAC address with the IP address of a legitimate computer or server on a network?

➡ ○ ARP poisoning

● ~~MAC spoofing~~

○ MAC flooding

○ Port mirroring

EXPLANATION

Address Resolution Protocol (ARP) poisoning is when an attacker sends fake ARP messages to link their MAC address with the IP address of a legitimate computer or server on the network. Once their MAC address is linked to an authentic IP address, the attacker can receive any messages directed to the legitimate address. As a result, the attacker can intercept, modify, or block communications to the legitimate MAC address.

Port mirroring creates a duplicate of all network traffic on a port and sends it to another device.

MAC flooding is when an attacker intentionally floods a content-addressable memory table with Ethernet frames, each originating from different MAC addresses. Once the table starts to overflow, the switch responds by broadcasting all incoming data to all ports, basically turning itself into a hub instead of a switch.

MAC spoofing is done to enable the bypass of access control lists on servers or routers by either hiding a computer on a network or by allowing it to impersonate another network device.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_arp_pois_01_secp7.question.fex

Question 35: ✕ Incorrect

To answer this question, complete the lab using the information below. **Launch Lab**

You did not attempt the lab.

You are the CorpNet IT administrator. Your support team says that CorpNet's customers are unable to browse to the public-facing web server. You suspect that it might be under some sort of denial-of-service attack, possibly a TCP-SYN flood attack. Your www_stage computer is on the same network segment as your web server, so you should use this computer to investigate the problem.

In this lab, your task is to:

- Capture packets from the network segment on **www_stage** using Wireshark.
  - Use the **enp2s0** interface.
- Analyze the attack using the following filters:
  - **tcp.flags.syn==1 and tcp.flags.ack==1**
  - **tcp.flags.syn==1 and tcp.flags.ack==0**
- Answer the question.

REFERENCES

11.6.4 Poison ARP and Analyze with Wireshark

11.6.6 Poison DNS

b24dff09-0296-4953-b93f-58a191f94b60

Question 36: ✓ Correct

Capturing packets as they travel from one host to another with the intent of altering the contents of the packets is a form of which type of attack?

- ○ Spamming
- ○ DDoS
- ➡ ● Man-in-the-middle attack
- ○ Passive logging

EXPLANATION

Capturing packets between two existing communication partners is a form of a man-in-the middle attack. As this attack type's name implies, traffic is intercepted somewhere in the middle of the communication. The best way to defend against man-in-the middle attacks is to use session encryption or line encryption solutions.

Passive logging is a means of recording information about network traffic or operations in a system without affecting either in any way.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_mtm_02_secp7.question.fex

Question 37: ✓ Correct

Which of the following roles would be MOST likely to use a protocol analyzer to identify frames that might cause errors?

➡ ◉ Security operations team

○ Network administrator

○ Malicious hacker

○ Standard user

EXPLANATION

The network SecOps team can use a protocol analyzer during a vulnerability assessment. The protocol analyzer can help the SecOps team to:

- Identify frames that might cause errors. For example, the network administrator can:
  - Determine which flags are set in a TCP handshake.
  - Detect any malformed or fragmented packets. This would indicate that someone is trying to get around the firewall.
- Discover passwords and other sensitive data being sent in cleartext.
- Find any open network ports that should not be open.

A network administrator can use a protocol analyzer to assist in the management of the network and employee usage. However, a network administrator would not be the most likely to use a protocol analyzer to identify frames that might cause errors.

A malicious hacker could use a protocol analyzer to identify frames that might cause errors, but they most likely would not use it for that purpose.

A standard user should not be using a protocol analyzer on a network for any reason.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_soar_secp7.question.fex

Question 38: ✓ Correct

Which of the following uses hacking techniques to proactively discover internal vulnerabilities?

○ Passive reconnaissance

○ Reverse engineering

○ Inbound scanning

➡ ● Penetration testing

EXPLANATION

Penetration testing is the practice of proactively testing systems and policies for vulnerabilities. This approach seeks to identify vulnerabilities internally before a malicious individual can take advantage of them. Common techniques are identical to those used by hackers and include network/target enumeration and port scanning.

REFERENCES

☰ 11.1.2 Penetration Testing Facts

q_pene_test_testing_01_secp7.question.fex

Question 39: ✓ Correct

A security administrator logs onto a Windows server on her organization's network. Then she runs a vulnerability scan on that server.

Which type of scan was conducted in this scenario?

○ Non-intrusive scan

○ Non-credentialed scan

○ Intrusive scan

➡ ● Credentialed scan

EXPLANATION

In a credentialed scan, the security administrator authenticates to the system prior to starting the scan. A credentialed scan usually provides detailed information about potential vulnerabilities. For example, a credentialed scan of a Windows workstation allows you to probe the registry for security vulnerabilities.

With a non-credentialed scan, the security administrator does not authenticate to the system prior to running the scan.

An intrusive scan finds a potential vulnerability and then actively attempts to exploit it.

A non-intrusive scan is the more common type of scan performed.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_cred_secp7.question.fex

Question 40: ✓ Correct

You want to use a tool to see packets on a network, including the source and destination of each packet. Which tool should you use?

○ OVAL

○ **nmap**

○ Nessus

➡ ● Wireshark

EXPLANATION

A protocol analyzer, also called a packet sniffer, is special software that captures (records) frames that are transmitted on a network. A protocol analyzer is a passive device. It copies frames and allows you to view frame contents, but it does not allow you to capture, modify, and retransmit frames (activities that are used to perform an attack). Wireshark is a popular protocol analyzer.

The **nmap** command is a tool that performs ping scans (finding devices on the network) as well as port scans (looking for open ports on the network).

Nessus is a vulnerability-scanning tool. While a protocol analyzer looks at packets on the network, a vulnerability scanner looks for weaknesses in systems, including open ports, running services, and missing patches.

Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting a system's security vulnerabilities.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_wireshark_secp7.question.fex

Question 41: ✗ Incorrect

As a security precaution, you have implemented IPsec that is used between any two devices on your network. IPsec provides encryption for traffic between devices.

You would like to implement a solution that can scan the contents of the encrypted traffic to prevent any malicious attacks.

Which solution should you implement?

- ○ VPN concentrator
- ○ Port scanner
- ● ~~Network-based IDS~~
- ○ Protocol analyzer
- ➡ ○ Host-based IDS

EXPLANATION

A host-based IDS is installed on a single host and monitors all traffic coming into the host. A host-based IDS can analyze encrypted traffic because the host operating system decrypts that traffic as it is received.

A network-based IDS is a dedicated device installed on the network. It analyzes all traffic on the network. It cannot analyze encrypted traffic because the packet contents are encrypted so that only the recipient can read the packet contents.

A protocol analyzer examines packets on the network, but it cannot look at the contents of encrypted packets. A port scanner probes a device to identify open protocol ports. A VPN concentrator is a device used to establish remote access VPN connections.

REFERENCES

☰ 11.3.2 IDS Facts

q_ids_host_01_secp7.question.fex

Question 42: ✓ Correct

A security administrator needs to run a vulnerability scan that analyzes a system from the perspective of a hacker attacking the organization from the outside.

Which type of scan should he or she use?

○ Credentialed scan

○ Port scan

○ Network-mapping scan

➡ ◉ Non-credentialed scan

EXPLANATION

In a non-credentialed scan, the security administrator does not authenticate to the system prior to running the scan. A non-credentialed scan can be valuable because it allows the scanner to see the system from the same perspective that an attacker would see it. However, a non-credentialed scan does not typically produce the same level of detail as a credentialed scan.

In a credentialed scan, the security administrator authenticates to the system prior to starting the scan.

A port scan probes systems for open ports, but it does not run a full vulnerability assessment.

A network-mapping scan is a type of port scan that discovers devices on the network and then organizes those devices in a graphical display.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_non_cred_secp7.question.fex