Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/11/2022 7:45:50 pm • Time spent: 01:11

Score: 100%

Passing Score: 80%

▼ Question 1: ✓ Correct

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

○ **tracert**

○ **netstat**

➡ ● **dig**

○ **route**

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 2: ✓ Correct

You want to identify all devices on a network along with a list of open ports on those devices. You want the results displayed in a graphical diagram. Which tool should you use?

- ○ Ping scanner
- ○ Port scanner
- ➡ ● Network mapper
- ○ OVAL

EXPLANATION

A network mapper is a tool that can discover devices on a network and show those devices in a graphical representation. Network mappers typically use a ping scan to discover devices and a port scanner to identify open ports on those devices.

A ping scanner only identifies devices on a network, but does not probe for open ports. A port scanner finds open ports, but it might not display devices in a graphical representation. Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

REFERENCES

11.2.2 Network Monitoring Facts

q_netmon_nmap_secp7.question.fex

Question 3: ✓ 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?

- ○ **tracert**
- ○ **nmap**
- ➡ ● **ping**
- ○ **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 4: ✓ Correct

You want to use a tool to scan a system for vulnerabilities, including open ports, running services, and missing patches. Which tool should you use?

➡ ◉ Nessus

○ Wireshark

○ OVAL

○ LC4

EXPLANATION

A vulnerability scanner is a software program that searches an application, computer, or network for weaknesses. These weaknesses could be things such as open ports, running applications or services, missing critical patches, default user accounts that have not been disabled, and default or blank passwords. Vulnerability scanning tools include Nessus, Retina Vulnerability Assessment Scanner, and Microsoft Baseline Security Analyzer (MBSA).

Wireshark is a protocol analyzer. LC4 is a password-cracking tool that you can use to identify weak passwords. Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

REFERENCES

11.2.8 Reconnaissance Facts

q_recon_nessus_secp7.question.fex

Question 5: ✓ 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?

○ **dnsenum**

➡ ● **nmap**

○ **nslookup**

○ **scanless**

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 6: ✓ Correct

Gathering as much personally identifiable information (PII) on a target as possible is a goal of which reconnaissance method?

○ Active

○ Packet sniffing

➡ ● OSINT

○ Passive

EXPLANATION

Open-source intelligence is any data that is collected from publicly available sources. The goal is to gather as much personally identifiable information (PII) as possible on the target.

Dumpster diving is when an attacker goes through the trash to find important information that may have accidentally been thrown away.

Active reconnaissance is the process of gathering information by interacting with the target in some manner.

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

REFERENCES

11.2.8 Reconnaissance Facts

q_recon_osint_secp7.question.fex

▾ **Question 7:** ✓ 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 8: ✓ Correct

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

○ scanless

➡ ● theHarvester

○ Packet sniffing

○ Shodan

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 9: ✓ Correct

Which of the following tools can be used to see if a target has any online IoT devices without proper security?

○ Packet sniffing

➡ ● Shodan

○ **scanless**

○ theHarvester

EXPLANATION

Shodan is a popular search engine for internet-connected devices. Users can search for specific types of devices and locations. This information can be used to see if a target has any online devices without proper security.

theHarvester is a passive reconnaissance tool that is used to gather information from a variety of public sources.

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

Use **scanless** for port scanning. Instead of the 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_recon_secp7.question.fex

Question 10: ✓ Correct

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

○ Driver signing

○ War dialing

➡ ● War driving

○ Daemon dialing

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

Copyright © 2022 TestOut Corporation All rights reserved.