Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/16/2022 9:54:00 pm • Time spent: 02:44

Score: 50% Passing Score: 80%

Question 1: ✕ Incorrect

Which command should you use to display both listening and non-listening sockets on your Linux system? (Tip: enter the command as if in Command Prompt.)

~~nmap~~ netstat -a

EXPLANATION

Use **netstat -a** to identify listening and non-listening sockets on a Linux system. A socket is an endpoint of a bidirectional communication flow across a computer network. Be aware of the other common **netstat** options:

- **-l** lists listening sockets.
- **-s** displays statistics for each protocol.
- **-i** displays a table of all network interfaces.

Question 2: ✕ Incorrect

Which command should you use to scan for open TCP ports on your Linux system? (Tip: enter the command as if in Command Prompt.)

nmap -sT

EXPLANATION

Use **nmap -sT** to scan for open TCP ports. Open ports can provide information about which operating system a computer uses and might provide entry points or information about ways to formulate an attack.

Use **nmap -sU** to scan for open UDP ports.

Question 3: ✕ Incorrect

You need to increase the security of your Linux system by finding and closing open ports. Which of the following commands should you use to locate open ports?

- **nslookup**
- ➡ **nmap**
- ~~**netstat**~~
- **traceroute**

EXPLANATION

Use **nmap** to locate open ports. Open ports can provide information about which operating system a computer uses and might provide entry points or information about ways to formulate an attack. Use one of the following commands to scan for open ports:

- **nmap -sT** scans for TCP ports.
- **nmap -sU** scan for UDP ports.

The **netstat** command shows the status of listening and non-listening sockets. A socket is an endpoint of a bidirectional communication flow across a computer network. The **nslookup** command is used for name resolution requests. The **traceroute** command tests and displays connectivity between devices.

Question 4: ✕ Incorrect

What does the **netstat -a** command show?

- All listening sockets
- ~~All connected hosts~~
- ➡ All listening and non-listening sockets
- All network users

EXPLANATION

The **netstat -a** command shows the status of all listening and non-listening sockets.

Question 5: ✔ Correct

You want to make sure no unneeded software packages are running on your Linux server.

Select the command from the drop-down list that you can use to see all installed RPM packages.

yum list installed ✔

EXPLANATION

Unneeded software takes disk space and could introduce security flaws. To see all the RPM packages installed on your Linux server, run the following command:

yum list installed

After running this command, complete the following:

- Research the function of any unrecognized RPM package to determine whether it is necessary.
- Use **yum** or **rpm** to uninstall unneeded packages.

Question 6: ✔ Correct

Which action would you use in a rule to disallow a connection silently?

- Reject
- Forward
- ➡ Drop
- Accept

EXPLANATION

The Drop action is used to silently disallow a connection; the sending system receives no notice. The Reject action also disallows a connection but sends a TCP RST packet or an ICMP port unreachable packet back to the system that sent the original packet.

Accept would allow the packet.

Forward is a chain, not an action in iptables.

Question 7: ✔ Correct

In which of the iptables default chains would you configure a rule to allow an external device to access the HTTPS port on the Linux server?

- Accept
- Output
- Forward
- ➡ Input

EXPLANATION

The Input chain would be where you would place the rule as it is used for inbound connections.

The Output chain is for outbound connections.

The Forward chain is for sending connections through the Linux server to another device.

The Accept action can be used in a rule to allow a connection. However, it is not a chain.

Question 8: ✘ Incorrect

Which type of packet would the sender receive if they sent a connection request to TCP port 25 on a server with the following command applied?

sudo iptables -A OUTPUT -p tcp --dport 25 -j REJECT

- ACK
- ➡ RST
- ~~SYN~~
- ICMP Unreachable Port

EXPLANATION

Because the packet is TCP and is blocked by the Reject action, the server would send a TCP RST packet back to the sender.

ICMP Unreachable Port is sent by iptables if a UDP packet is blocked by the Reject action.

A SYN packet would indicate that the server is proceeding with the connection, which would not happen with the Reject action. If it were allowed, the ACK would generally be sent with the SYN to acknowledge the initial connection while the SYN starts the next part of the TCP three-way handshake.

Question 9: ✔ Correct

You have configured the following rules. What is the effect?

sudo iptables -A INPUT -p tcp --dport 25 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 25 -m conntrack --ctstate ESTABLISHED -j ACCEPT

- ➡ Allow SMTP traffic
- Allow SSH traffic
- Block SSH traffic
- Block SMTP traffic

EXPLANATION

These rules would allow inbound and outbound Simple Mail Transfer Protocol (SMTP) connections on TCP port 25, which is the default port for SMTP.

These rules use the Accept action, so they would not block SMTP or Secure Shell (SSH).

SSH is on TCP port 22, so these rules would not affect SSH.

Question 10: ✔ Correct

Which command would you use to list all of the currently defined iptables rules?

- **sudo /sbin/iptables-save**
- **sudo iptables -F**
- **sudo iptables -A INPUT -j DROP**
- ➡ **sudo iptables -L**

EXPLANATION

sudo iptables -L lists all of the currently defined rules.

sudo iptables -A INPUT -j DROP would drop all incoming traffic.

sudo /sbin/iptables-save saves changes to iptables on Ubuntu.

sudo iptables -F would flush all current rules from iptables.