Exam Report: 7.6.4 Practice Questions

Date: 1/22/2020 6:37:45 pm
Time Spent: 2:54

Candidate: Garsteck, Matthew
Login: mGarsteck

## Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

## Individual Responses

**Question 1:** Incorrect

Which command should you use to scan for open TCP ports on your Linux system? (Tip: Enter the command as if at the 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.

### References

LabSim for Security Pro, Section 7.6.
[All Questions SecPro2017_v6.exm LINUX_HOST_SEC_01]

**Question 2:** Correct

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**

○ **netstat**

➡ ● **nmap**

○ **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

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

### References

LabSim for Security Pro, Section 7.6.
[All Questions SecPro2017_v6.exm LINUX_HOST_SEC_02]

**Question 3:** Incorrect

Which command should you use to display both listening and non-listening sockets on your Linux system?

(Tip: Enter the command as if at the command prompt.)

netstat -a

## Explanation

Use **netstat -a** to identify the 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.

## References

LabSim for Security Pro, Section 7.6.
[All Questions SecPro2017_v6.exm LINUX_HOST_SEC_03]

### Question 4: Incorrect

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

● ~~All connected hosts~~

➡ ○ All listening and non-listening sockets

○ All network users

○ All listening sockets

## Explanation

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

## References

LabSim for Security Pro, Section 7.6.
[All Questions SecPro2017_v6.exm LINUX_HOST_SEC_04]

### Question 5: Incorrect

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 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, do the following:

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

## References

LabSim for Security Pro, Section 7.6.
[All Questions SecPro2017_v6.exm LINUX_HOST_SEC_05]