15.4.4 Practice Questions

Candidate: Ethan Bonavida (suborange)
Date: 12/8/2022 11:50:25 pm • **Time Spent:** 00:52

Score: 100% Passing Score: 80%

Question 1: ✓ Correct

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

15.4.3 Network Security Facts

q_netsec_f_lp5_01.question.fex

Question 2: ✔ Correct

What should you enter at the command prompt to scan for open TCP ports on your Linux system?

nmap -sT ✔

Explanation

Use **nmap -sT** to scan for open TCP ports. Open ports can provide information about what 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

15.4.3 Network Security Facts

q_netsec_f_lp5_02.question.fex

Question 3: ✔ 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?

- **nmap**
- **netstat**
- **nslookup**
- **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** scans 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

15.4.3 Network Security Facts

q_netsec_f_lp5_03.question.fex

Question 4: ✔ Correct

What should you enter at the command prompt to display both listening and non-listening sockets on your Linux system?

netstat -a ✔

Explanation

Use **netstat** -a to identify the listening and non-listening sockets on the 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

15.4.3 Network Security Facts

q_netsec_f_lp5_04.question.fex

Question 5: ✔ Correct

Removing unnecessary software increases the security of your Linux system. If your system uses RPM for package management, what can you enter at the command prompt to look for unnecessary software that might be installed on your system?

dnf list installed ✔

Explanation

On a system that uses RPM for package management, you can enter any of these commands to look for unnecessary software that might be installed on your system:

- **dnf list installed**
- **yum list installed**
- **rpm -qa**

References

- 6.1.1 Red Hat Package Manager (RPM)
- 6.1.2 RPM Package Management
- 6.1.3 Manage RPM Packages
- 6.1.7 RPM Facts
- 6.2.1 Yellowdog Updater, Modified (YUM)
- 6.2.2 Install Packages with YUM
- 6.2.3 Install Packages with Dandified YUM (DNF)
- 6.2.4 YUM and DNF Facts
- 6.3.1 Debian Package Manager (dpkg)
- 6.3.2 Advanced Packaging Tool (apt-get)
- 6.3.3 Managing Debian Packages
- 6.3.4 Debian Package Management Facts

q_netsec_f_lp5_05.question.fex

Question 6: ✔ Correct

Unnecessary network services might provide attackers with an entry point for an attack. To view a list of services, or units, installed or running on a systemd-based system, what could you enter at the command prompt?

systemctl list-units ✔

Explanation

To view a list of services, or units, running on a systemd-based system, you can enter either **systemctl** or **systemctl list-units**. **systemctl list-unit-files** lets you see all the units installed on your system.

References

15.4.3 Network Security Facts

q_netsec_f_lp5_06.question.fex

Question 7: ✔ Correct

Sam, a system administrator, is implementing measures to harden the Linux systems on the network. Sam wants to modify kernel parameters at runtime to protect the system from syn flood attacks using the **sysctl** command.

Which file would Sam modify to implement the following changes?

```
# TCP SYN Flood Protection
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 3
```

- /proc/sys
- /etc/sysconfig/iptables
- /etc/sysconfig/kernel
- ➡ /etc/sysctl.conf

Explanation

/etc/sysctl.conf is a text file containing sysctl values to be read in and set by sysctl at boot time.

/etc/sysconfig/iptables contains the current firewall configuration.

/proc/sys is a directory under the /proc virtual filesystem. The parameters available for sysctl are listed under /proc/sys/.

/etc/sysconfig/kernel is the configuration file used to set the default kernel.

References

15.4.3 Network Security Facts

q_netsec_f_lp5_sysctl.question.fex