Exam Report: 12.6.7 Practice Questions

Date: 4/4/28 4:41:16 pm
Time Spent: 1:05

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 27%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

Maria, a system administrator, wants to setup IP forwarding on a server for both IPv4 and IPv6.

Which of the following files should be modified to enable IP forwarding? (Choose TWO).

➡ □ /proc/sys/net/ipv4/ip_forward

☑ ~~/usr/lib/modules/*kernelversion*/kernel/net/ipv6~~

☑ ~~/usr/lib/modules/*kernelversion*/kernel/net/ipv4~~

□ /etc/services

➡ □ /proc/sys/net/ipv6/ip_forward

Explanation

IP forwarding is another name for routing. It is sometimes called kernel IP forwarding because it is a feature of the Linux kernel. Enable IP forwarding by writing a 1 to the ip_forward file.

- Enable IPv4 forwarding by writing to the /proc/sys/net/ipv4/ip_forward file.
- Enable IPv6 forwarding by writing to the /proc/sys/net/ipv6/ip_forward file.

Be cautious about enabling IP forwarding without a firewall, especially if an interface connects to the internet or to a subnet you don't control.

Many firewall applications read from the /etc/services file. This file is a list of well-known services and their port assignments.

References

Linux Pro - 12.6 Linux Firewalls
[e_firewall_lp5.exam.xml Q_FIREALL_LP5_IP_FORWARDING]

Question 2: Incorrect

Which of the following are Python scripts classified as intrusion prevention software that provide dynamic rule sets to automate the rules iptables use to filter network traffic? (Choose TWO.)

☑ ~~firewalld~~

➡ □ DenyHosts

□ IPset

➡ □ Fail2ban

☑ ~~Uncomplicated Firewall (UFW)~~

Explanation

DenyHosts and Fail2ban are two popular Python scripts that are classified as instruction prevention software. Both scripts monitor log files and react to common security problems, such as brute force attacks, by adding or modifying firewall rules.

Uncomplicated Firewall (UFW) provides a user-friendly framework for managing Netfilter.

IPset is a companion application to IPTables that allows you to easily set firewall rules for a block of IP addresses.

firewalld is a front-end controller for IPTables.

References

Linux Pro - 12.6 Linux Firewalls
[e_firewall_lp5.exam.xml Q_NETSEC_F_LP5_DENYHOSTS_FAIL2BAN]

▼ **Question 3:** Correct

Alex, a webmaster, recently deployed a new web server. After checking external access to the new web server, he was unable to communicate on port 80. Alex verified that the host-based firewall's configuration had been changed and that the httpd service is running.

Which of the following commands will most likely resolve the communication issue?

○ **systemctl restart httpd**

○ **firewall-cmd --permanent --zone=public --add-port= 80/tcp**

➡ ● **systemctl restart firewalld**

○ **Install firewalld on the same system as the webserver**

Explanation

systemctl restart firewalld restarts the firewall service. This is important because if you make any changes to the firewall configuration, you need to restart the firewalld daemon in order to have that change take effect. This is most likely the step that Alex did not complete for the configuration changes to take effect.

firewall-cmd --permanent --zone=public --add-port= 80/tcp changes the configuration, which Alex had already done.

Install firewalld on the same system as the webserver is not a command.

systemctl restart httpd will restart the webserver, which will have no impact on the issue since the webserver is running.

References

Linux Pro - 12.6 Linux Firewalls
[e_firewall_lp5.exam.xml Q_NETSEC_F_LP5_FIREWALLD]

▼ **Question 4:** Incorrect

Which of the following popular Linux firewalls are based on Netfilter? (Choose THREE).

☐ IP Forwarding

➡ ☐ firewalld

☐ netcat

☑ ~~netstat~~

➡ ☐ Uncomplicated Firewall (UFW)

➡ ☑

➡ ☐ IPTables

☐ Wireshark

Explanation

Iptables, Uncomplicated Firewall (UFW), and firewalld are all firewalls based on Netfilter.

The other options are not firewalls.

References

Linux Pro - 12.6 Linux Firewalls
[e_firewall_lp5.exam.xml Q_NETSEC_F_LP5_NETFILTER]

▼ **Question 5:** Incorrect

In an effort to secure the internal network, the system administrator has implemented a host-based firewall and set up explicit allow and deny statements for specific ports and services. Some of the employees are complaining they can no longer access the applications they need. The server was on the internal network connected to an internal router, which is connected to the DMZ and an external router to the internet.

Which of the following is the most likely causing problems?

○ The internal network router is now misconfigured.

➡ ○ Restrictive ACLs on the firewall.

● ~~The external network router is now misconfigured.~~

○ The DMZ is blocking access.

Explanation

Restrictive ACLs on the firewall is most like the issue since access was disrupted after implementing the firewall. ACLs determine whether routed packets are accepted, rejected, or dropped.

- Accepted packets are forwarded on to their destinations.
- Rejected packets are blocked, and a message is sent back to the packet's sender.
- Dropped packets are also blocked, but no message is sent.

Changes to the host-based firewall would not impact the internal router, DMZ, or the external router.

References

Linux Pro - 12.6 Linux Firewalls
[e_firewall_lp5.exam.xml Q_NETSEC_F_LP5_RESTRICTIVE_ACLS]