15.5.4 Practice Questions

Candidate: Ethan Bonavida (suborange)

Date: 12/8/2022 11:56:27 pm • **Time Spent:** 01:20

Score: 100% Passing Score: 80%

▼ Question 1: ✓ Correct

You manage a Linux server that occasionally needs to provide ftp services at irregular intervals. To save on resources, you want to have the ftp server service running only when it is needed, and stopped the rest of the time.

Which of the following solutions would satisfy these requirements and require the LEAST amount of effort?

○ Create a link to the ftp services init script in the /etc/rc3.d directory.

➡ ● Enable the ftp service to be managed by the xinetd service.

○ Manually start and stop the ftp service at regular intervals.

○ Write a shell script that starts the ftp server at random times.

Explanation

The xinetd service is also known as a super server. A super server is a service that listens on behalf of other services, starting them only when they are requested, and stopping them when finished.

Starting the ftp service at random or scheduled times may not allow the service to be available when needed.

Creating a link to the ftp services init script in the /etc/rc3.d directory would only enable the service to start automatically in runlevel 3.

References

15.12.1 Security Best Practices

15.12.2 Security Best Practices Facts

q_xinitd_f_01.question.fex

▼ Question 2: ✓ Correct

You want to limit Telnet access to three specific users.

Which of the following strategies will BEST accomplish this goal?

○ Set a limit for Telnet in the /etc/inetd.conf file.

➡ ● Enter IP address entries for the three users in the /etc/hosts.allow file.

○ Create invalid remote shells for all but the three users allowed access.

○ Enter the three users' IP addresses in the /etc/usertty file.

Explanation

Use the /etc/hosts.allow file to list the IP address of the only hosts allowed access.

In the /etc/inetd.conf file, you can only enable or disable telnet completely and cannot place users limits there. The /etc/usertty file can hold restrictions for users based on username, but cannot hold restrictions based on IP address.

References

12.2.6 Network Configuration Facts

q_xinitd_f_02.question.fex

Question 3: ✓ Correct

You are modifying the **tcpd** control files of the xinetd super daemon. Of the two **tcpd** control files, what is the full path and filename of the file that is applied first?

/etc/hosts.allow ✓

Explanation

The following **tcpd** control files determine which computers can access the services through xinetd:

- /etc/hosts.deny denies services to the specified host(s) or subnets.
- /etc/hosts.allow permits services to the specified host(s) or subnets.

Be aware of the following details:

- The /etc/hosts.allow is read first and applied before /etc/hosts.deny.
- In each of these files, if **tcpd** finds a matching rule, the search is stopped, and all remaining rules are ignored.

References

12.2.6 Network Configuration Facts

q_xinitd_f_03.question.fex

Question 4: ✓ Correct

What should you enter at the command prompt to check the TCP wrapper configuration on your system?

tcpdchk ✓

Explanation

Use **tcpdchk** to test and display any potential or real problems with the TCP wrapper configuration. **tcpdchk** compares the /etc/hosts.deny and/etc/hosts.allow files against the configuration files.

References

15.5.3 The xinetd Daemon and TCP Wrapper Facts

q_xinitd_f_04.question.fex

▾ Question 5: ✓ Correct

Which of the following would enable the rsync service to be managed by the xinetd super daemon?

○ Type **xinetd rsync on**.

○ Create a link to the rsync init script in the /etc/xinetd.d directory.

➡ ● Create the rsync file in **/**etc/xinetd.d

○ Add *XINETD* = *true* to the rsync init script.

Explanation

You enable services to be managed by the xinetd super server by creating a file containing the service description in the /etc/xinetd.d directory and then restarting the xinetd service.

Creating a link to the rsync init script in the /etc/xinetd.d directory would not work because the xinetd service does not use standard init scripts to manage services. The xinetd service cannot be made aware of a service by executing xinetd with the service as an operand.

References

☰ **15.5.3 The xinetd Daemon and TCP Wrapper Facts**

q_xinitd_f_05.question.fex

▼ Question 6: ✓ Correct

Which of the following is the super daemon that is most commonly found in modern Linux distributions?

- ○ init
- ➡ ● xinetd
- ○ inetd
- ○ xserver

Explanation

Even though inetd and xinetd are both super daemons, xinetd is the one most commonly found in modern Linux distributions.

Although init does manage service it does not start and stop the services on demand. xserver is not the name of a super server; it is a name for the X window environment server.

References

15.5.3 The xinetd Daemon and TCP Wrapper Facts

q_xinitd_f_06.question.fex

Question 7: ✓ Correct

Which of the following is an advantage of xinetd over inetd?

- ➡ ● xinetd uses separate configuration files for each managed service.
- ○ xinetd does not require an external program, such as tcpd, to restrict access to its services.
- ○ xinetd can listen on behalf of more than one service at a time.
- ○ xinetd is written in Java and is, therefore, more secure.

Explanation

inetd will run on any Linux distribution, but most modern distribution maintainers use xinetd instead of inetd. Instead of storing configuration settings for all managed services in a single file (as inetd does), xinetd provides greater flexibility by using separate configuration files for each managed service.

The computer language xinetd is written in has nothing to do with xinetd security.

References

☰ **15.5.3 The xinetd Daemon and TCP Wrapper Facts**

q_xinitd_f_07.question.fex

▼ Question 8: ✓ Correct

Which of the following is the main purpose of the xinetd service?

○ To listen for http requests.

○ To listen for internet traffic on the external network interface.

○ To act as a firewall for your Linux system.

➡ ● To receive client requests for network services and start and stop them on demand.

Explanation

Xinetd is what is known as a super server. Its purpose is to listen on behalf of other network services and start and stop them on demand. It can be configured to listen to traffic on any interface for any service.

The firewall on a Linux system is managed by iptables on kernel 2.4 and newer systems and ipchains on kernel 2.2 and earlier systems.

Apache is the most common web server (a server that listens and responds to http requests). Xinetd can be configured to listen for http requests and start and stop the Apache server on demand, but doing so is not xinetd's main purpose.

References

15.5.3 The xinetd Daemon and TCP Wrapper Facts

q_xinitd_f_08.question.fex

▼ Question 9: ✓ Correct

Management wants a compilation of specific data to occur every night. The only way to accomplish this task is to copy files throughout all network hosts to one server via TFTP.

Which of the following files MUST be edited to enable xinetd to manage TFTP on the Linux server?

○ /etc/services

○ /etc/tftpd

➡ ◉ /etc/xinetd.d/tftp

○ /etc/tftpd.conf

Explanation

Virtually all Linux distributions today use the newer version of inetd called xinetd. If this is the case, then the correct file would be /etc/xinetd.d/tftp. /etc/xinetd.d contains separate configuration files for daemons being managed by xinetd.

References

15.5.3 The xinetd Daemon and TCP Wrapper Facts

q_xinitd_f_09.question.fex

Question 10: ✓ Correct

You want to allow any host from westsim.com to have access to your system.

Which of the following line items would you add to the **/etc/hosts.allow** file to accomplish this task?

➡ ● ALL: .westsim.com

○ ALLOW: .westsim.com = YES

○ ANY: .westsim.com

○ ALLOW: .westsim.com

Explanation

The correct line is *ALL: .westsim.com. ALL* means all services are available; ***.**westsim.com* means any host at westsim.com.

There are no keywords such as ANY, ALLOW, or YES for the /etc/hosts.allow file.

References

12.2.6 Network Configuration Facts

q_xinitd_f_10.question.fex

▾ Question 11: ✓ Correct

You want to allow any host from westsim.com to have access to your system except a system called testsvr.westsim.com.

Which of the following line items would you add to the /etc/hosts.allow file to accomplish this task?

○ ALLOW: .westsim.com, testsvr.westsim.com = NO

➡ ● ALL: .westsim.com EXCEPT testsvr.westsim.com

○ ANY: .westsim.com EXCEPT testsvr.westsim.com

○ ALLOW: .westsim.com ALL EXCEPT testsvr.westsim.com

Explanation

The correct line is **AL**_L: .westsim.com EXCEPT testsvr.westsim.com. ALL_ means all services are available. _.westsim.com_ means any host at westsim.com and the keyword _EXCEPT_ sets the exception for testsvr.westsim.com.

There are no keywords such as ANY and ALLOW for the /etc/hosts.allow file.

References

12.2.6 Network Configuration Facts

q_xinitd_f_11.question.fex

Question 12: ✓ Correct

Your site is dependent upon the use of the rlogin utility for remote access. For security reasons, you want to prevent the hosts in the marketing department from accessing the payroll server, but allow all others to do so.

Which of the following files should you use to create this restriction?

➡ ● hosts.deny

○ hosts

○ hosts.allow

○ hostname

Explanation

The hosts.deny file (which resides in the /etc directory) is an optional file that can be created. If it exists, then hosts whose IP addresses are listed in this file will be denied remote access. All host IP addresses not listed in this file are allowed access.

References

▷ **15.12.1 Security Best Practices**

☰ **15.12.2 Security Best Practices Facts**

q_xinitd_f_12.question.fex