Topic 110: Security

Topic 110: (10) Security

110.1 (3) Perform security administration tasks

110.2 (3) Setup host security

110.3 (4) Securing data with encryption

110.1 (3) Perform security administration tasks

Question:

With X11 forwarding in ssh, what environment variable is automatically set in the remote host shell that is not set when X11 forwarding is not enabled? (Specify only the environment variable withoutany additional commands or values.)

Answer: DISPLAY, $DISPLAY

Question: 149

The presence of what file will temporarily prevent all users except root from logging into the system?

(Specify the full name of the file, including path.)

Answer: /etc/nologin

Question: 152

Which comand is used to set restrictions on the size of a core file that is created for a user when a program crashes?

A. core

B. edquota

C . ulimi

D. quota

Answer: C

Question: 153

When trying to unmount a device it is reported as being busy. Which of the following commands could be used to determine which process is causing this?

A . debug

B . lsof

C. nesus

D. strace

E. traceroute

Answer: B

Question: 155

Which of the following find commands will print out a list of files owned by root and with the SUID bit set in /usr?

A. find /usr -uid 0 -perm +4000

B. find -user root +mode +s /usr

C. find -type suid -username root -d /usr

D. find /usr -ls *s* -u root

E. find /usr -suid -perm +4000

Answer: A

Question: 157

Which file lists which users can execute commands using sudo? (Specify the full name of the file, including path.)

Answer: /etc/sudoers

Question: 161

Which of the following commands can be used to limit the amount of memory a user may use?

A . umask

B . usermod

C . ulimit

D. passwd

E. chage

Answer: C

Question: 162

On a Linux system with shadow passwords enabled, which file in the file system contains the password hashes of all local users? (Specify the full name of the file, including path.)

Answer: /etc/shadow

Question: 193

Which of the following commands can identify the PID of a process which opened a TCP port?

A. ptrace

B. strace

C . debug

D. lsof

E . nessus

Answer: D

Question: 191

Given the following excerpt of the sudo configuration:

jane ANY=NOPASSWD: /bin/kill, /bin/id, PASSWD: /sbin/fdisk

Which of the following statements are true? (Choose three.)

A. Jane can run /bin/id only after specifying her password.

B. Jane can run /sbin/fdisk after specifying root's password.

C. Jane can run /sbin/fdisk after specifying her password.

D. Jane can run /bin/kill without specifying a password.

E. Jane can run /bin/id without specifying her password.

Answer: C,D,E

110.2 (3) Setup host security

Question: 151

Which of the following programs uses the hosts.allow file to perform its main task of checking for

access control restrictions to system services?

A. tcpd

B. inetd

C. fingerd

D. mountd

E. xinetd

Answer: A

Question: 156

Which directory holds the files that configure the xinetd service when using several configuration

files instead of an integrated configuration file? (Specify the full path to the directory.)

Answer: /etc/xinetd.d/, /etc/xinetd.d

Question: 158

Which file contains a set of services and hosts that will be allowed to connect to the server by going through a
TCP Wrapper program such as tcpd? (Specify the full name of the file, including path.)

Answer: /etc/hosts.allow

Question: 190

What is the purpose of TCP wrapper?

A. Manage and adjust bandwidth used by TCP services.

B. Bind a network service to a TCP port.

C. Encapsulate TCP messages in IP packets.

D. Add SSL support to plain text TCP services.

E. Limit access to a network service.

Answer: E

110.3 (4) Securing data with encryption

Question: 150

Which configuration file would be edited to change the default options for outbound SSH sessions?

A. /etc/ssh/sshd_config

B. /etc/ssh/ssh

C. /etc/ssh/client

D. /etc/ssh/ssh_config

E. /etc/ssh/ssh_client

Answer: D

Question: 154

Which configuration file would be edited to change default options for the OpenSSH server?

A. /etc/ssh/sshd_config

B. /etc/ssh/ssh

C. /etc/ssh/server

D. /etc/ssh/ssh_config

E. /etc/ssh/ssh_server

Answer: A

Question: 159

Which of the following commands preloads and manages keys that are used for automatic authentication while logging in to other machines using SSH?

A . sshd

B . ssh-agent

C. ssh-keygen

D. ssh-add

Answer: B

Question: 160

What is a purpose of an SSH host key?

A. It must be sent by any SSH client in addition to a user key in order to identify the client's host.

B. It provides the server's identity information to connecting SSH clients.

C. It is the root key by which all user SSH keys must be signed.

D. It authenticates any user that logs into a remote machine from the key's host.

E. It is used by system services like cron, syslog or a backup job to automatically connect to remote hosts.

Answer: B

Question: 163

Which of the following commands connects to the remote host example.com which has OpenSSH listening on TCP port 2222? (Choose TWO correct answers.)

A. ssh --port 2222 example.com

B. ssh -p 2222 example.com

C. ssh -o Port=2222 example.com

D. ssh -o GatewayPort=2222 example.com

E. ssh example.com:2222

Answer: B, C

Question: 192

Which configuration file contains the default options for SSH clients?

A. /etc/ssh/sshd_config

B. /etc/ssh/ssh

C. /etc/ssh/ssh_config

D. /etc/ssh/client

E. /etc/ssh/ssh_client

Answer: C

Question: 194

Which of the following features are provided by SPICE? (Choose two.)

A. Connecting local USB devices to remote applications.

B. Accessing graphical applications on a remote host.

C. Replacing Xorg as local X11 server.

D. Downloading and locally installing applications from a remote machine.

E. Uploading and running a binary program on a remote machine.

Answer: A,D