Chapter 10
Security (Domain 110)

THE FOLLOWING COMPTIA LINUX+/LPIC-1 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- **✓110.1 Perform security administration tasks**
- Audit a system to find files with the suid/sgid bit set
- Set or change user passwords and password aging information
- Being able to use nmap and netstat to discover open ports on a system
- Set up limits on user logins, processes and memory usage
- Determine which users have logged in to the system or are currently logged in
- Basic sudo configuration and usage
- The following is a partial list of the used files, terms and utilities:
- find
- passwd
- fuser
- lsof
- nmap
- chage
- netstat
- sudo
- /etc/sudoers
- su
- usermod
- ulimit
- who, w, last
- **✓110.2 Set up host security**
- Awareness of shadow passwords and how they work
- Turn off network services not in use
- Understand the role of TCP wrappers
- The following is a partial list of the used files, terms and utilities:
- /etc/nologin
- /etc/passwd
- /etc/shadow
- /etc/xinetd.d/*
- /etc/xinetd.conf
- /etc/inetd.d/*
- /etc/inetd.conf

- /etc/hosts.allow
- /etc/hosts.deny
- ✓**110.3 Securing data with encryption**
- Perform basic OpenSSH 2 client configuration and usage
- Understand the role of OpenSSH 2 server host keys
- Perform basic GnuPG configuration, usage and revocation
- Understand SSH port tunnels (including X11 tunnels)
- The following is a partial list of the used files, terms and utilities:
- ssh
- ssh-keygen
- ssh-agent
- ssh-add
- ~/.ssh/id_rsa and id_rsa.pub
- ~/.ssh/id_dsa and id_dsa.pub
- /etc/ssh/ssh_host_rsa_key and ssh_host_rsa_key.pub
- /etc/ssh/ssh_host_dsa_key and ssh_host_dsa_key.pub
- ~/.ssh/authorized_keys
- /etc/ssh_known_hosts
- gpg
- ~/.gnupg/*

1. 1. You need to prevent users temporarily from logging into the system using ssh or another means. Which of the following describes one method for accomplishing this task?

1. Use the command `touch /etc/nologin`.
2. Disable sshd.
3. Remove `/etc/login`.
4. Add a shadow file.

2. 2. Which of the following commands searches the entire filesystem for files with the `setuid` bit set?

1. `find ./ -perm suid`
2. `find / -perm 4000`
3. `find / -type suid`
4. `find / -type f -perm setuid`

3. 3. Which of the following commands displays the currently open ports and the process that is using the port?

1. `netstat -a`
2. `lsof -i`
3. `ps auwx`
4. `netlist`

4. 4. You are attempting to unmount a filesystem using the `umount` command. However, when you do so, you receive a message indicating that the filesystem is in use. Which of the following commands can be used to determine what process is keeping a filesystem open?

1. `fuser`
2. `ls`
3. `find`
4. `ps`

5. 5. Which of the following commands displays account information such as expiration date, last password change, and other related details?

1. `usermod -l`
2. `userinfo -a`

3. `chageuser -l`
4. `chage -l`

6. 6. Which of the following commands scans the IP address `192.168.1.154` for open ports?

1. `nmap 192.168.1.154`
2. `lsof 192.168.1.154`
3. `netstat 192.168.1.154`
4. `netmap 192.168.1.154`

7. 7. Which command is used to create a public/private key pair for use with ssh?

1. `ssh -k`
2. `ssh-keygen`
3. `ssh-genkey`
4. `ssh -key`

8. 8. Which of the following configuration options sets a hard limit of 25 processes for a user called suehring in `/etc/security/limits.conf`?

1. `suehring hard proc 25`
2. `suehring hard nproc 25`
3. `suehring proc 25 hard-limit`
4. `proc 25 suehring hard`

9. 9. Within which file should you place public keys for servers from which you will accept key-based ssh authentication?

1. `~/.ssh/authorized_keys`
2. `~/.ssh/keys`
3. `~/.ssh/keyauth`
4. `~/.sshd/authkeys`

10. 10. The system on which you are working does not have the `lsof` command installed, and you are not allowed to install software without going through four levels of approval and scheduling the installation weeks in advance. However, the `netstat` command is available. Which option to `netstat` will show the process ID to which a given network port is connected?

1. `-a`
2. `-n`
3. `-p`
4. `-l`

11. 11. You need to look at information on logins beyond that which is captured by the current log file for the `last` command. Which option to the `last` command can be used to load information from an alternate file?

1. `-a`
2. `-t`
3. `-e`
4. `-f`

12. 12. You need to examine who is currently logged in to the system. Which of the following commands will display this information?

1. `listuser`
2. `fuser`
3. `ls -u`
4. `w`

13. 13. You need to execute a command as a specific user. Which of the following commands enables this to occur?

    1. `sudo -u`
    2. `sudo -U`
    3. `sudo -s`
    4. `sudo -H`

14. 14. Which option in `/etc/sudoers` will cause the specified command to not prompt for a password?

    1. `PASSWORD=NO`
    2. `NOPASSWD`
    3. `NOPASSWORD`
    4. `NOPROMPT`

15. 15. Which of the following commands will display the cputime, memory, and other limits for the currently logged-in user?

    1. `reslimit`
    2. `limitres -a`
    3. `ulimit -a`
    4. `proclimit -n`

16. 16. Which line within the `/etc/hosts.deny` file will prevent any host within the `192.168.1.0/24` network from accessing services that operate from xinetd?

    1. `BLOCK: 192.168.1.0/24`
    2. `REJECT: 192.168.1.0`
    3. `ALL: 192.168.1.0/255.255.255.0`
    4. `NONE: 192.168.1/255.255.255.0`

17. 17. When expiring a user account with `usermod -e`, which of the following represents the correct date format?

    1. `YYYY-MM-DD`
    2. `MM/DD/YYYY`
    3. `DD/MM/YY`
    4. `MM/DD/YY HH:MM:SS`

18. 18. Which of the following directives in a configuration file found within `/etc/xinetd.d` will prevent the service from starting?

    1. `enable no`
    2. `start no`
    3. `disable yes`
    4. `boot no`

19. 19. You are using an RSA-based key pair for SSH. By default, what is the name of the private key file in `~/.ssh`?

    1. `id_rsa`
    2. `id_rsa.priv`
    3. `id_rsa.key`
    4. `rsa_key.priv`

20. 20. Which option to the `su` command will execute a single command with a non-interactive session?

    1. `-s`
    2. `-u`
    3. `-c`
    4. `-e`

21. 21. After specifying the `keyserver`, which option to `gpg` is used to specify the key to send to the key server?

    1. `key-name`
    2. `keyname`
    3. `send-key`
    4. `sendkey`

22. 22. Which of the following best describes the method to use with ssh in order to execute a single command on a remote server?

    1. Use the `-e` option followed by the command.
    2. Send the command after the other options as part of the command line.
    3. Use the `--execute` option followed by the command.
    4. Use the `-s` option followed by the command.

23. 23. When using `ssh-agent`, which command and option lists the currently loaded keys?

    1. `ssh-agent -l`
    2. `ssh -l`
    3. `ssh-list-keys`
    4. `ssh-add -l`

24. 24. Which of the following commands should be used to edit the `/etc/sudoers` file?

    1. Any text editor such as vi or emacs
    2. `editsudo`
    3. `visudo`
    4. `visudoers`

25. 25. Which of the following commands can be used to stop a given service, such as `httpd.service`, from starting on boot with a `systemd`-based system?

    1. `systemctl disable httpdservice`
    2. `systemctl stop httpd.service`
    3. `systemd disable httpd.service`
    4. `systemd enable httpd.service boot=no`

26. 26. Which of the following commands will set an account to expire based on the number of days elapsed since January 1, 1970?

    1. `passwd -e`
    2. `chage -E`
    3. `usermod -l`
    4. `chguser`

27. 27. You are using `nmap` to scan a host for open ports. However, the server is blocking ICMP echo requests. Which option to `nmap` can you set in order to continue the scan?

    1. `-P0`
    2. `-no-ping`
    3. `-s0`
    4. `-ping-0`

28. 28. Which option within `/etc/security/limits.conf` is used to control the number of times that a given account can log in simultaneously?

    1. `nlogins`
    2. `loginmax`

3. `maxlogins`
4. `loginlimit`

29. 29. Which file can be used to store a server-wide cache of hosts whose keys are known for ssh?

1. `/etc/sshd_known_hosts`
2. `/etc/ssh_known_hosts`
3. `~/.ssh/known_hosts`
4. `/root/ssh_known_hosts`

30. 30. Within the following entry in `/etc/shadow`, to what does the number `15853` refer?

```
mail:*:15853:0:99999:7:::
```

1. The UID of the mail user
2. The number of files owned by mail
3. The date of the last password change (since 1/1/1970)
4. The number of days until the account expires

31. 31. Which of the following commands sets up a local port forwarding session on local port 5150 to remote port 80 of www.example.com? (http://www.example.com?)

1. `ssh -L 5150:www.example.com:80`
2. `ssh 5150:www.example.com`
3. `ssh -p 5150 www.example.com`
4. `ssh -e 5150 www.example.com:80`

32. 32. Which option must be enabled in `/etc/sshd_config` on the destination server in order for X11 forwarding to work?

1. `XForward yes`
2. `Xenable yes`
3. `X11Forwarding yes`
4. `Xconnection yes`

33. 33. Which of the following commands generates a GnuPG key pair?

1. `gpg --gen-key`
2. `gpg --key`
3. `gpg --send-key`
4. `gpg --create-key`

34. 34. Which of the following represents a group called `admins` within `/etc/sudoers`?

1. `@admins`
2. `admins`
3. `-admins`
4. `%admins`

35. 35. Which option to ssh is used to set the port for the remote host?

1. `-p`
2. `-P`
3. `-l`
4. `@`

36. 36. Which option to `nmap` sets the scan to use TCP SYN packets for finding open ports?

1. `-sS`

2. `-sT`
3. `-sY`
4. `-type SYN`

37. 37. Which of the following logs is used by the last command for detailing recent logins?

1. `/var/log/last`
2. `/var/log/all.log`
3. `/var/log/wtmp`
4. `/var/log/logins`

38. 38. Which option to ssh enables the use of a key for authentication?

1. `-i`
2. `-k`
3. `-f`
4. `--key`

39. 39. In a scripting scenario, you need to prevent sudo from prompting for credentials or for any other reason. Which option to sudo is used to indicate this?

1. `-n`
2. `--noprompt`
3. `-i`
4. `-q`

40. 40. Which of the following commands generates an RSA key for use with ssh?

1. `ssh -key rsa`
2. `ssh --gen-key rsa`
3. `ssh-keygen -t rsa`
4. `ssh-keygen rsa`

41. 41. You need to disable a service found in `/etc/inetd.conf`. Which of the following is used as a comment character in that file?

1. `-`
2. `#`
3. `/`
4. `%`

42. 42. Which of the following commands can be used to lock an account?

1. `usermod -L`
2. `usermod -l`
3. `passwdlock`
4. `lockacct`

43. 43. Which file is used as the default storage for public keyrings for gpg?

1. `publickeys.gpg`
2. `pubring.gpg`
3. `public.gpg`
4. `pubkeys.gpg`

44. 44. Which file in `~/.gnupg`, if present, indicates that files have been migrated to gpg version 2.1 or later?

1. `.gpg-v21`
2. `.gpg-updated`

3. `.gpg-v21-migrated`
4. `.gpg-files-v21`

45. 45. Which of the following commands searches a server for files with the `setgid` bit enabled?

1. `find / -perm 4000`
2. `find ./ -perm setgid`
3. `grep setgid *`
4. `find / -perm 2000`

46. 46. Which of the following commands creates links within `/etc/rc.d/*` for starting and stopping services on a Debian system?

1. `createsym`
2. `startstop-service`
3. `update-rc.d`
4. `createconfig`

47. 47. Which runlevel is typically used for single-user mode, as indicated in `/etc/inittab`?

1. 1
2. 2
3. 5
4. 6

48. 48. Which option to the `su` command is used to obtain the normal login environment?

1. `-u`
2. `-U`
3. `-`
4. `-login`

PREV
Chapter 9 Networking Fundamentals (Domain 109)

NEXT
Part II LPIC-2