Chapter 23
System Security (Topic 212)

THE FOLLOWING LPIC-2 EXAM TOPICS ARE COVERED IN THIS CHAPTER:

- ✓**212.1 Configuring a router**
- iptables and ip6tables configuration files, tools and utilities
- Tools, commands and utilities to manage routing tables.
- Private address ranges (IPv4) and Unique Local Addresses as well as Link Local Addresses (IPv6)
- Port redirection and IP forwarding
- List and write filtering and rules that accept or block IP packets based on source or destination protocol, port and address
- Save and reload filtering configurations
- The following is a partial list of the used files, terms and utilities:
- /proc/sys/net/ipv4/
- /proc/sys/net/ipv6/
- /etc/services
- iptables
- ip6tables
- ✓**212.2 Managing FTP servers**
- Configuration files, tools and utilities for Pure-FTPd and vsftpd
- Awareness of ProFTPd
- Understanding of passive vs. active FTP connections
- The following is a partial list of the used files, terms and utilities:
- vsftpd.conf
- important Pure-FTPd command line options
- ✓**212.3 Secure shell (SSH)**
- OpenSSH configuration files, tools and utilities
- Login restrictions for the superuser and the normal users
- Managing and using server and client keys to login with and without password
- Usage of multiple connections from multiple hosts to guard against loss of connection to remote host following configuration changes
- The following is a partial list of the used files, terms and utilities:
- ssh
- sshd
- /etc/ssh/sshd_config
- /etc/ssh/
- Private and public key files

- ✓**212.4 Security tasks**
- Tools and utilities to scan and test ports on a server
- Locations and organisations that report security alerts as Bugtraq, CERT or other sources
- Tools and utilities to implement an intrusion detection system (IDS)
- Awareness of OpenVAS and Snort
- The following is a partial list of the used files, terms and utilities:
- telnet
- nmap
- fail2ban
- nc
- iptables
- ✓**212.5 OpenVPN**
- OpenVPN
- The following is a partial list of the used files, terms and utilities:
- /etc/openvpn/
- openvpn

1. 1. Which of the following options within an OpenSSH server configuration is used to determine whether the root user can log in directly with an ssh client?

1. `PermitRootLogin`
2. `AllowRoot`
3. `RootLogin`
4. `PermitDirectRootLogin`

2. 2. Which of the following files is used as the primary configuration file for `vsftpd`?

1. `vsftp.cfg`
2. `vsftpd.conf`
3. `vsftpd.cfg`
4. `vsftp.conf`

3. 3. Which iptables chain is used to create a port redirect?

1. REDIRECT
2. PREROUTING
3. PORTREDIR
4. ROUTING

4. 4. Which of the following files is the primary server configuration file for OpenSSH?

1. `/etc/ssh/sshd_config`
2. `/etc/sshserver.conf`
3. `/etc/openssh.conf`
4. `/etc/openssh/sshd.conf`

5. 5. Which of the following commands saves the current set of iptables rules into a file?

1. `save-iptables`
2. `iptables-create`
3. `iptables-save`
4. `ipt-save`

6. 6. When starting Pure FTPd, which command-line option is used to indicate that host names should not be resolved on client connection?

   1. `-n`
   2. `-H`
   3. `-r`
   4. `-z`

7. 7. Which of the following commands can be used to generate a private and public key pair for authentication with ssh?

   1. `ssh-createkey`
   2. `sshkey`
   3. `ssh-key`
   4. `ssh-keygen`

8. 8. Which of the following commands tests a connection to `mail.example.com` on the standard SMTP port?

   1. `telnet mail.example.com smtp`
   2. `telnet mail.example.com 25`
   3. `telnet mail.example.com`
   4. `smtptest mail.example.com`

9. 9. Which of the following commands lists the current iptables rules while not attempting to resolve host or port names?

   1. `iptables -L`
   2. `iptables -List -no-resolve`
   3. `iptables -a`
   4. `iptables -nL`

10. 10. Which command-line option to Pure FTPd disables anonymous upload?

    1. `-n`
    2. `-a`
    3. `-i`
    4. `-m`

11. 11. Which option within an OpenSSH configuration is used to specify the port on which the daemon will listen?

    1. `Port`
    2. `ListenOn`
    3. `ListenPort`
    4. `PortNum`

12. 12. Which option within an OpenVPN configuration lets a client know that it can reach the network `192.168.5.0/24`?

    1. `client-route 192.168.5.0`
    2. `push "route 192.168.5.0 255.255.255.0"`
    3. `send "route 192.168.5.0/24"`
    4. `client-route "192.168.5.0/24"`

13. 13. Which of the following commands executes a port scan using TCP Connect to the host `192.168.2.3`?

    1. `portscan 192.168.2.3`
    2. `nmap -sT 192.168.2.3`
    3. `maphost 192.168.2.3`
    4. `tcpscan -C 192.168.2.3`

14. 14. Which of the following directories contains configuration files for the fail2ban system?

    1. `/etc/fail2ban.cfg`
    2. `/etc/fail2ban.d`
    3. `/etc/f2b`
    4. `/etc/fail2ban`

15. 15. Which option on the client side of an SSH connection is used to specify the private key for authentication?

    1. `ssh -i`
    2. `ssh -k`
    3. `ssh -p`
    4. `ssh -l`

16. 16. Which of the following commands saves the current IPv6 iptables configuration?

    1. `iptables6-save`
    2. `ip6tables-save`
    3. `iptables6save`
    4. `save-iptables6`

17. 17. Within an OpenSSH configuration, which option disables the use of empty passwords?

    1. `DisableEmptyPass`
    2. `PermitEmptyPasswords`
    3. `EmptyPasswordAuth`
    4. `PermitPasswordLength`

18. 18. Which of the following commands sets the default policy for the INPUT chain to discard packets that don't have a specific rule allowing them?

    1. `iptables INPUT DROP`
    2. `iptables chain INPUT policy DROP`
    3. `iptables -P INPUT DROP`
    4. `iptables POLICY=DROP CHAIN=INPUT`

19. 19. On which port and protocol does OpenVPN listen?

    1. ICMP/1194
    2. UDP/1194
    3. TCP/1194
    4. VPN/1194

20. 20. Which directive in an OpenSSH configuration is used for specifying the version of the SSH protocol to use?

    1. `Proto`
    2. `Protocol`
    3. `ProtoVer`
    4. `Version`

21. 21. Which of the following best describes the difference between the `DROP` and `REJECT` targets in iptables?

    1. Both `DROP` and `REJECT` do the same thing.
    2. `DROP` silently discards packets, while `REJECT` sends back an ICMP acknowledgement.
    3. `REJECT` silently discards packets, while `DROP` sends back an ICMP acknowledgement.
    4. `DROP` sends back a direct message, and `REJECT` sends a redirect.

22. 22. Which file contains a list of keys that will be accepted for authentication for a given user?

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

23. 23. Which of the following partial iptables rules sets up a configuration that limits log entries to three per minute?

    1. `-m limit 3 -j LOG`
    2. `-m limit --limit 3/minute --limit-burst 3 -j LOG`
    3. `-m limit --limit 3`
    4. `-m limit --limit-minute 3 --burst 3 -j LOG`

24. 24. Which option to the `ssh` command is used for X11 application forwarding?

    1. `-X11`
    2. `-A`
    3. `-X`
    4. `-F`

25. 25. The command `netstat -a` is reporting that port 80 is in use on the server. Which of the following commands can be used to determine what is actually using that port?

    1. `listPorts`
    2. `portlist -a`
    3. `lsof -i`
    4. `tcpdump`

26. 26. Which of the following partial `iptables` rules allows incoming ICMP traffic?

    1. `-A INPUT -p ICMP -j ACCEPT`
    2. `-A IN -P ICMP`
    3. `-A INPUT -P ACCEPT-ICMP`
    4. `-A IN -P ICMP -j ACCEPT`

27. 27. Which option in an OpenSSH configuration is used to determine whether port forwarding will be enabled?

    1. `AllowPortForwarding`
    2. `PortForwarding`
    3. `ForwardPort`
    4. `AllowTcpForwarding`

28. 28. Which of the following partial iptables rules blocks all traffic from `192.168.51.50`?

    1. `-A INPUT -p ALL 192.168.51.50 -j ACCEPT`
    2. `-A INPUT -p ALL -s 192.168.51.50 -j DROP`
    3. `-A INPUT -p ALL -s 192.168.51.50 -j BLOCK`
    4. `-A INPUT -p ALL -f 192.168.51.50 -j DISCARD`

29. 29. Which of the following partial iptables rules will allow all hosts to connect to TCP port 2222?

    1. `-A INPUT -p TCP -s 0/0 --destination-port 2222 -j ACCEPT`
    2. `-A TCP -s ALL -p 2222 -j ACCEPT`
    3. `-A INPUT -p TCP -s *.* --destination-port 2222 -j ALLOW`
    4. `-A INPUT --destination-port */* -j ACCEPT`

30. 30. Which of the following commands enables forwarding such as would be used for NAT?

    1. `echo "1" > /proc/sys/net/ipv4/nat`
    2. `echo "1" > /proc/sys/net/ipv4/ip_forward`
    3. `iptables --enable-forwarding`
    4. `ip-forward --enable`

31. 31. Within the `vsftpd.conf` file, which directive enables IPv6?

    1. `ipv6_enable`
    2. `ipv6`
    3. `ipv6_listen`
    4. `listen_ipv6`

32. 32. Which configuration directive for OpenSSH determines whether key-based authentication will be used?

    1. `KeyAuth`
    2. `PubKeyAuth`
    3. `PubkeyAuthentication`
    4. `AuthenticationKey`

33. 33. Within a jail configuration for fail2ban, which configuration option sets the name and location of the log file to monitor for failures?

    1. `logpath`
    2. `monitor`
    3. `logfile_mon`
    4. `monitor_log`

34. 34. Which command sends a copy of the public key identity to another server for use with SSH?

    1. `ssh-key`
    2. `ssh-copy-key`
    3. `ssh-sendkey`
    4. `ssh-copy-id`

35. 35. Which command is used for creation and maintenance of firewall rules for IPv6?

    1. `iptables6`
    2. `ip6tables`
    3. `ipv6tables`
    4. `ipfw6`

36. 36. Which of the following OpenVPN configuration entries sends a DHCP option to a client to indicate the DNS server (`192.168.2.1`) to be used by the client?

    1. `push "dhcp-option ns 192.168.2.1"`
    2. `push "dhcp-nameserver 192.168.2.1"`
    3. `push "dhcp-option DNS 192.168.2.1"`
    4. `push "dhcp-dns 192.168.2.1"`

37. 37. Which option in `vsftpd.conf` specifies whether users will be able to authenticate to the server?

    1. `local_enable`
    2. `users_login`
    3. `user_login`
    4. `local_users`

PREV
Chapter 22 E-Mail Services (Topic 211)

NEXT
Chapter 24 Practice Test 1