

## LPI Level 2 RPM (Exam 202)

1

Given a CIDR mask of /25 and a netmask of 255.255.255.128 how many host IP addresses are available?

\_\_\_\_\_ IP Addresses

(Please type your answer in the text field below.)

Answer:

---

2

Given a CIDR mask of /23 and a netmask of 255.255.254.0 how many usable host IP addresses are available?

\_\_\_\_\_ IP Addresses

(Please type your answer in the text field below.)

Answer:

---

3

Given the CIDR mask /29, the equivalent subnet mask in dotted quad format would be 255.255.255.\_\_\_\_\_.

(Please type your answer in the text field below.)

Answer:

---

4

What file should be edited to make the `route` command show human-readable names for networks? (Please enter the full path)

(Please type your answer in the text field below.)

Answer:

---

5

How would you display your system's current ARP cache?

- A. `arp -a`
- B. `netstat -a`
- C. `netstat -arp`
- D. `cat /etc/arp`

6

You find that a host (192.168.1.4) being used on one of your client's networks has been compromised with a backdoor program listening on port 31337. Your client requests a list of originating IP addresses connecting to that port. Using a Linux workstation as traffic analyzer, which of the following commands would gather the data requested by the client?

- Ⓐ A. `tcpdump host 192.168.1.4 and port 31337 -w out`
- Ⓑ B. `nmap host 192.168.1.4:31337`
- Ⓒ C. `arpwatch -n 192.168.1.4/32 -p 31337 > capture`
- Ⓓ D. `pcap -d 192.168.1.4:31337`
- Ⓔ E. `ipwatch --syn 192.168.1.4 -p 31337 --log=out`

7

While performing a security audit, you discover that a machine is accepting connections on TCP port 184, but it is not obvious which process has the port open. Which of the following programs would you use to find out?

- Ⓐ A. `traceroute`
- Ⓑ B. `strace`
- Ⓒ C. `debug`
- Ⓓ D. `nessus`
- Ⓔ E. `lsof`

8

What command is used to add a route to the 192.168.4.0/24 network via 192.168.0.2?

- Ⓐ A. `route add -network 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2`
- Ⓑ B. `route add -net 192.168.4.0/24 gw 192.168.0.2`
- Ⓒ C. `route add -network 192.168.4.0/24 192.168.0.2`
- Ⓓ D. `route add -net 192.168.4.0 netmask 255.255.255.0 192.168.0.2`
- Ⓔ E. `route add -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2`

9

All of the following commands can be used to determine open TCP ports on `localhost` **EXCEPT**:

- Ⓐ A. `lsof`
- Ⓑ B. `netstat`
- Ⓒ C. `nmap`
- Ⓓ D. `fuser`
- Ⓔ E. `ifconfig`

10

The following is an excerpt from the output of `tcpdump -nli eth1 'udp'`:

```
13:03:17.277327 IP 192.168.123.5.1065 > 192.168.5.112.53: 43653+ A? lpi.org.  
(25)  
13:03:17.598624 IP 192.168.5.112.53 > 192.168.123.5.1065: 43653 1/0/0 A  
24.215.7.109 (41)
```

Which network service or protocol was used?

- A. FTP
- B. HTTP
- C. SSH
- D. DNS
- E. DHCP

11

Which **TWO** of the following commands could be used to add a second IP address to `eth0`?

- A. `ifconfig eth0 --add-ip 192.168.123.10`
- B. `ifconfig eth0:1 192.168.123.10`
- C. `ifconfig eth0-1 192.168.123.10`
- D. `ifconfig eth0 +192.168.123.10`
- E. `ifconfig eth0:sub1 192.168.123.10`

12

Which network service or protocol is used by `sendmail` for RBLs (Realtime Blackhole Lists)?

- A. RBLP
- B. SMTP
- C. FTP
- D. HTTP
- E. DNS

13

Your users request that you process their incoming mail so that duplicate forwarded messages are deleted. Which of the following could be used to accomplish this task?

- A. `fetchmail`
- B. `mqueue`
- C. `procmail`
- D. `elm`
- E. `rmail`