## QUESTIONS

1. Which of the following is *not* part of the CEH scanning methodology?
   - **A.** Check for live systems.
   - **B.** Check for open ports.
   - **C.** Perform banner grabbing.
   - **D.** Prepare proxies.
   - **E.** Check for social engineering attacks.
   - **F.** Scan for vulnerabilities.
   - **G.** Draw network diagrams.
2. What is the second step in the TCP three-way handshake?
   - **A.** SYN
   - **B.** ACK
   - **C.** SYN/ACK
   - **D.** ACK-SYN
   - **E.** FIN
3. Which of the following tools are used for enumeration? (Choose three.)
   - **A.** SolarWinds
   - **B.** User2SID
   - **C.** Snow
   - **D.** SID2User
   - **E.** DumpSec
4. You want to perform a ping sweep of a subnet within your target organization. Which of the following Nmap command lines is your best option?
   - **A.** nmap 192.168.1.0/24
   - **B.** nmap -sT 192.168.1.0/24
   - **C.** nmap –sP 192.168.1.0/24
   - **D.** nmap –P0 192.168.1.0/24
5. Which of the following TCP flags is used to reset a connection?
   - **A.** SYN
   - **B.** ACK
   - **C.** PSH
   - **D.** URG
   - **E.** FIN
   - **F.** RST

6. A pen test team member is attempting to enumerate a Windows machine and uses a tool called enum to enumerate user accounts on the device. Doubtful this can be done, a junior team member is shocked to see the local users enumerated. The output of his enum use is provided here:

```
C:\>enum –U 192.168.17.5
server 192.168.17.5
setting up session... success.
gettings user list (pass 1, index 0)... success, got 6
Admin  JfiedlerMsander Poop  Guest  Support123
cleaning up... success.
```

The junior team member asks what type of connection is used by this tool to accomplish its task and is told it requires a NULL session to be established first. If the machine allows null connections, which of the following command strings will successfully connect?

**A.** net use "" /u: \\192.169.5.12\share ""

**B.** net use \\192.168.5.12\c$ /u:""

**C.** net use \\192.168.5.12\share "" /u:""

**D.** net use \\192.168.5.12\c$ /u:""

7. A colleague enters the following command:

```
root@mybox: # hping3 –A 192.168.2.x –p 80
```

What is being attempted here?

**A.** An ACK scan using hping3 on port 80 for a single address

**B.** An ACK scan using hping3 on port 80 for a group of addresses

**C.** Address validation using hping3 on port 80 for a single address

**D.** Address validation using hping3 on port 80 for a group of addresses

8. You are examining traffic between hosts and note the following exchange:

```
Source            Prot  Port  Flag        Destination
192.168.5.12      TCP   4082  FIN/URG/PSH 192.168.5.50
192.168.5.12      TCP   4083  FIN/URG/PSH 192.168.5.50
192.168.5.12      TCP   4084  FIN/URG/PSH 192.168.5.50
192.168.5.50      TCP   4083  RST/ACK     192.168.5.12
192.168.5.12      TCP   4085  FIN/URG/PSH 192.168.5.50
```

Which of the following statements are true regarding this traffic? (Choose all that apply.)

**A.** It appears to be part of an ACK scan.

**B.** It appears to be part of an XMAS scan.

**C.** It appears port 4083 is open.

**D.** It appears port 4083 is closed.

9. You are examining traffic and notice an ICMP type 3, code 13, response. What does this normally indicate?
   - **A.** The network is unreachable.
   - **B.** The host is unknown.
   - **C.** Congestion control is enacted for traffic to this host.
   - **D.** A firewall is prohibiting connection.
10. You have a zombie system ready and begin an IDLE scan. As the scan moves along, you notice that fragment identification numbers gleaned from the zombie machine are incrementing randomly. What does this mean?
   - **A.** Your IDLE scan results will not be useful to you.
   - **B.** The zombie system is a honeypot.
   - **C.** There is a misbehaving firewall between you and the zombie machine.
   - **D.** This is an expected result during an IDLE scan.
11. As a pen test on a major international business moves along, a colleague discovers an IIS server and a mail exchange server on a DMZ subnet. You review a ping sweep accomplished earlier in the day on that subnet and note neither machine responded to the ping. What is the most likely reason for the lack of response?
   - **A.** The hosts might be turned off or disconnected.
   - **B.** ICMP is being filtered.
   - **C.** The destination network might be down.
   - **D.** The servers are Linux based and do not respond to ping requests.
12. Which of the following tools is not the best choice for determining possible vulnerabilities on live targets you have identified?
   - **A.** SAINT
   - **B.** Nmap
   - **C.** Nessus
   - **D.** Retina
13. Which of the following commands is the best choice to use on a Linux machine when attempting to list processes and the UIDs associated with them in a reliable manner?
   - **A.** ls
   - **B.** chmod
   - **C.** pwd
   - **D.** lsof

14. Which of the following tools can be used for operating system prediction from network and communication analysis? (Choose all that apply.)

    **A.** Nmap

    **B.** Whois

    **C.** Queso

    **D.** ToneLoc

    **E.** MBSA

15. You are in training for your new pen test assignment. Your trainer enters the following command:

    ```
    telnet 192.168.12.5 80
    ```

    After typing the command, he hits ENTER a few times. What is being attempted?

    **A.** A DoS attack against a web server

    **B.** A zone transfer

    **C.** Banner grabbing

    **D.** Configuring a port to "listening" state

16. What is being attempted with the following command?

    ```
    nc -u -v -w2 192.168.1.100 1-1024
    ```

    **A.** A full connect scan on ports 1–1024 for a single address

    **B.** A full connect scan on ports 1–1024 for a subnet

    **C.** A UDP port scan of ports 1–1024 on a single address

    **D.** A UDP scan of ports 1–1024 on a subnet

17. You are told to monitor a packet capture for any attempted DNS zone transfer. Which port should you focus your search on?

    **A.** TCP 22

    **B.** TCP 53

    **C.** UDP 22

    **D.** UDP 53

18. In the scanning and enumeration phase of your attack, you put tools such as ToneLoc, THC-Scan, and WarVox to use. What are you attempting to accomplish?

    **A.** War dialing

    **B.** War driving

    **C.** Proxy discovery

    **D.** Ping sweeping

19. Which of the following are SNMP enumeration tools? (Choose all that apply.)
    - **A.** Nmap
    - **B.** SNMPUtil
    - **C.** ToneLoc
    - **D.** OpUtils
    - **E.** Solar Winds
    - **F.** NSAuditor
20. The following results are from an Nmap scan:

```
Starting nmap V. 3.10A ( www.insecure.org/nmap/
<http://www.insecure.org/nmap/> )
Interesting ports on 192.168.15.12:
(The 1592 ports scanned but not shown below are in state: filtered)
Port State Service
21/tcp open ftp
25/tcp open smtp
53/tcp closed domain
80/tcp open http
443/tcp open https
Remote operating system guess: Too many signatures match to
    reliably guess the OS.
Nmap run completed -- 1 IP address (1 host up) scanned in 263.47 seconds
```

    Which of the following is the best option to assist in identifying the operating system?
    - **A.** Attempt an ACK scan.
    - **B.** Traceroute to the system.
    - **C.** Run the same Nmap scan with the -vv option.
    - **D.** Attempt banner grabbing.
21. You want to run a scan against a target network. You're concerned about it being a reliable scan, with legitimate results, but want to take steps to ensure it is as stealthy as possible. Which scan type is best in this situation?
    - **A.** nmap –sN targetIPaddress
    - **B.** nmap –sO targetIPaddress
    - **C.** nmap –sS targetIPaddress
    - **D.** nmap –sT targetIPaddress

22. Which of the following ports are not required for a NULL session connection? (Choose all that apply.)

    **A.** 135

    **B.** 137

    **C.** 139

    **D.** 161

    **E.** 443

    **F.** 445

23. You are enumerating a subnet. While examining message traffic, you discover SNMP is enabled on multiple targets. If you assume default settings in setting up enumeration tools to use SNMP, which community strings should you use?

    **A.** Public (read-only) and Private (read/write)

    **B.** Private (read-only) and Public (read/write)

    **C.** Read (read-only) and Write (read/write)

    **D.** Default (both read and read/write)

24. Nmap is a powerful scanning and enumeration tool. What does the following Nmap command attempt to accomplish?

    ```
    nmap –sA –T4 192.168.15.0/24
    ```

    **A.** A serial, slow operating system discovery scan of a Class C subnet

    **B.** A parallel, fast operating system discovery scan of a Class C subnet

    **C.** A serial, slow ACK scan of a Class C subnet

    **D.** A parallel, fast ACK scan of a Class C subnet

25. You are examining a packet capture of all traffic from a host on the subnet. The host sends a segment with the SYN flag set in order to set up a TCP communications channel. The destination port is 80, and the sequence number is set to 10. Which of the following statements are *not* true regarding this communications channel? (Choose all that apply.)

    **A.** The host will be attempting to retrieve an HTML file.

    **B.** The source port field on this packet can be any number between 1023 and 65535.

    **C.** The first packet from the destination in response to this host will have the SYN and ACK flags set.

    **D.** The packet returned in answer to this SYN request will acknowledge the sequence number by returning 10.

26. Which TCP flag instructs the recipient to ignore buffering constraints and immediately send all data?

    **A.** URG

    **B.** PSH

    **C.** RST

    **D.** BUF

27. You receive a RST-ACK from a port during a SYN scan. What is the state of the port?

    **A.** Open

    **B.** Closed

    **C.** Filtered

    **D.** Unknown

28. Which port-scanning method presents the most risk of discovery but provides the most reliable results?

    **A.** Full-connect

    **B.** Half-open

    **C.** Null scan

    **D.** XMAS scan

29. The following output appears on the screen after an attempted telnet session to a machine:

```
HTTP/1.0 200 OK
Date: Wed, 19 Feb 2014 10:16:22 GMT
Content-Length: 30344
Content-Type: text/html
Expires: Wed, 19 Feb 2014 10:22:22 GMT
Cache-Control: max-age=300
Server: Apache/1.3.33 <Darwin> PHP /4.3.10
Age: 120
```

    Which of the following best matches the output provided?

    **A.** An attacker has attempted a zone transfer successfully.

    **B.** An attacker has attempted a zone transfer unsuccessfully.

    **C.** An attacker has successfully grabbed a banner.

    **D.** An attacker has successfully uploaded a denial-of-service script.