Midterm Practice

1. Which command is used to listen to open ports with netstat?

A. $ netstat –an
B. $ netstat –ports
C. $ netstat –n
D. $ netstat –s

2. What item should not be included in the Rules of Engagement?

A. test dates and time
B. permission to test
C. contact information
D. daily debriefing conference call

3. Jason invokes the following Nmap command at a Linux command line. Which Nmap scan is performed?

 # nmap –n 10.10.10.10-60

A. a connect scan
B. a syn stealth scan
C. a null scan
D. a ping sweep

4. To make Tcpdump to sniff on network interface eth0, do not resolve host and service names, for tcp packets to and from host 10.10.10.10. Which of the following command should be invoked?

A. tcpdump –nn –i eth0 and tcp and host 10.10.10.10
B. tcpdump –n –i eth0 and tcp and host 10.10.10.10
C. tcpdump –nn –i eth0 tcp and host 10.10.10.10
D. tcpdump –nn –i eth0 and tcp and net 10.10.10.10

5. Which one is not a vulnerability?

A. The computers in the Personnel Department do not have up-to-date anti-malware software.
B. Our employees don't understand what information is sensitive so they don't know how to protect it.
C. Employees (insiders) might release confidential information to our competitors.
D. Our office is too small. So our database server is in the same room where guests come in and out.

6. Which port uses SSL to secure web traffic?

A. 443
B. 25
C. 23
D. 80

7. Which of the following types of attack has no flags set?

A. SYN
B. NULL
C. Xmas tree
D. FIN

8. What network appliance senses irregularities and plays an active role in stopping that irregular activity from continuing?

A. IPS
B. IDP
C. IDS
D. Firewall

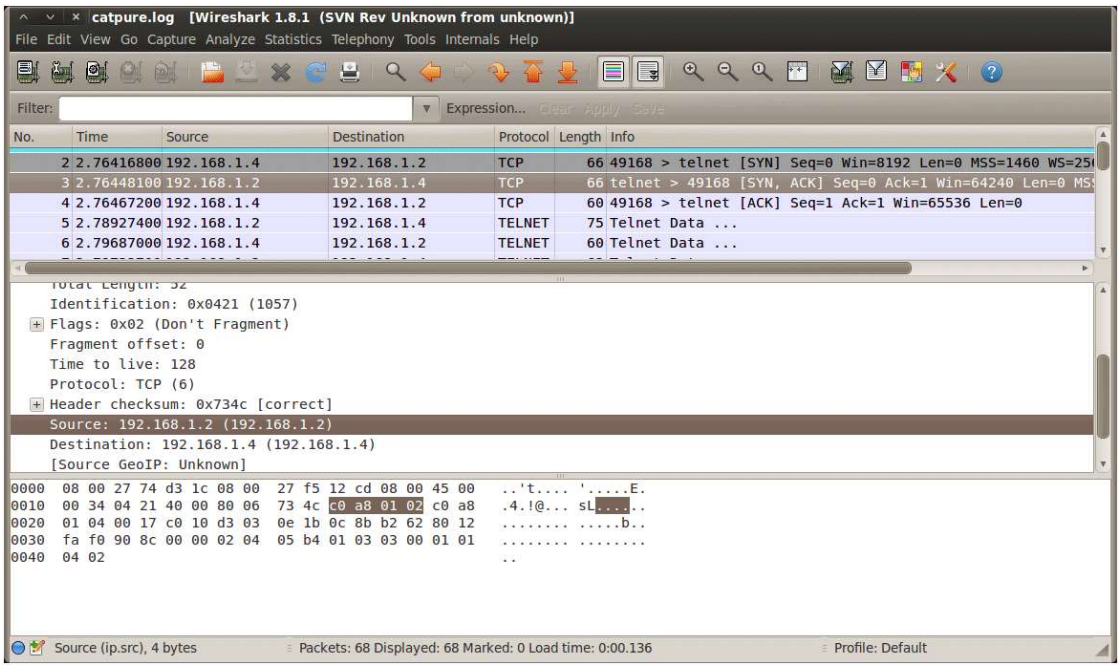
9. Which Wireshark filter displays only traffic from 10.10.10.10?

A. ip.addr =! 10.10.10.10
B. ip.addr ne 10.10.10.10
C. ip.addr == 10.10.10.10
D. ip.addr – 10.10.10.10

10. Which of the following is a major security problem with FTP?

A. password files are stored in an unsecure area on disk
B. memory traces can corrupt file access
C. user IDs and passwords are unencrypted
D. FTP sites are unregistered

11. Based on the packet capture shown in the graphic, what is contained in the highlighted section in the middle (Source: 192.168.1.2 …) of the packet?



A. The frame value of the packet
B. The MAC address of the sending host
C. Source IP addresses
D. The routed protocol value

12. The D-DoS attack is an attack against _____ .

A. Confidentiality
B. Integrity
C. Availability
D. Assurance

13. Enumeration is useful to system hacking because it provides which of the following?

A. Passwords
B. IP ranges
C. Configurations
D. Usernames

14. You want to block ping requests to your system silently. Which command do you need to use?

A. $ iptables -A INPUT -p tcp --dport 22 –j DROP
B. $ iptables -A INPUT -p tcp --dport 24 –j REJECT
C. $ iptables -A OUTPUT -p icmp --icmp-type echo-request –j DROP
D. $ iptables -A INPUT -p icmp --icmp-type echo-request –j DROP

15. Which one is the sequence of the three-way handshake?

A. SYN, SYN-ACK, ACK
B. SYN, SYN-ACK
C. SYN, ACK, SYN-ACK
D. SYN, ACK, ACK

16. Which technology allows the use of a single public address to support many internal clients while also preventing exposure of internal IP addresses to the outside world?

A. VPN
B. Tunneling
C. NTP
D. NAT

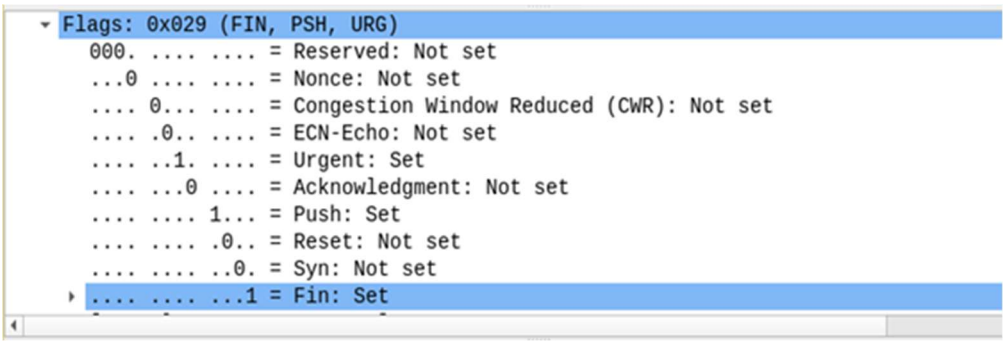
17. A crystal-box test means the tester has which of the following?

A. No knowledge
B. Some knowledge
C. Complete knowledge
D. Permission

18. The Wayback Machine is used to do which of the following?

A. Get job postings
B. View websites
C. View archived versions of websites
D. Back up copies of websites

19. As a network admin, if you're seeing these flag bits in Wireshark, what is happening on your machines?



A. There is a Xmas tree scan is happening
B. There is a stealthy SYN scan is happening
C. Someone is trying to change our machine flag setting
D. Someone is sending urgent signal to us

20. Which command would retrieve banner information from a website at port 80?

A. nc 192.168.10.27 80
B. nc 192.168.19.27 443
C. nc 192.168.10.27 –p 80
D. nc 192.168.10.27 –p –l 80

21. Which record will reveal information about a mail server for a domain?

A. A
B. Q
C. MS
D. MX

22. Which tool can trace the path of a packet?

A. ping
B. tracert
C. whois
D. DNS

23. Jason is responsible to scan the target environment. Below is a screenshot of tcpdump showing some captured packets from his scanning activity. Which scanning activity most likely Jason is conducting?

```
root@kali:~# tcpdump -nnv udp and host 192.168.1.65 and not arp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
22:06:30.561737 IP (tos 0x0, ttl 1, id 21953, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.36355 > 8.8.8.8.33434: UDP, length 32
22:06:30.561923 IP (tos 0x0, ttl 1, id 21954, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.43842 > 8.8.8.8.33435: UDP, length 32
22:06:30.562057 IP (tos 0x0, ttl 1, id 21955, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.41507 > 8.8.8.8.33436: UDP, length 32
22:06:30.562146 IP (tos 0x0, ttl 2, id 21956, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.45182 > 8.8.8.8.33437: UDP, length 32
22:06:30.562230 IP (tos 0x0, ttl 2, id 21957, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.56741 > 8.8.8.8.33438: UDP, length 32
22:06:30.562306 IP (tos 0x0, ttl 2, id 21958, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.50211 > 8.8.8.8.33439: UDP, length 32
22:06:30.562382 IP (tos 0x0, ttl 3, id 21959, offset 0, flags [none], proto UDP
(17), length 60)
    192.168.1.65.53850 > 8.8.8.8.33440: UDP, length 32
```

A. ping sweeping
B. network tracing
C. port scanning
D. version scanning

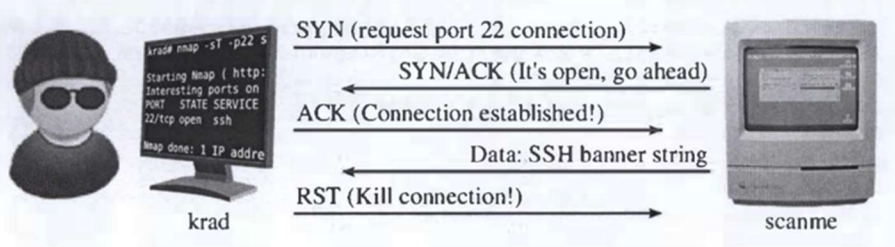
24. What does a SYN scan accomplish?

A. It establishes a full TCP connection.
B. It establishes only a “half open” connection.
C. It opens an ACK connection with the target.
D. It detects all closed ports on a target system.

25. Which of the following best describes DNS poisoning?

A. The adversary intercepts and replaces the victims MAC address with their own.
B. The adversary replaces their malicious IP address with the victim’s IP address for the domain name.
C. The adversary replaces the legitimate domain name with the malicious domain name.
D. The adversary replaces the legitimate IP address that is mapped to the domain name with the malicious IP address.

26. Which of the nmap scan option will do the following scan order?



A. nmap -sS -p 22 -n scanme.nmap.org
B. nmap -sV -p 22 -n scanme.nmap.org
C. nmap -sn -p 22 -n scanme.nmap.org
D. nmap -sT -p 22 -n scanme.nmap.org

27. Which file or application has the permission set with 644?

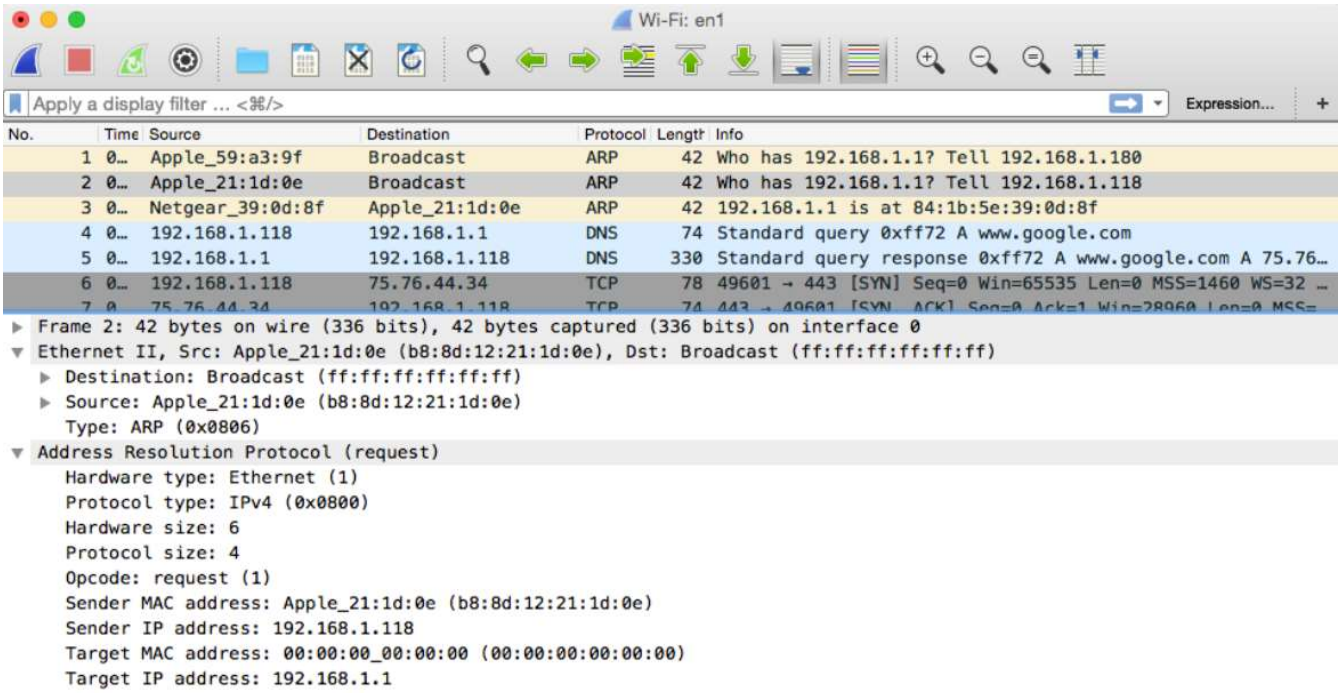
```
Rays-MBP:/ rblockmon$ ls -l
total 45
drwxrwxr-x+ 47 root  admin  1598 Nov 14 13:50 Applications
drwxr-xr-x+ 60 root  wheel  2040 Nov 11 18:20 Library
drwxr-xr-x@  2 root  wheel    68 Sep  9  2014 Network
drwxr-xr-x+  4 root  wheel   136 Oct 29  2014 System
drwxr-xr-x   6 root  admin   204 Oct 29  2014 Users
drwxrwxrwt@  4 root  admin   136 Nov 20 20:41 Volumes
drwxr-xr-x@ 39 root  wheel  1326 Sep  2 16:02 bin
drwxrwxr-t@  2 root  admin    68 Sep  9  2014 cores
dr-xr-xr-x   3 root  wheel  4322 Nov 20 16:53 dev
lrwxr-xr-x@  1 root  wheel    11 Oct 29  2014 etc -> private/etc
dr-xr-xr-x   2 root  wheel     1 Nov 21 20:55 home
-rw-r--r--@  1 root  wheel   313 Oct  1  2014 installer.failurerequests
dr-xr-xr-x   2 root  wheel     1 Nov 21 20:55 net
drwxr-xr-x@  6 root  wheel   204 Oct 29  2014 private
drwxr-xr-x@ 59 root  wheel  2006 Sep  2 16:02 sbin
lrwxr-xr-x@  1 root  wheel    11 Oct 29  2014 tmp -> private/tmp
drwxr-xr-x@ 10 root  wheel   340 Oct 29  2014 usr
lrwxr-xr-x@  1 root  wheel    11 Oct 29  2014 var -> private/var
Rays-MBP:/ rblockmon$
```

A. usr
B. net
C. Volumes
D. Installer.failurerequests

28. Which of the following provides free information about a website that includes phone numbers, administrator's email, and even the domain registration authority?

A. Nslookup
B. Dig
C. Whois.net
D. Ping

29. What type of protocol is primarily being used in this diagram? (You're seeing the contents of No.2 packet)



A. Broadcast
B. ARP request
C. Ping
D. DHCP lease

30. Which one prevents IP packets from circulating throughout the Internet forever?

A. TTL
B. Spanning tree
C. Broadcast domains
D. NAT

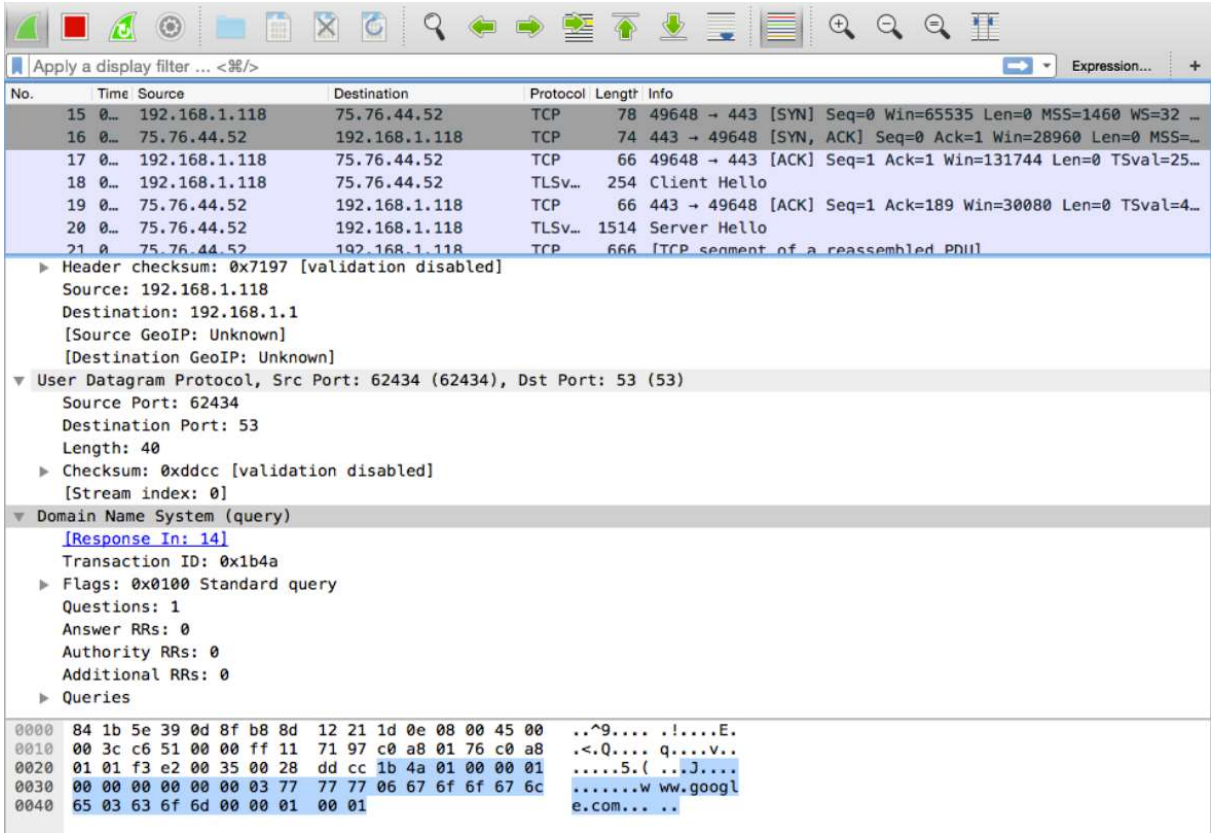
31. In the TCP three-way handshake, which is next after the initial SYN packet is sent?

A. An ACK is received.
B. A SYN is received.
C. A SYN/ACK is sent.
D. An ACK is sent.

32. Which flag forces both sender and receiver on the network to terminate their connection with one another?

A. FIN
B. RST
C. URG
D. SYN

33. Which DNS system is being queried by the client in the following screenshot?



A. Google
B. Port 53
C. Port 64234
D. None

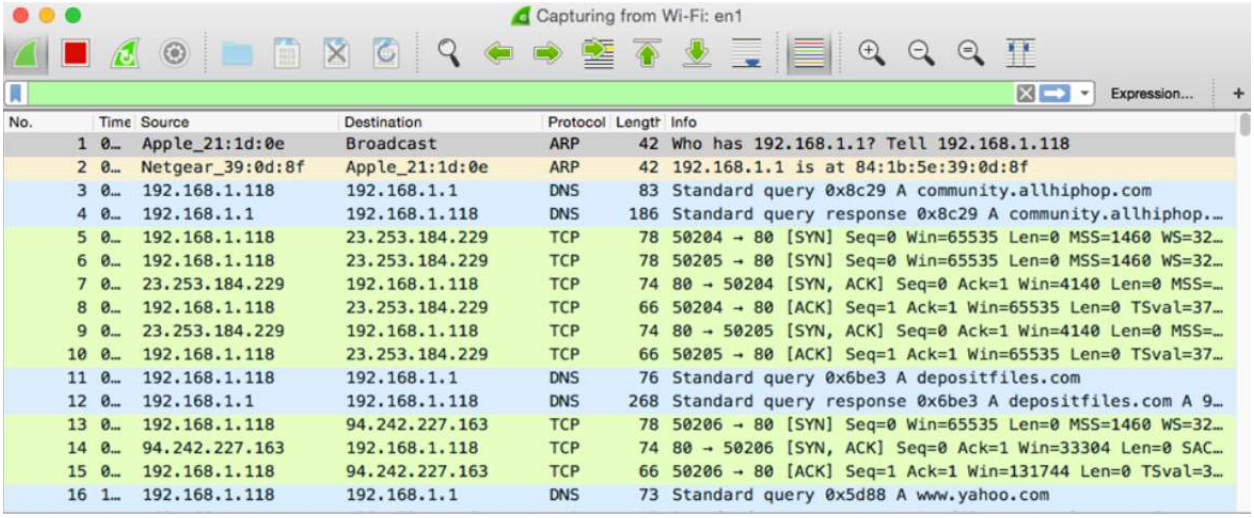
34. In Linux, which of the following accounts denotes the administrator?

A. Admin
B. Administrator
C. root
D. su

35. Which of the following is part of the overall portion of the SID?

A. UID
B. RID
C. USD
D. L5R

36. In the following screen shot, which sequence number completes the three-way handshake with 23.253.184.229?



A. 5025
B. 1
C. 74
D. 64

37. When trying to identify all the workstations on a subnet, what method might you choose?

A. Port scan
B. Anonymizer
C. Ping sweep
D. Web crawler

38. Which switch in Nmap allows for a full TCP connect scan?

A. –sS
B. –sU
C. –FC
D. –sT

39. An attacker was able to install a device at an unattended workstation and was able to recover passwords, account information, and other information the next day. What did the attacker install?

A. Keylogger
B. Key scanner
C. Rootkit
D. Randsomware

40. What command displays the network configuration in Linux OS?

A. ipconfig
B. netstat
C. ls
D. ifconfig

41. Which Nmap switch utilizes the slowest scan?

A. -T0
B. -sT
C. -s0
D. -sX

42. Which of the following has no flags set and does not respond if a port is open?

A. XMAS scan
B. NULL scan
C. Half-open connection
D. ACK scan

Key

1. A, 2. B, 3. B, 4. C, 5. C, 6. A, 7. B, 8. A, 9. C, 10. C, 11. C, 12. C, 13. D, 14. D, 15. A, 16. D, 17. C, 18. C, 19. A, 20. A, 21. D, 22. B, 23. B, 24. B, 25. D, 26. D, 27. D, 28. C, 29. B, 30. A, 31. C, 32. A, 33. A, 34. C, 35. B, 36. B, 37. C, 38. D, 39. A, 40. D, 41. A, 42. B