Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Written exam, 10th of September 2019

Student name: ______________________________

Matricola: ______________________________

Open questions (60%)

Provide an answer within the space allocated for each question.

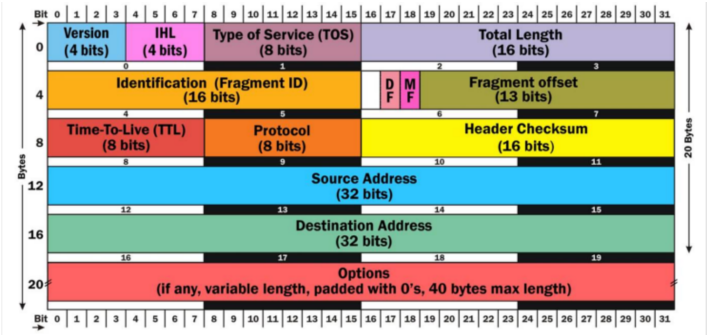
1. Explain the benefits of encapsulation.

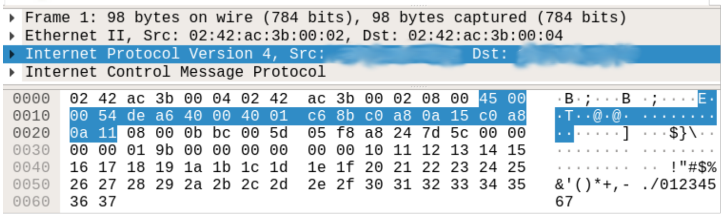
2. Provide the sequence of *iptables* commands you would use in a firewall with two interfaces (`$INT_IF` and `$EXT_IF`) that acts as the gateway for `$INSIDE_NET` (that is reachable from interface `$INT_IF`), considering that:

   - internal *host1* (with IP `$HOST1_IP`) has to be allowed only to access remote hosts with HTTPS and DNS and
   - internal *host1* can operate via `ssh` with the firewall and
   - no other traffic has to be allowed

   All IP addresses are public and routable.

3. Considering the structure of the IP packet header provided below, report the following info related to the shown packet:


Bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version (4 bits)
IHL (4 bits)
Type of Service (TOS) (8 bits)
Total Length (16 bits)
Identification (Fragment ID) (16 bits)
D F
M F
Fragment offset (13 bits)
Time-To-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
Source Address (32 bits)
Destination Address (32 bits)
Options (if any, variable length, padded with 0's, 40 bytes max length)
0
4
8
12
16
20
Bytes
20 Bytes



```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: 02:42:ac:3b:00:02, Dst: 02:42:ac:3b:00:04
▸ Internet Protocol Version 4, Src: [redacted] Dst: [redacted]
▸ Internet Control Message Protocol

0000  02 42 ac 3b 00 04 02 42  ac 3b 00 02 08 00 45 00   ·B·;···B ·;····E·
0010  00 54 de a6 40 00 40 01  c6 8b c0 a8 0a 15 c0 a8   ·T··@·@· ········
0020  0a 11 08 00 0b bc 00 5d  05 f8 a8 24 7d 5c 00 00   ·······] ···$}\··
0030  00 00 01 9b 00 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

- Header length: ________________
- IP data size: ________________
- Time-to-live: ________________
- Source IP address in dotted-decimal: ________________________________

4. Explain the differences between source NAT and destination NAT.

5. You have to setup a VPN in a company composed of two networks: DMZ and INTERNAL. Where would you place the VPN gateway device? Explain your motivations for your choice.

6. Explain why it is important to have a code in the Common Vulnerabilities and Exposures for a given vulnerability and how this can help the writing of a detection rule for a IDS.

7. Describe what is the role of Ticket-Granting Tickets (TGT) in Kerberos.

8. Why it is important to have a methodology for performing security assessments? Mention at least one known methodoloy.

9. Explain how a proxy that uses HTTP CONNECT works.

10. Describe the mechanism of the extension headers in IPv6

Multi-choice questions (40%)

Mark all the options you think are correct.

1. Mark the IPv6 multicast addresses:

   A. FE80::FE99:47FF:FE75:C3E0
   B. FF02::1 ★
   C. FE80::1
   D. FF18::CAFE:1234 ★

2. Which types of filters can you find in tcpdump?

   A. Custom filters
   B. Capture filters ★
   C. All of the others
   D. Display filters

3. Which of the following is NOT an IDS?

   A. fail2ban
   B. snort
   C. burp ★
   D. suricata

4. Mark the wrong LDAP naming associations between attributes and strings:

   A. CN: Common Name
   B. L: Locality Name
   C. C: Country Name
   D. OU: Organization Name ★

5. Which of the following is a main and expected feature of a SIEM?

   A. Protect the traffic exchanged in a complex network
   B. Provide an efficient and effective log management ★
   C. Give a picture of the main events in a complex system ★
   D. Raise alarms and block suspicious activity in the system

6. What is unlikely to find in a DMZ?

   A. A VPN gateway
   B. A proxy server
   C. A server hosting a sensitive database ★
   D. A server hosting a web service

7. What is the final purpose of SSL bump?

   A. To realize a man-in-the-middle attack
   B. To cache the digital certificates of a CA
   C. To read TLS-ecrypted traffic ★
   D. To exchange and validate digital certificates

8. What is a primary use of forward proxies?

   A. Caching ★
   B. Load balancing
   C. Application level control
   D. Authentication and authorization ★

9. Which of the following are considered “well-known ports”?

   A. 1088
   B. 22 ★
   C. 443 ★
   D. 62123

10. Which iptables chain is not found by default in the FILTER table?

    A. OUTPUT
    B. FORWARD
    C. INPUT
    D. POSTROUTING ★

11. Which of the following is a function of RADIUS?

    A. Audit the user accesses to network services
    B. Account for use of network services ★
    C. Authorize users to access requested network services ★
    D. Authenticate users trying to establish connection to network ★

12. Which is the mechanism used to delivery packets around the Internet?

    A. Routing ★
    B. Fragmentation
    C. Encapsulation
    D. Tunnel

13. What is the purpose of the following snort rule?
    `log ip any any -> $HONEY_IP any`

    A. To raise an alert for any IP packet with destination the honeypot host
    B. If snort is inline, to block all the traffic with destination the honeypot host
    C. If snort is in promiscuous mode, to sniff all the traffic involving the honeypot host
    D. To record any traffic with destination the honeypot host ★

14. What is the purpose of the following iptables command?
    `iptables -L -n -v`

    A. To erase all the rules in the filter table
    B. To display all the rules in the filter table ★
    C. To display all the rules in all the tables
    D. To erase all the rules in all the tables

15. Which of the following can be used by TLS to encrypt the traffic in a VPN tunnel?

    A. AES ★
    B. 3DES ★
    C. SHA1
    D. RSA

16. Which of the following is a valid IPv4 address that can be assigned to a host?

    A. 10.20.30.63/29
    B. 10.20.30.40/30
    C. 10.20.30.40/24 ★
    D. 10.20.30.63/26

17. Which of the following is NOT a phase of vulnerability scanners?

A. Debugging ★
B. Serice detection
C. Port scan
D. Discovery

18. Which of the following is likely to be an IP address that has to be subjcet to a source NAT?

A. 172.160.32.34
B. 192.168.250.250 ★
C. 11.20.30.40
D. 10.20.30.40 ★

19. Which of the following is a type of packet NOT intended for realizing the IPv6 Neighbor Discovery?

A. Echo Request ★
B. Neighbor Advertisement Message
C. Router Solicitation Message
D. Neighbor Solicitation Message

20. Which statements about VPNs are true?

A. VPN based on IPSec operate at network level ★
B. VPN based on TLS operate at transport level ★
C. VPN based on IPSec operate at transport level
D. VPN based on IPSec operate at application level

Please, transcript your answers in the boxes below:

bd	b	c	d	bc	c	c	ad	bc	d	bcd	a	d	b	ab	c	a	bd	a	ab
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20