Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Written exam, 13th of January 2020

Student name: ______________________

Matricola: ______________________

Open questions (60%)

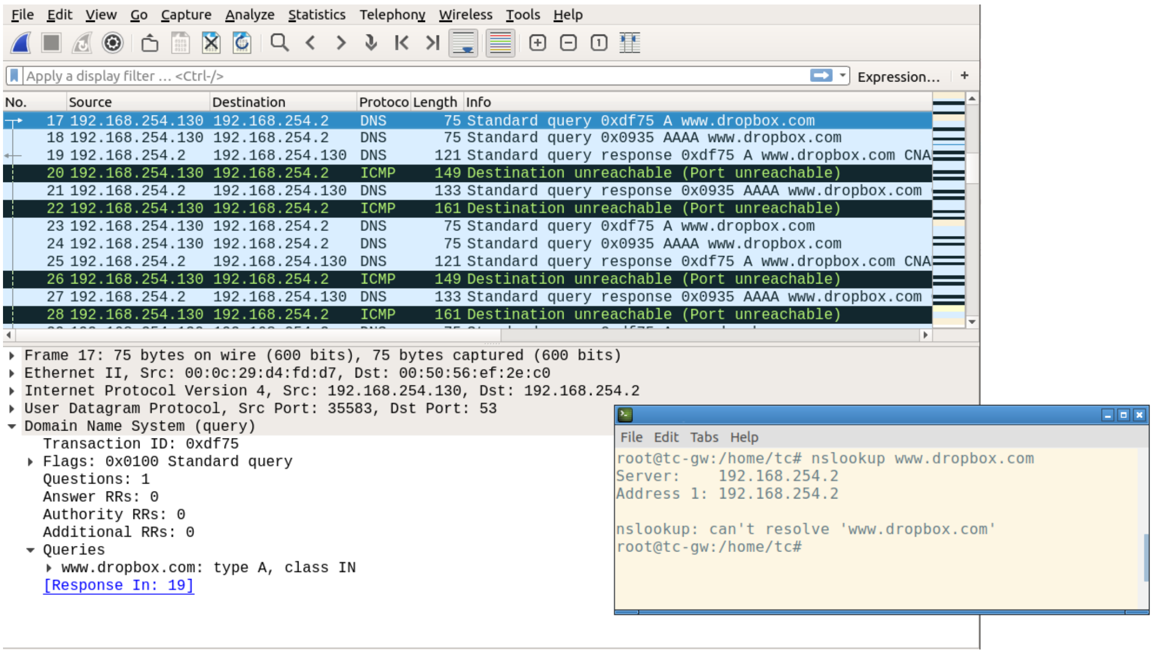
Provide an answer within the space allocated for each question.

1. Explain the main differences between a MAC address and an IP address.

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 network `$INSIDE_NET` has to be NAT'd
   - internal network `$INSIDE_NET` is allowed only to exchange traffic with external hosts using HTTPS and DNS protocols and
   - no other traffic has to be allowed

3. In the following image, there is a terminal window with the execution of a command and the related Wireshark captured packets. Explain what you can recognize in the packet exchange captured by Wireshark, and provide a motivation for the output of the command.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.   Source          Destination     Protoco Length Info
   17 192.168.254.130 192.168.254.2   DNS      75 Standard query 0xdf75 A www.dropbox.com
   18 192.168.254.130 192.168.254.2   DNS      75 Standard query 0x0935 AAAA www.dropbox.com
   19 192.168.254.2   192.168.254.130 DNS     121 Standard query response 0xdf75 A www.dropbox.com CNA
   20 192.168.254.130 192.168.254.2   ICMP    149 Destination unreachable (Port unreachable)
   21 192.168.254.2   192.168.254.130 DNS     133 Standard query response 0x0935 AAAA www.dropbox.com
   22 192.168.254.130 192.168.254.2   ICMP    161 Destination unreachable (Port unreachable)
   23 192.168.254.130 192.168.254.2   DNS      75 Standard query 0xdf75 A www.dropbox.com
   24 192.168.254.130 192.168.254.2   DNS      75 Standard query 0x0935 AAAA www.dropbox.com
   25 192.168.254.2   192.168.254.130 DNS     121 Standard query response 0xdf75 A www.dropbox.com CNA
   26 192.168.254.130 192.168.254.2   ICMP    149 Destination unreachable (Port unreachable)
   27 192.168.254.2   192.168.254.130 DNS     133 Standard query response 0x0935 AAAA www.dropbox.com
   28 192.168.254.130 192.168.254.2   ICMP    161 Destination unreachable (Port unreachable)
```

```
▸ Frame 17: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
▸ Ethernet II, Src: 00:0c:29:d4:fd:d7, Dst: 00:50:56:ef:2e:c0
▸ Internet Protocol Version 4, Src: 192.168.254.130, Dst: 192.168.254.2
▸ User Datagram Protocol, Src Port: 35583, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xdf75
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.dropbox.com: type A, class IN
    [Response In: 19]
```

```
root@tc-gw:/home/tc# nslookup www.dropbox.com
Server:    192.168.254.2
Address 1: 192.168.254.2

nslookup: can't resolve 'www.dropbox.com'
root@tc-gw:/home/tc#
```

Student name: ____________________

Matricola: ____________________

4. Explain why the NAT mechanism is also said to provide some kind of security to the NAT'd network.

5. Enumerate and briefly describe the type of VPN implementations you know. Highlight pros and cons.

6. Enumerate the types of outcomes you can have when a network IDS evaluates a sample.

7. Describe what is the primary use of Kerberos.

8. Describe what a reverse proxy is and what can provide.

9. Explain the differences between an IPv6 Global address and an IPv6 Link-local address.

10. Enumerate and briefly describe the mechanisms of IPv6 to dynamically assign Global Unicast addresses to the hosts of a network.

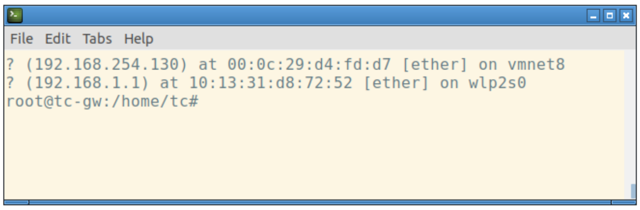
Multi-choice questions (40%)

Mark all the options you think are correct.

1. Which of the following is NOT a type of IDS?

A. HIDS
B. SIDS ★
C. NIDS
D. WIDS

2. Which command is the most likely to have generated the output in the following picture?



```
? (192.168.254.130) at 00:0c:29:d4:fd:d7 [ether] on vmnet8
? (192.168.1.1) at 10:13:31:d8:72:52 [ether] on wlp2s0
root@tc-gw:/home/tc#
```

A. `arp` ★
B. `ping`
C. `nmap`
D. `tcpdump`

3. Which of the following requires a user to be aware of its presence?

A. Forward proxy ★
B. Anonymous proxy ★
C. Reverse proxy
D. Transparent proxy

4. Which of the following `iptables` targets have a function similar to the `DROP` target?

A. `MASQUERADE`
B. `REJECT` ★
C. `JUMP`
D. `ABORT`

5. Mark the IPv6 link-local addresses:

A. FE80::1 ★
B. FF18::CAFE:1234
C. FE80::FE99:47FF:FE75:C3E0 ★
D. 2001:DB8:CAFE:1:6909:CB1C:36A0:A595

6. Which of the following is a typical service of a SIEM?

A. Network Address Translation
B. Reconnaissance
C. Vulnerability scanning
D. Event correlation ★

7. What is the aim of a SSL forward proxy?

A. To receive the requests from the Internet as if it were the server and then forward to the actual server
B. To provide access to the Web for hosts on closed subnets who can only access the Internet through a firewall machine
C. To block application input/output from detected intrusions or malformed communication, or block content that violates policies
D. To decrypt and inspect SSL/TLS traffic from internal users to the Internet ★

8. Which of the following is a common use of LDAP?

A. Scan network hosts
B. Provide user authentication ★
C. Store and access information from different systems ★
D. Inspect network packets

9. Which of the following IPv4 addresses belonging to the network 172.16.128.0/19 (namely with subnet 255.255.224.0)?

A. 172.16.138.255 ★
B. 172.16.224.1
C. 172.16.158.13 ★
D. 172.16.240.12

10. Which of the following is a filter you can use with the tcpdump command?

A. `-n -s0  port 53 and udp` ★
B. `tcp.port eq 25 or icmp`
C. `-i eth0 dst 10.10.1.20` ★
D. `ip.addr == 10.43.54.65`

11. What is the purpose of a program like `fail2ban`?

A. to detect and possibly react to the presence of attacks ★
B. to forward all the traffic directed to one network
C. to provide a secure communications mechanism for the traffic between two endpoints
D. to collect and process information from distributed sources

12. What is true about `openvpn`?

A. It is based on the IPSec protocol
B. It can use both the transport mode and the tunnel mode
C. It can use both symmetric and asymmetric cryptography ★
D. It can only use pre-shared keys

13. Which of the following can be considered an example of SIEM?

A. QRadar ★
B. suricata
C. splunk ★
D. snort

14. Which of the following types of packets are used in IPv6 to realize the same mechanism of ARP in IPv4?

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

15. In iptables, what is a likely sequence of chains traversed by a packet received by a host?

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

16. A VPN implemented with TLS/SSL...

    A. generally needs the existence of a Certification Authority known to the all the communicating endpoints ★
    B. usually does not hide the type of traffic exchanged between two communicating endpoints
    C. typically cannot hide the IP addresses of the actual communicating endpoints, if it is used for site-to-site tunneling
    D. can only be used for HTTP traffic

17. What is likely to find in a DMZ?

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

18. What is FALSE when talking about Kerberos?

    A. A Resource Ticket is likely to be used with several servers ★
    B. Resource Tickets are encrypted with a short term session key ★
    C. Mutual authentication is granted using symmetric cryptography
    D. Short term session keys are encrypted in Resource Tickets

19. Which iptables chain is found by default in the FILTER table?

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

20. Which of the following IPv4 addresses are unlikely to be assigned to a host in a NAT'd network?

    A. 173.16.10.20 ★
    B. 11.10.9.8 ★
    C. 10.10.10.10
    D. 192.168.254.254

Please, transcript your answers in the boxes below:

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