Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Written exam, 11th of July 2019

Student name: _____

Matricola: _____

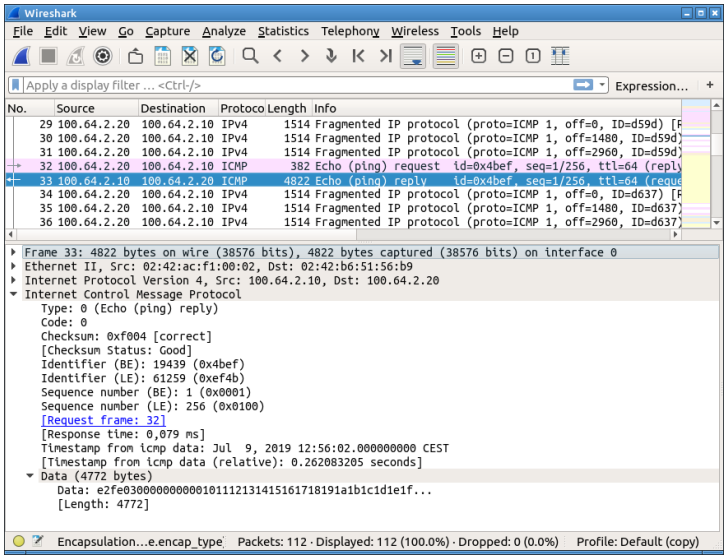
Open questions (60%)

Provide an answer within the space allocated for each question.

1. Explain why address spoofing is a problem for network protections and which techniques can mitigate its effects.

2. Write the sequence of *iptables* commands you would use in a firewall to block all the traffic incoming from `$OUTSIDE_IF` toward your `$INSIDE_NET`, with the exception of pings and ssh requests—and related traffic—from `$MONITOR_IP`. All IP addresses are public and routable.

3. Describe what you can recognize in the following figure:



4. Describe how the NAT table of *iptables* works and is arranged.

Student name: _____

Matricola: _____

5. From a point of view of performances like bandwidth, latency and throughput, which VPN solution you think is better between OpenVPN and IPSec? Explain your motivations.

6. Describe which are pros-and-cons of behavioral-based intrusion detection systems.

7. Define and describe the main characteristics of directories in the context of LDAP.

8. List and briefly describe the services a complete SIEM is likely to provide.

9. Describe the main differences between a forward proxy and a reverse proxy.

10. Describe the role of ICMPv6 in the IPv6 management of fragmentation and make a comparison with IPv4.

Student name: _____

Matricola: _____

Multi-choice questions (40%)

Mark all the options you think are correct.

1. What is true when considering an SSL-tunnel-based site-to-site VPN?

   A. The security parameters of the tunnel can be negotiated by the internal hosts of the sites.
   B. It is by far more efficient than an IPSec-tunnel-based site-to-site VPN.
   C. The IP addresses of the two endpoints of the SSL tunnel are likely to be eavesdropped. ★
   D. All the IP addresses of the tunneled traffic are likely to be eavesdropped.

2. If a user wants to hide its source IP address, which of the following tools could she use?

   A. A forward proxy ★
   B. A transparent proxy
   C. A SOCKS proxy ★
   D. A reverse proxy

3. What actually the following filter does?
   `ip and not net 10.0.0.0`

   A. It only matches IPv4 packets that are not sent to the 10.0.0.0 network
   B. It is syntactically wrong
   C. It only matches IPv4 packets with an IP address not in the 10.0.0.0 network ★
   D. It only matches IP addresses that does not belong to the 10.0.0.0 network

4. Which function is not expected from RADIUS?

   A. Assignment ★
   B. Authorization
   C. Accounting
   D. Authentication

5. To inspect HTTPS traffic before reaching your servers, you can use:

   A. SOCKS
   B. Modsecurity ★
   C. HTTP CONNECT
   D. SSL bump ★

6. If > denotes the relation "has higher priority", mark the correct relations about the *iptables* chains:

   A. RAW > MANGLE > FILTER ★
   B. NAT > FILTER > RAW
   C. MANGLE > NAT > FILTER ★
   D. NAT > MANGLE > FILTER

7. Which type of events are likely to be found in a SIEM log?

   A. Every firewall rule match
   B. Every operating system patch installed by critical systems ★
   C. Every alert raised by IDS/IPS ★
   D. User log-in attempts in critical systems ★

8. The Header Checksum in IPv6

   A. has been removed ★
   B. has been taken of a similar length than IPv4 (16 bits)
   C. has been provided extra bits (32 bits)
   D. has been moved in an extension header

9. A typical firewall has the following interfaces:

   A. monitor
   B. inside ★
   C. partner
   D. DMZ ★

10. Which statements about subnet masks are true?

    A. A subnet masks consists of a string of zeroes and ones
    B. Every network client has a unique subnet mask
    C. A subnet masks consists of a string of ones followed by a string of zeroes ★
    D. Every client on a network shares the same subnet mask ★

11. Which of the following *iptables* targets are used to configure the destination NAT?

    A. `SNAT`
    B. `DNAT` ★
    C. `MASQUERADING`
    D. `MASQUERADE`

12. LDAP is not well suited for

    A. Information that is read more often than it is written
    B. Information that is unstructured ★
    C. Information that needs to be accessed from more than one location
    D. Information that is referenced by many entities and applications

13. What is true about vulnerabiliy scanners?

    A. They can be used to find unknown buffer overflow vulnerabilities in applications
    B. They can be used to find unknown bugs in applications
    C. They are used to verify if a system has patched some application ★
    D. They can be used to check if a system has users with default logins ★

14. Which of the following are tools that are not well suited to be used in an IDS for comparing the traffic features against a normal behavior?

    A. Neural networks
    B. Hamming distance
    C. Markov models
    D. Signatures ★

15. Mark the invalid wireshark display filters:

    A. `eth.addr != 00:01:02:03:04:05`
    B. `protocol == ftp` ★

Student name: _____

Matricola: _____

C. `ip.host == error`
D. `ip.address eq 10.0.0.2` ★

16. Which of the following network traffic elements is not well suited to be used as a feature for an IDS?

A. Domain names of involved hosts ★
B. % of connections to same host with SYN errors
C. Connection lifetimes
D. Illegal fragments

17. Which of the following IPv6 addresses is NOT a Link-Local multicast address?

A. FF02::1
B. FF18::BABA:1234 ★
C. FF05::1:3 ★
D. FF12::BABA:1234

18. Which of the following IP addresses can be assigned to a host within the network 12.34.48.1/20?

A. 12.34.48.255 ★
B. 12.34.48.0
C. 12.34.56.0 ★
D. 12.34.63.254 ★

19. What is false about the *openvpn* tool?

A. It cannot be used for a host-to-site VPN ★
B. It cannot be used to establish a VPN without a valid certificate ★
C. It is used to establish a IPSec VPN ★
D. It can be used to establish a VPN on any reachable port

20. What is the decision for a HTTPS GET request on the standard port when thee firewall that protects the webserver has the following set of rules?

```
iptables -A INPUT -p tcp --destination-port 80 -j ACCEPT
iptables -A INPUT -p tcp --destination-port 443 -j ACCEPT
iptables -A INPUT -j REJECT
```

A. HTTP 200 OK if the requested resource is available, HTTP 404 ERROR otherwise ★
B. It depends on the source IP address
C. No connection will be possible
D. The request will be dropped and a ICMP PORT UNREACHABLE will be sent back

Please, transcript your answers in the boxes below:

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