Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Written exam, 24th of June 2020

Student name: ____________________

Matricola: ____________________

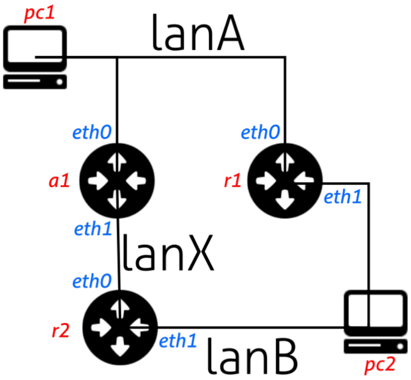
Open questions (60%)

Provide an answer within the space allocated for each question.

1. List and detail which are the characteristics a host needs to have in a LAN for being the next hop for a given destination network.

2. Describe the 3-1-4 rule for /64 GUA in IPv6 and explain why you think it is useful.

3. Describe the main differences between IPv4 and IPv6 about the mechanism of IP-MAC address resolution.



4. Considering the above figure, mention the possible attacks host *a1* could mount if the addressing of the network is based on IPv6.

5. Considering the following list of iptables commands, find all the syntax errors you can recognize and how would you fix them.

```
INTERNAL=10.10.10.0/24
WAN=151.100.170.0/24

1. iptables -P FORWARD DENY
2. iptables -A FORWARD -s $WAN -p TCP -m state --state NEW,ESTABLISHED -j ACCEPT
3. iptables -A FORWARD -s $WAN -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
4. iptables -A FORWARD -d $WAN -p TCP -m state --state ESTABLISHED -j ACCEPT
```

Student name: ______________________

Matricola: ______________________

```
5. iptables -A FORWARD -d $WAN -p UDP -m state --state ESTABLISHED -j ACCEPT
6. iptables -A FORWARD -s $WAN -p icmp --icmp-type echo-request -j ACCEPT
7. iptables -A FORWARD -d $WAN -p icmp --icmp-type echo-response -j ACCEPT
8. iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADING
```

6. You have to setup a network with 30 hosts and allow all of such hosts to reach the Internet. Moreover, 2 of them have to also be reachable from the Internet. You only have one public IP address assigned from your ISP. Explain the type of mechanisms you would use to properly configure your network.

7. Explain the most important differences on having a VPN that protects data at transport-level and one that protects data at network-level.

8. Describe pros and cons of transparent proxies.

9. Detail how a signature-based IDS works.

10. Explain how a SIEM can help to meet the IT Regulatory Compliance of an organization.

Student name: ____________________

Matricola: ____________________

Multi-choice questions (40%)

Mark all the options you think are correct.

1. What can be used to realize a MITM attack?

   A. A malicious ICMP redirect packet ★
   B. A spoofed gratuitous ARP message ★
   C. A forward proxy that uses the `HTTP CONNECT`
   D. A forged digital certificate ★

2. What is true with respect to SLAAC?

   A. It is used to delegate the address assignment to the hosts ★
   B. It cannot be used in conjunction with a DHCP server
   C. It cannot be used in conjunction with the privacy extension
   D. It must use the EUI-64 format to work

3. Which of the following properly sets the IP address in a host, without giving a syntax error?

   A. `ip addr add 10.0.0.1 dev eth0` ★
   B. `ip addr add 10.0.0.1/8 dev eth0` ★
   C. `ip addr add 10.0.0.1 netmask 255.0.0.0 dev eth0`
   D. `ip addr add 10.0.0.1/8 eth0`

4. In which tables of `iptables` you can not find the built-in PREROUTING chain?

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

5. What is true about SSL/TLS?

   A. It cannot provide mutual authentication between the communicating parties
   B. It only uses asymmetric encryption to exchange data between the two communicating parties
   C. It operates on top of the transport-layer ★
   D. It is used to implement IPSec VPNs

6. What is true about the `HTTP CONNECT`?

   A. It is used to check and scan all the data exchanged between an internal host and a remote host
   B. It is mainly used in forward proxies ★
   C. It is mainly used in reverse proxies
   D. It requires the client that wants to use it to explicitly configure a proxy address ★

7. Which type of filter would you use in `tcpdump` to only capture DNS packets?

   A. `dns`
   B. `port 53` ★
   C. `udp and port 53` ★
   D. `proto dns`

8. Which functions do you expect to be realized by a SIEM when managing the logs of a monitored network system?

   A. Correlation of the events ★
   B. Indexing for improving lookup speed ★
   C. Normalization of the received data ★
   D. Log correction

9. What is a CVE?

   A. It is a proof-of-concept type of attack
   B. It is an unknown vulnerability
   C. It is a reference to a public database ★
   D. It is the definition of an attack

10. In which type of proxy is generally realized the SSL offloading?

    A. Forward proxy
    B. Transparent proxy
    C. Reverse proxy ★
    D. None of the other mentioned

11. Which of the following is NOT a typical link-local attack?

    A. Eavesdropping
    B. ICMP redirect
    C. ARP poisoning
    D. DNS cache poisoning ★

12. What is the destination address of a ICMPv6 Router Solicitation?

    A. FF02::1
    B. FF02::2 ★
    C. FE80::1
    D. FF11::1

13. What is true about IPSec?

    A. Multiple SAs can exist for handling the different types of data exchanges between two hosts ★
    B. A Security Policy is a simplex channel that describes the way how packets need to be processed (e.g. employed encryption/authentication algorithms and keys)
    C. A Security Association specifies which and how security services should be provided to IP packets
    D. The protocol mode (transport/tunnel) is requested using a SA

14. A network is configured to have private IP addressing. You need to allow all of the internal hosts to reach the Internet. Which of the following `iptables` targets might be suitable for such a need when forwarding the packets to the ISP?

    A. DNAT
    B. ACCEPT
    C. SNAT ★
    D. MASQUERADE ★

15. What would you use to encrypt traffic using IPv6?

    A. TLS/SSL ★
    B. The ESP extension header ★
    C. IKEv2
    D. The AH extension header

16. Which of the following can act as a NIPS?

    A. Suricata configured in line ★
    B. Fail2ban configured in the firewall
    C. Snort configured out of band
    D. None of the other mentioned

17. Which command would you use to see the associations between IP and MAC addresses known by a host?

    A. `ip route`
    B. `arping`
    C. `ip neigh show` ★
    D. `arp -a` ★

18. Which of the following should not be considered when configuring a firewall to allow the internal host `$HOSTA` to open a ssh connections with a remote host `$HOSTB`?

    A. `iptables -A FORWARD -s $HOSTB -p TCP -m state -state ESTABLISHED,RELATED -j ACCEPT`
    B. `iptables -A FORWARD -s $HOSTA -p TCP -sport 22 -j ACCEPT` ★
    C. `iptables -A FORWARD -d $HOSTB -p TCP -dport 22 -j ACCEPT`
    D. `iptables -A FORWARD -p TCP -dport 22 -j ACCEPT`

19. If you want to block all the HTTP/HTTPS traffic from a network towards all the hosts of a certain domain name...

    A. you can not use an application-level firewall (like a proxy)
    B. you can not use a NIDS ★
    C. you can not use a stateful firewall
    D. you can not use a stateless firewall

20. What is the IPv6 equivalent of an IPv4 broadcast address within a network?

    A. FF02::2
    B. FF02::1 ★
    C. FE80::1
    D. FF11::1

Please, transcript your answers in the boxes below:

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