Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Written exam, 7th of June 2019

Student name: _____

Matricola: _____

Open questions (60%)

Provide an answer within the space allocated for each question.

1. Consider the connection tracking mechanism (implemented for example in iptables): in which type of firewalls can you find it? Describe how it works and explain why it is important.

2. What function does each of the following *iptables* rules serve?

```
a) iptables -A INPUT -s 192.168.23.12 -p tcp --sport 22 -j ACCEPT
b) iptables -t nat -A POSTROUTING -o $ext_if -j MASQUERADE
c) iptables -t nat -P DROP
d) iptables -A FORWARD -p udp -m state --state ESTABLISHED -j ACCEPT
e) iptables -A INPUT -j DROP
```

```
tc@tc-client:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:14:2F:44
          inet addr:192.168.99.25  Bcast:192.168.99.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10406 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:740985 (723.6 KiB)  TX bytes:6696710 (6.3 MiB)
          Interrupt:19 Base address:0x2000

tc@tc-client:~$ cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.99.1     0x1         0x2         00:0c:29:55:f9:44     *        eth0
192.168.99.150   0x1         0x2         00:0c:29:53:e4:59     *        eth0
192.168.211.2    0x1         0x2         00:50:56:ef:05:c0     *        eth1
192.168.99.25    0x1         0x2         00:0c:29:14:2f:44     *        eth0
192.168.99.50    0x1         0x2         00:0c:29:55:f9:44     *        eth0
192.168.211.1    0x1         0x2         00:50:56:c0:00:08     *        eth1
tc@tc-client:~$
```

Figure 1: Bash snapshot

3. Figure 1 reports the outcome of some *bash* commands. Describe what you can observe and explain what you think is relevant. Finally, suggest what you would explore further and why.

Student name: _____

Matricola: _____

4. It is not always true that its better to have false positives than false negatives. Explain what they are in their wider meaning and provide two examples: one in which you think it is better to have less false negatives and one in which it is the opposite.

5. Consider a security solution like **snort**. Describe its main functionalities and the internal working mechanism.

6. Describe the differences between a **tun** and a **tap** drive.

7. Explain if a user can trust an anonymizer proxy for not eavesdropping her HTTP traffic, when browsing a web server via HTTPS.

8. Explain if –and if yes, how– a SIEM is different from an IDS/IPS.

9. Describe the main roles and characteristics of Link-local Unicast addresses in IPv6.

10. Host A in LAN1 has to send a UDP packet to host B in LAN2. Succinctly describe source and destination MAC and IP addresses host A will use and if it needs to use ARP. Also report how the same process changes when using IPv6.

Student name: _____

Matricola: _____

Multi-choice questions (40%)

Mark all the options you think are correct.

1. Mark the most likely wrong associations of IPv6 addresses, given that:

```
A=2001:DB8:1000::1
B=FE80::FE99:47FF:FE75:C3E0
C=2001:DB8:CAFE:1:50A5:8A35:A5BB:66E1
D=2001:DB8:CAFE:1:FE99:47FF:FE75:C3E0
```

   A. A: GUA via SLAAC with random IID, B: Link-local with EUI-64 ★
   B. C: GUA via SLAAC with EUI-64, D: link-local with EUI-64 ★
   C. A: static GUA, C: GUA via SLAAC with random IID
   D. B: Link-local with EUI-64, D: GUA via SLAAC with EUI-64

2. When a packet is processed in an iptables chain,

   A. once a matching rule has been applied, under no circumstances other rules will be considered
   B. the rules are considered in order and if no matching rule is found, the default policy is applied ★
   C. the rules are considered in order and the decision is made according to the first one matching ★
   D. all the rules are always considered and the matching ones are applied

3. What is true when talking about Kerberos?

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

4. Which of the following is NOT a typical service of a SIEM?

   A. Vulnerability scanning ★
   B. Event correlation
   C. Endpoint security
   D. Reconnaissance ★

5. Which of the following filters allows to capture DNS queries?

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

6. If $<$ is the relation "happens before than", mark the right statements:

   A. Non-intrusive target search $<$ Data analysis $<$ Reporting ★
   B. Planning $<$ Data analysis $<$ Intrusive target search
   C. Planning $<$ Intrusive target search $<$ Reporting ★
   D. Data analysis $<$ Threat modeling and Exploitation $<$ Intrusive target search

7. Which of the following are typical features of forward proxies?

   A. Possibility to perform load balancing between different origin servers
   B. Possibility to check the identity of the user making a request and verify her authorization ★
   C. Possibility to check the integrity of the fetched resources
   D. Possibility to cache fetched resources, to save bandwidth and increase latency ★

8. The TLS protocol

   A. is a protocol that works at the APPLICATION level
   B. can only be used with HTTP
   C. can also provide client authentication ★
   D. uses both symmetric and asymmetric cryptography ★

9. Which type of IDS makes use of "rules"?

   A. Only HIDS signature-based
   B. Only NIDS behavioral-based
   C. NIDS Signature-based ★
   D. HIDS Signature-based ★

10. In a VPN

   A. we cannot use SSL/TLS to secure the VPN network layer
   B. site-to-site tunneling makes PDUs of a network to pass encrypted through an insecure network, to reach another secure network ★
   C. site-to-site tunneling makes possible ARP spoofing attacks within the VPN itself
   D. we can use IPSec to secure the VPN network layer ★

11. To take a decision about a packet, what a packet filtering firewall DOES NOT consider?

   A. The payload of the packet ★
   B. The IP addresses of the packet
   C. The context of the packet ★
   D. The TCP flags of the packet

12. What is true with respect to ICMPv6?

   A. When a host wants to ping another host, it keeps sending Echo Request packets with increasing Hop Limit field

Student name: _____

Matricola: _____

B. When a host needs to know the MAC address related to a IPv6 address, it sends a multicast message ★
C. When a host connects to a new network, it sends a Router Solicitation packet ★
D. When a host receives a packet for a port not in listening, it sends a Destination Unreachable, No route to destination message

13. For protecting a legacy server that does not makes use of TLS, which type of proxy could you use?

A. Forward proxy with SSL offloading
B. Transparent proxy
C. Forward proxy with SSL bump
D. Reverse proxy as TLS termination ★

14. In a company that only has one single public IP address, you would use DNAT for doing what?

A. To make possible the internal DNS server to contact other DNS servers
B. To make possible an external customer to visit the company website hosted in an internal server ★
C. To make possible an employee that is inside the network to reach an external service
D. To make possible an employee that is abroad to reach the VPN gateway of the company ★

15. Mark the wrong descriptions of commands:

A. `ip addr` is used to assign or modify IP addresses
B. `ip ntable` is used to manage ARP cache entries ★
C. `ip link` is used to manage a network device
D. `ip route` is used to manage routing table entries

16. What is true about Wireshark?

A. It makes use of filters to only display packets with certain field values ★
B. It can easily recognize protocols used in non-standard ports
C. It cannot be used without having an interface in promiscuous mode
D. It can dissect raw data of a packet in the different logical fields ★

17. An Intrusion Detection System has failed raising an alarm when a real attack was occurring. Which of the following is true?

A. A True Positive should have occurred, but a False Positive eventually occurred
B. A True Positive should have occurred, but a False Negative eventually occurred ★
C. A False Negative should have occurred, but a False Positive eventually occurred
D. A True Negative should have occurred, but a False Negative eventually occurred

18. In which directories are different from databases?

A. Data that would normally be stored in an LDAP service would not be expected to change on every access ★
B. To query both of them you need detailed knowledge of the data organization into tables, joins, primary keys and so on
C. Only directories are characterized as a write-once-read-many-times service ★
D. Only with LDAP you can have data to be consistent at all times, even if distributed among multiple servers

19. A firewall transforms each packet reaching its WAN interface and a certain port, changing the destination IP address with the IP address of an internal host. Which mechanism is the firewall probably adopting?

A. dynamic NAT
B. port forwarding ★
C. connection tracking
D. destination NAT ★

20. Which of the following is NOT a RADIUS packet?

A. Access-accept
B. Server-hello ★
C. Accounting-request
D. Bind-request ★

Please, transcript your answers in the boxes below:

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