Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
Written exam, 17th of July 2020

Student name: _____

Matricola: _____

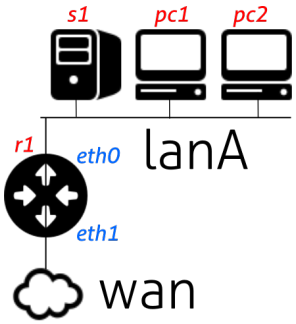
Open questions (60%)

Provide an answer within the space allocated for each question.

1. Explain what is routing and how it is realized.

2. Write a `tcpdump` filter to only capture DHCP traffic on interface eth2, not involving the DHCP server `$DHCPSERV`.

3. Explain how in `iptables` a connection-less protocol like UDP is managed by the `state` module.



4. Considering the above figure, where all the hosts in *lanA* have private IP addresses. Write the `iptables` rules for the router *r1* to:
   - enable the use of the NAT mechanism in *lanA*,
   - allow all the hosts in *lanA* to reach all the services of Internet (*wan*)
   - only allow the HTTP traffic originating from *wan* to reach the web server running in *s1* and to block all the other traffic to all the hosts in *lanA*
   - only allow ssh traffic from *lanA* to reach the *r1* router and to block all the other traffic to it.

Student name: _____

Matricola: _____

5. Describe how IPSec realizes the mechanism of encryption and authentication, considering the differences between IPv4 and IPv6.

6. Explain why it is needed to implement mechanisms like the SSLBump of squid to inspect traffic when using proxy servers.

7. Explain if and why a device that is *out-band* (i.e. NOT "*in line*") can act as a IPS.

8. Describe what is the IPv6 SLAAC mechanism and how it is realized.

9. Explain what is the function called log normalization in a SIEM and why it is important.

10. Explain what is a NVT in the context of a vulnerability scanner like OpenVAS.

Student name: _____

Matricola: _____

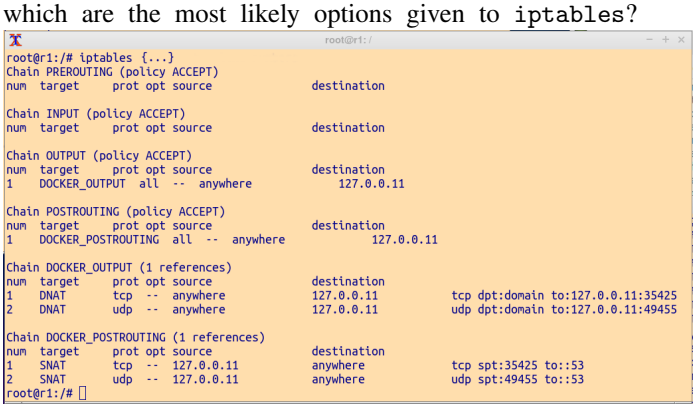
Multi-choice questions (40%)

Mark all the options you think are correct.

1. Which type of proxy is generally employed for purposes like load balancing or application level control?

   A. Transparent proxies
   B. Reverse proxies ★
   C. Forward proxies
   D. SOCKS proxies

2. Considering the output shown in the following figure, which are the most likely options given to `iptables`?



   A. `-X`
   B. `-v`
   C. `-t NAT` ★
   D. `--line-numbers` ★

3. In which of the following tools can you find a rule like `alert tcp $WEB_IP any -> $EXT_NET 22 (msg.....)`?

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

4. Which of the following can be the representation of an IPv4 octet?

   A. AG
   B. FF02
   C. CC ★
   D. 192 ★

5. In which of the following possible VPN options are generally encrypted the real IP addresses of both the communicating end-points (i.e. the two final hosts)?

   A. IPSec VPN transport mode
   B. Site-to-site VPN using TLS ★
   C. Host-to-site VPN using TLS
   D. IPSec VPN tunnel mode ★

6. Which can be the functions a DHCP server can perform in IPv6?

   A. Providing to requesting routers, the network prefix for the prefix delegation mechanism ★
   B. Providing to the requesting hosts, the full configuration (full IP address, DNS and GW) ★
   C. Providing to all the host of a network, the network prefix for the SLAAC mechanism
   D. Providing the IP address of the domain server a host should use in a network ★

7. Which chains have the purpose to handle the network packets directed to and generated by the host that runs `iptables`?

   A. OUTPUT chain ★
   B. none of the other options
   C. FORWARD chain
   D. INPUT chain ★

8. Which of the following commands enables the source NAT mechanism of `iptables` for the interface `$WAN_IF` with IP `$WAN_IF_IP`?

   A. `iptables -A POSTROUTING -o $WAN_IF -j MASQUERADE`
   B. `iptables -A PREROUTING -o $WAN_IF -j MASQUERADE`
   C. `iptables -A POSTROUTING -o $WAN_IF -j SNAT --to-source $WAN_IF_IP`
   D. none of the other options ★

9. In which of the following details do IPv4 and IPv6 differ?

   A. The length of the header ★
   B. The number of IP addresses in the header
   C. Only one of them has a header field that is decremented every time the packet is forwarded
   D. The number of header fields ★

10. Which protocol does IPv6 use to realize the association between MAC and IP of a host?

    A. DNS
    B. ICMPv6 ★
    C. ARP
    D. Ethernet

11. What is challenging for realizing an optimal behavioral-based IDS?

    A. Have an effective string-matching algorithm for detecting malicious packets
    B. Choose the best set of features to train the IDS ★
    C. Reduce the number of True Positive while increasing the number of False Negative
    D. Define what is the normal behavior of a network ★

Student name: _____

Matricola: _____

12. In ICMPv6, which packet is generally sent to all the devices of a network to provide the details of the prefix of that network?
    A. Neighbor advertisement
    B. Router advertisement ★
    C. Router solicitation
    D. None of the other options

13. Which of the following commands returns a syntax error?
    A. `iptables -D INPUT -p TCP -j ACCEPT`
    B. `iptables -P INPUT -j ACCEPT` ★
    C. `iptables -A INPUT -p TCP -j ACCEPT`
    D. `iptables -D INPUT 2`

14. Which of the following steps is not generally included in a penetration test?
    A. Data-analysis
    B. Threat modeling
    C. Audit ★
    D. Exploitation

15. What would you observe if you want to detect a MITM attempt?
    A. The NAT table of a host
    B. The packets a host receives on a given interface ★
    C. The arp table of a host ★
    D. The routing table of a host

16. Which types of filters can you apply in Wireshark?
    A. Executive filters
    B. Anomaly filters
    C. Display filters ★
    D. Capture filters ★

17. Which command do you use for showing the routing tables of a host?
    A. `ip route` ★
    B. `route` ★
    C. `show ip route`
    D. `ip show routes`

18. Which mechanism allows a host to establish a HTTPS connection with a remote host, asking and entrusting a third, relaying host, without losing the confidentiality of HTTPS?
    A. HTTP CONNECT ★
    B. SSL offload
    C. MITM
    D. SSLBump

19. What is true regarding IPSec?
    A. In transport mode, it provides protection for an IP packet embedded as payload in an IP packet
    B. In tunnel mode, it provides protection for an IP packet embedded as payload in an IP packet ★
    C. In tunnel mode, it provides protection for a T-layer packet embedded as payload in an IP packet
    D. In transport mode, it provides protection for a T-layer packet embedded as payload in an IP packet ★

20. What is true regarding `openvpn`?
    A. It cannot guarantee key secrecy when using digital certificates
    B. It makes use of Security Policies and Security Associations
    C. It makes use of both symmetric and asymmetric cryptography ★
    D. It cannot guarantee key secrecy when using a static key

Please, transcript your answers in the boxes below:

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