Sapienza Master's Degree in Cybersecurity
Practical Network Defense (prof. Spognardi)
First Mid-term, 16th April 2019

Student name: ____________________

Matricola: ____________________

Open questions (60%)

Provide an answer within the space allocated for each question.

1. Explain why firewall rules based on IP address blacklisting do not provide enough protection against the spoofing attack.

2. Describe how packet filtering firewalls are different from stateful firewalls.

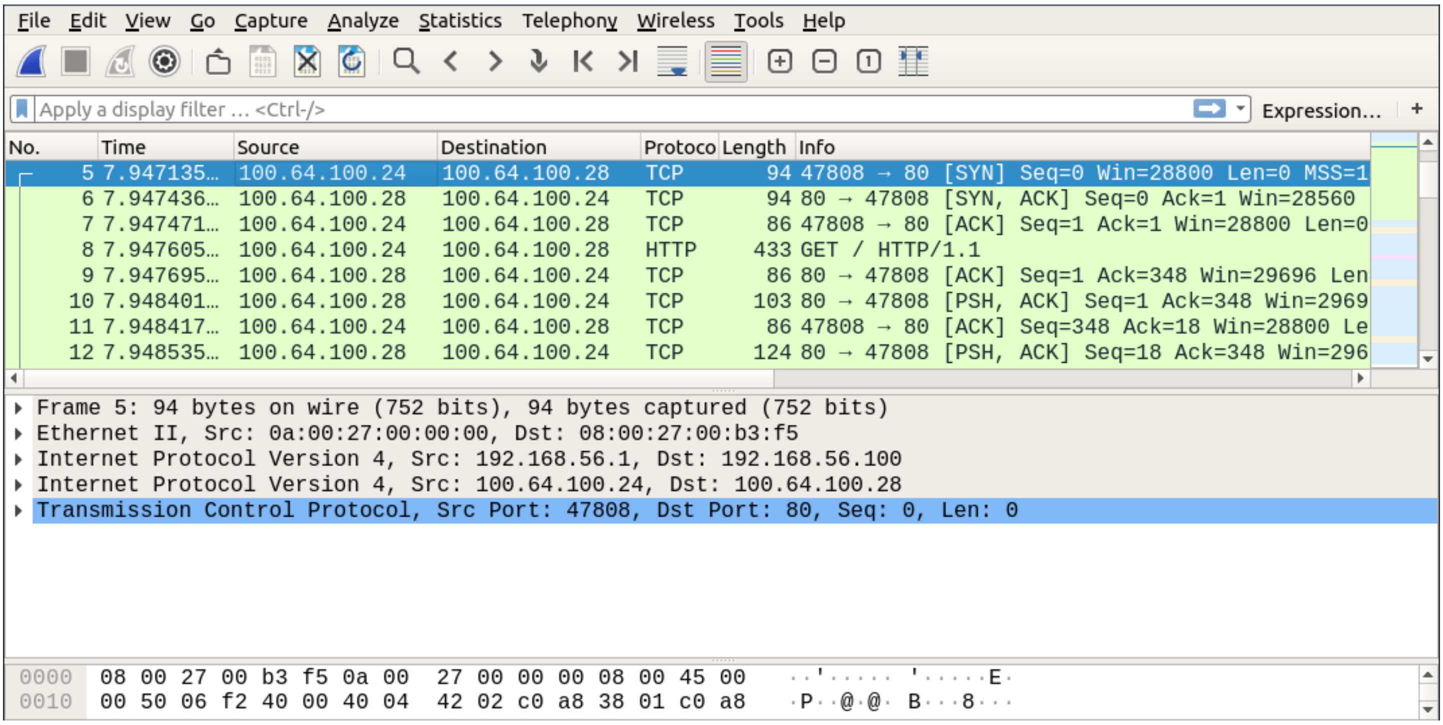
3. List and briefly describe the chains traversed by a packet that has to be forwarded by a firewall that uses `iptables`.

4. Compare pros and cons of a VPN operating at Network Layer with respect to a VPN operating at Transport Layer.

5. Describe the challenges of using NAT with a VPN.

6. Enumerate and succintly describe the messages of a SSL handshake.

7. Describe the second A of the AAA functions of RADIUS.


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

```
No.  Time       Source         Destination    Protoco Length Info
   5 7.947135… 100.64.100.24  100.64.100.28  TCP       94 47808 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1
   6 7.947436… 100.64.100.28  100.64.100.24  TCP       94 80 → 47808 [SYN, ACK] Seq=0 Ack=1 Win=28560
   7 7.947471… 100.64.100.24  100.64.100.28  TCP       86 47808 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0
   8 7.947605… 100.64.100.24  100.64.100.28  HTTP     433 GET / HTTP/1.1
   9 7.947695… 100.64.100.28  100.64.100.24  TCP       86 80 → 47808 [ACK] Seq=1 Ack=348 Win=29696 Len
  10 7.948401… 100.64.100.28  100.64.100.24  TCP      103 80 → 47808 [PSH, ACK] Seq=1 Ack=348 Win=2969
  11 7.948417… 100.64.100.24  100.64.100.28  TCP       86 47808 → 80 [ACK] Seq=348 Ack=18 Win=28800 Le
  12 7.948535… 100.64.100.28  100.64.100.24  TCP      124 80 → 47808 [PSH, ACK] Seq=18 Ack=348 Win=296
```

```
▸ Frame 5: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
▸ Ethernet II, Src: 0a:00:27:00:00:00, Dst: 08:00:27:00:b3:f5
▸ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.100
▸ Internet Protocol Version 4, Src: 100.64.100.24, Dst: 100.64.100.28
▸ Transmission Control Protocol, Src Port: 47808, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  08 00 27 00 b3 f5 0a 00  27 00 00 00 08 00 45 00   ··'····· '·····E·
0010  00 50 06 f2 40 00 40 04  42 02 c0 a8 38 01 c0 a8   ·P··@·@· B···8···
```

8. Describe what can you recognize in the captured packets of the above figure.

9. Describe what the client has to present to a resource server when using Kerberos.

10. Describe the functions of the Berkeley Packet Filters and provide two examples of their use.

Multi-choice questions (40%)

Mark all the options you think are correct.

1. In `iptables`:

A. MANGLE is a possible target
B. MASQUERADE is a possible target ★
C. DNAT is a possible target ★
D. another chain is a possible target ★

2. Which of the following protocol/port-number associations are correct?

A. LDAP/389 ★
B. RADIUS/1812 ★
C. TLS/445
D. ICMP/501

3. Which statement is false when considering `iptables`:

A. the PREROUTING chain is used to perform NAT
B. the POSTROUTING chain is used to perform NAT
C. the INPUT chain is used to perform filtering
D. the OUTPUT chain is used to perform NAT ★

4. Heartbleed is...

A. A mechanism to keep a TLS connection alive
B. A mechanism to establish a TLS connection
C. A bug in the TLS connection establishement
D. An bug in an old implementation of TLS ★

5. Which of the following steps do not occur during the establishment of a HTTPS connection?

A. The server send to the client the shared key that they will use to encrypt the communication. ★
B. The client sends to the server the shared key that they will use to encrypt the communication. ★
C. The client receives from the server a certificate with its public key.
D. Server and client generate the shared key that they will use to encrypt the communication.

6. Which of the following fields is not mentioned in the standard format of RADIUS packets?

A. BindRequest ★
B. AddRequest ★
C. Code
D. Length

7. In which directories are different from databases?

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

8. The TLS protocol

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

9. Which of the following encryption methods are supported by Kerberos?

A. ECDSA
B. DES ★
C. AES ★
D. RSA

10. What is a firewall condition in which any traffic not specifically permitted by a previous rule in the rule set is denied?

A. Packet filtering
B. Flood guarding
C. Implicit deny ★
D. Explicit deny

11. An IP packet with the `fraglag` set to 1:

A. can be dropped by `iptables` ★
B. is automatically dropped by `iptables`
C. must have the `offset` field set to 0
D. is the last packet of a group of fragmented IP packet

12. Which of the following is true in LDAP?

A. A RDN must be unique for any single entry in the whole DIT
B. A DN must be unique for any single entry in the whole DIT ★
C. All the values defined by a `objectclass` schema are mandatory
D. An entry is composed by several attributes, each with one or more values ★

13. You have a firewall configured with the following `iptables` commands (consider the variables names as self explanatory):

```
iptables -A INPUT ! -s $ADMIN_CONSOLE_IP -p tcp \
        --dport 22 -j DROP
iptables -A FORWARD -i $INTERN_IFACE -p udp \
        --dport 53 -j ACCEPT
iptables -A FORWARD -i $INTERN_IFACE -p udp \
        -m state --state ESTABLISHED -j ACCEPT
iptables -P FORWARD DROP
iptables -A FORWARD -d $DMZ_PROXY -p tcp \
        --dport 443 -j ACCEPT
iptables -A FORWARD -s $DMZ_PROXY -p tcp \
        -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Which of the following packets will pass the set of rules?

A. an ssh connection from `$ADMIN_CONSOLE_IP` to `$EXTERNAL_FW_IP` ★
B. a ping from `$ADMIN_CONSOLE_IP` to `$EXTERNAL_FW_IP` ★
C. a ping from `$ADMIN_CONSOLE_IP` to `$INTERNAL_HOST`
D. a DNS query from `$INTERNAL_HOST` to `8.8.8.8` ★
E. an ssh connection from `$ADMIN_CONSOLE_IP` to `$INTERNAL_HOST`
F. an HTTPS GET request from `$INTERNAL_HOST` to `$WEB_SERVER_IP`

14. What is taking place when a network device uses the MAC address of another device, attempting to change the ARP tables of third device through forged traffic and the ARP table-update mechanism?

A. MAC flooding
B. ARP poisoning ★
C. ARP flooding
D. MAC poisoning

15. What is the difference between transport mode and tunnel mode in IPSec?

A. Only transport mode is unencrypted
B. Only tunneling mode does not encrypt the header
C. Only tunneling mode is unencrypted
D. Only transport mode does not encrypt the header ★

16. If you want to configure a firewall so that the hosts within the internal network can only browse the Internet over HTTPS and ping external hosts, which of the following rules are likely to be required, among others?

A. accept the TCP packets with source port 80 starting from the internal network
B. allow all ICMP traffic
C. accept the TCP packets with destination port 443 directed to the internal network, that are part of an established connection
D. only allow ICMP echo-requests from to the internal network to the Internet, and ICMP echo-replies directed to the internal network ★

17. Which statements are false regarding a DMZ?

A. It is the network where the most critical servers of an enterprise are placed ★
B. In a dual-homed host configuration, the bastion host is the only point of access to the internal network
C. It is a type of network that encrypts all the traffic before sending it to internet ★
D. In a screened subnet configuration, there is the need of two routers

18. In the string `TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA`:

A. DSS stands for Digital Secure Socket
B. 3DES is the system required to sign
C. CBC stands for Cipher Block Chaining ★
D. DH stands for Diffie-Hellman key exchange ★

19. We can NOT use `iptables` to:

A. filter unwanted packets
B. perform NAT
C. block ICMP packets
D. establish a VPN ★

20. Considering the priorities of `iptables` chains

A. NAT chain is processed before FILTER but after MANGLE ★
B. MANGLE chain is processed before NAT but after FILTER
C. MANGLE chain is processed before FILTER but after NAT
D. NAT chain is processed before MANGLE but after FILTER