Computer and Information Security, TC-2027
Design: Ing. Rafael Emilio Dávalos Villarreal
Teacher: José de Jesús Jiménez Martínez
Lab Practice 02
Wireshark

Matrícula	**A01366288**	Nombre	**Alan Macedo Esparza**	Group	**4**	Date	**19/08/2020**

Write the requested answers on this document. Create a PDF file and upload it to Canvas

1. Software
Install the program Wireshark on your laptop

link	https://www.wireshark.org

2. Run the program and open the file smtp.pcap

3. Research and answer the protocols seen on Wireshark

Protocol	Description	OSI Model level	Explain
DNS	Domain name service	7	It's a service that translates between names of websites and their ip address.
TCP	Transmission control protocol	4	It's a transmission protocol that ensures ordered and error-checked package streams
SMTP	Simlple mail transfer protocol	7	It's a protocol that specifies how to send mails.
ICMP	Internet controll message protocol	3	It's a protocol that is used by network devices.

4. Based on frame #1

Ethernet Protocol

Number of Ethernet bytes (on Wireshark)	76	
Destination address (hex)	001f33d98160x	
Source address (hex)	00e01c3c17c2x	
Protocol (hex)	0800	
Encapsulates the protocol	IPv4	(IPv4, IPv6, TCP, UDP, DNS, SMTP, HTTP)

IPv4 Protocol

Length of package (bytes)	62
Source IP (decimal dot)	10.10.1.4
Source IP (hex)	0a0a0104x
Destination IP	10.10.1.1

Computer and Information Security, TC-2027
Design: Ing. Rafael Emilio Dávalos Villarreal
Teacher: José de Jesús Jiménez Martínez

(decimal dot)	
Destination IP (hex)	0a0a0101x
Protocol (decimal)	17
Protocol (hex)	11
Protocol	UDP

(IPv4, IPv6, TCP, UDP, DNS, SMTP, HTTP)

UDP Protocol

Length of segment (bytes)	42
Source port (decimal)	56166
Source port (hex)	db66
Destination port (decimal)	53
Destination port (hex)	00 35
Application level protocol	DNS

(IPv4, IPv6, TCP, UDP, DNS, SMTP, HTTP)

DNS Protocolo

Length of message (bytes)	16
Query (site name)	mail.patriots.in

Find on frame #2 the answer given by the DNS server to the client searching the email server

Answers (IP addr en decimal dot)	74.53.140.153

5. Handshake

Based on frames #3, #4 y #5

Which are the flags used by the handshake	
SYN	
SYN, ACK	
ACK	

6. Revisa el frame #3

IPv4 Protocol

Protocol (decimal)	6
Protocol (hexadecimal)	0x06
Protocol	TCP

(IPv4, IPv6, TCP, UDP, DNS, SMTP, HTTP)

TCP Protocol

Length of segment (bytes)	28
Source port (decimal)	1470
Source port (hex)	05be
Destination port (decimal)	25
Destination port (hex)	0019

Computer and Information Security, TC-2027
Design: Ing. Rafael Emilio Dávalos Villarreal
Teacher: José de Jesús Jiménez Martínez

Application level port	smtp	(IPv4, IPv6, TCP, UDP, DNS, SMTP, HTTP)

Flags	SYN
Flags (2 bytes hexadecimal)	7002
Flags (3 nibbles on bits)	0000 0000 0010
Corresponding Flag	SYN

Watch the flag inside the bits

Investigate how a DoS (Denial of Service) attack is made and in particular the SYN Flood
A DoS attack when an attacker attempts to prevent service to other users. The SYN flood is a form of DoS where the attacker sends a lot of SYNs in order to consume server resources.

7. On frames #4 and #5

Frame #4, TCP Protocol	

Flags	SYN, ACK
Flags (2 bytes on hexadecimal	70 12
Flags (3 nibbles on bits)	0000 0001 0010
Corresponding Flag	SYN ACK

Frame #5, TCP Protocolo	

Flags	SYN
Flags (2 bytes on the flags)	7002
Flags (3 nibbles en bits)	0000 0000 0010
Flag correspondiente	SYN

8. On these frames you can see a user and a password on clear text, find them.

User	Z3VycGFydGFwQHBhdHJpb3RzLmlu
Password	cHVuamFiQDEyMw==

9. Reflection

Write a reflection about this lab in at least 5 lines. (what you thought before, during and after this lab practice).

It’s interesting to see that it is possible to read emails, as well as usernames and passwords in clear text with very rudimentary tools/techniques. It definitely highlights the need for internet security protocols. Also, it definitely makes it so that I see the importance of things such as https in a more clear light. Another thing is that this wireshark sniffing tool is definitely a good tool to diagnose networking problems