

Tarea 2

Ejercicio 1

I) *Exercise One: Good old telnet*

File: telnet.pcap

Work: reconstruct the telnet session

Questions

1. Who logged into 192.168.0.1?

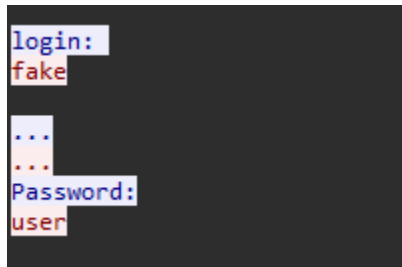
Username: _____ Password: _____

2. After logged what the user do?

TIP: telnet traffic is not secure

1. Quién se inició sesión en 192.168.0.1

- a. Nombre de usuario: fake
- b. Contraseña: user



```
login:
fake

...
Password:
user
```

2. Qué hizo el usuario después de iniciar sesión: El usuario realiza un ping a yahoo.com, revisó el contenido del directorio y cerró su sesión.

Ejercicio 2

II) Exercise two: massive TCP SYN

File: `massivesyn1.pcap` and `massivesyn2.pcap`

Work: Find files differences

Questions

1. `massivesyn1.pcap` is a _____ attempt

1. `massivesyn2.pcap` is a _____ attempt

1. `Massivesyn1.pcap` es un intento de escaneo de puertos, debido que tiene una única dirección de origen y una de destino y se analizan distintos puertos de la IP destino, como el 21, 22, 23, 25, 80, 139, entre otros, mediante el envío de muchos paquetes SYN. Parece que se intenta encontrar puertos abiertos en la dirección de destino.
2. `Massivesyn1.pcap` es un intento de ataque distribuido, debido a que tiene muchas IPs de origen y destino distintas. En este caso se analizan puertos al azar. También se puede interpretar como una simulación de tráfico.

Ejercicio 3

III) Exercise three: compare traffic

Files: `student1.pcap` and `student2.pcap`

Scenario: You are an IT admin in UCR, you had reported that *student1* (a new student) cannot browse or mail with its laptop. After some research, *student2*, sitting next to *student1*, can browse with any problems.

Work: compare these two capture files and state why *student1*'s machine is not online

Solution

1. *student1* must _____

TIP: pay attention to first ARP package

1. El estudiante 1 debería revisar si tiene bien configurado el gateway, DNS o incluso la IP.

Ejercicio 4

IV) Exercise four: chatty employees

File: chat.pcap

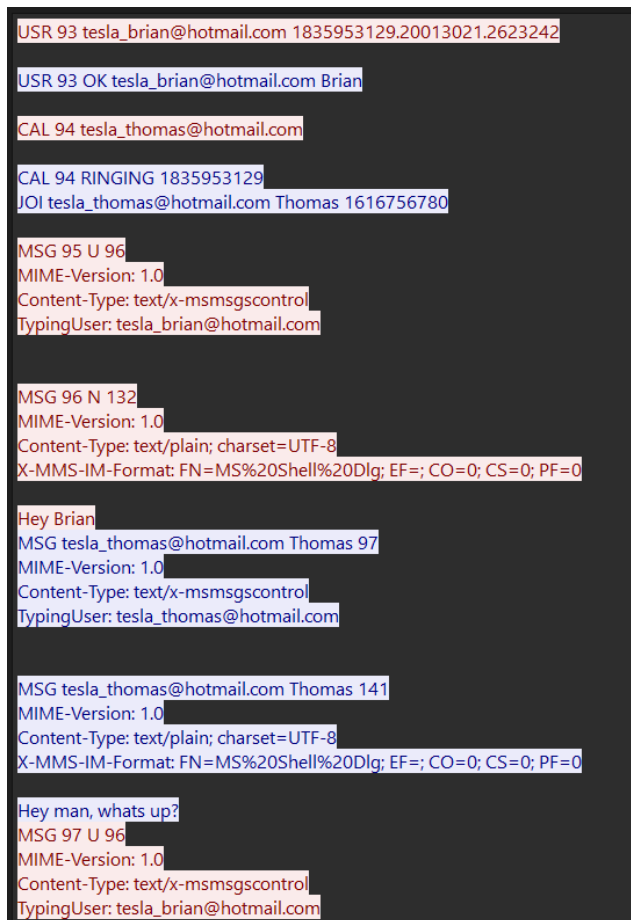
Work: compare these two capture files and state why *student1*'s machine is not online

Question

1. What kind of protocol is used?
2. Who are the chatters?
3. What do they say about you (sysadmin)?

TIP: your chat can be monitored by network admin

1. El protocolo utilizado para la comunicación es MSNMS, que es el protocolo de Microsoft MSN Messenger.
2. Las personas que participan en la conversación son Brian y Thomas, como se puede ver en la siguiente imagen:



The image shows a network capture of MSN Messenger traffic. It includes several messages and their corresponding metadata. The messages are as follows:

- USR 93 tesla_brian@hotmail.com 1835953129.20013021.2623242
- USR 93 OK tesla_brian@hotmail.com Brian
- CAL 94 tesla_thomas@hotmail.com
- CAL 94 RINGING 1835953129
- JOI tesla_thomas@hotmail.com Thomas 1616756780
- MSG 95 U 96
- MIME-Version: 1.0
- Content-Type: text/x-msmsgscontrol
- TypingUser: tesla_brian@hotmail.com
- MSG 96 N 132
- MIME-Version: 1.0
- Content-Type: text/plain; charset=UTF-8
- X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0
- Hey Brian
- MSG tesla_thomas@hotmail.com Thomas 97
- MIME-Version: 1.0
- Content-Type: text/x-msmsgscontrol
- TypingUser: tesla_thomas@hotmail.com
- MSG tesla_thomas@hotmail.com Thomas 141
- MIME-Version: 1.0
- Content-Type: text/plain; charset=UTF-8
- X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0
- Hey man, whats up?
- MSG 97 U 96
- MIME-Version: 1.0
- Content-Type: text/x-msmsgscontrol
- TypingUser: tesla_brian@hotmail.com

3. Las personas involucradas en la conversación mencionan que escucharon que el nuevo administrador es un idiota. Uno de ellos sugiere hackear un servidor para molestar al administrador y el otro responde diciendo que le parece una buena idea.

```
Hey man, whats up?
MSG 97 U 96
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_brian@hotmail.com

MSG 98 U 96
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_brian@hotmail.com

MSG 99 N 178
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0

Not much, did you hear about the new IT guy they hired?
MSG tesla_thomas@hotmail.com Thomas 97
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_thomas@hotmail.com

MSG tesla_thomas@hotmail.com Thomas 156
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0

ohh yea, i hear he is a real jerk
MSG 100 U 96
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_brian@hotmail.com
```

```
I've heard the same
MSG tesla_thomas@hotmail.com Thomas 97
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_thomas@hotmail.com

MSG tesla_thomas@hotmail.com Thomas 97
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_thomas@hotmail.com

MSG tesla_thomas@hotmail.com Thomas 97
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_thomas@hotmail.com

MSG tesla_thomas@hotmail.com Thomas 182
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0

maybe we should try hacking into a server to mess with him?
MSG 104 U 96
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: tesla_brian@hotmail.com
```

maybe we should try hacking into a server to mess with him?

MSG 104 U 96

MIME-Version: 1.0

Content-Type: text/x-msmsgscontrol

TypingUser: tesla_brian@hotmail.com

MSG 105 U 96

MIME-Version: 1.0

Content-Type: text/x-msmsgscontrol

TypingUser: tesla_brian@hotmail.com

MSG 106 N 140

MIME-Version: 1.0

Content-Type: text/plain; charset=UTF-8

X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; CO=0; CS=0; PF=0

sounds good to me