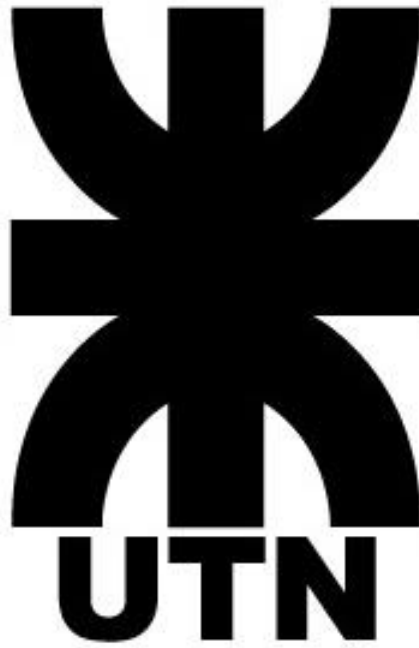


Universidad Tecnológica Nacional



Facultad Regional Delta

Asignatura

Ciclo Lectivo

**Trabajo Práctico N°12 | Seguridad
informática**

Alumno: Gonzalez, Tomas

Profesor: Carrizo, Carlos

Asignatura – Trabajo Practico N° Título		
Gonzalez Tomas	4to año	Ingeniería en Sistemas de información
2024		

Contenido

Consignas3

Resolución4

Asignatura – Trabajo Practico N° Título		
Gonzalez Tomas	4to año	Ingeniería en Sistemas de información
2024		

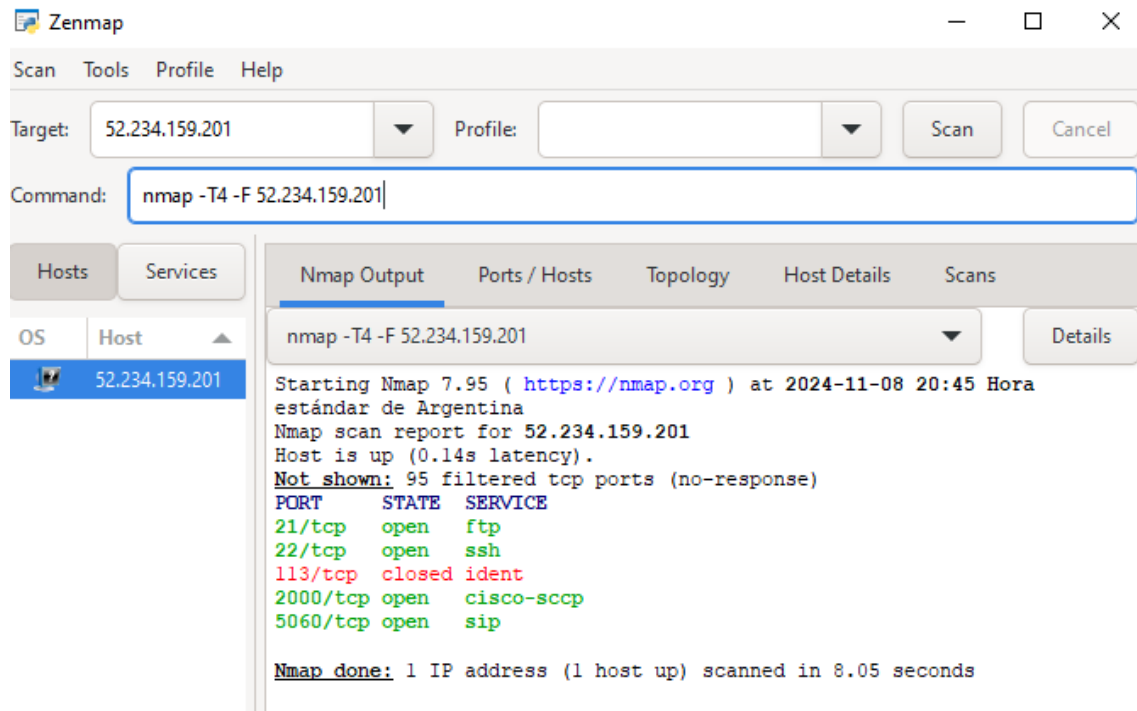
Consignas

1) Desde una PC:

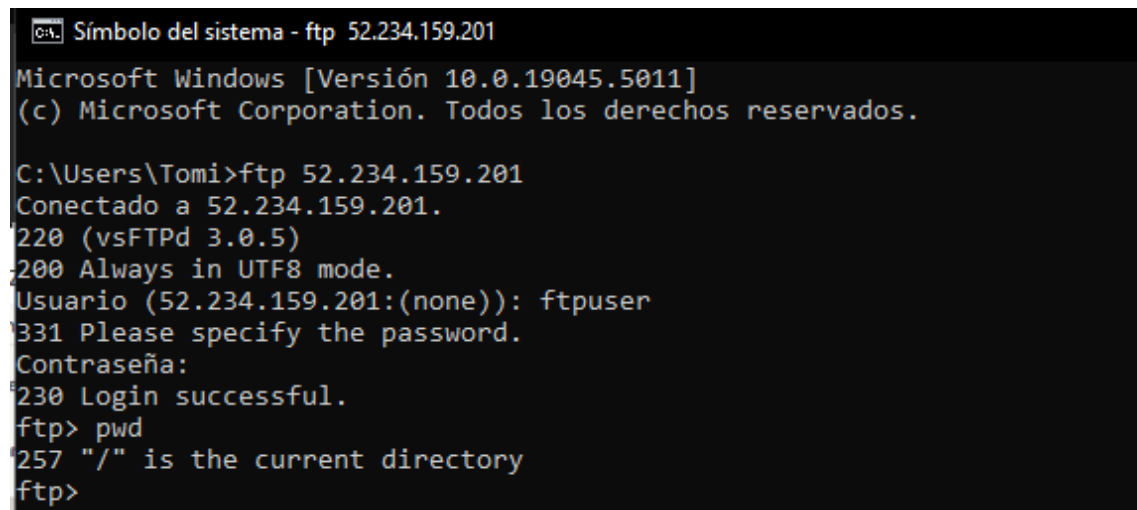
- Utilizando nmap realice un escaneo de puertos TCP a la IP 104.45.137.213 y documente los puertos abiertos.
nmap -T4 -F 52.234.159.201
- Desde línea de comando de Windows conéctese por FTP a la IP anterior y determine qué software es utilizado como Servidor FTP.
Usuario: ftpuser
Password: redes2024
- Monitoree con Wireshark una nueva conexión FTP y luego ejecute el comando: pwd
Identifique usuario y password de la conexión y documéntelo.
- Determine de qué forma puede evitar visualizar el texto plano de los datos de la conexión.

Resolución

Realizo el escaneo de los puertos:



Comienzo el monitoreo en wireshark y luego ejecuto los comandos en CMD:



Analizo lo monitoreado en el wireshark:

*Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 52.234.159.201

No.	Time	Source	Destination	Protocol	Length	Info
727	19.969577	172.30.4.190	52.234.159.201	TCP	66	61712 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
731	20.177257	52.234.159.201	172.30.4.190	TCP	66	21 → 61712 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM=1 WS=128
732	20.177508	172.30.4.190	52.234.159.201	TCP	54	61712 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
741	20.486582	52.234.159.201	172.30.4.190	FTP	74	Response: 220 (vsFTPD 3.0.5)
742	20.513016	172.30.4.190	52.234.159.201	FTP	68	Request: OPTS UTF8 ON
790	20.702305	52.234.159.201	172.30.4.190	TCP	60	21 → 61712 [ACK] Seq=21 Ack=15 Win=64256 Len=0
791	20.702305	52.234.159.201	172.30.4.190	FTP	80	Response: 200 Always in UTF8 mode.
792	20.749944	172.30.4.190	52.234.159.201	TCP	54	61712 → 21 [ACK] Seq=15 Ack=47 Win=8146 Len=0
1063	27.853506	172.30.4.190	52.234.159.201	FTP	68	Request: USER ftpuser
1103	28.015815	52.234.159.201	172.30.4.190	FTP	88	Response: 331 Please specify the password.
1109	28.060224	172.30.4.190	52.234.159.201	TCP	54	61712 → 21 [ACK] Seq=29 Ack=81 Win=8112 Len=0
1259	32.240242	172.30.4.190	52.234.159.201	FTP	70	Request: PASS redes2024
1262	32.468073	52.234.159.201	172.30.4.190	FTP	77	Response: 230 Login successful.
1263	32.511914	172.30.4.190	52.234.159.201	TCP	54	61712 → 21 [ACK] Seq=45 Ack=104 Win=8089 Len=0
1910	47.442474	172.30.4.190	52.234.159.201	FTP	60	Request: XPWD
1919	47.621347	52.234.159.201	172.30.4.190	FTP	88	Response: 257 "/" is the current directory
1920	47.663141	172.30.4.190	52.234.159.201	TCP	54	61712 → 21 [ACK] Seq=51 Ack=138 Win=8055 Len=0

Se observa marcado en celeste el usuario y la contraseña de la conexión.

Para que no se pueda determinar el contenido del texto plano, se debería encriptar esa información sensible, utilizando algún protocolo como por ejemplo SFTP.