

Hito 3 - Final

Evaluación de Seguridad en una Red
Insegura: De las Malas Prácticas a las
Mejores Soluciones

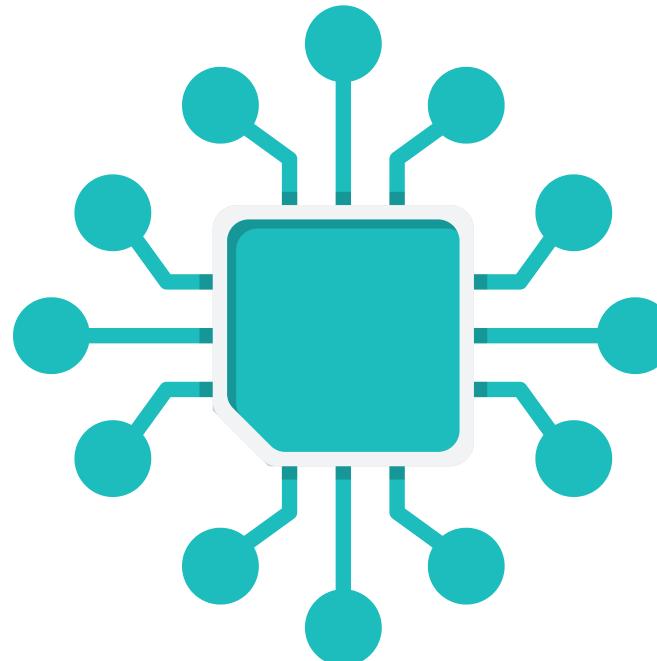
Grupo C

Docente: Juan Ignacio Iturbe

Redes Computacionales / Redes de Comunicación



Agenda



Parte 1: Equipo	03	Parte 4: Simulación y riesgos con Wireshark	09
Parte 2: Cambios realizados	04	Parte 5: Vulnerabilidades y Propuestas	16
Parte 3: Simulación en Vivo	08	Parte 6: Incidentes de seguridad	21



Grupo C

Equipo

Stephan Paul PROJECT MANAGER

- Centralizar la planificación general del proyecto.
- Asegurarse de que cada integrante tenga claras sus tareas, plazos y responsabilidades.
- Preparar y supervisar la Carta Gantt.

Benjamín Zúñiga PLANNING & RISK ANALYST

- Identificar y documentar riesgos y vulnerabilidades presentes en la red.
- Reconocer y proponer posibles soluciones para mitigar los posibles riesgos de seguridad dentro de la red.

Bastián Olea Díaz DOCUMENTATION LEAD

- Mantener registros detallados de configuración, topología y comandos usados.
- Redactar informes técnicos con procedimientos, resultados y análisis de las conexiones..
- Garantizar claridad, precisión y estructura en la documentación.
- Incluir diagramas, capturas y descripciones para facilitar la comprensión en Cisco Packet Tracer.

William Jiménez DOCUMENTATION LEAD

Reinaldo Pacheco NETWORK DESIGNER

- Proponer el esquema inicial de la red en Packet Tracer (topología, interconexión, dispositivos).
- Definir aspectos técnicos de IPs, rangos y servidores
- Trabajar en conjunto a Packet Tracer Admin para asegurar e identificar posibles riesgos o vulnerabilidades en la red.

Byron Caices Lima NETWORK DESIGNER

Matías Cortés PACKET TRACER ADMIN

- Implementar y refinar el esquema de red propuesto por los Network Designer.
- Encargarse de las configuraciones, asignaciones de servidores y pruebas de conectividad básicas.
- Generar capturas de tráfico de red.

Nicolás Alarcón PACKET TRACER ADMIN



RECAPITULACIÓN

Cambios
realizados respecto
a hitos anteriores

Modificación en la Carta Gantt

Debido al cambio de fecha de la presentación del Hito 2, el inicio de la elaboración del Hito 3 sufrió una leve modificación

Hito 2: Avance Intermedio								
Evaluación de avances en relación al anteproyecto	Documentation Lead Project Manager	29/03/2025	09/04/2025					
Ajustes en el diseño de la red según retroalimentación inicial	Network Designer Packet Tracer Admin	29/03/2025	06/04/2025					
Revisión de conectividad y configuración en Packet Tracer	Packet Tracer Admin Planning & Risk Analyst	24/03/2025	06/04/2025					
Análisis preliminar de captura de tráfico con Wireshark	Packet Tracer Admin Planning & Risk Analyst	29/03/2025	09/04/2025					
INFORME FINAL								
Contrastar lo definido en el anteproyecto con lo realizado	Project Manager Documentation Lead	14/04/2025	21/04/2025					
Identificar problemas de seguridad en la red	Network Designer Packet Tracer Admin	10/04/2025	14/04/2025					
Investigar los impactos de las vulnerabilidades	Planning & Risk Analyst	10/04/2025	14/04/2025					
Proponer mejoras de seguridad	Network Designer	10/04/2025	14/04/2025					
Posibles incidentes de seguridad	Packet Tracer Admin	10/04/2025	14/04/2025					
Indicar las apreciaciones sobre el presente trabajo	Documentation Lead	14/04/2025	21/04/2025					

172.16.1.10



172.16.1.11



Server-PT

Descripción de diseño de red e implementación final en PT

Laptop-PT
Laptop0

Laptop-PT
Laptop1

Laptop-PT
Laptop2

6.1.1

ON
outer0

Server-PT
ServerSMTP/IMAP

Server-PT
ServerDNS

172.16.1.12



Server-PT

ServerSMTP/IMAP

172.16.1.13



Server-PT

ServerDNS

2960-24TT
Switch2

PC-PT
PC4

PC-PT
PC5

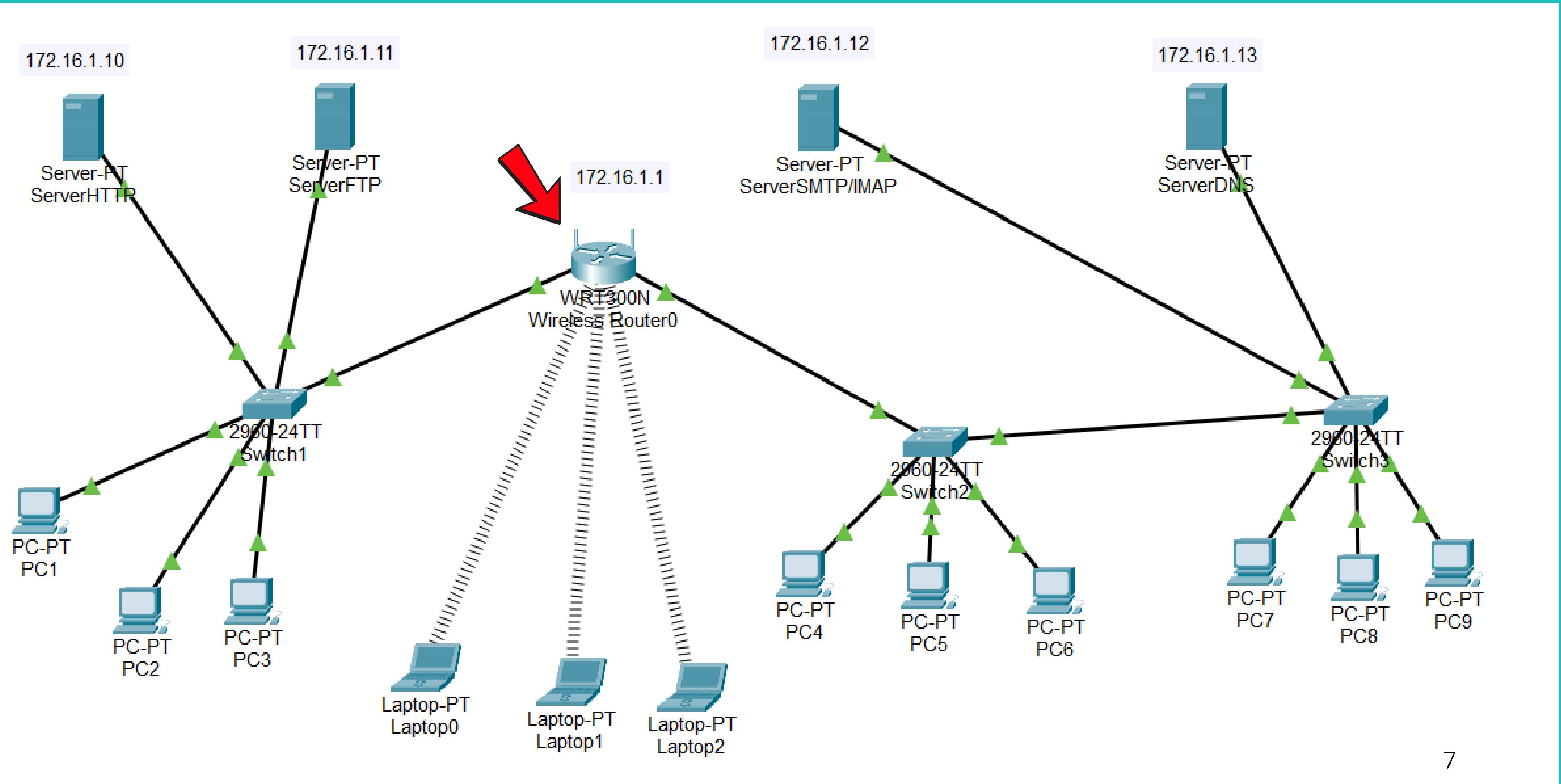
PC-PT
PC6

PC-PT
PC7

PC-PT
PC8

PC-PT
PC9

2960-24TT
Switch3



Simulación en vivo

Destination	Protocol	Length	Info
127.0.0.1	FTP-DA...	128	FTP Data: 84 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	126	FTP Data: 82 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	137	FTP Data: 93 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	112	FTP Data: 68 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	117	FTP Data: 73 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	117	FTP Data: 73 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	137	FTP Data: 93 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	114	FTP Data: 70 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	113	FTP Data: 69 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	114	FTP Data: 70 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	112	FTP Data: 68 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	137	FTP Data: 93 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	124	FTP Data: 80 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	122	FTP Data: 78 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	130	FTP Data: 86 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	139	FTP Data: 95 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	131	FTP Data: 87 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	208	FTP Data: 164 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	148	FTP Data: 104 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	151	FTP Data: 107 bytes (PASV) (MLSD)
127.0.0.1	FTP-DA...	151	FTP Data: 107 bytes (PASV) (MLSD)
127.0.0.1	FTP	70	Response: 226 Operation successful
127.0.0.1	FTP	141	Response: 220-FileZilla Server 1.10.1
127.0.0.1	FTP	58	Request: USER Bastian
127.0.0.1	FTP	79	Response: 331 Please, specify the password.
127.0.0.1	FTP	59	Request: PASS pass1234
127.0.0.1	FTP	67	Response: 230 Login successful.
127.0.0.1	FTP	51	Request: CWD /
127.0.0.1	FTP	72	Response: 250 CWD command successful
127.0.0.1	FTP	52	Request: TYPE I
127.0.0.1	FTP	63	Response: 200 Type set to I
127.0.0.1	FTP	50	Request: PASV
127.0.0.1	FTP	91	Response: 227 Entering Passive Mode (127,0,0,1,253,219)
127.0.0.1	FTP	63	Request: RETR logoZeus.jpg
127.0.0.1	FTP	79	Response: 150 About to start data transfer.
127.0.0.1	FTP-DA...	5515	FTP Data: 5471 bytes (PASV) (RETR logoZeus.jpg)
127.0.0.1	FTP	70	Response: 226 Operation successful

bits), 5515 bytes captured (44120 bits) on interface \Device\NPF_Loopback, id 08c0 07 60 50 02 86 8b
08d0 2b 26 fd 77 8b 77
08e0 ef 97 20 4b 71 56
08f0 d0 4e 21 81 23 23
0900 ff 00 bd 46 e2 73
0910 0e c3 40 1a 0f af
0920 34 8e 27 f7 48 2e
0930 8c ac 45 d7 0f 34
0940 85 cd d9 7d bf b9
0950 1e 6a 4a b9 a9 2a
0960 2a e6 a4 ab 9a 92
0970 92 ae 6a 4a b9 a9
0980 21 8c 41 03 16 32
0990 07 2d 33 14 71 ff
09a0 6a 95 cb b0 64 01
09b0 ca 14 c4 31 d4 3a

0.0.1, Dst: 127.0.0.1
Port: 64987, Dst Port: 64988, Seq: 1, Ack: 1, Len: 5471

Análisis de tráfico y exposición de riesgos en el protocolo FTP



Autenticación -Análisis de tráfico

No.	Time	Source	Destination	Protocol	Length	Info
15	11.636184	127.0.0.1	127.0.0.1	FTP	141	Response: 220-FileZilla Server 1.10.1
17	11.653633	127.0.0.1	127.0.0.1	FTP	58	Request: USER Bastian
23	11.653901	127.0.0.1	127.0.0.1	FTP	79	Response: 331 Please, specify the password.
25	11.653980	127.0.0.1	127.0.0.1	FTP	59	Request: PASS pass1234
31	11.696748	127.0.0.1	127.0.0.1	FTP	67	Response: 230 Login successful.
33	11.700977	127.0.0.1	127.0.0.1	FTP	49	Request: PWD
37	11.701319	127.0.0.1	127.0.0.1	FTP	75	Response: 257 "/" is current directory.

File Transfer Protocol

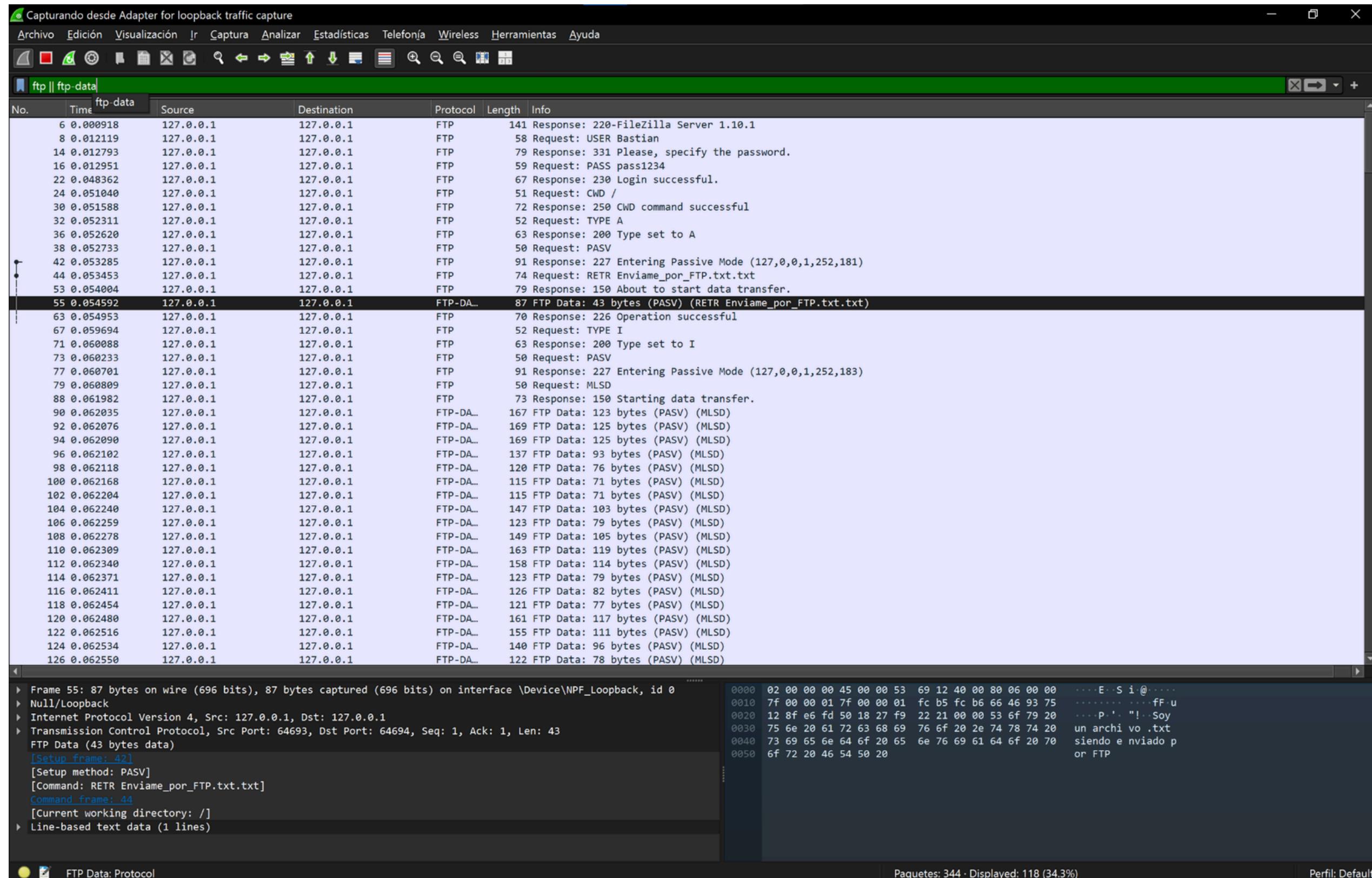
PASSWORD (PASS)

The argument field is a Telnet string specifying the user's password. This command must be immediately preceded by the user name command, and, for some sites, completes the user's identification for access control. Since password information is quite sensitive, it is desirable in general to "mask" it or suppress typeout. It appears that the server has no foolproof way to achieve this. It is therefore the responsibility of the user-FTP process to hide the sensitive password information.

Comandos usados:

1. **USER**
2. **PASS**

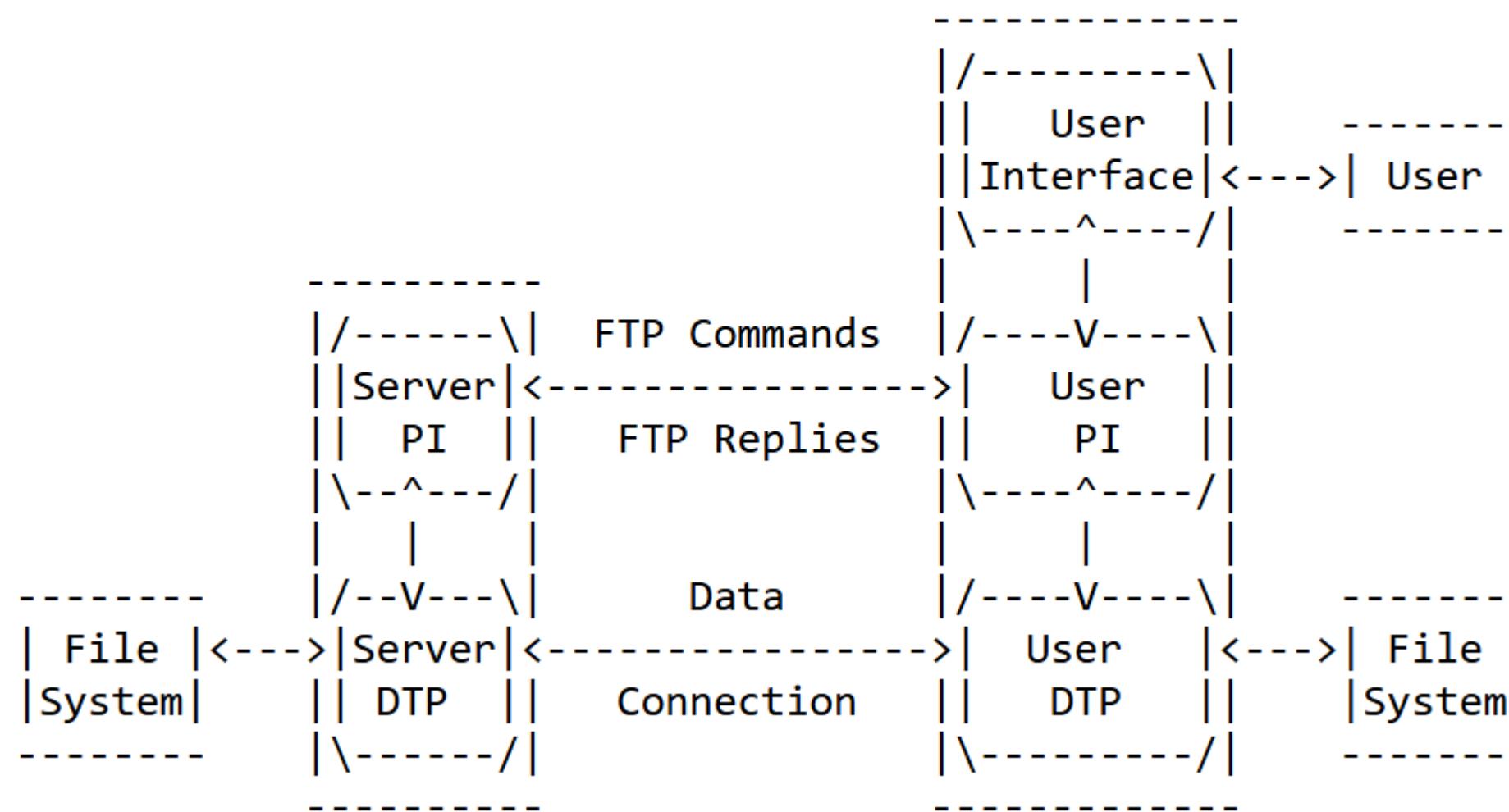
Transferencia txt - Análisis de tráfico



FTP y FTP-DATA -Análisis de tráfico

2.3. THE FTP MODEL

With the above definitions in mind, the following model (shown in Figure 1) may be diagrammed for an FTP service.



Interacción TCP – Análisis de tráfico

3 0.000140	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
6 0.000921	127.0.0.1	127.0.0.1	FTP	141 Response: 220-FileZilla Server 1.10.1
7 0.000950	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=1 Ack=98 Win=2619648 Len=0
8 0.011348	127.0.0.1	127.0.0.1	FTP	58 Request: USER Bastian
9 0.011380	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=98 Ack=15 Win=2619648 Len=0
14 0.011697	127.0.0.1	127.0.0.1	FTP	79 Response: 331 Please, specify the password.
15 0.011712	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=15 Ack=133 Win=2619648 Len=0
16 0.011750	127.0.0.1	127.0.0.1	FTP	59 Request: PASS pass1234
17 0.011764	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=133 Ack=30 Win=2619648 Len=0
22 0.033700	127.0.0.1	127.0.0.1	FTP	67 Response: 230 Login successful.
23 0.033721	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=30 Ack=156 Win=2619392 Len=0
24 0.037814	127.0.0.1	127.0.0.1	FTP	51 Request: CWD /
25 0.037850	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=156 Ack=37 Win=2619648 Len=0
30 0.038190	127.0.0.1	127.0.0.1	FTP	72 Response: 250 CWD command successful
31 0.038203	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=37 Ack=184 Win=2619392 Len=0
32 0.038336	127.0.0.1	127.0.0.1	FTP	49 Request: PWD
33 0.038356	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=184 Ack=42 Win=2619648 Len=0
36 0.038606	127.0.0.1	127.0.0.1	FTP	75 Response: 257 "/" is current directory.
37 0.038615	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=42 Ack=215 Win=2619392 Len=0
38 0.039073	127.0.0.1	127.0.0.1	FTP	52 Request: TYPE A
39 0.039099	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=215 Ack=50 Win=2619648 Len=0
42 0.039238	127.0.0.1	127.0.0.1	FTP	63 Response: 200 Type set to A
43 0.039250	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=50 Ack=234 Win=2619392 Len=0
44 0.039301	127.0.0.1	127.0.0.1	FTP	50 Request: PASV
45 0.039321	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=234 Ack=56 Win=2619648 Len=0
48 0.039667	127.0.0.1	127.0.0.1	FTP	91 Response: 227 Entering Passive Mode (127,0,0,1,235,254)
49 0.039683	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=56 Ack=281 Win=2619392 Len=0
50 0.039808	127.0.0.1	127.0.0.1	FTP	74 Request: RETR Enviame por FTP.txt.txt
51 0.039828	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=281 Ack=86 Win=2619648 Len=0
57 0.040148	127.0.0.1	127.0.0.1	FTP	79 Response: 150 About to start data transfer.
60 0.040267	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=86 Ack=316 Win=2619392 Len=0
69 0.041140	127.0.0.1	127.0.0.1	FTP	70 Response: 226 Operation successful
70 0.041165	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=86 Ack=342 Win=2619392 Len=0
77 60.047360	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [FIN, ACK] Seq=86 Ack=342 Win=2619392 Len=0
78 60.047454	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [ACK] Seq=342 Ack=87 Win=2619648 Len=0
80 60.048129	127.0.0.1	127.0.0.1	TCP	44 21 → 60413 [FIN, ACK] Seq=342 Ack=87 Win=2619648 Len=0
82 60.048290	127.0.0.1	127.0.0.1	TCP	44 60413 → 21 [ACK] Seq=87 Ack=342 Win=2619392 Len=0

Autenticación (con cifrado) - Análisis de tráfico

tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	59506 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000056	127.0.0.1	127.0.0.1	TCP	56	21 → 59506 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000093	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
6	0.000794	127.0.0.1	127.0.0.1	FTP	141	Response: 220-FileZilla Server 1.10.1
7	0.000819	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=1 Ack=98 Win=2619648 Len=0
8	0.000908	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH TLS
9	0.000936	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=98 Ack=11 Win=2619648 Len=0
10	0.001742	127.0.0.1	127.0.0.1	FTP	80	Response: 234 Using authentication type TLS.
11	0.001762	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=11 Ack=134 Win=2619648 Len=0
14	0.002314	127.0.0.1	127.0.0.1	TLSv1.3	471	Client Hello
15	0.002336	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=134 Ack=438 Win=2619136 Len=0
16	0.004642	127.0.0.1	127.0.0.1	TLSv1.3	236	Server Hello
17	0.004678	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=438 Ack=326 Win=2619392 Len=0
18	0.004703	127.0.0.1	127.0.0.1	TLSv1.3	50	Change Cipher Spec
19	0.004719	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=438 Ack=332 Win=2619392 Len=0
20	0.005112	127.0.0.1	127.0.0.1	TLSv1.3	100	Application Data
21	0.005132	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=438 Ack=388 Win=2619392 Len=0
22	0.005155	127.0.0.1	127.0.0.1	TLSv1.3	474	Application Data
23	0.005171	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=438 Ack=818 Win=2618880 Len=0
24	0.005193	127.0.0.1	127.0.0.1	TLSv1.3	144	Application Data
25	0.005209	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=438 Ack=918 Win=2618880 Len=0
26	0.005229	127.0.0.1	127.0.0.1	TLSv1.3	118	Application Data
27	0.005249	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=438 Ack=992 Win=2618624 Len=0
0000	02 00 00 00 45 00 00 e8 73 ea 40 00 80 06 00 00	... E ... s @ ...	1.3	50	Change Cipher Spec	
0010	7f 00 00 01 7f 00 00 01 00 15 e8 72 96 54 7f 29	... r.T.)	1.3	44	21 → 59506 [ACK] Seq=992 Ack=444 Win=2619136 Len=0	
0020	68 bb f8 76 50 18 27 f7 d1 56 00 00 16 03 03 00	h.vP' V.	1.3	118	Application Data	
0030	bb 02 00 00 b7 03 03 67 4c bb fa 7b 4a f0 87 ed	g L {J	1.3	44	21 → 59506 [ACK] Seq=992 Ack=518 Win=2619136 Len=0	
0040	a5 a7 e2 d3 95 a8 52 1f 47 d6 46 c1 30 ba 7e 64	R G F ~d	1.3	20	Application Data	
0050	5f 87 61 aa f0 f8 20 21 61 d3 91 b8 1e 07 31	_a! a~ 1	1.3	0000	02 00 00 00 45 00 00 60 73 ee 40 00 80 06 00 00	
0060	20 6a ea e4 40 b7 a0 61 63 6b bd 40 44 1b a7 2e	@ a ck @D	1.3	0010	7f 00 00 01 7f 00 00 01 00 15 e8 72 96 54 7f ef	
0070	85 e7 3e 4c fd 5d 8d 92 13 02 00 00 6f 00 2b 00	>Lo o+	1.3	0020	68 bb f8 76 50 18 27 f7 0a 6f 00 00 17 03 03 00	
0080	02 03 04 00 33 00 65 00 18 00 61 04 17 72 7c a6	3 e a r	1.3	0030	33 2e de ef a9 02 95 40 8e be 5f c8 6b 81 c6 0c	
0090	e9 61 91 ba b4 00 d3 c4 f2 80 04 ae 34 7c 56 e5	a 4 V	1.3	0040	6d 72 41 cb 52 2c 95 db a2 6f 07 ca b5 55 fa c5	
00a0	71 68 df b5 20 4d 8f e6 3b 3e 9a fd f7 6a c3 72	q M ;> jr	1.3	0050	mrA R o U	
00b0	ce 39 fc f1 84 81 e5 22 7c 2d a0 af 08 cc 82 08	9 -	1.3	0060	' k ^ 7X AJ	
00c0	52 d8 06 e3 d1 7e 33 87 93 f4 6c c4 fb b1 42 41	R ~3 l BA	1.3	0070	88 41 4a cd	
00d0	b6 35 47 85 1b f7 6a 6e b3 34 bc ff 72 2c 0d 53	5G jn 4 r, S	1.3	0080	00 00 00 00 45 00 00 32 73 e2 40 00 80 06 00 00	
00e0	5b 65 e4 97 ee e2 08 69 9c e2 a7 8c	[e i]	1.3	0090	... E s @ ...	
				0010	7f 00 00 01 7f 00 00 01 e8 72 00 15 68 bb f6 c1	
				0020	96 54 7f 05 50 18 27 f9 1d 19 00 00 41 55 54 48	
				0030	20 54 4c 53 0d 0a TLS	

Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_Loopback, id 0

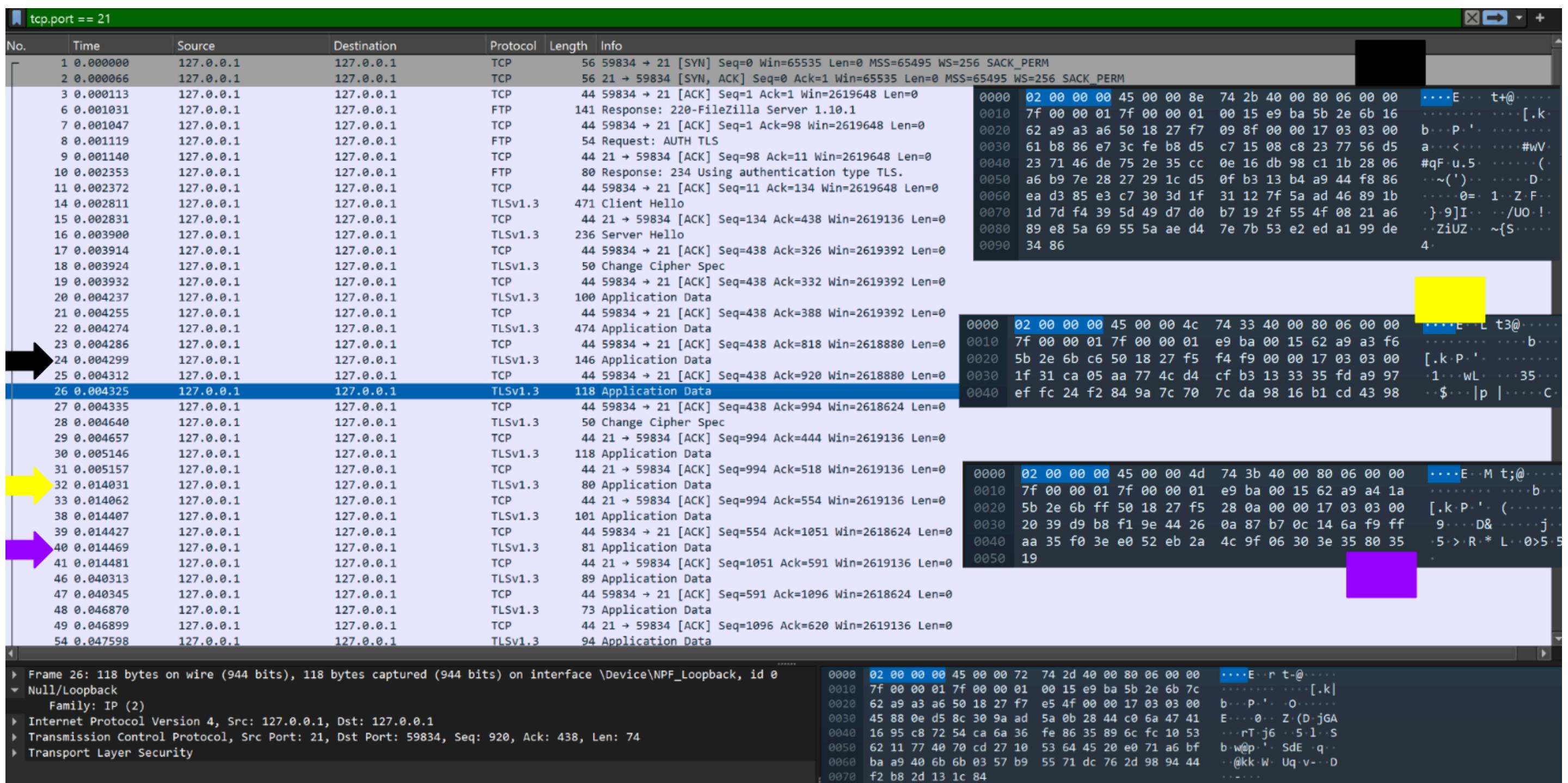
Null/Loopback

Family: IP (2)

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

16 20 22 14

Transferencia txt (con cifrado) - Análisis de tráfico

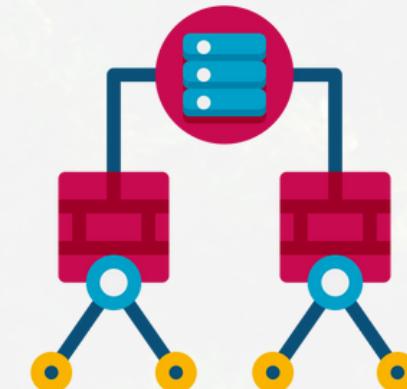
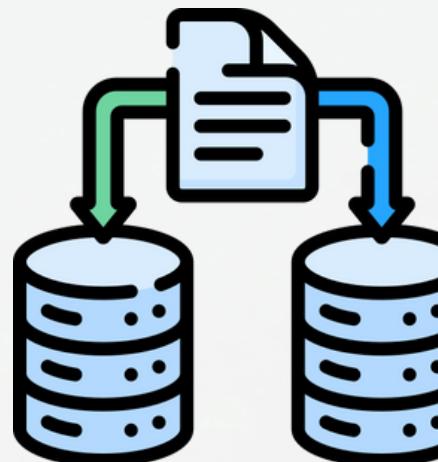




Identificación de problemas y propuestas de seguridad

Problemas identificados

1. Intercepción de datos por tráfico no cifrado
2. Spoofing por falta de cifrado IP
3. Falta de control de acceso para los dispositivos
4. Uso de protocolos inseguros
5. Riesgo de propagación de malware y ransomware
6. Falta de segmentación de red
7. Ausencia de filtrado de tráfico de red
8. Falta de redundancia en servicios críticos

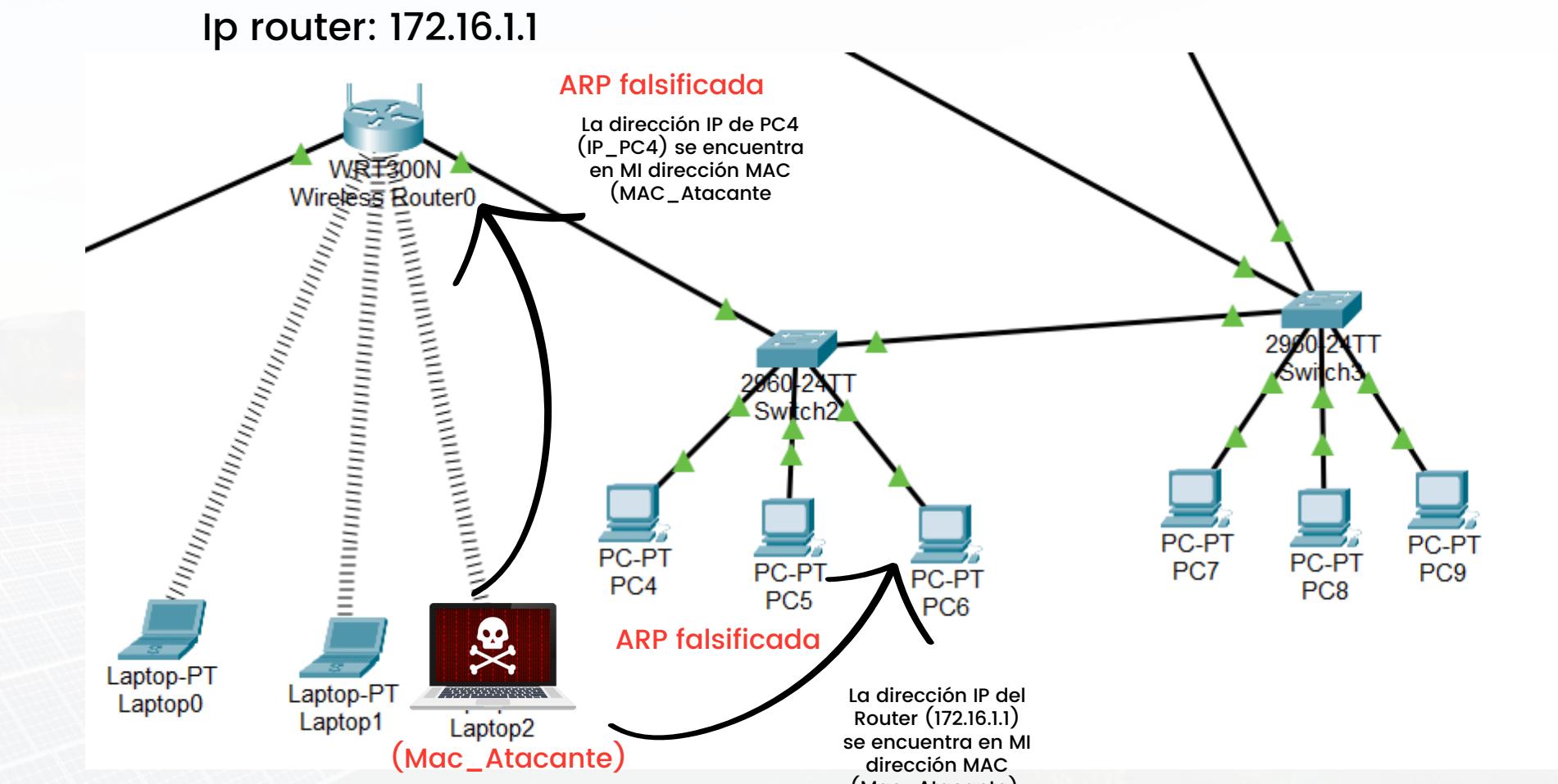


Problemas

2. Spoofing por falta de cifrado IP

La red no cifra los paquetes IP por lo que un atacante podría suplantar una dirección IP o una dirección MAC para redireccionar datos a su dispositivo:

1. El atacante se conecta a través de un switch o directamente al Router a través de un dispositivo
2. Envía una ARP falsificada al router suplantando la dirección IP de otro dispositivo
3. Envía UNA ARP falsificada al PC con la dirección IP del router



Propuesta de mejora

- Habilitar Dynamic ARP Inspection (DAI)
- Configurar Seguridad de Puertos



7. Ausencia de Filtrado de Tráfico de Red

1. Next-Gen Firewall (NGFW)

Inspecciona tráfico

- Se configura para analizar tráfico como:
- HTTP/HTTPS → inspección de contenido
- DNS → bloqueo de sitios maliciosos
- Aplicaciones específicas → permitir o denegar

En la red **no existe un filtrado de tráfico** que controle las comunicaciones permitidas entre segmentos de red

Cualquier dispositivo podría enviar y recibir peticiones hacia un puerto específico

Facilita ataques de escaneo, explotación de vulnerabilidades o ataques de denegación de servicios (DoS).

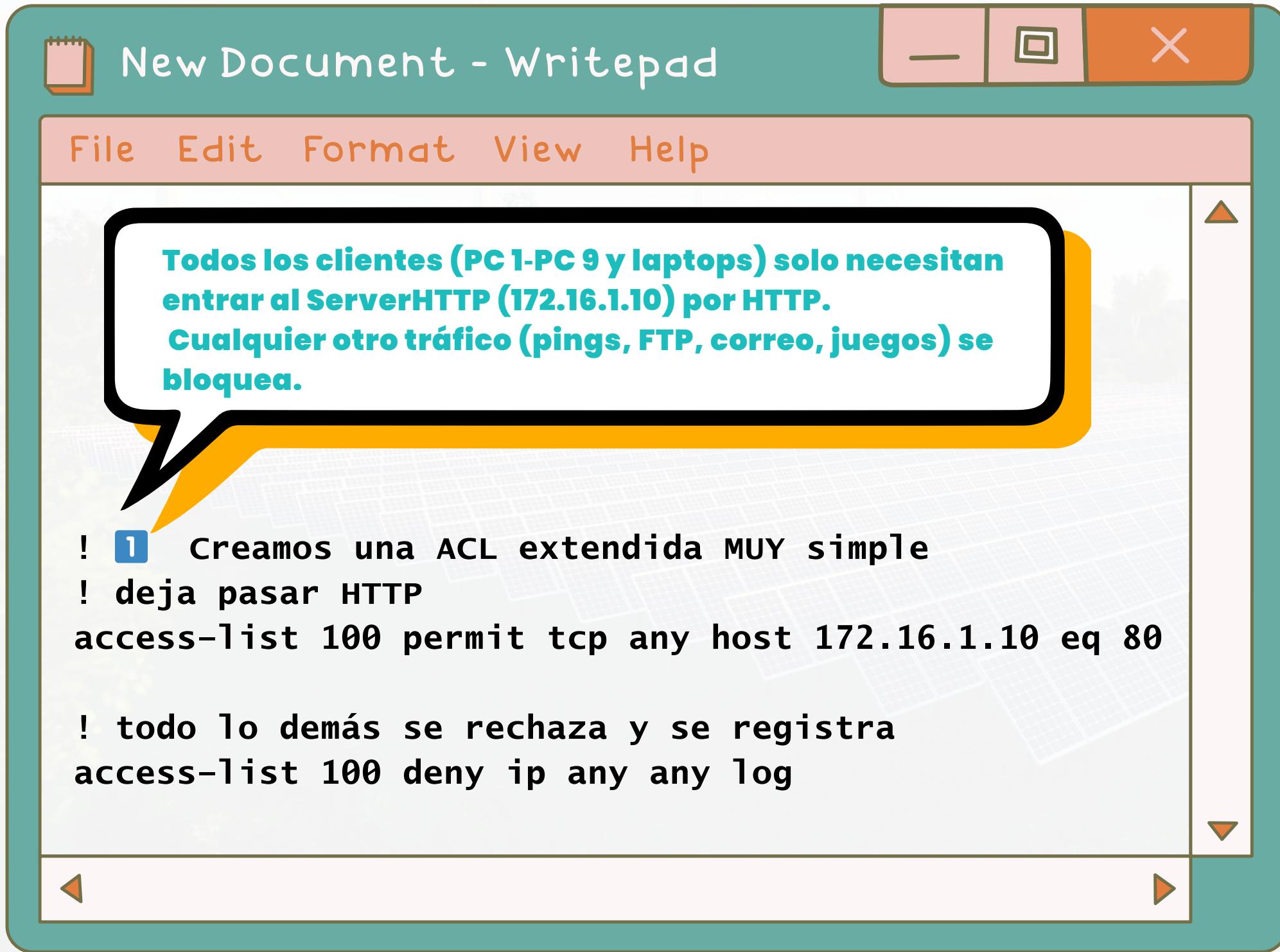
2. ACLs restrictivas en routers/switches

Definen explícitamente qué IPs/puertos están permitidos; todo lo demás queda denegado por defecto

3. Proxies y gateways de aplicación

Obligan a que el tráfico pase por un intermediario (proxy) que filtra, inspecciona y controla las peticiones. No hay comunicación directa entre cliente y destino externo.

2. ACLs restrictivas en routers/switches



New Document - Writepad

File Edit Format View Help

Todos los clientes (PC 1-PC 9 y laptops) solo necesitan entrar al ServerHTTP (172.16.1.10) por HTTP. Cualquier otro tráfico (pings, FTP, correo, juegos) se bloquea.

! 1 Creamos una ACL extendida MUY simple
! deja pasar HTTP
access-list 100 permit tcp any host 172.16.1.10 eq 80

! todo lo demás se rechaza y se registra
access-list 100 deny ip any any log

¿Qué hace?

- Controla el tráfico entre dispositivos a nivel de IP y puerto (capas 3 y 4). Solo permite lo definido (HTTP al servidor), todo lo demás se bloquea y registra.

¿Cómo se implementa?

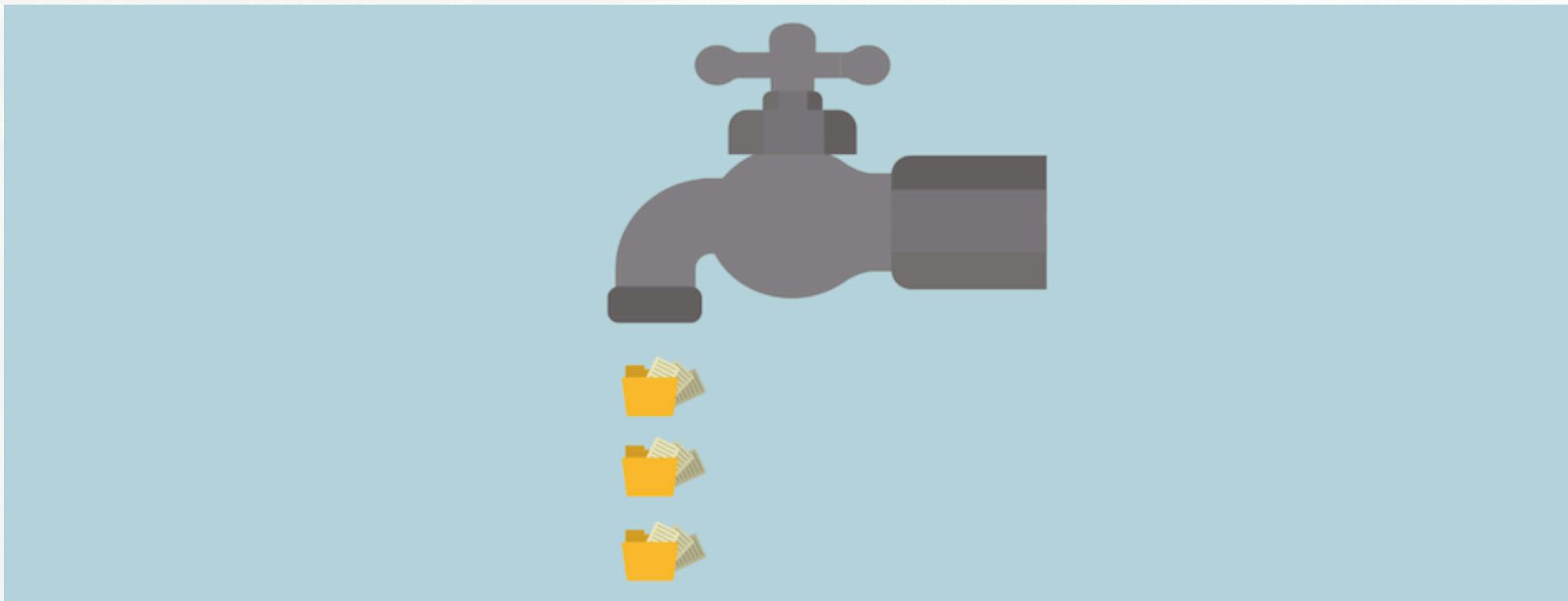
- Se aplica en routers o switches capa 3, usando listas de acceso (ACLs).
- Esta es una ACL extendida porque permite filtrar por protocolo y puerto.

Incidentes de seguridad posibles en caso de no aplicar medidas de seguridad



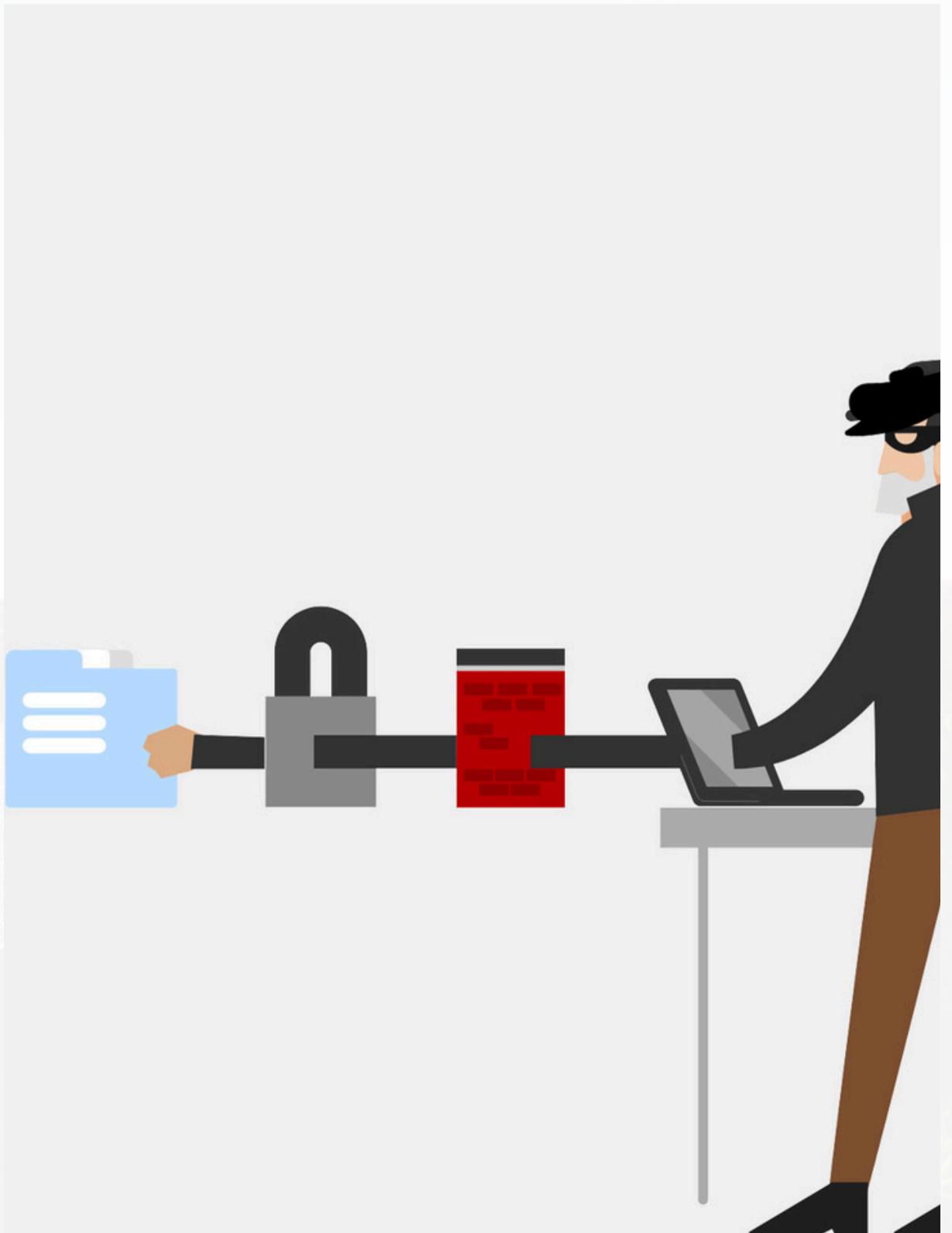
! Filtración de información sensible

- FTP transmite datos, incluyendo credenciales y archivos, en texto claro. Esto permite que un atacante con acceso a la red pueda interceptar y visualizar información crítica sin necesidad de técnicas avanzadas.
- La falta de cifrado convierte al protocolo FTP en una vía común de filtración accidental de datos sensibles.



!!Acceso no autorizado al sistema

- El protocolo FTP carece de medidas de seguridad modernas, como cifrado o autenticación fuerte. Las credenciales viajan en texto claro, lo que facilita su interceptación por parte de atacantes.
- Además, muchos servidores FTP quedan expuestos con cuentas por defecto o configuraciones inseguras, como usuarios anónimos habilitados o contraseñas débiles. Estas prácticas permiten que terceros obtengan acceso no autorizado al sistema, comprometiendo la integridad y confidencialidad de los datos almacenados.



Incidentes de seguridad relacionados a FTP

BBC

Home News Sport Business Innovation Culture Arts Travel Earth | Audio Video Live

Facebook confirms millions of phone numbers exposed

5 September 2019

Share Save



INDUSTRY NEWS • 1 min read

Hackers breach NASA; employee data may have been exposed

Filip TRUĀ December 20, 2018

Promo Protect all your devices, without slowing them down. Free 30-day trial.



After security breaches in 2014 and 2016, the US National Aeronautics and Space Administration (NASA)

RIGHT NOW

TOP POSTS

How to Protect Your WhatsApp from Hackers and Scammers

How to Protect Your WhatsApp from Hackers and Scammers Key Settings and Best Practices April 03, 2025 • 8 min read

Outpacing Cyberthreats: Bitdefender Together with Scuderia Ferrari HP in 2025

Outpacing Cyberthreats: Bitdefender Together with Scuderia Ferrari HP in 2025 March 12, 2025 • 1 min read

Streamjacking Scams On You Leverage CS2 Pro Player Championships to Defraud Gamers

Streamjacking Scams On You Leverage CS2 Pro Player Championships to Defraud Gamers February 20, 2025 • 5 min read

How to Identify and Protect Yourself from Gaming Laptop Scams

How to Identify and Protect Yourself from Gaming Laptop Scams February 11, 2025 • 5 min read

Data Security

Toyota Confirms Exposure of Customer and Employee Data in Data Breach

Toyota has confirmed that its network was breached, resulting in a 240 GB data leak. Learn more about the incident and its implications for the auto manufacturer.

Anuj Mudaliar Assistant Editor - Tech, SWZD August 22, 2024



Spiceworks Community

Want to host a private AI server

hi all, I want to host a private opensource AI server, i've seen videos about llama here host ALL your AI locally i've seen other LLM's ...

Time check: What's your average weekly work hour count in 2025?

Last month, we asked what hours you usually start and end your workday. The majority of us begin our days around 8am, and many of us end

Products Solutions Pricing Resources Customers Login

Free trial Get a demo

w A Verizon Partner Exposed Millions of Customer Accounts

Blog Breaches Resources News

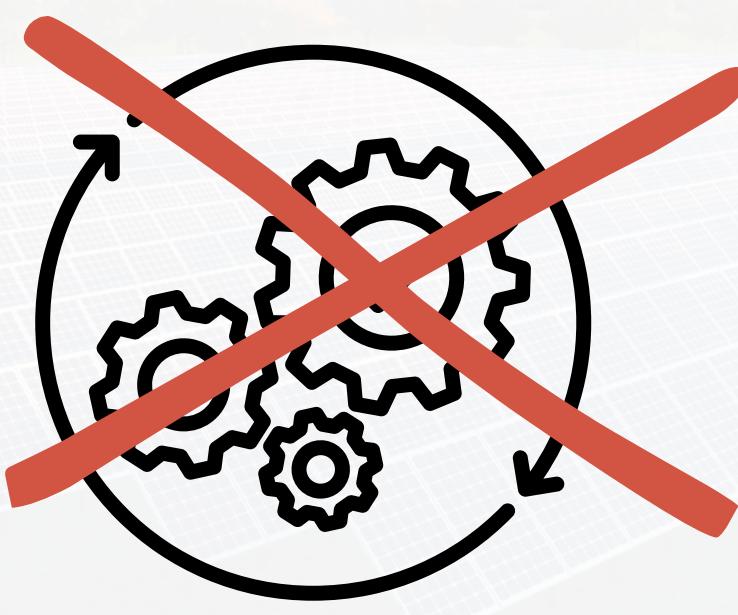
UpGuard Team Published Jul 12, 2017

Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts

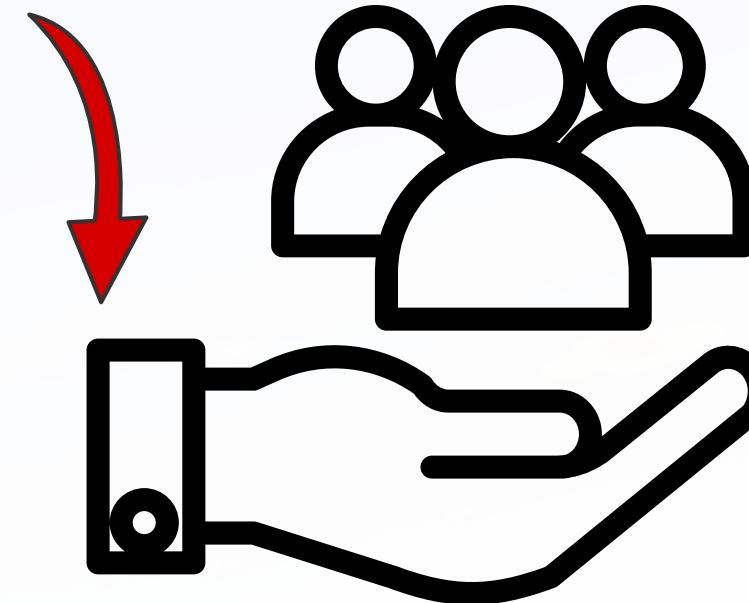
Repercusiones de un ataque cibernético



Pérdidas económicas



Interrupción de operaciones



Pérdida de confianza del cliente



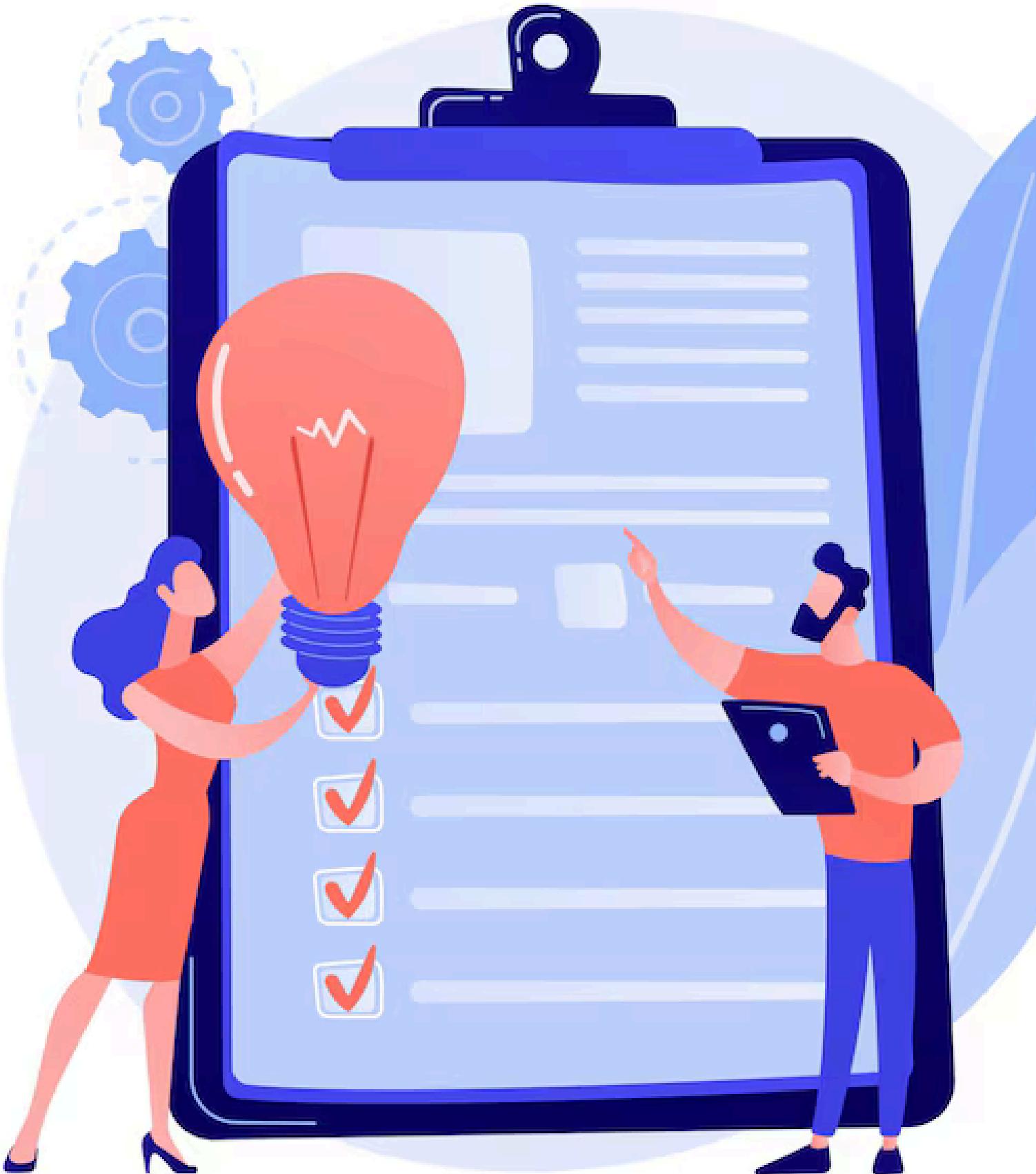
Impacto en la continuidad del negocio

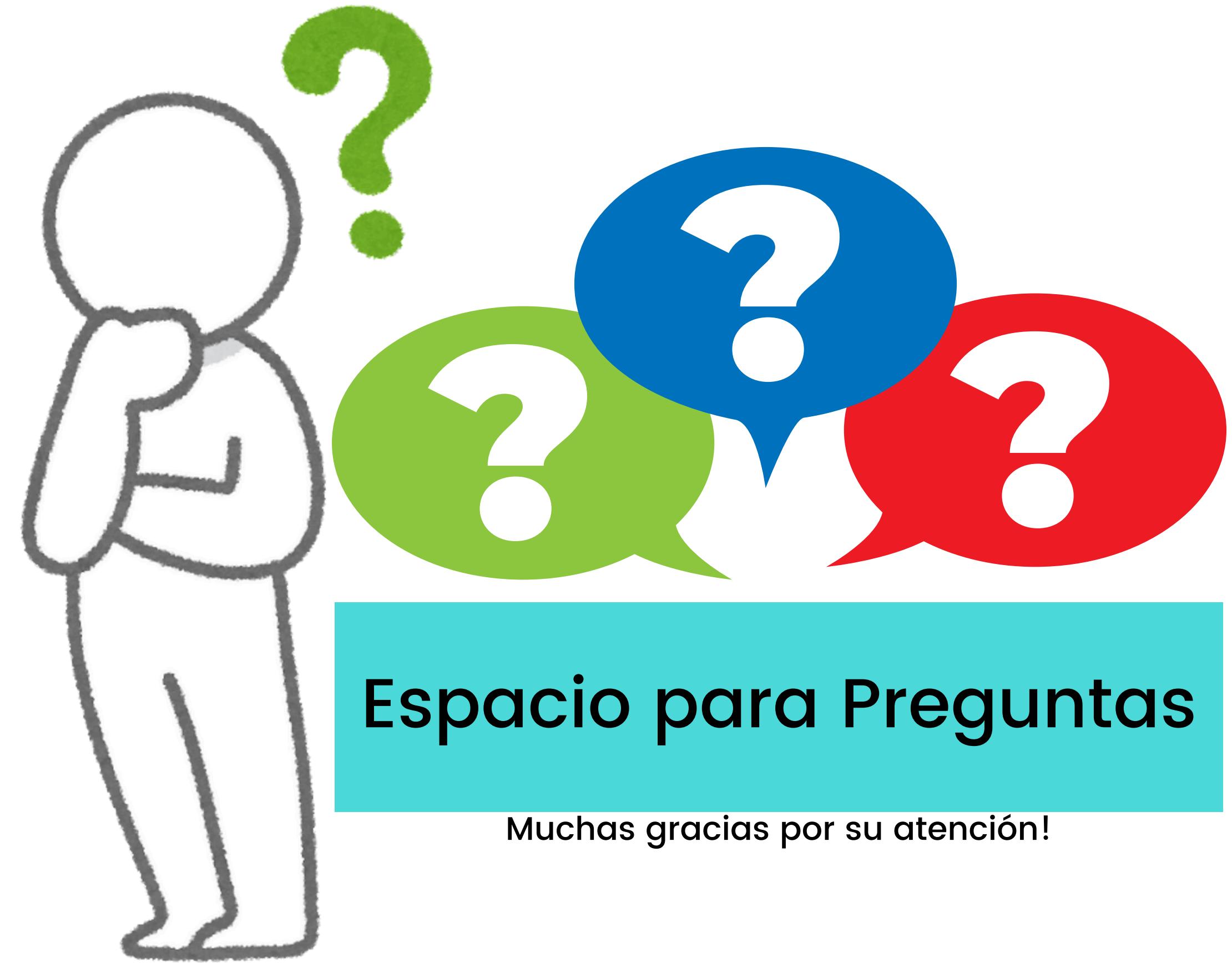


Conclusiones

Conclusiones

- Implementación en Cisco Packet Tracer de requerimientos funcionales para empresa TechMove (servicios DHCP, DNS, SMTP, FTP y HTTP)
- Revisión teórica y práctica de protocolo FTP utilizando herramientas de análisis de tráfico como Wireshark
- Identificación de vulnerabilidades y necesidad de métodos más seguros, como FTPS
- Casos de riesgos de seguridad materializado





Espacio para Preguntas

Muchas gracias por su atención!



Grupo C

Hito 3 - Final

Evaluación de Seguridad en una Red Insegura: De las Malas Prácticas a las Mejores Soluciones

Grupo C

Docente: Juan Ignacio Iturbe

Redes Computacionales / Redes de Comunicación