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

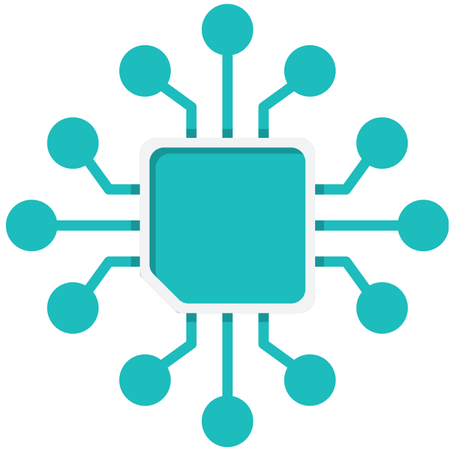
Parte 2: Cambios realizados 04

Parte 3: Simulación en Vivo 08

Parte 4: Simulación y riesgos con Wireshark 09

Parte 5: Vulnerabilidades y Propuestas 16

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

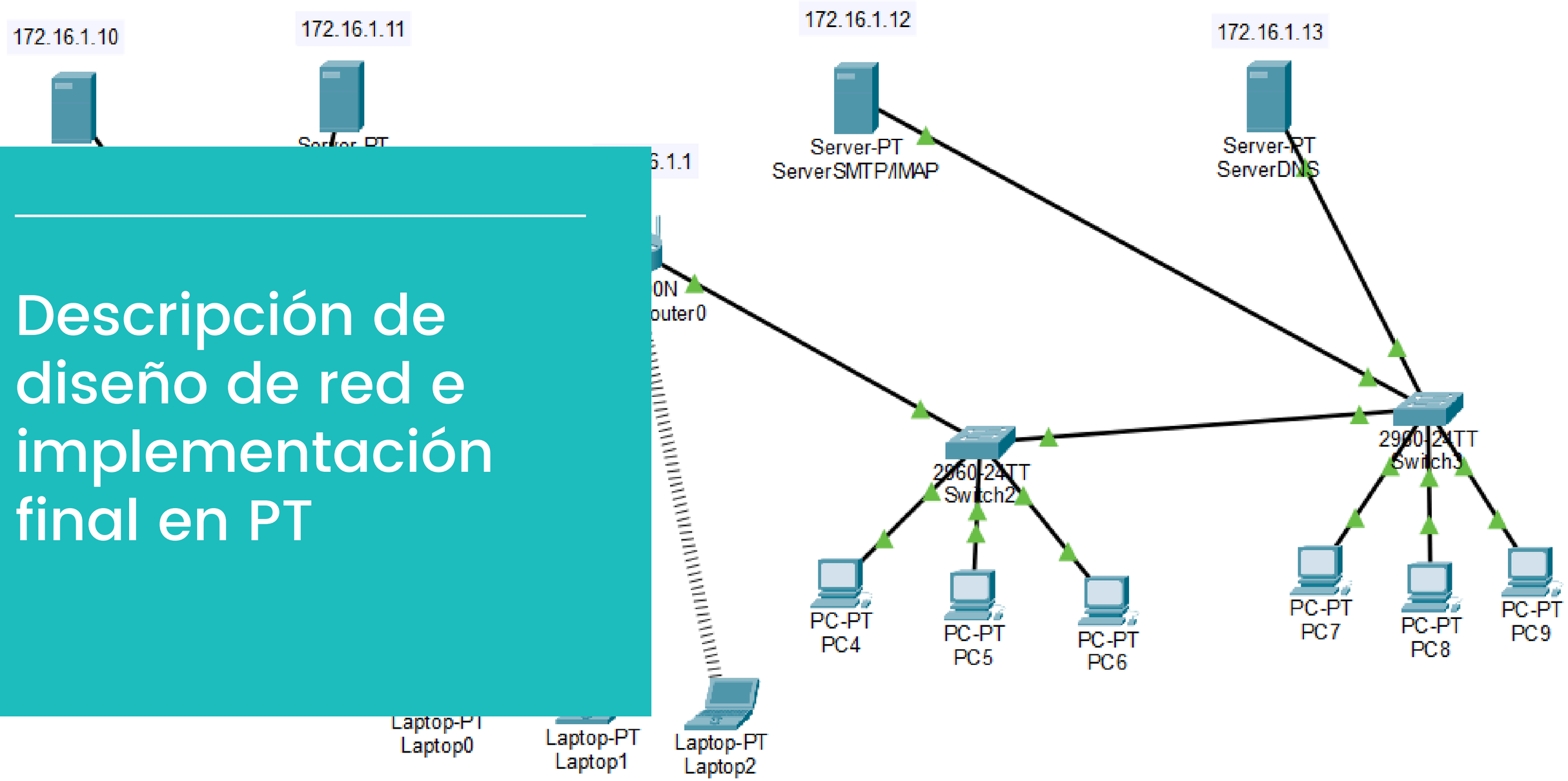
Cambios realizados respecto a hitos anteriores

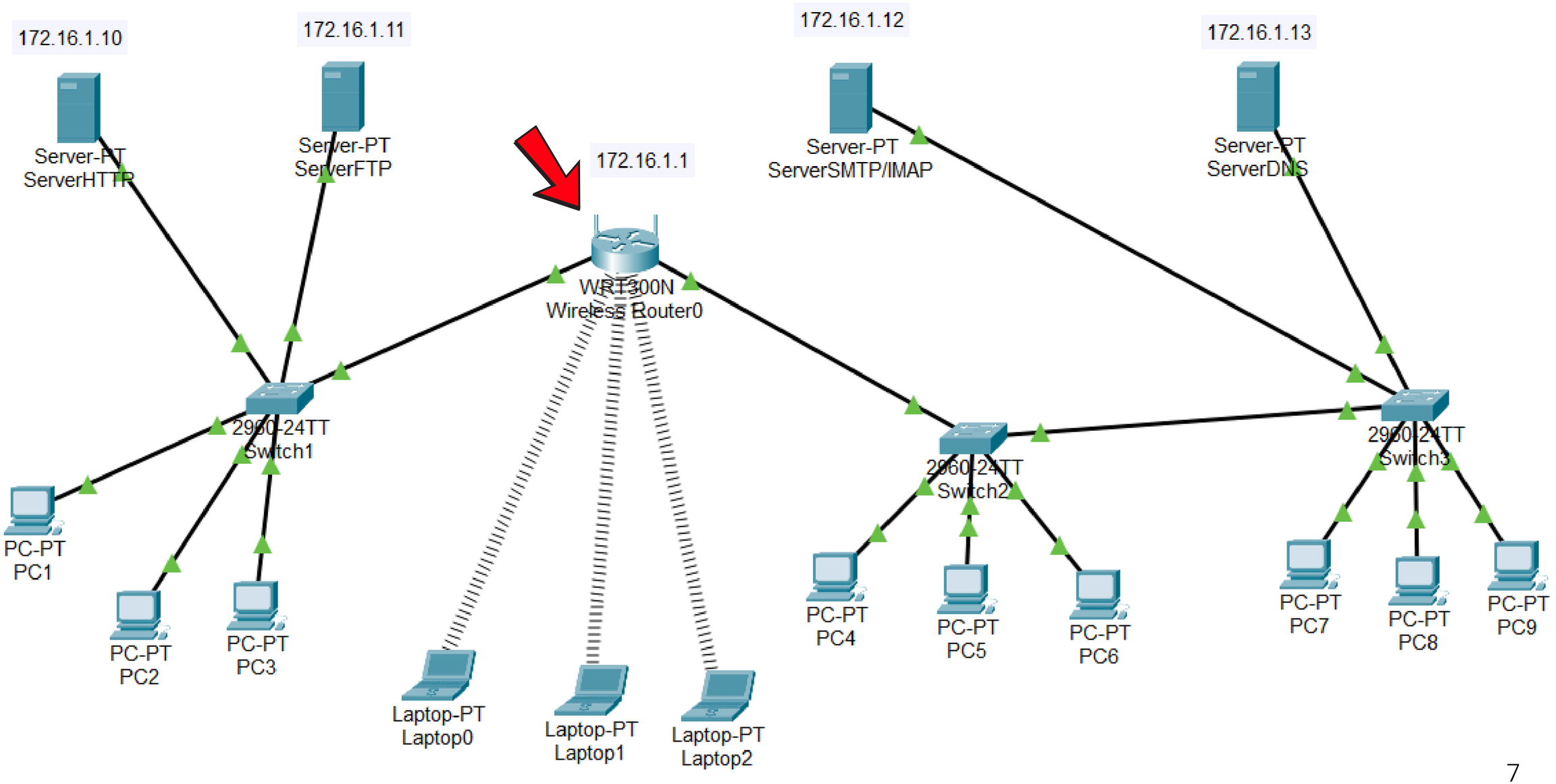
Modificación en la Carta Gantt

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

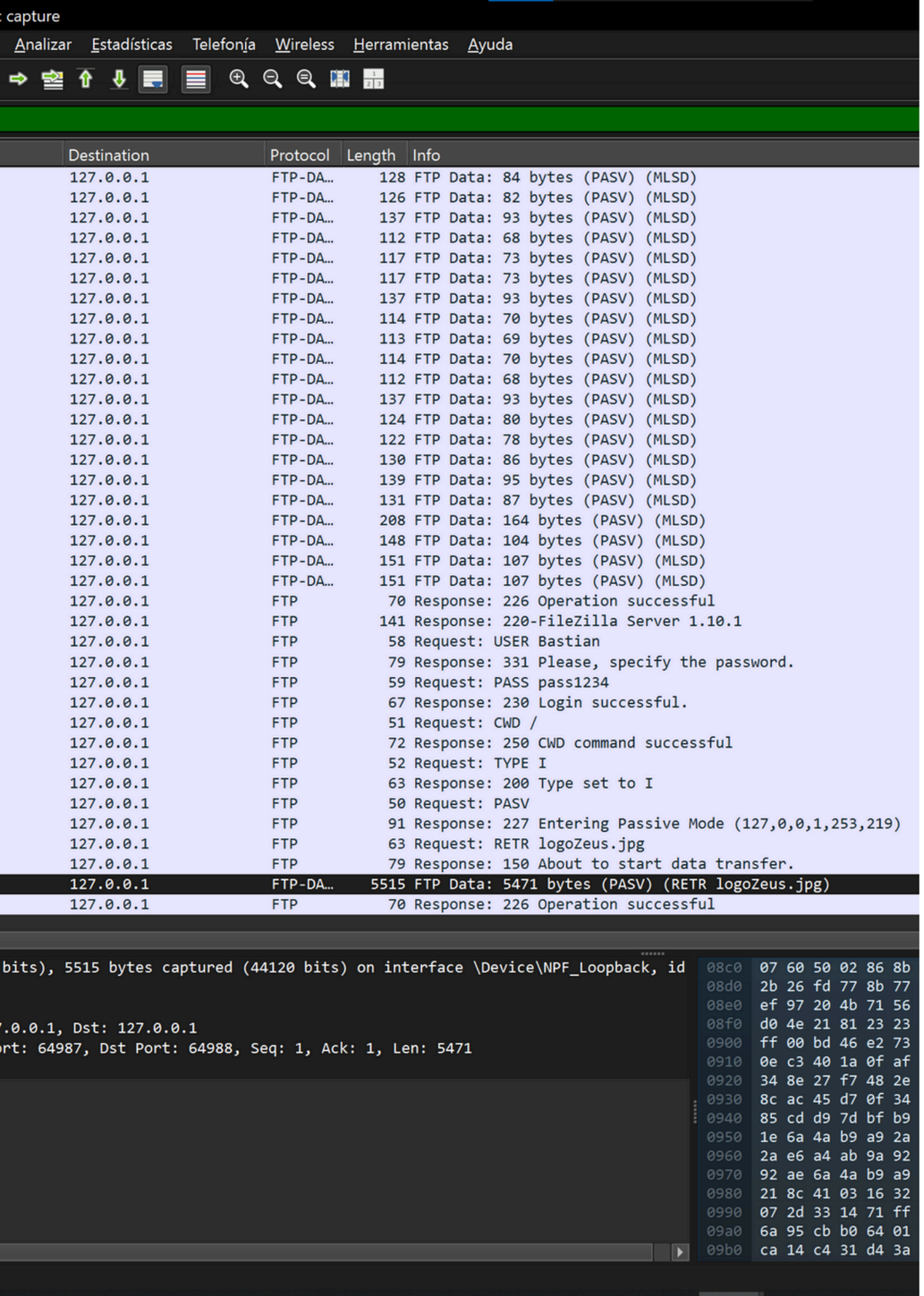
Hito 2: Avance Intermedio				
Evaluación de avances en relación al anteproyecto	Documentation Lead Project Manager	29/03/2025	09/04/2025	
Ajustes en el diseño de la red según retroalimentación inicial	Network Designer Packet Tracer Admin	29/03/2025	06/04/2025	
Revisión de conectividad y configuración 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	

Descripción de diseño de red e implementación final en PT

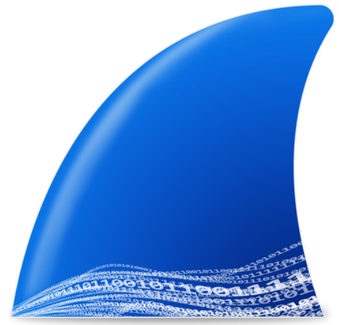



172.16.1.10
Server-PT
ServerHTTP
172.16.1.11
Server-PT
ServerFTP
172.16.1.1
WRT300N
Wireless Router0
172.16.1.12
Server-PT
ServerSMTP/IMAP
172.16.1.13
Server-PT
ServerDNS
2960-24TT
Switch1
2960-24TT
Switch2
2960-24TT
Switch3
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Laptop-PT
Laptop0
Laptop-PT
Laptop1
Laptop-PT
Laptop2
PC-PT
PC4
PC-PT
PC5
PC-PT
PC6
PC-PT
PC7
PC-PT
PC8
PC-PT
PC9

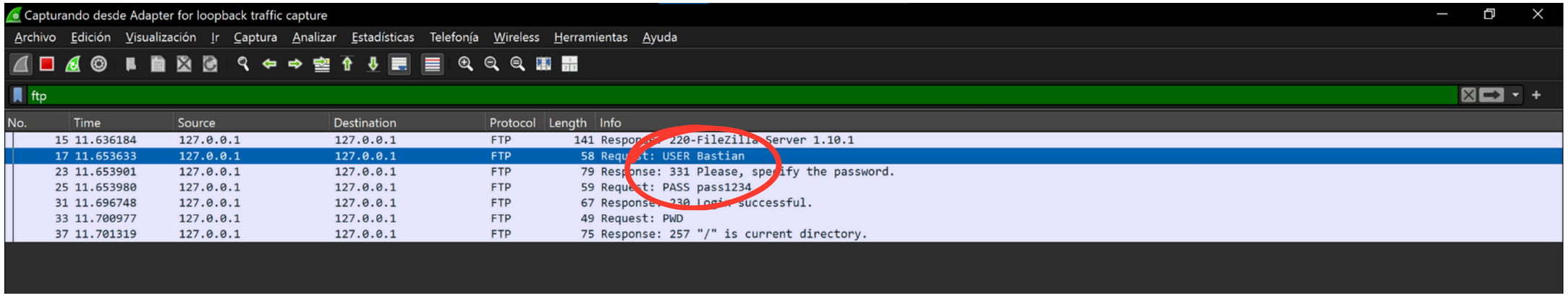
Simulación en vivo



Análisis de tráfico y exposición de riesgos en el protocolo FTP



Autenticación -Análisis de trafico



File Transfer Protocol

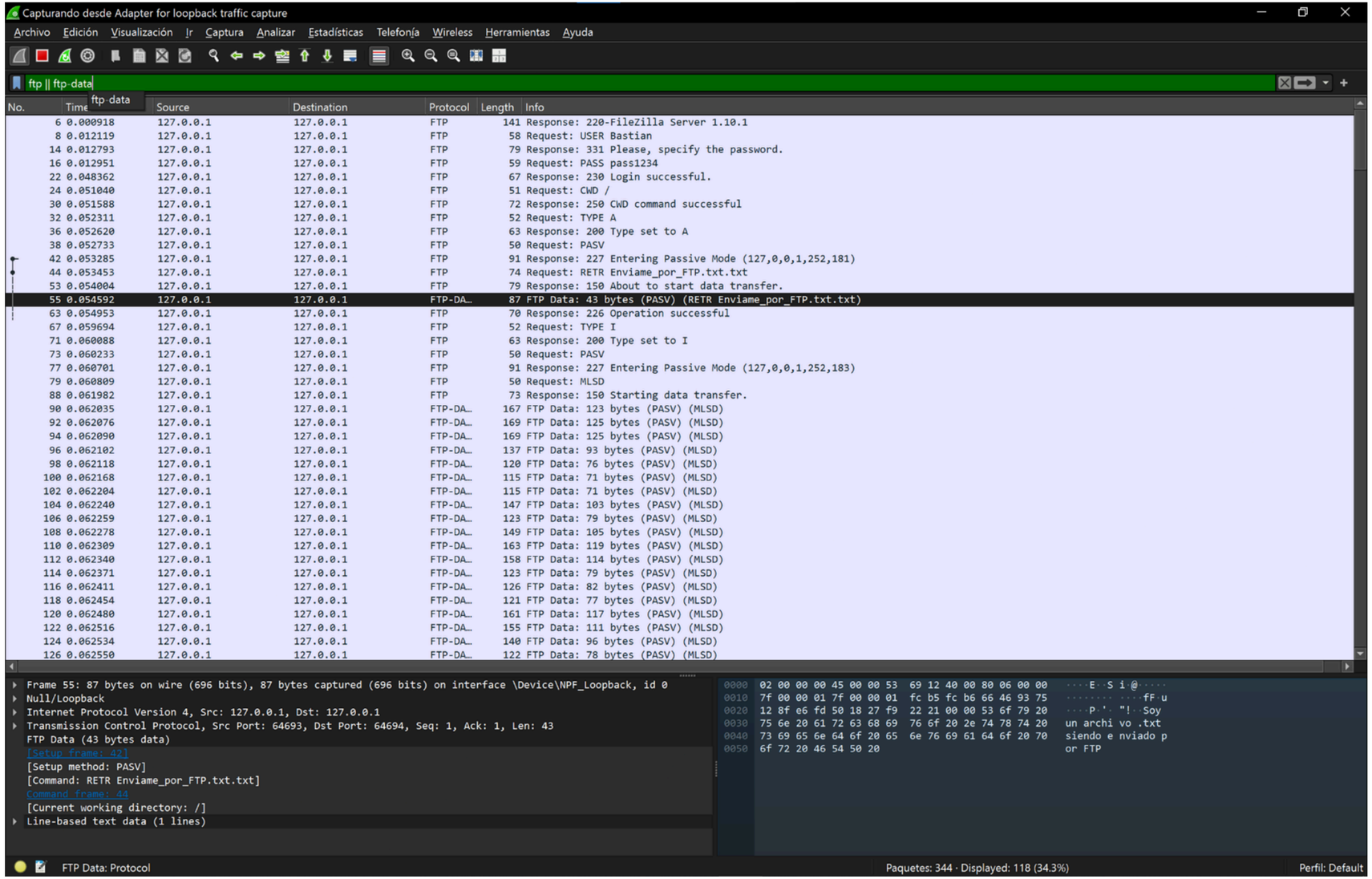
PASSWORD (PASS)

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

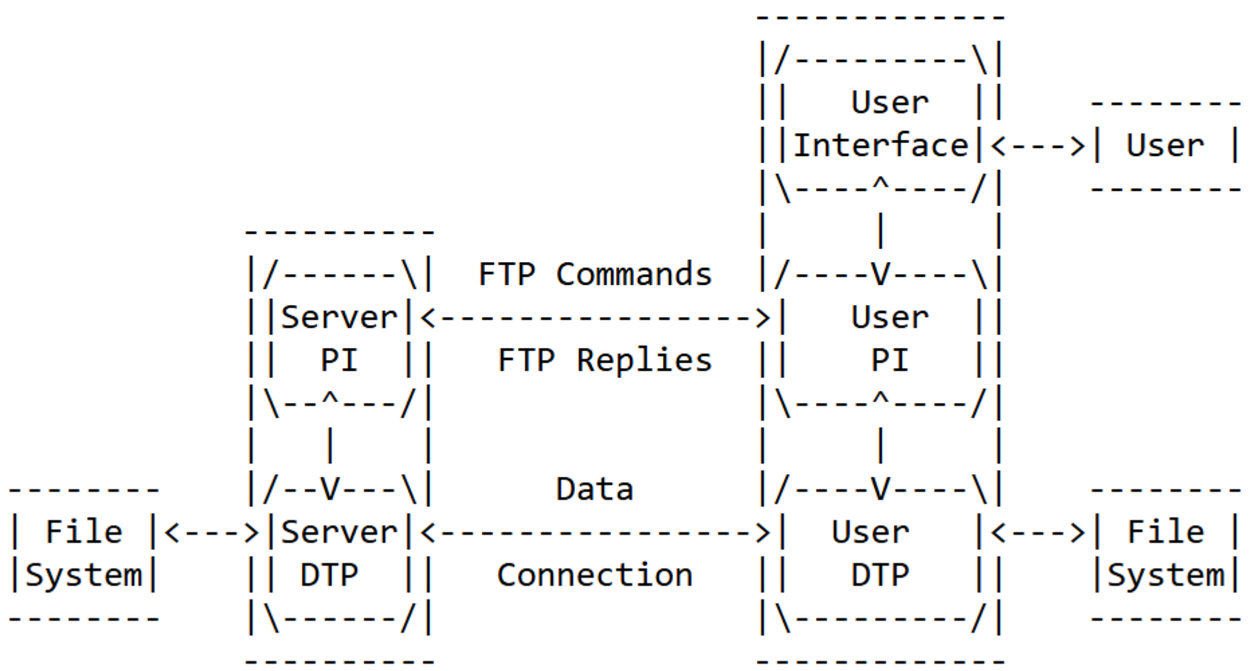
Transferencia txt -Análisis de trafico



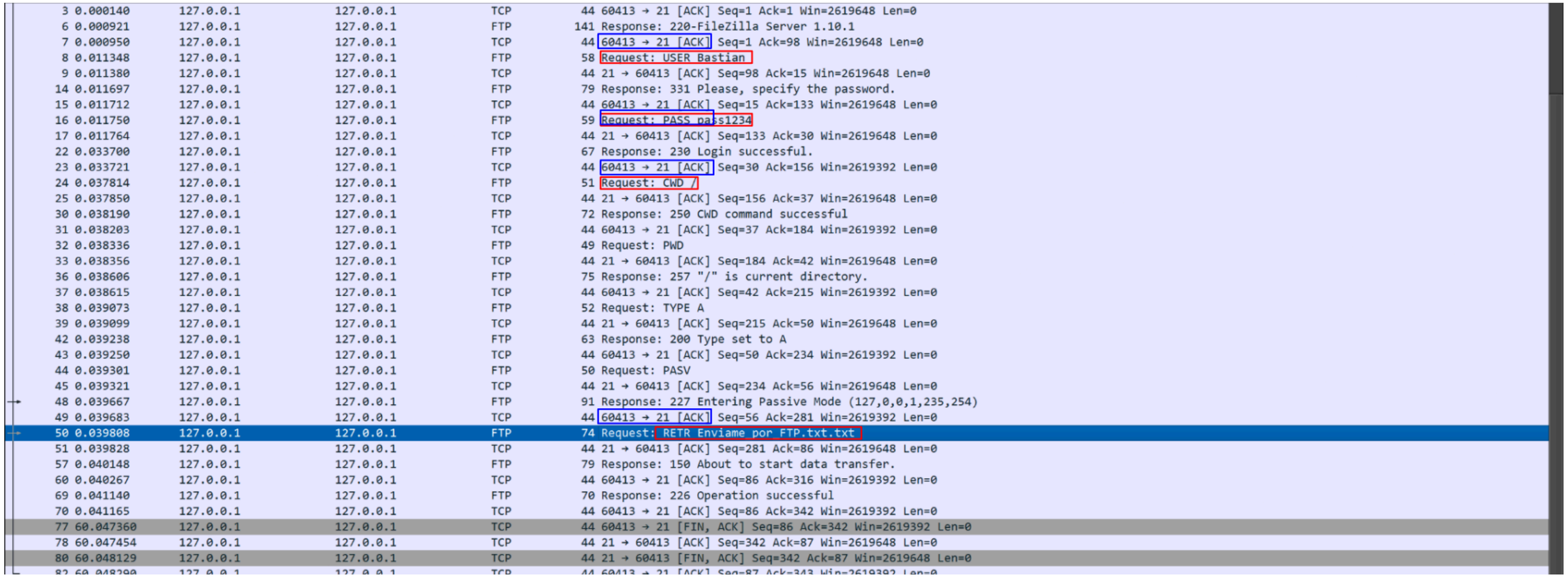
FTP y FTP-DATA -Análisis de trafico

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.

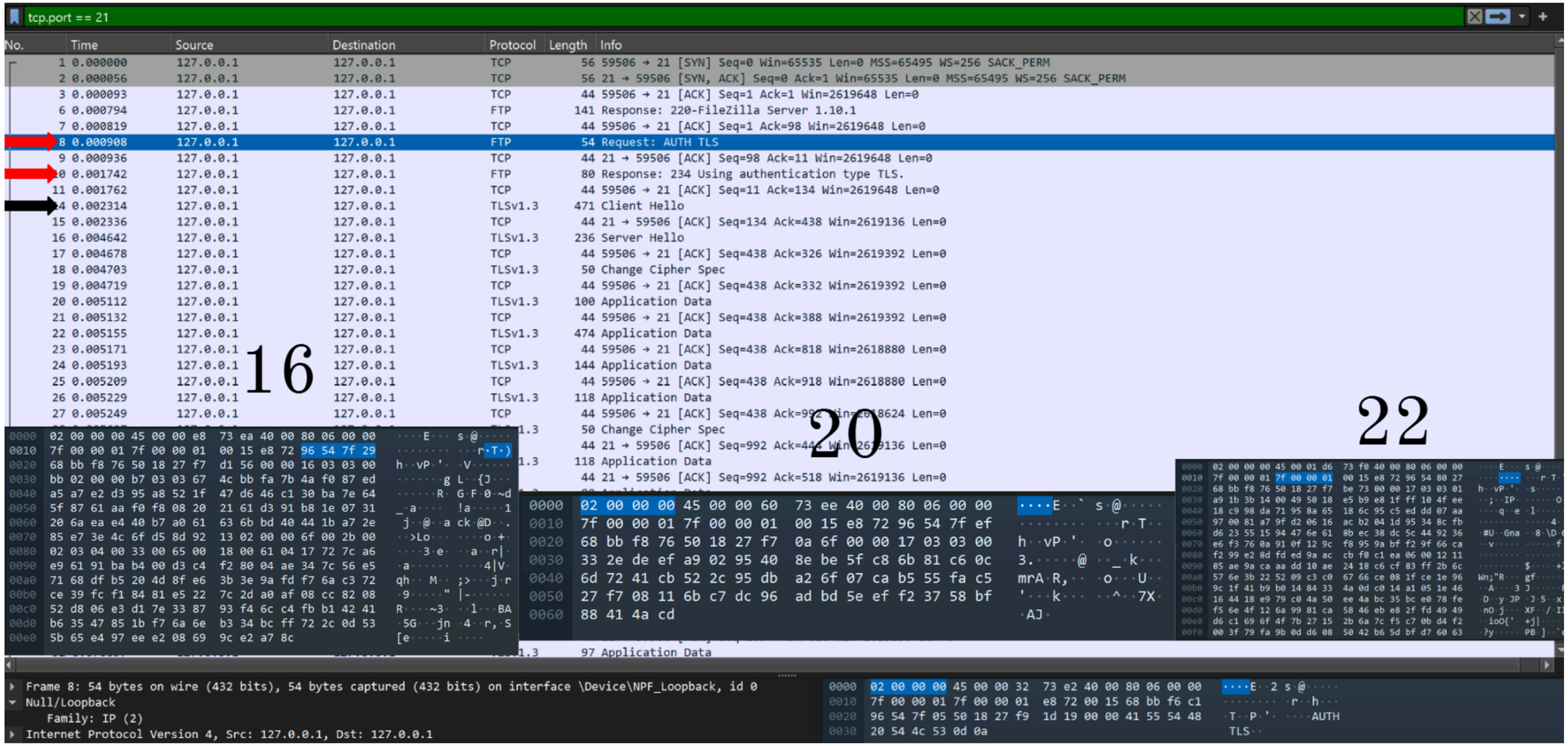


Interacción TCP -Análisis de trafico

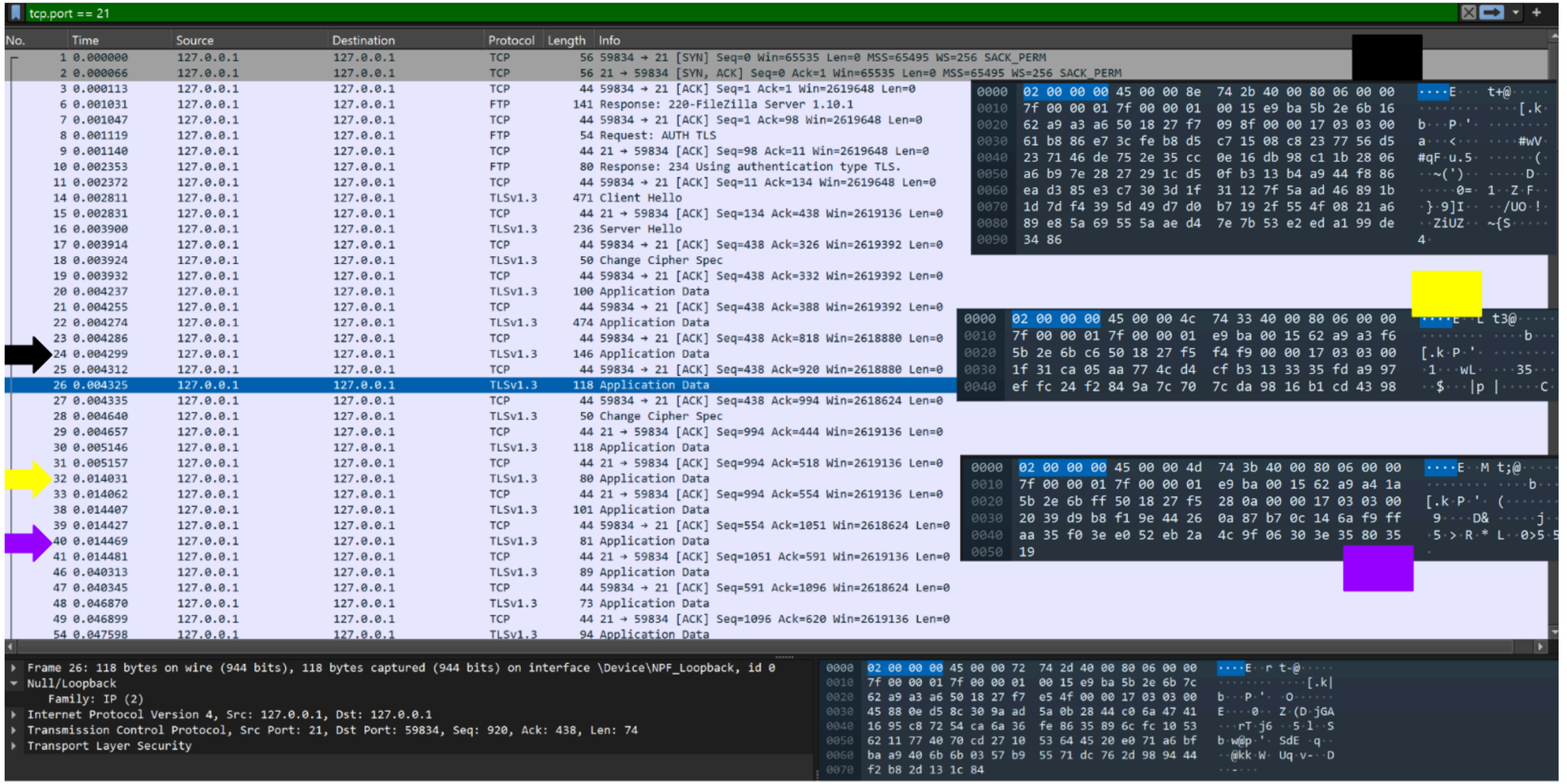


3	0.000140	127.0.0.1	127.0.0.1	TCP	44	60413 → 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
6	0.000921	127.0.0.1	127.0.0.1	FTP	141	Response: 220-FileZilla Server 1.10.1
7	0.000950	127.0.0.1	127.0.0.1	TCP	44	60413 → 21 [ACK] Seq=1 Ack=98 Win=2619648 Len=0
8	0.011348	127.0.0.1	127.0.0.1	FTP	58	Request: USER Bastian
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

Autenticación (con cifrado) -Análisis de trafico



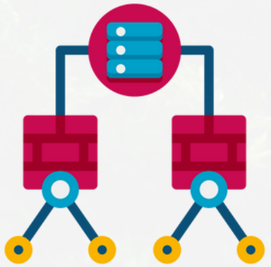
Transferencia txt (con cifrado) -Análisis de trafico



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

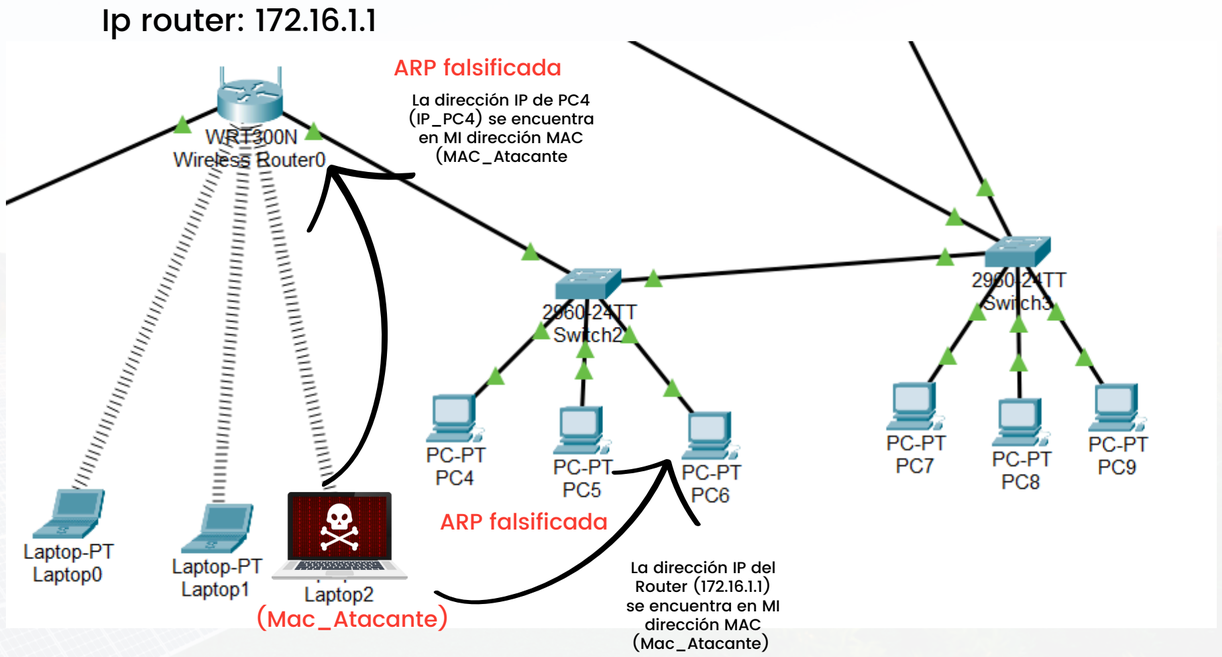


Problemas

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

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).

🔐 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

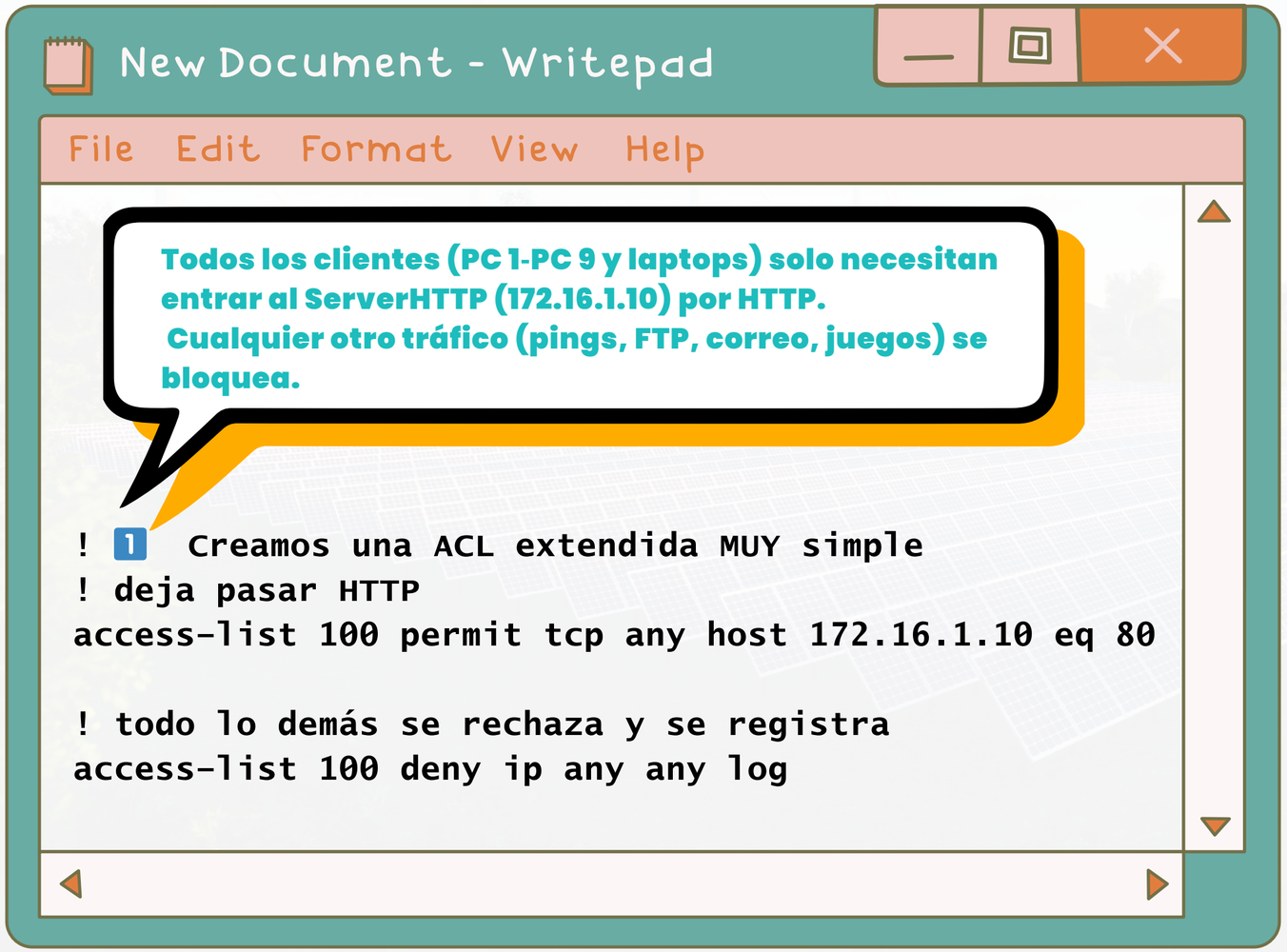
📜 2. ACLs restrictivas en routers/switches

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



¿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.

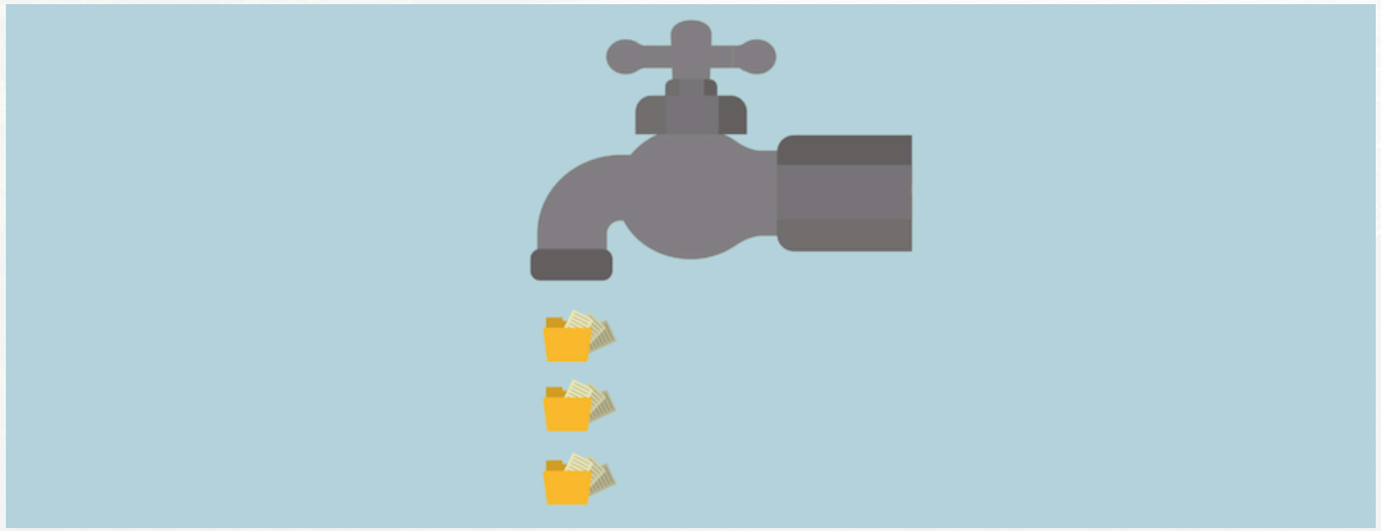
¿Cómo se implementa?

- 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

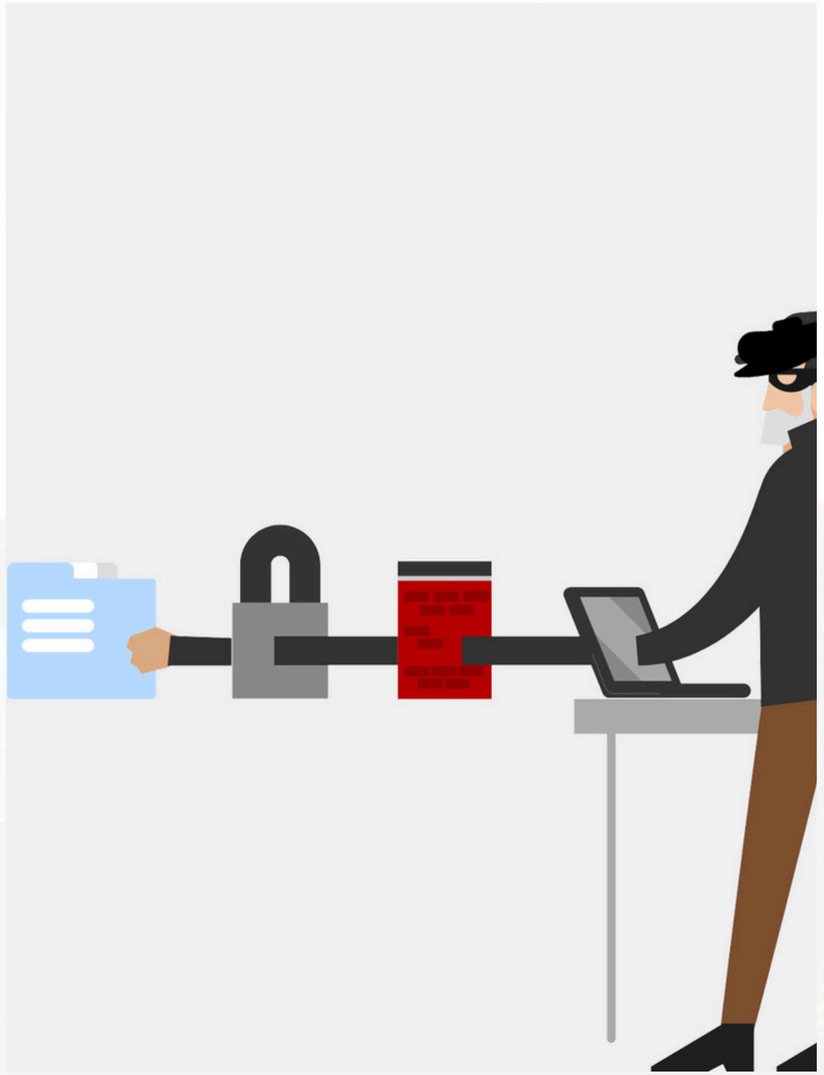
- FTP transmite datos, incluyendo credenciales y archivos, en texto claro. Esto permite que un atacante con acceso a la red pueda interceptar y visualizar información crítica sin necesidad de técnicas avanzadas.
- La falta de cifrado convierte al protocolo FTP en una vía común de filtración accidental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



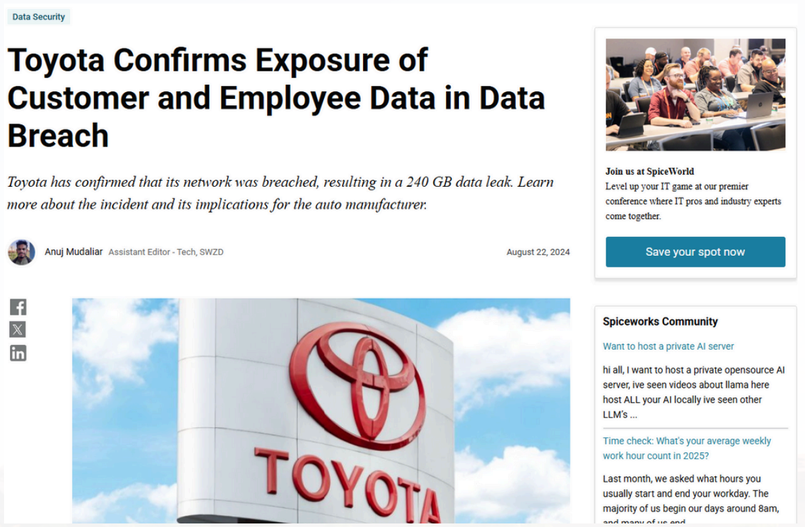
!!Acceso no autorizado al sistema

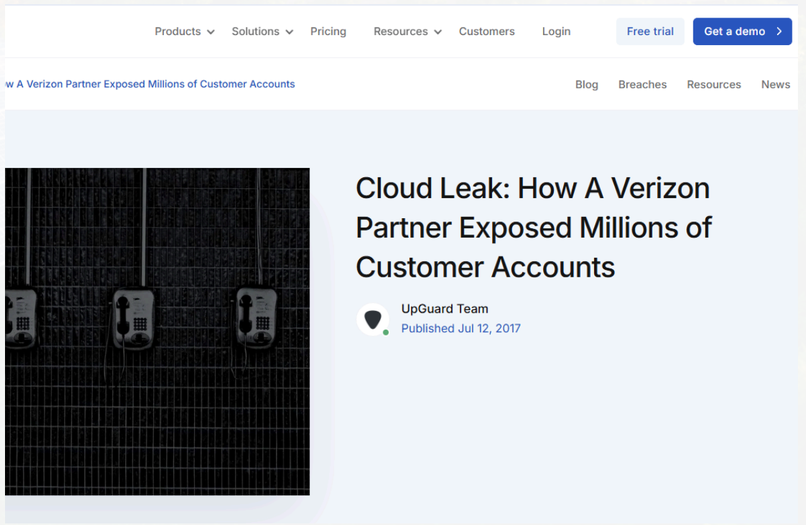
- El protocolo FTP carece de medidas de seguridad modernas, como cifrado o autenticación fuerte. Las credenciales viajan en texto claro, lo que facilita su interceptación por parte de atacantes.

- 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.



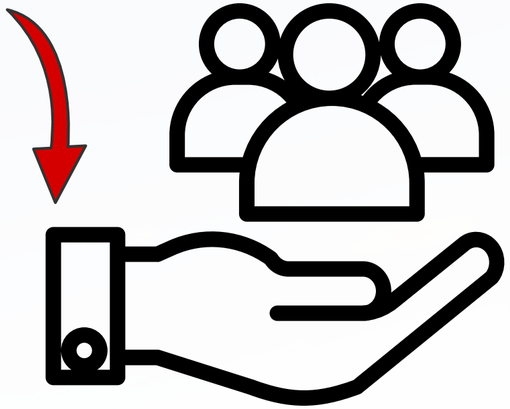
Incidentes de seguridad relacionados a FTP



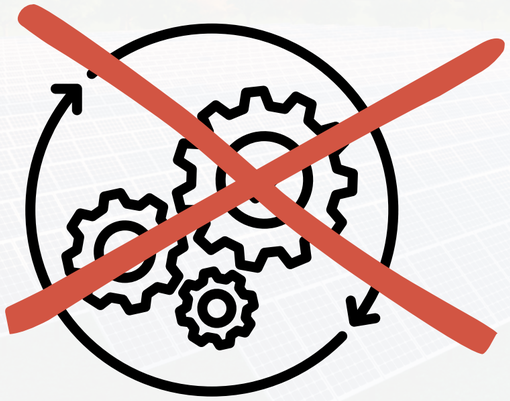


Repercusiones de un ataque cibernético

Pérdidas económicas



Pérdida de confianza del cliente



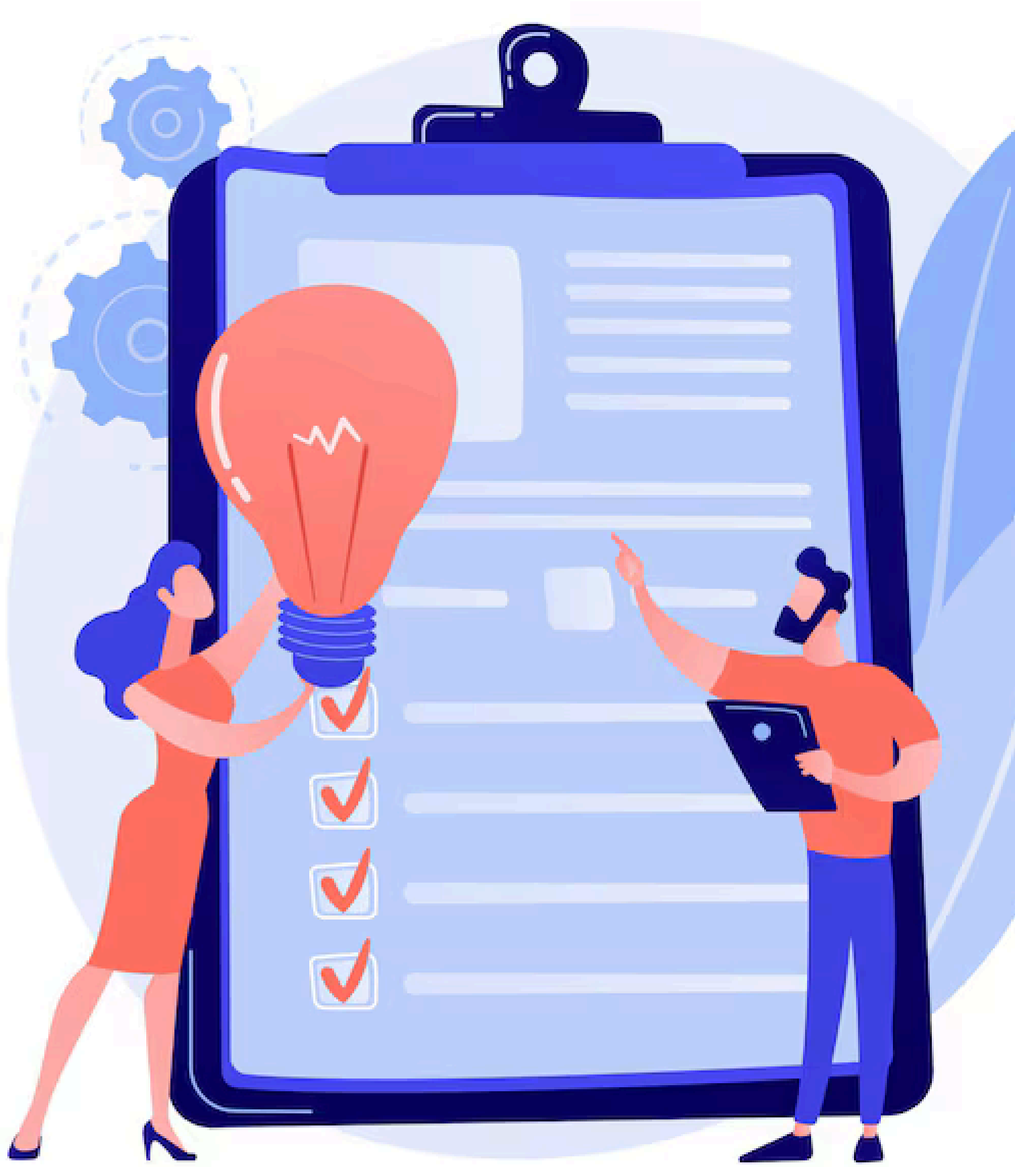
Interrupción de operaciones

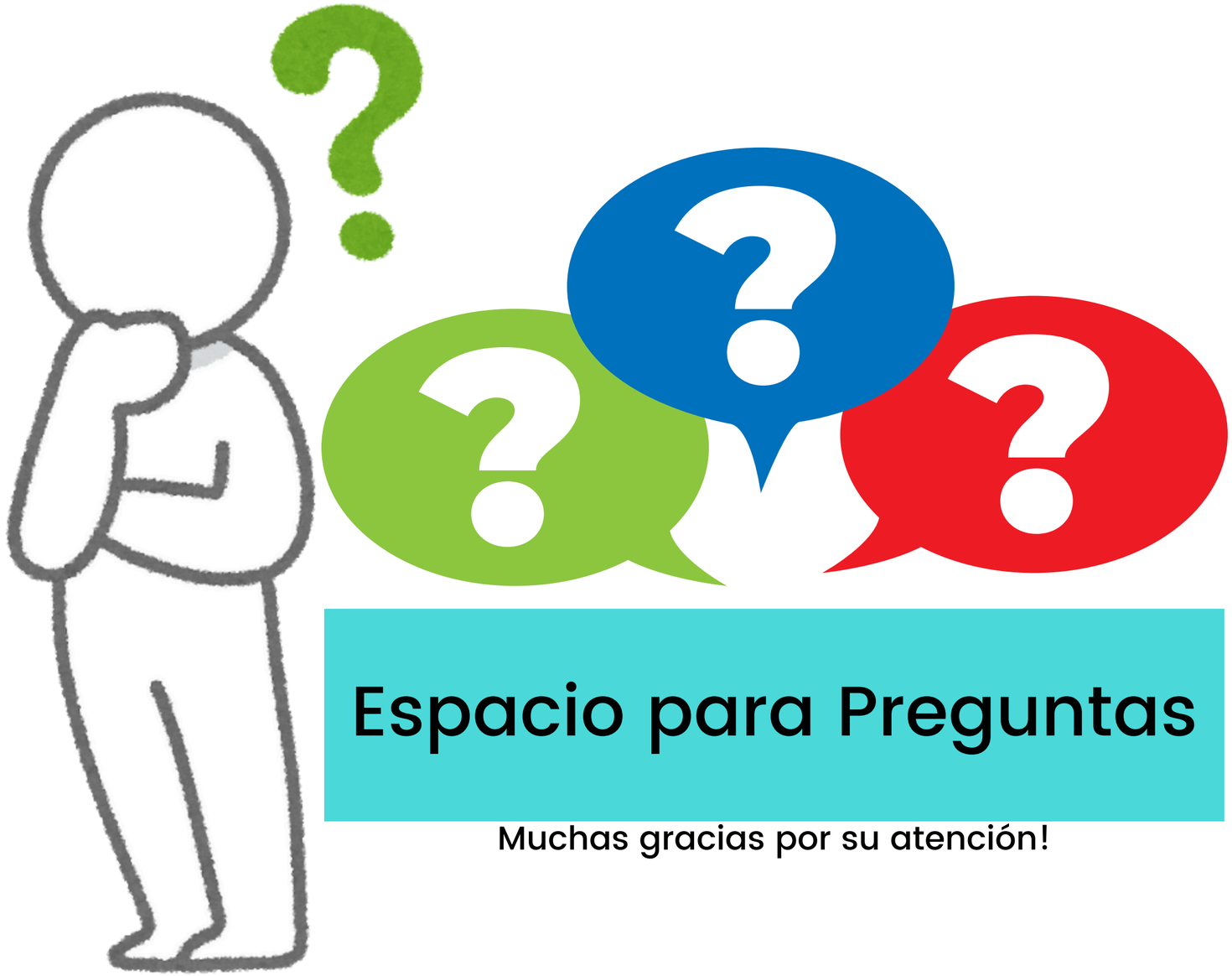
Impacto en la continuidad del negocio

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