

Informe Final – Diseño y Configuración de Red para TechMove

Redes De Comunicación: Hito 3

Integrantes Grupo C:

Nicolás Alarcón

Byron Caices

Matías Cortés

Williams Jimenez

Bastián Olea

Reinaldo Pacheco

Stephan Paul

Benjamín Zuñiga

Docente:

Juan Ignacio Iturbe

Índice

Índice	2
1. Introducción	3
2. Objetivos	3
2.1 Objetivos generales	3
2.2 Objetivos específicos	4
3. Contraste de lo definido en el anteproyecto con lo finalmente realizado	4
3.1 Roles y responsabilidades	4
3.2 Aportes y brechas de cada integrante	7
3.3 Identificación de problemáticas y cómo se solucionaron	9
3.4 Asignación de Tiempos y Esfuerzos (HH) y horas efectivas	10
3.5 Cambios Carta Gantt	13
3.6 Matriz RACI	13
3.7 Evaluación de Avances en relación a lo planificado en el Anteproyecto	13
4. Marco Teórico	14
4.1 ¿Qué es RFC?	14
4.2 ¿Qué es el protocolo FTP y FTPS?	14
4.3 Información y Documentación del protocolo FTP-FTPS	15
4.4 Diferencias entre FTP y FTPS	15
5. Captura de datos	16
5.1 Ajustes del Diseño de la red con respecto al esquema inicial	16
5.2 Análisis de captura de tráfico con Wireshark contrastando con documentación de los RFC de los protocolos.	17
6. Identificación de problemas y propuestas de Seguridad	21
6.1 Intercepción de datos por tráfico no cifrado	21
6.2 Posibilidad de suplantación de identidad (spoofing) por falta de cifrado IP	21
6.3 Falta de control de acceso a red para los dispositivos	22
6.4 Uso de protocolos de comunicación inseguros	22
6.5 Alto riesgo de propagación de malware y ransomware	22
6.6 Falta de segmentación de red	22
6.7 Ausencia de filtrado de tráfico de red	23
6.8 Falta de redundancia en servicios críticos	23
7. Incidentes de seguridad potenciales de no aplicar medidas de seguridad	23
7.1 Filtración de información sensible	23
7.2 Acceso no autorizado al sistema	24
7.3 Escalada de privilegios por mala configuración	24
7.4 Acceso a archivos sensibles fuera del directorio permitido	24
7.5 Ejecución remota de comandos a través del servicio FTP	24
7.6 Casos de vulneraciones en empresas reales	25
8. Conclusión	25
9. Bibliografía	27
10. Anexos	28
10.1 Anexo 1	28
10.2 Anexo 2	28

1. Introducción

“TechMove” es una empresa especializada en logística y distribución de última milla la cual ha tenido un crecimiento en el último tiempo. Actualmente se planea digitalizar su sistema de rastreo de paquetes y gestión de inventario. Con lo anterior presente, enfocándose en la rapidez de implementación y en mitigar riesgos de seguridad, se ha solicitado por parte de gerencia que la red sea funcional de inmediato, confiable y accesible para sus empleados.

Se requiere una red de Wi-Fi abierta para los empleados que permita que todos los dispositivos puedan conectarse sin restricciones.

Requerimientos de la Red:

- Se debe diseñar una red LAN cableada e inalámbrica para los empleados
- La asignación de IPs será automática en el rango 172.16.1.100-240
- La dirección del router será 172.16.1.1, funcionando como puerta de enlace y asignador de direcciones IP mediante DHCP
- La empresa cuenta con cuatro servidores esenciales:
 - Servidor Web (HTTP/HTTPS) - 172.16.1.10
 - Servidor de Archivos (FTP) - 172.16.1.11
 - Servidor de Correo (SMTP/IMAP) - 172.16.1.12
 - Servidor DNS - 172.16.1.13
- Todos los dispositivos deben poder comunicarse sin restricciones entre sí
- Se debe incluir al menos 3 switch de 24 puertos para los dispositivos cableados
- La red Wi-Fi debe ser abierta y accesible sin autenticación
- Se debe configurar una conexión a Internet simulada en Packet Tracer

En el presente informe se expone el progreso alcanzado en relación con el proyecto descrito en el informe anterior. Además de detallar las modificaciones realizadas respecto a la planificación y los diseños iniciales, se incluye un análisis más profundo de uno de los protocolos implementados en el sistema, el cual será abordado con mayor detalle en el marco teórico. Finalmente, también se detallan vulnerabilidades y las propuestas de seguridad en la red.

2. Objetivos

2.1 Objetivos generales

Entregar la red LAN propuesta en la entrega anterior a la empresa “TechMove”, realizar una simulación y análisis del tráfico mediante Cisco Packet Tracer y Wireshark, realizar una comparación entre protocolos seguros y no seguros (FTPS Y FTP) y también

incluir la identificación de problemas o vulnerabilidades de la red, junto a sus propuestas de soluciones de seguridad. Incluyendo los cambios en el proyecto hasta la actualidad.

2.2 Objetivos específicos

En esta entrega los objetivos específicos son:

- Cumplir los requerimientos de la empresa sobre la red en Packet Tracer
 - Diseño y Configuración de la Red en Packet Tracer
 - Asignación Automática de IPs (DHCP)
 - Asignación de IPs Fijas a los Servidores
 - Conexión de la red a internet
- Simular y analizar la captura de tráfico con Wireshark, realizando un contraste con la documentación RFC de los protocolos. Más específicamente los protocolos FTP y FTPS y comparar los mismos entre sí
- Contrastar lo definido en el anteproyecto con lo finalmente realizado: Identificar brechas y aportes de cada integrante del grupo. Indicar problemáticas y cómo se solucionaron
- Identificar problemas de seguridad en la red: Analizar teóricamente las vulnerabilidades presentes en la red diseñada, basándose en las malas prácticas establecidas desde el inicio del proyecto
- Investigar los impactos de las vulnerabilidades: Investigar las posibles consecuencias de las vulnerabilidades identificadas, incluyendo la exposición a ataques
- Proponer mejoras de seguridad: Proponer soluciones específicas para mitigar los riesgos de seguridad en la red
- Mencionar posibles incidentes de seguridad si estas medidas no se materializan.
- Indicar las apreciaciones sobre el presente trabajo y realizar sugerencias para la siguiente parte

3. Contraste de lo definido en el anteproyecto con lo finalmente realizado

3.1 Roles y responsabilidades

A continuación, se presentan los roles de cada integrante del grupo, junto con la descripción y función asociada cada uno, estos roles fueron utilizados para distribuir las actividades en el cronograma y la matriz RACI. Posterior a la presente tabla se encuentra otra tabla con los aportes y brechas de cada integrante para contrastar las responsabilidades planificadas con las tareas que efectivamente fueron realizadas por cada uno.

Rol	Descripción de responsabilidades y funciones asociadas al rol	Integrante
Project Manager	<ul style="list-style-type: none">● Centralizar la planificación general del proyecto.● Asegurarse de que cada	<ul style="list-style-type: none">● Stephan Paul

Rol	Descripción de responsabilidades y funciones asociadas al rol	Integrante
	<p>integrante tenga claras sus tareas, plazos y responsabilidades.</p> <ul style="list-style-type: none"> • Preparar y supervisar la Carta Gantt • Coordinar las reuniones del equipo y resolver conflictos 	
Network Designer	<ul style="list-style-type: none"> • Proponer el esquema inicial de la red en Packet Tracer (topología, interconexión, dispositivos) • Definir aspectos técnicos de IPs, rangos, servidores y conexión a internet simulada • Trabajar en conjunto a Packet Tracer Admin para asegurar e identificar posibles riesgos o vulnerabilidades en la red 	<ul style="list-style-type: none"> • Reinaldo Pacheco • Byron Caices
Packet Tracer Admin	<ul style="list-style-type: none"> • Implementar y refinar el esquema de red propuesto por el Network Designer • Encargarse de las configuraciones, asignaciones de servidores y pruebas de conectividad básicas • Generar capturas de tráfico de red 	<ul style="list-style-type: none"> • Nicolás Alarcón • Matías Cortés
Documentation Lead	<ul style="list-style-type: none"> • Elaborar y mantener registros detallados de la configuración de dispositivos, topologías de red y comandos utilizados en cada laboratorio • Redactar informes técnicos que incluyan objetivos, procedimientos, resultados y análisis de las prácticas realizadas • Asegurar que la documentación cumpla con estándares de claridad, precisión y estructura • Incluir diagramas, capturas de pantalla y descripciones que faciliten la interpretación de la configuración en Cisco Packet Tracer 	<ul style="list-style-type: none"> • Bastián Olea Díaz • Williams jimenez
Planning & Risk Analyst	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Benjamín Zuñiga

3.2 Aportes y brechas de cada integrante

Integrante	Rol	Aportes	Brechas
Stephan Paul	Project Manager	Coordinación general, seguimiento de planificación, revisión de cronograma y consolidación final.	Faltó una supervisión más estricta sobre el cumplimiento de horas hombre planificadas. Debido a que existen varias diferencias en las horas de la tabla de HH.
Reinaldo Pacheco	Network Designer	Diseñó la topología inicial de la red, participó activamente en la implementación en Cisco Packet Tracer. Realizó propuestas en las mejoras de seguridad como segmentación por VLAN y uso de protocolos cifrados.	Se generó un desfase por cambios en el diseño de red a mitad del proyecto (tras recibir retroalimentación), lo que implicó rehacer partes del esquema y reasignar tiempo técnico no previsto.
Byron Caices	Network Designer	Participó en la revisión y mejora del diseño lógico y físico de la red. Junto con proponer medidas para mitigar las vulnerabilidades.	La redistribución de actividades para realizar el análisis de seguridad generó cambios en sus responsabilidades originales. Esto implicó asumir nuevas tareas no consideradas anteriormente.
Nicolás Alarcón	Packet Tracer Admin	Configuración de los dispositivos en Cisco Packet Tracer, realizó pruebas de conectividad y colaboró en la generación de	Presentó retrasos en las capturas iniciales por falta de familiaridad con Wireshark.

		capturas de tráfico para el análisis en Wireshark.	
Matías Cortés	Packet Tracer Admin	Colaboró en el desarrollo de la red en Cisco Packet Tracer y en la resolución de errores de configuración. También realizó parte de la documentación del comportamiento de los protocolos capturados en Wireshark.	Hubo un leve percance a la hora de definir las actividades de los Packet Tracer Admins, lo que provocó una duplicación del trabajo.
Williams Jimenez	Documentation Lead	Redactó secciones centrales de los informes realizados, incluyendo la comparación técnica entre FTP y FTPS. Aportó con referencias a RFC y análisis teórico del protocolo.	Se retrasó la entrega de documentación por falta de organización en la recolección de capturas y pruebas.
Bastían Olea	Documentation Lead	Participó en la redacción de informes, análisis de tráfico y en la identificación de incidentes posibles si no se implementan medidas de seguridad.	Su tarea se vio retrasada por depender de insumos de otros integrantes (como análisis de tráfico y vulnerabilidades).
Benjamín Zuñiga	Planning & Risk Analyst	Identificación de vulnerabilidades presentes en la red (falta de segmentación, protocolos inseguros,	Su análisis se vio demorado porque inicialmente no se había planificado un bloque específico para riesgos. Se adaptó el flujo del

		spoofing), investigó consecuencias posibles y colaboró en la planificación de soluciones preventivas.	proyecto para incorporar sus hallazgos de forma integrada en la parte final.
--	--	---	--

3.3 Identificación de problemáticas y cómo se solucionaron

A lo largo del desarrollo del proyecto se presentaron diversas dificultades y obstáculos vinculados principalmente con desajustes, variaciones en la realización de tareas y modificaciones vinculadas a la retroalimentación obtenida en las fases intermedias. Estas dificultades, a pesar de no tener un efecto significativo en el progreso del proyecto, impactaron en lo previsto en el borrador del proyecto y demandaron una adaptación del equipo. Las siguientes son algunas dificultades que aparecieron durante el desarrollo del proyecto:

- **Actualización de la Carta Gantt:** Luego de la modificación de la fecha del Hito 2, se produjo una variación en la planificación. Esta situación se corrigió modificando la Carta Gantt y se comunicó la nueva programación al equipo a través de una reunión interna
- **Rediseño parcial de la red:** A la mitad del proyecto, se hicieron modificaciones en la estructura de la red a raíz de observaciones técnicas. Esto obligó a rehacer secciones del diseño y modificar los tiempos que se habían asignado previamente
- **Retrasos en las capturas de tráfico en Wireshark:** Los integrantes que debían realizar capturas con Wireshark presentaron retrasos en las mismas debido a que no estaban familiarizados con el software. Luego de realizar reuniones grupales para resolverlo en conjunto, se logró ejecutar la tarea y a su vez conseguir capturas con la información que necesitaban otros roles para continuar su trabajo
- **Desajuste leve entre roles parecidos:** Hubo ocasiones en donde hubo una repetición de tareas entre miembros con responsabilidades parecidas (como los Packet Tracer Admins)

En todos los casos se utilizó el mecanismo de solución de conflictos definido en el anteproyecto: una comunicación directa y oportuna en el medio de comunicación principal definido por el grupo. Generalmente se resolvieron los problemas mediante una conversación grupal, y en ocasiones se convocó a una reunión interna algunos días antes de las presentaciones para consolidar avances, revisar pendientes y asegurar la coherencia del trabajo final. El mecanismo interno de solución de conflictos original que se había definido era el siguiente.

- **Identificación y comunicación inmediata:**
Al primer indicio de conflicto, el miembro afectado lo comunica de inmediato al equipo para evitar que el problema escale.
- **Reunión grupal:**
Se convoca una reunión extraordinaria donde todos los miembros participan. El

coordinador facilita el diálogo y asegura un ambiente respetuoso.

- **Búsqueda de solución colaborativa:**
Se proponen y analizan alternativas. Se busca consenso o se vota por mayoría. En conflictos técnicos, puede intervenir un experto.
- **Escalamiento (si es necesario):**
Si no hay solución interna, se recurre al profesor o ayudante con evidencia del conflicto y los intentos previos de resolución.
- **Seguimiento y cierre:**
Se documenta la solución, se asignan responsables y plazos, y se verifica que el problema no persista.

3.4 Asignación de Tiempos y Esfuerzos (HH) y horas efectivas

Actividad	Responsable	Horas por responsable (HH)	HH efectivamente utilizadas
Planificar la distribución de los elementos de la red para aplicarlo a Packet Tracer	Project Manager Network Designer Packet Tracer Admin	1	1
Configurar el correcto funcionamiento de la red teórica simulando en Packet Tracer	Network Designer Packet Tracer Admin	2	2
Comprobar que el modelo teórico funcione correctamente según los objetivos establecidos	Network Designer Packet Tracer Admin Planning & Risk Analyst	1	1
Simular interacciones con las configuraciones del simulador	Network Designer Planning & Risk Analyst	2	1
Recopilar información de los comportamientos de los protocolos en el simulador	Documentation Lead	2	3
Documentar y señalar la información reunida	Documentation Lead	3	2
Investigar patrones de	Documentation Lead	2	1

Actividad	Responsable	Horas por responsable (HH)	HH efectivamente utilizadas
protocolos comunes de la vida real	Planning & Risk Analyst		
Utilizar Wireshark para capturar y analizar tráfico real de los mismos protocolos	Packet Tracer Admin Planning & Risk Analyst	2	2
Identificar y analizar los protocolos y patrones de comunicación en la red	Network Designer Packet Tracer Admin Planning & Risk Analyst Documentation Lead	2	1
Comparar los resultados de la simulación en Packet Tracer y las capturas en Wireshark con la teoría oficial de los protocolos, basada en la documentación de las RFCs	Project Manager Documentation Lead Network Designer Packet Tracer Admin	1	1
Señalar similitudes y diferencias además de señalar las posibles razones de las diferencias	Documentation Lead	2	1
Elaborar un informe técnico con el análisis de tráfico, incluyendo capturas, diferencias entre lo simulado y lo real	Documentation Lead	4	1
Explicando el funcionamiento de los protocolos a través de la teoría y conclusiones sobre el funcionamiento de los protocolos en distintos entornos.	Project Manager Documentation Lead	3	2
Contrastar lo definido en el anteproyecto con lo finalmente realizado	Project Manager Documentation Lead	2	2

Actividad	Responsable	Horas por responsable (HH)	HH efectivamente utilizadas
Analizar teóricamente las vulnerabilidades presentes en la red diseñada, basándose en las malas prácticas establecidas desde el inicio del proyecto.	Network Designer Packet Tracer Admin	2	2
Investigar las posibles consecuencias de las vulnerabilidades identificadas, incluyendo la exposición a ataques.	Planning & Risk Analyst	1	2
Proponer soluciones específicas para mitigar los riesgos de seguridad en la red.	Network Designer	2	1
Posibles incidentes de seguridad	Packet Tracer Admin	2	2
Indicar las apreciaciones sobre el presente trabajo	Documentation Lead	1	1

- Se realizaron ajustes en el diseño de la red en función de la retroalimentación recibida en las presentaciones.
- Se efectuó una revisión de la conectividad y de la configuración básica utilizando la herramienta Packet Tracer.
- Se actualizó el análisis preliminar de captura de tráfico mediante Wireshark, agregando y mejorando la información con respecto a la retroalimentación recibida en la presentación del Hito 2.
- Se agregó una sección relacionada a las vulnerabilidades de la red y a su vez los impactos que podrían implicar estas mismas.

4. Marco Teórico

4.1 ¿Qué es RFC?

El Request for Comments (RFC) es una serie de documentos numéricos en el que se describen y definen protocolos, conceptos, métodos y programas de Internet. La gestión de los RFC se realiza a través de IETF (el consorcio de colaboración técnica más importante de Internet, Internet Engineering Task Force). Una gran parte de los estándares utilizados en Internet están publicados en RFC (NFON, 2025). Sin embargo, su objetivo no es la estandarización de los protocolos sino su mejora.

Siendo su objetivo la mejora de los canales de comunicación, cada RFC (tanto antiguos como nuevos) tiene asociado un status, que está sujeto a modificaciones futuras. Entre los distintos status que pueden adoptar los RFC, se encuentran el **informativo**, que busca informar y no crear un consenso, el **experimental**, que denota que el documento es parte de un esfuerzo de desarrollo, **histórico**, que dicta que el documento ha sido reemplazado por una versión más reciente, y todos los que corresponden a estándares, entre los que están **propuesta de estándar**, **bosquejo de estándar**, **estándar de internet** (el estadio final de un RFC) y la **mejor práctica actual**, que suple la brecha que puede existir entre las distintas organizaciones y grupos dentro de internet (IETF, s.f.).

Dentro de todos los RFC existentes, se puede encontrar el protocolo RFC 959 que es el protocolo File Transfer Protocol, o por sus siglas FTP, y el protocolo RFC 2228, que es el protocolo File Transfer Protocol Safe, o por sus siglas FTPS (siendo esta una extensión del anterior). Actualmente, FTP se considera un **estándar de internet**, mientras que FTPS aparece como **propuesta de estándar**.

4.2 ¿Qué es el protocolo FTP y FTPS?

El **File Transfer Protocol (FTP)** es un protocolo de red creado en **1971** para la **transferencia de archivos** entre computadoras a través de redes TCP/IP. Su especificación más conocida está en el **RFC 959 (1985)** (Postel and Reynolds, 1985).

FTP funciona bajo una arquitectura cliente-servidor y utiliza los **puertos 21 (control)** y **20 (datos)**. Permite subir, descargar y gestionar archivos en un servidor remoto. Sin

embargo, al transmitir datos en **texto plano**, presenta riesgos de seguridad, lo que llevó al desarrollo de versiones más seguras como **FTPS** (FTP sobre TLS) (Ford-Hutchinson, 2005).

Hoy sigue siendo usado, especialmente en entornos internos y automatización de transferencias.

4.3 Información y Documentación del protocolo FTP-FTPS

- Protocolo no seguro: FTP
- Protocolo seguro: FTPS
- Puerto no seguro: 21
- Puerto seguro: 990
- Enfoque: Comparar transferencias de archivos con y sin cifrado

Según lo establecido en el RFC 959, el protocolo FTP (File Transfer Protocol) define sus objetivos principales de la siguiente manera:

1. Promocionar el uso compartido de ficheros (programas y/o datos)
2. Animar el uso indirecto o implícito a través de programas de servidores remotos
3. Hacer transparente al usuario las variaciones entre la forma de almacenar ficheros en diferentes ordenadores
4. Transferir datos de forma fiable y eficiente

Aunque FTP puede ser utilizado directamente por un usuario a través de una terminal, está diseñado principalmente para ser utilizado por programas (Paniagua, 2000).

Para transferir archivos mediante FTP, se necesitará un cliente FTP y un servidor FTP. Normalmente, se usa un cliente FTP para conectarse al servidor e iniciar la sesión de transferencia de archivos. En la mayoría de los casos, se conectará al servidor en el puerto 21. Este es el número de puerto que un servicio FTP estándar escucha para las solicitudes de conexión entrantes (Glass, 2025).

En cambio, FTPS es una versión segura de FTP, que posee todas las propiedades principales del protocolo FTP, pero reforzadas con funciones de seguridad que garantizan la confidencialidad de los datos, la autenticación de cliente y servidor, y la integridad de los datos. Estas funciones son necesarias si se va a utilizar un protocolo de transferencia de archivos en procesos empresariales o en cualquier transacción que involucre datos confidenciales (Glass, 2025).

4.4 Diferencias entre FTP y FTPS

Antes que nada hay que aclarar que no existe un único protocolo FTPS, ya que este tiene 2 variables, implícito sobre SSL o explícito sobre SSL. Estas se diferencian únicamente en qué punto de la conexión empieza FTPS, si desde el inicio de la conexión, o si después de la solicitud del cliente. (Andres, 2020). Sin embargo, independientemente de si se utiliza la variante implícita o explícita de FTPS, las diferencias que este protocolo presenta frente a

otros métodos de transferencia de archivos, como el FTP o SFTP, permanecen constantes. Las principales diferencias a destacar son:

1. **Cifrado en canales de comunicación:** Aunque ambos puedan usar 2 canales de comunicación, en el protocolo FTPS se cifra como mínimo, el canal de control usando SSL/TLS, a diferencia del protocolo FTP donde ninguno de los 2 canales posibles está cifrado (Andres, 2020).
2. **Diferencia en tiempo de transmisión:** Aunque ambos protocolos son rápidos, el protocolo FTPS posee una mayor carga en el tiempo de transmisión en comparación con el protocolo FTP, esto debido a una pequeña sobrecarga de proceso debido a las operaciones de cifrado y descifrado para asegurar los datos. Aunque cabe recalcar que la diferencia de tiempo no es tan significativa y en comparación a la seguridad entregada, esta vale significativamente la pena. (Andres, 2020).
3. **Compatibilidad con firewalls:** El protocolo FTP, al ser no cifrado y usar los puertos, no presenta mayores problemas con el uso de firewalls. En cambio, en FTPS se pueden presentar mayores desafíos debido a que al utilizar más de un canal, puede requerir configuraciones de firewall más específicas, por lo que requiere una mayor supervisión de los parámetros en comparación a su versión no segura. (Piensa Solutions, 2022).

5. Captura de datos

5.1 Ajustes del Diseño de la red con respecto al esquema inicial

En cuanto al diseño de la red, se realizó una modificación clave respecto al esquema inicial: se reemplazó el router originalmente planeado el cual era un HomeRouter por un WAN Router utilizando el modelo WRT300N.

El motivo principal del cambio se dió debido a que el HomeRouter es un dispositivo diseñado para entornos domésticos y presenta limitaciones para un red de escala empresarial, tales como:

- Limitaciones en el rango de direcciones IP en el servidor DHCP
- Cantidad de sesiones simultáneas acotado
- Un escaso número de puertos físicos para conectar dispositivos cableados
- Bajo rendimiento y congestión de red con la cantidad de dispositivos a implementar

Por este motivo, se designó un router que permitiera interconectar una red escalable hasta 100 PCs de forma simultánea y sin las limitaciones que podría provocar el HomeRouter.

Las configuraciones de los servidores, switches y PC se mantuvieron como en las entregas anteriores funcionando correctamente.

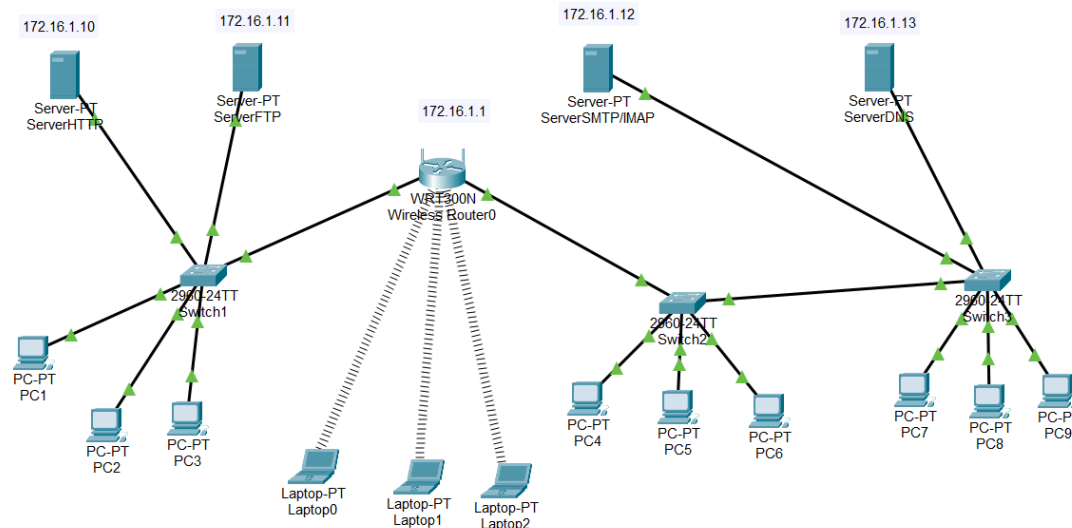


Figura 3: Nuevo esquema de red implementado

5.2 Análisis de captura de tráfico con Wireshark contrastando con documentación de los RFC de los protocolos.

A continuación se registra lo observado durante la captura de tráfico FTP utilizando Wireshark, contrastándolo con lo especificado en el RFC respectivo.

La siguiente imagen muestra el tráfico que se genera al realizar una autenticación en un servidor FTP, como podemos ver en los paquetes número 8 y 16, a través de los comandos **USER** y **PASS** el usuario inicia sesión en el servidor, podemos ver en texto plano, el nombre del usuario "**Bastian**" y su contraseña "**pass1234**". Esto desde ya se puede considerar una falta a la seguridad severa, ya que es sabido que la contraseña es una información que se considera altamente confidencial y el hecho de que sea transportada en texto plano la expone a ser interceptada fácilmente por cualquier persona.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	63433 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000045	127.0.0.1	127.0.0.1	TCP	56	21 → 63433 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000072	127.0.0.1	127.0.0.1	TCP	44	63433 → 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
6	0.000489	127.0.0.1	127.0.0.1	FTP	141	Response: 220-FileZilla Server 1.10.1
7	0.000503	127.0.0.1	127.0.0.1	TCP	44	63433 → 21 [ACK] Seq=1 Ack=98 Win=2619648 Len=0
8	0.019286	127.0.0.1	127.0.0.1	FTP	58	Request: USER Bastian
9	0.019331	127.0.0.1	127.0.0.1	TCP	44	21 → 63433 [ACK] Seq=98 Ack=15 Win=2619648 Len=0
14	0.019987	127.0.0.1	127.0.0.1	FTP	79	Response: 331 Please, specify the password.
15	0.020010	127.0.0.1	127.0.0.1	TCP	44	63433 → 21 [ACK] Seq=15 Ack=133 Win=2619648 Len=0
16	0.020194	127.0.0.1	127.0.0.1	FTP	59	Request: PASS pass1234
17	0.020232	127.0.0.1	127.0.0.1	TCP	44	21 → 63433 [ACK] Seq=133 Ack=30 Win=2619648 Len=0
22	0.046121	127.0.0.1	127.0.0.1	FTP	67	Response: 230 Login successful.
23	0.046145	127.0.0.1	127.0.0.1	TCP	44	63433 → 21 [ACK] Seq=30 Ack=156 Win=2619392 Len=0
24	0.048742	127.0.0.1	127.0.0.1	FTP	49	Request: PWD
25	0.048770	127.0.0.1	127.0.0.1	TCP	44	21 → 63433 [ACK] Seq=156 Ack=35 Win=2619648 Len=0
28	0.049080	127.0.0.1	127.0.0.1	FTP	75	Response: 257 "/" is current directory.
29	0.049099	127.0.0.1	127.0.0.1	TCP	44	63433 → 21 [ACK] Seq=35 Ack=187 Win=2619392 Len=0

Figura 4: Tráfico de autenticación [Wireshark]

Esta falta es identificada y mencionada en el RFC como se puede ver a continuación.

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.

Figura 5: Mención a la falta de seguridad [RFC]

Aquí se menciona como la contraseña es una información sensible que debiera ser enmascarada de alguna manera pero que el servidor no tiene la capacidad de hacerlo por lo que aquella responsabilidad recae en el lado del usuario.

Para continuar con el análisis del tráfico se realizaron pruebas con el traspaso de un archivo .txt el archivo fue nombrado "Enviame_por_FTP.txt.txt" y el contenido de este fue "Soy un archivo .txt siendo enviado por FTP". A continuación la figura que muestra el tráfico obtenido al realizar el traspaso del archivo.

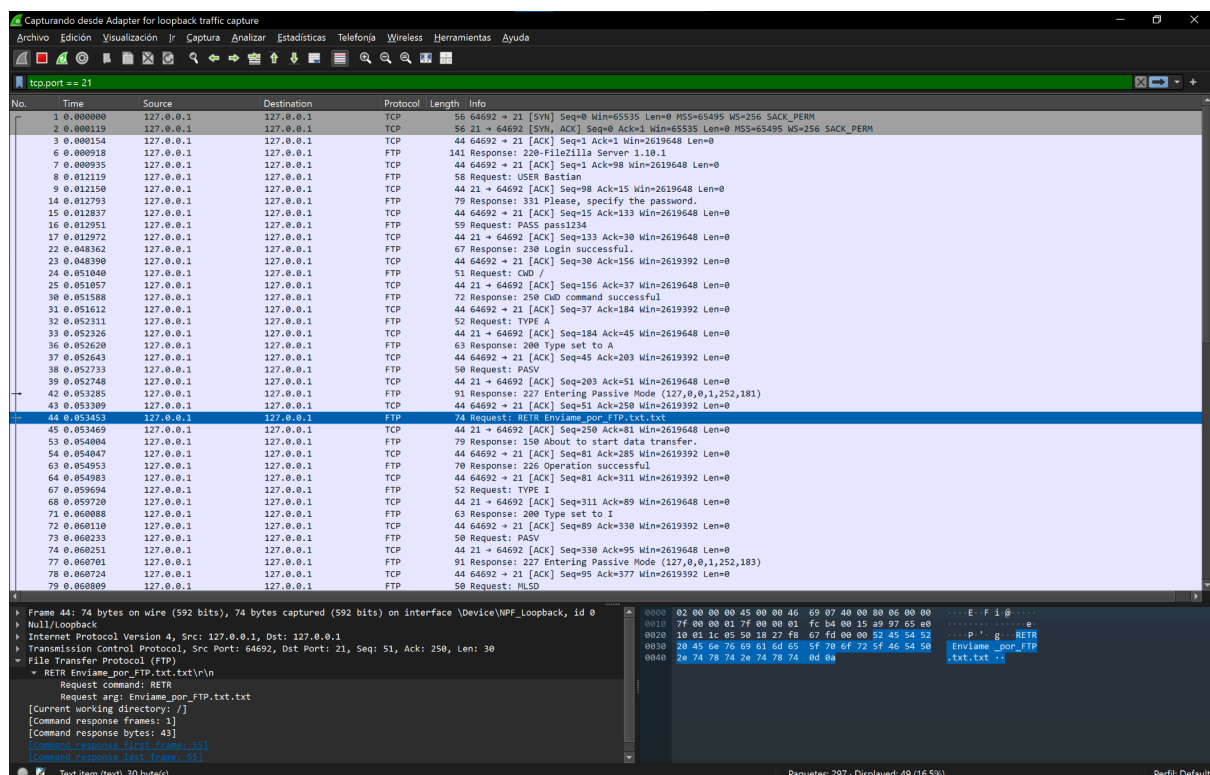


Figura 6: Tráfico transferencia archivo .txt [Wireshark]

Podemos ver como se hace uso del comando **RETR** y también podemos ver en texto plano el nombre del archivo que está siendo enviado. Posteriormente, se modificó el filtro utilizado para visualizar el tráfico. El nuevo filtro fue `ftp || ftp-data`. A continuación el tráfico visto.

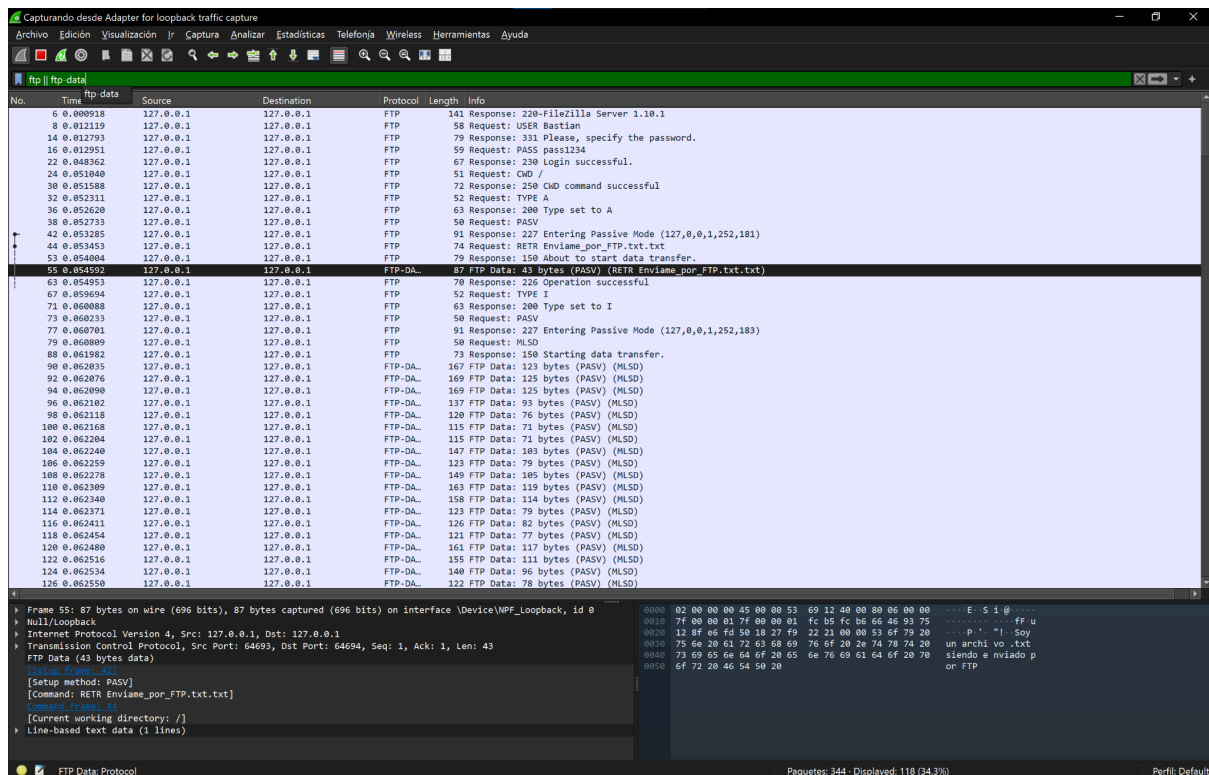


Figura 6: Tráfico contenido archivo .txt [Wireshark]

Acá podemos ver directamente el contenido (mencionado anteriormente) del archivo que hemos traspasado, también podemos notar como el protocolo ftp parece dividirse en dos con FTP y FTP-DATA. Al corroborar con el RFC se puede notar que el funcionamiento del protocolo divide el tráfico. Por una parte se tiene la interacción del usuario y por otra el contenido de lo que se está transfiriendo.

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.

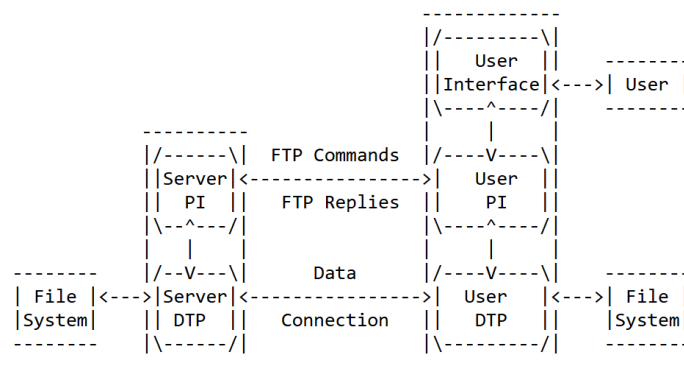


Figura 7: Diagrama flujo FTP [RFC]

Por un flujo se tiene el tráfico de los comandos FTP y las respuestas correspondientes del servidor, tanto como comandos como las respuestas pasan previamente por el correspondiente PI (Protocol Interpreter). En el otro flujo, separado, se encuentra el contenido real de los archivos que están siendo enviados o recibidos, aquí es donde ocurre el DTP (Data Transfer Process).

Lo siguiente fue realizar la misma autenticación pasada, pero esta vez con la versión segura de FTP. A continuación se muestra el tráfico que se generó:

The image shows a Wireshark packet capture of an FTPS session. The top pane displays a list of 54 packets. The middle pane shows the details of the selected packet (No. 54), which is a TLSv1.3 Application Data packet. The bottom pane shows the raw packet data in hexadecimal and ASCII. The session starts with a TCP connection (No. 1), followed by FTP commands and responses (Nos. 2-7). The authentication process begins with packet 8 (AUTH TLS), packet 9 (234 Using authentication type TLS), and packet 10 (Client Hello). The subsequent packets (11-54) show the TLS handshake and data transfer.

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	0.000055	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	0.000841	127.0.0.1	127.0.0.1	TCP	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
28	0.005627	127.0.0.1	127.0.0.1	TLSv1.3	50	Change Cipher Spec
29	0.005655	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=992 Ack=444 Win=2619136 Len=0
30	0.006328	127.0.0.1	127.0.0.1	TLSv1.3	118	Application Data
31	0.006347	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=992 Ack=518 Win=2619136 Len=0
32	0.028712	127.0.0.1	127.0.0.1	TLSv1.3	80	Application Data
33	0.028776	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=992 Ack=554 Win=2619136 Len=0
38	0.029450	127.0.0.1	127.0.0.1	TLSv1.3	101	Application Data
39	0.029508	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=554 Ack=1049 Win=2618624 Len=0
40	0.029587	127.0.0.1	127.0.0.1	TLSv1.3	81	Application Data
41	0.029603	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=591 Ack=1094 Win=2619136 Len=0
46	0.064390	127.0.0.1	127.0.0.1	TLSv1.3	89	Application Data
47	0.064427	127.0.0.1	127.0.0.1	TCP	44	59506 → 21 [ACK] Seq=591 Ack=1094 Win=2618624 Len=0
48	0.070339	127.0.0.1	127.0.0.1	TLSv1.3	71	Application Data
49	0.070370	127.0.0.1	127.0.0.1	TCP	44	21 → 59506 [ACK] Seq=1094 Ack=618 Win=2619136 Len=0
52	0.070697	127.0.0.1	127.0.0.1	TLSv1.3	97	Application Data

Figura 8: Autenticación con FTPS [Wireshark]

De la secuencia de tráfico podemos ver que:

1. El cliente envía el comando AUTH TLS.
2. El servidor responde con 234 Using authentication type TLS.
3. A continuación, el cliente inicia el handshake TLS enviando el mensaje ClientHello.
4. Desde ese punto en adelante, todo el tráfico entre cliente y servidor aparece cifrado.

Este comportamiento está alineado con lo especificado en el RFC 4217, que describe el uso de TLS en FTP, conocido como FTPS. Según este documento, el cliente puede solicitar asegurar la sesión enviando el comando AUTH TLS. Si el servidor lo acepta, responde con el código 234, indicando que procederá a negociar un canal seguro mediante TLS.

Este procedimiento asegura confidencialidad, integridad y autenticación en la sesión FTP. Contrario al FTP tradicional, que transmite credenciales y datos en texto plano, FTPS protege la información frente a ataques de interceptación o manipulación en redes no confiables.

Por tanto, la captura observada es coherente con la operación esperada según los estándares: el uso del comando AUTH TLS como señal para comenzar la negociación segura, seguida por el handshake TLS definido en el RFC 2246, y la posterior protección cifrada del canal de comunicación.

Para la transferencia de archivos, se hizo la misma transferencia de “Enviame_por_FTP.txt.txt” pero manteniendo el protocolo FTPS, el tráfico obtenido fue el siguiente:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	59834 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000066	127.0.0.1	127.0.0.1	TCP	56	21 → 59834 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000113	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
6	0.001031	127.0.0.1	127.0.0.1	FTP	141	Response: 220-FileZilla Server 1.10.1
7	0.001047	127.0.0.1	127.0.0.1	FTP	44	59834 → 21 [ACK] Seq=1 Ack=98 Win=2619648 Len=0
8	0.001119	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH TLS
9	0.001140	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=98 Ack=11 Win=2619648 Len=0
10	0.002353	127.0.0.1	127.0.0.1	FTP	80	Response: 234 Using authentication type TLS.
11	0.002372	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=11 Ack=134 Win=2619648 Len=0
14	0.002811	127.0.0.1	127.0.0.1	TLSv1.3	471	Client Hello
15	0.002831	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=134 Ack=438 Win=2619136 Len=0
16	0.003900	127.0.0.1	127.0.0.1	TLSv1.3	236	Server Hello
17	0.003914	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=438 Ack=326 Win=2619392 Len=0
18	0.003924	127.0.0.1	127.0.0.1	TLSv1.3	59	Change Cipher Spec
19	0.003932	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=438 Ack=332 Win=2619392 Len=0
20	0.004237	127.0.0.1	127.0.0.1	TLSv1.3	100	Application Data
21	0.004255	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=438 Ack=388 Win=2619392 Len=0
22	0.004274	127.0.0.1	127.0.0.1	TLSv1.3	474	Application Data
23	0.004286	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=438 Ack=818 Win=2618880 Len=0
24	0.004299	127.0.0.1	127.0.0.1	TLSv1.3	146	Application Data
25	0.004312	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=438 Ack=920 Win=2618880 Len=0
26	0.004315	127.0.0.1	127.0.0.1	TLSv1.3	111	Application Data
27	0.004335	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=438 Ack=994 Win=2618624 Len=0
28	0.004640	127.0.0.1	127.0.0.1	TLSv1.3	50	Change Cipher Spec
29	0.004657	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=994 Ack=444 Win=2619136 Len=0
30	0.005146	127.0.0.1	127.0.0.1	TLSv1.3	118	Application Data
31	0.005157	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=994 Ack=518 Win=2619136 Len=0
32	0.014031	127.0.0.1	127.0.0.1	TLSv1.3	80	Application Data
33	0.014062	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=994 Ack=554 Win=2619136 Len=0
38	0.014407	127.0.0.1	127.0.0.1	TLSv1.3	101	Application Data
39	0.014427	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=554 Ack=1051 Win=2618624 Len=0
40	0.014469	127.0.0.1	127.0.0.1	TLSv1.3	81	Application Data
41	0.014481	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=1051 Ack=591 Win=2619136 Len=0
46	0.040313	127.0.0.1	127.0.0.1	TLSv1.3	89	Application Data
47	0.040345	127.0.0.1	127.0.0.1	TCP	44	59834 → 21 [ACK] Seq=591 Ack=1096 Win=2618624 Len=0
48	0.040670	127.0.0.1	127.0.0.1	TLSv1.3	73	Application Data
49	0.040899	127.0.0.1	127.0.0.1	TCP	44	21 → 59834 [ACK] Seq=1096 Ack=620 Win=2619136 Len=0
54	0.047558	127.0.0.1	127.0.0.1	TLSv1.3	94	Application Data

Figura 9: Transferencia de archivo con FTPS [Wireshark]

Como podemos ver en la captura, a diferencia del protocolo FTP tradicional donde los datos del archivo son visibles en texto claro, en FTPS la transferencia se realiza mediante un canal cifrado. Esto impide que el contenido del archivo, así como los comandos asociados, puedan ser interpretados por terceros, asegurando la confidencialidad de la información transmitida.

6. Identificación de problemas y propuestas de Seguridad

6.1 Intercepción de datos por tráfico no cifrado

La red permite la intercepción de paquetes (sniffing) mediante herramientas como Wireshark debido a la ausencia de protocolos de comunicación seguros y mecanismos de monitoreo o registro de accesos. Cualquier persona conectada a la red podría capturar datos confidenciales y personales tales como contraseñas, sesiones, correos, números telefónicos entre otros.

Propuesta de mejora: Implementar cifrado en tránsito mediante protocolos seguros en todos los servicios requeridos (HTTPS, SSH, FTPS/SFTP, WPA2/3-Enterprise) para proteger los datos contra la interceptación.

6.2 Posibilidad de suplantación de identidad (spoofing) por falta de cifrado IP

La red no tiene cifrado en los paquetes IP por lo que podría permitir la suplantación de identificadores de red, tales como direcciones IP y direcciones MAC. Un atacante podría falsificar las direcciones para redirecciones de datos hacia dispositivos maliciosos, permitiendo la obtención de información sensible desde la red.

Propuesta de mejora: Habilitar Dynamic ARP Inspection (DAI) para prevenir ARP Spoofing y configurar Port Security en switches para controlar el acceso por dirección MAC, bloqueando las direcciones no autorizadas.

6.3 Falta de control de acceso a red para los dispositivos

La red no cuenta con un control efectivo que determine qué dispositivos pueden conectarse y obtener una dirección IP a través de DHCP. Esta falta de control podría permitir conexiones no autorizadas poniendo en riesgo la confidencialidad e integridad de la información sensible que circula diariamente o es almacenada en la red.

Propuesta de mejora: Implementar Network Access Control (NAC) con 802.1X para exigir autenticación de dispositivos/usuarios antes de conceder acceso a la red y condicionar la asignación DHCP a dicha autenticación.

6.4 Uso de protocolos de comunicación inseguros

La red utiliza los protocolos estándar para los servicios, los cuales no cifran la información (HTTP, FTP, SMTP). Al no tener implementado los protocolos seguros en la red, cualquier persona con acceso al tráfico de red puede visualizar directa o indirectamente el contenido de las comunicaciones incluyendo datos sensibles.

Propuesta de mejora: Reemplazar obligatoriamente protocolos inseguros por sus alternativas cifradas (HTTP por HTTPS, FTP por FTPS/SFTP, SMTP por SMTPS) utilizando TLS/SSL, y bloquear los protocolos inseguros a nivel de firewall o servidor.

6.5 Alto riesgo de propagación de malware y ransomware

La red carece de defensa ante software maliciosos, como antivirus y controles de acceso robustos, por lo que un malware o un ransomware podría ingresar a la LAN a través de un dispositivo infectado y propagarse rápidamente a través de los múltiples sistemas o dispositivos.

Propuesta de mejora: Implementar protección endpoint, IDS/IPS y filtrado de contenido para frenar el ingreso de código malicioso, mantener el sistema y apps parcheados y respaldar datos en copias inmutables, así se detiene la infección en el origen y se garantiza recuperación rápida ante ransomware.

6.6 Falta de segmentación de red

Todos los dispositivos y servidores de la organización residen en un único segmento de red lógico, no hay ningún tipo de separación a través de zonas con distintos niveles de seguridad, por lo que sería posible atacar toda la red o un dispositivo específico de inmediato incluyendo algún servicio crítico.

Propuesta de mejora: Dividir la red en VLANs (usuarios, servidores, invitados) con ACLs y colocar los servicios públicos en una DMZ protegida por un

firewall/Zone-Based FW la segmentación limita el movimiento lateral y aísla los recursos críticos.

6.7 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 o hacia/desde internet, por lo que cualquier dispositivo podría enviar y recibir peticiones hacia un puerto específico, lo que facilita ataques de escaneo, explotación de vulnerabilidades o ataques de denegación de servicios.

Propuesta de mejora: Desplegar un NGFW + ACLs (deny-all + permit-lo-necesario) y fuerza HTTP/SMTP/FTP a pasar por proxies o gateways con inspección junto a logs centralizados en un SIEM, bloquear puertos no autorizados y detectar escaneos o DoS al instante.

6.8 Falta de redundancia en servicios críticos

En la red, al existir solamente un servidor por cada servicio, frente a un ataque, el servicio podría quedar totalmente denegado e inútil, ya que, no existen mecanismos de respaldo automáticos, lo que podría generar la pérdida de transacciones y datos.

Propuesta de mejora: Configurar routers en HSRP/VRRP, enlaces EtherChannel y clústeres o balanceadores para los servicios, todo alimentado por UPS y si un nodo o enlace falla, el secundario asume automáticamente, eliminando puntos únicos de caída y manteniendo la disponibilidad.

7. Incidentes de seguridad potenciales de no aplicar medidas de seguridad

A continuación se presentan diversos incidentes de seguridad que podrían producirse si no se implementan las mejoras de seguridad documentadas para el protocolo FTP. Cada uno detalla la causa técnica, el vector de ataque y las posibles consecuencias derivadas de su explotación.

7.1 Filtración de información sensible

Causa: Transmisión de datos en texto plano – Cleartext Transmission of Sensitive Information (CWE-319)

Descripción: Usar protocolos como FTP sin cifrado permite que herramientas como Wireshark puedan capturar fácilmente usuarios, contraseñas y otros datos sensibles durante la transmisión.

Vector de ataque: Un atacante conectado a la misma red puede capturar tráfico de red para interceptar credenciales y otra información sensible.

Escalamiento del ataque: Con las credenciales obtenidas, el atacante puede acceder a otros servicios autenticados, realizar movimientos laterales en la red, comprometer cuentas privilegiadas o acceder a bases de datos con información crítica.

7.2 Acceso no autorizado al sistema

Causa: Autenticación inadecuada – Improper Authentication (CWE-287)

Descripción: FTP con el usuario anonymous habilitado y permisos de escritura, lo que permite el acceso sin autenticación real al sistema.

Vector de ataque: El atacante se conecta directamente como usuario anonymous y obtiene acceso al servidor.

Escalamiento del ataque: El acceso inicial puede permitir la carga de archivos maliciosos, la ejecución de scripts automatizados o el reconocimiento interno de la infraestructura para comprometer otros servicios o sistemas vinculados.

7.3 Escalada de privilegios por mala configuración

Causa: Autorización inadecuada – Improper Authorization (CWE-285)

Descripción: Usuarios del servicio FTP con permisos de escritura en directorios críticos como /var/ y /etc/, lo que permite modificar archivos sensibles del sistema.

Vector de ataque: El atacante puede modificar archivos de configuración o scripts del sistema mediante su acceso FTP.

Escalamiento del ataque: Al alterar archivos sensibles del sistema, el atacante podría obtener persistencia, ejecutar código con privilegios elevados o deshabilitar mecanismos de seguridad del sistema operativo.

7.4 Acceso a archivos sensibles fuera del directorio permitido

Causa: Path Traversal – Path Traversal (CWE-22).

Descripción: Posibilidad de salir del directorio raíz definido en la configuración del servidor mediante payloads como ../../etc/passwd, accediendo así a archivos del sistema.

Vector de ataque: A través de un cliente FTP, el atacante accede a archivos del sistema fuera del sandbox esperado.

Escalamiento del ataque: El atacante podría extraer archivos con contraseñas (como /etc/shadow), leer claves privadas, obtener información de red o credenciales de servicios que le permitan expandir el compromiso.

7.5 Ejecución remota de comandos a través del servicio FTP

Causa: Validación insuficiente de entradas – Improper Input Validation (CWE-20).

Descripción: El servidor FTP acepta comandos maliciosos enviados por el cliente sin una validación adecuada, lo que podría permitir la ejecución remota de comandos arbitrarios si se combinan con configuraciones incorrectas o scripts automatizados vinculados al servicio.

Vector de ataque: El atacante envía comandos especialmente diseñados al servidor FTP, aprovechando scripts o automatizaciones mal configuradas, para ejecutar código en el sistema sin autorización.

Escalamiento del ataque: Si logra ejecutar comandos arbitrarios, puede establecer shells reversos, descargar malware, o pivotar hacia otros sistemas en la red, obteniendo control total del entorno comprometido.

7.6 Casos de vulneraciones en empresas reales

A continuación se presentan incidentes de seguridad ocurridos en entornos reales y en organizaciones de alto perfil, derivados del uso inadecuado del protocolo FTP. Estos casos permiten demostrar que los riesgos previamente descritos no son meramente teóricos, sino que continúan ocurriendo en la actualidad, generando pérdidas económicas significativas y afectando seriamente la reputación de las empresas involucradas.

- **Filtración de datos de clientes de Verizon.**

Causa: Configuración incorrecta de almacenamiento en la nube – Improper Authorization (CWE-285).

Descripción: Un bucket de Amazon S3, propiedad del proveedor externo NICE Systems, fue configurado incorrectamente, permitiendo el acceso público sin autenticación. Esta falla expuso información sensible de hasta 14 millones de clientes de Verizon, incluyendo nombres, direcciones y números PIN de cuentas.

- **Compromiso de datos de empleados de NASA.**

Causa: Acceso no autorizado a servidores internos – Improper Access Control (CWE-284).

Descripción: Un servidor de la NASA que almacenaba información personal identificable (PII), como números de Seguro Social, fue comprometido por actores maliciosos. La falta de controles de acceso adecuados permitió la intrusión y posible exfiltración de datos de empleados actuales y anteriores.

- **Exposición de datos de clientes y empleados de Toyota.**

Causa: Fuga de datos a través de terceros – Improper Authorization (CWE-285).

Descripción: Un actor de amenazas filtró 240 GB de datos robados de Toyota en un foro clandestino, incluyendo contratos, correos electrónicos y detalles financieros. La brecha se originó en un proveedor externo, evidenciando deficiencias en la gestión de accesos y controles de seguridad en la cadena de suministro.

- **Exposición masiva de números telefónicos de usuarios de Facebook.**

Causa: Acceso no autorizado a datos mediante scraping – Improper Access Control (CWE-284).

Descripción: En 2019, se descubrió una base de datos no protegida que contenía más de 419 millones de registros de usuarios de Facebook, incluyendo números telefónicos, identificadores de usuario y datos de ubicación. Esta información fue recopilada mediante técnicas de scraping, aprovechando una funcionalidad que permitía buscar usuarios por número de teléfono. Aunque Facebook desactivó esta función en 2018, los datos recopilados antes de esa fecha permanecieron expuestos en línea sin medidas de seguridad adecuadas.

8. Conclusión

En el presente informe se lograron documentar los avances y hallazgos correspondientes a la entrega final para la configuración de red para “TechMove”. Se logró la implementación funcional de la red en Cisco Packet Tracer satisfaciendo los requerimientos operativos iniciales de la empresa, incluyendo la configuración de los servicios DHCP, DNS, SMTP, FTP y HTTP.

Un componente principal de la fase fue el análisis práctico y teórico del protocolo FTP, en el cual mediante una captura de tráfico con Wireshark, se pudo demostrar la inseguridad de este protocolo, evidenciando transmisión de credenciales y contenido de archivos en texto plano. Este análisis permitió identificar la necesidad de adoptar protocolos seguros como FTPS.

Adicional a esto, se identificaron y describieron otras posibles vulnerabilidades presentes en el diseño de la red, tales como falta de cifrado, ausencia de control de acceso o exposición a malware, en donde para cada punto se formularon propuestas de mejora para mitigar los posibles riesgos que podrían terminar en incidentes de seguridad potenciales que fueron detallados en la sección correspondiente.

Finalmente, se cumplieron los objetivos iniciales, entregando no solo una red simulada operativa, sino también un diagnóstico clave de sus debilidades de seguridad y una hoja de ruta clara para mitigarlas, asegurando así que la red pueda proteger los activos y datos de la empresa mientras cumple sus funciones.

9. Bibliografía

References

- Andres (2020) *FTP, FTPS Y SFTP: Diferencias, Ventajas E Inconvenientes*, ahierro programación internet tecnología y otras historias. Available at: <https://blog.ahierro.es/ftp-ftp-sftp-diferencias-ventajas-inconvenientes/> (Accessed: 20 April 2025).
- Piensa Solutions (2022) *FTP vs SFTP VS FTPS: Principales Diferencias*, Blog Piensa Solutions. Available at: https://www.piensasolutions.com/blog/diferencias-ftp-sftp-ftp#Intercambio_de_datos 1 (Accessed: 20 April 2025).
- NFON (2025) *Request for comments (RFC)*, NFON Base de Conocimientos ES. Available at: <https://www.nfon.com/es/get-started/cloud-telephony/lexicon/base-de-conocimiento-de-estacar/cti-de-tercerosrequest-for-comments-rfc/> (Accessed: 20 April 2025).
- Postel, J. and Reynolds, J. (1985) *RFC 959: File transfer protocol*, IETF Datatracker. Available at: <https://datatracker.ietf.org/doc/html/rfc959> (Accessed: 20 April 2025).
- Ford-Hutchinson, P. (2005) *RFC 4217: Securing FTP with TLS*, IETF Datatracker. Available at: <https://datatracker.ietf.org/doc/html/rfc4217> (Accessed: 20 April 2025).
- Paniagua, G. (2000) *PROTOCOLO DE TRANSFERENCIA DE FICHEROS (FTP)*, RFC. Available at: <https://www.rfc-es.org/rfc/rfc0959-es.txt> (Accessed: 20 April 2025).
- Glass, V. (2025) *Understanding key differences between FTP, FTPS and SFTP*, JSCAPE. Available at: https://www.jscape-com.translate.goog/blog/understanding-key-differences-between-ftp-ftp-sftp?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc (Accessed: 20 April 2025).


- IETF. (s.f.). *RFC process*. Internet Engineering Task Force. Available at:
<https://www.ietf.org/process/rfc/>

10. Anexos

10.1 Anexo 1

Matriz RACI:  Matriz RACI

10.2 Anexo 2

Carta Gantt:  Carta Gantt Actividad Grupal - parte 1.xlsx