MÁSTER EN REVERSING, ANÁLISIS DE MALWARE Y BUG HUNTING

MÁSTER EN *ANÁLISIS DE MALWARE Y REVERSING*

María Sonia Salido Fernández

Módulo 5 - Tarea 1

Campus Internacional CIBERSEGURIDAD

ENIIT INNOVA IT BUSINESS SCHOOL

UCAM UNIVERSIDAD CATÓLICA DE MURCIA

La infraestructura

- Esquema de la Red:

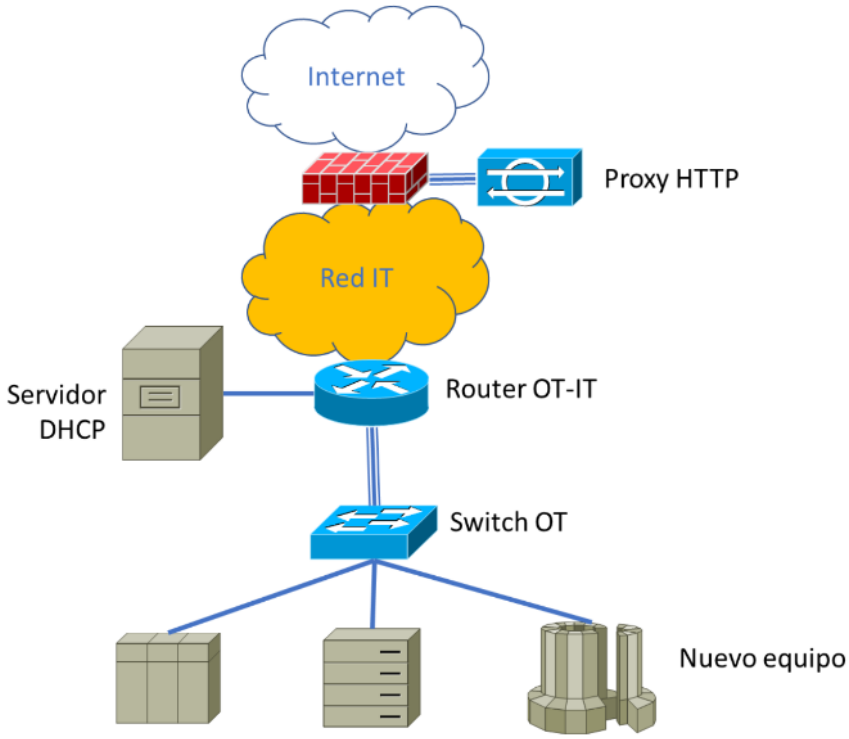


Figura 1 – Esquema de la red

- **El Nuevo Equipo:**
  - Se conecta a un Switch Ethernet OT a través de un puerto Fast Ethernet de 100Mbps.
  - Tiene SO propietario.
  - Sólo ofrece panel web de configuración.
  - No permite ejecutar comandos.
- **El Switch Ethernet OT:**
  - Tiene un enlace uplink de 10 Gbps con un Router OT-IT que le permite conectarse a la red IT de la organización.
  - No soporta port mirroring.
- **Equipos de la red industrial:**
  - Obtienen su dirección IPv4 y la configuración de red de un Servidor DHCP que está conectado al Router OT-IT.
  - Algunos equipos de la red industrial requieren que el servidor DHCP les proporcione parámetros de arranque.
  - Algunos equipos de la red industrial acceden a Internet.
- **El Router OT-IT:**
  - Interconecta las redes IT y OT.
  - Permite que los equipos industriales se comuniquen con un servidor DNS y un Proxy Web con conexión a Internet.

    - La infraestructura IT (incluyendo el router de interconexión) dispone de capacidades de port mirroring. Esto es es vital para capturar el tráfico que sale hacia la red IT o Internet.

- **El Proxy Web:**

    - Debe ser configurado en cada cliente.
    - El cliente debe disponer de un usuario y contraseña.
    - El proxy web es la única forma de salir a Internet desde dentro de la organización.
    - Almacena en un logs las URIs a las que se conecta cada cliente
    - No almacena en el log el contenido (payload) de los mensajes HTTP que se intercambian.

Se pide

- **I. Analizar “todos y cada uno” de los mecanismos/técnicas del Capítulo 3.**

    - Explicar cómo se podrían usar.
    - Explicar si son recomendables o no, para este caso.
    - Analizar los protocolos que emplea el nuevo equipo en sus comunicaciones internas y hacia Internet (incluyendo lo que se pueda inferir del uso del proxy HTTP y del servidor DHCP).
    - Analizar la información que se intercambia con el fabricante.

- **II. Proponer un mecanismo de captura de tráfico que cumpla:**

    - Configuración necesaria en la estación de captura.
    - Despliegue en la estación de captura.
    - Capturar todo el tráfico que envío o recibe el Equipo nuevo con otros equipos de la red.
    - Capturar todo el tráfico que envío o recibe el Equipo nuevo con Internet.
    - Tener impacto mínimo en OT.
    - No comprometer la fiabilidad.
    - Quedar desplegado en la ventana corta de mantenimiento y no requerir cambios posteriores, incluso si hay incidencias con la captura.
    - Se puede contar con la colaboración de los administradors de red IT siempre que no se comprometa la fiabilidad de OT, porque abre la puerta a soluciones basadas en port mirroring en el router, TAPs, etc.

I. Análisis de las técnicas de captura de Tráfico de Red

Para cada una de las técnicas y herramientas del capítulo 3, vamos a ir respondiendo a las siguientes preguntas:

- Cómo se podría usar esa técnica | herramienta en este caso. Explicar la configuración y su despliegue.
- Protocolos que podríamos ver usando esa técnica | herramienta.
- Información intercambiada con el fabricante.
- ¿Esta técnica | herramienta tiene un impacto mínimo en OT?
- ¿Esta técnica | herramienta compromete la fiabilidad?
- Conclusión: ¿Es recomendable esta técnica | herramienta en el ámbito de este ejercicio?

1. Estrategias de Captura de Tráfico de Red

1.1 En el propio equipo

Cómo se podría usar. Configuración y Despliegue:
Consistiría en instalar en el `Nuevo equipo` un sniffer como `tcpdump` o `Wireshark`, y capturar el tráfico en todos sus interfaces, incluido `loopback`, para ver todo el tráfico que genera y recibe. Permitiría además combinar la captura con herramientas tipo `netstat` o `strace` para mapear sockets, puertos y llamadas a sistema, enriqueciendo mucho el análisis de protocolos e información que se envía al fabricante.

Protocolos que podriamos ver:

- Todo el tráfico IP del equipo:
  - Loopback IP y tráfico normal de LAN.
  - DHCP para la obtención de IPv4 y parámetros de arranque.
  - Tráfico no-IP como ARP.
  - DNS ya que el router permite comunicación con el servidor DNS.
  - HTTP hacia el proxy.
- Podriamos analizar cabeceras y, si no hay cifrado, también el payload:
  - URLs completas.
  - Parámetros de actualización.
  - Contenido de informes de estado.
  - Identificadores de dispositivo, etc.
- Protocolos Industriales: Protocolos industriales del fabricante para la comunicación con otros equipos de la red OT.

Información intercambiada con el fabricante:

- Se podría identificar con precisión qué datos manda el equipo: versión de firmware, configuración, métricas de uso, logs, posibles datos sensibles y también cómo recibe datos, como ficheros de actualización, comandos de control, políticas.
- Al estar en el propio host no se pierde tráfico local, aunque ciertas optimizaciones de la `NIC` (`LSO`/`LRO`, `checksum offload`) pueden distorsionar tamaños y checksums en la captura, algo mitigable ajustando la configuración de `offloading`.

Impacto en la OT:

- Tiene un impacto alto en la OT, porque la ejecución de un proceso de captura consume recursos críticos de CPU y de memoria RAM, afectando el rendimiento del equipo monitorizado.

Fiabilidad en la OT:

- Compromete la fiabilidad: en un sistema propietario, cualquier proceso adicional no validado por el fabricante puede provocar bloqueos y no sería fácil de mantener si falla tras la ventana de mantenimiento
- Además, los efectos de `offloading` y `segmentación` pueden generar `ruido` en la captura como checksums incorrectos o paquetes demasiado grandes, y complicar la interpretación del tráfico.

Conclusión: ¿Es recomendable en el ámbito de este ejercicio?
Aunque la técnica es muy potente, en este escenario hay dos inconvenientes claros:

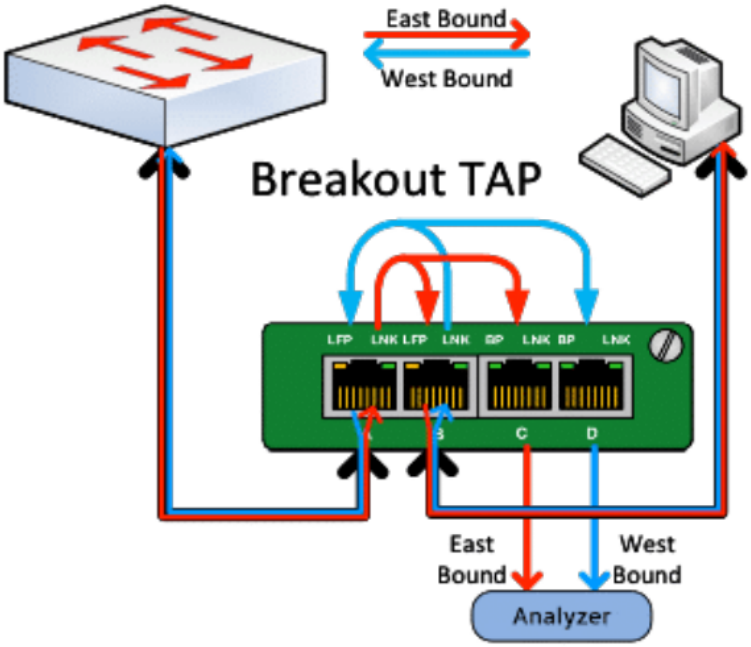
- Falta de acceso al equipo. No podemos instalar ni lanzar herramientas de captura.
- Requisitos estrictos de fiabilidad en la red OT.

Por tanto, para nuestro ejercicio es teóricamente la mejor para visibilidad, pero NO es aplicable ni recomendable.

1.2 Nivel físico o de Enlace

1.2.1 Network TAP - Sonda de Red - Pasivo

Un TAP - Test Access Point - de red es un dispositivo hardware que se inserta directamente en un enlace de red para duplicar el tráfico que circula por él hacia una estación de monitorización sin alterar el flujo original.



Cómo se podría usar. Configuración y despliegue:

- Se instalaría la sonda física, network TAP, entre el `Nuevo equipo` y el `Switch OT`, intercalándola en el enlace `Fast Ethernet 100 Mbps` para replicar todas las tramas entre ambos extremos hacia una o dos interfaces de la estación de captura.
- Switch OT ↔ TAP ↔ Nuevo equipo.
  - Switch → puerto A del TAP
  - Nuevo equipo → puerto B del TAP
- Estación de captura → puerto C (tráfico de A→B) y puerto D (tráfico de B→A).
  - La estación de captura se conectaría a los puertos de monitorización del TAP con sus interfaces en `modo promiscuo`, sin IP configurada, y con un sniffer como `tcpdump` o `Wireshark` grabando el tráfico. No se envía ningún paquete desde esos interfaces, sólo se recibe.

Protocolos que podríamos ver:

- Todo el tráfico Ethernet del Equipo nuevo: tramas ARP, DHCP, DNS, tráfico IP interno con otros equipos OT y tráfico IP hacia el router OT-IT, incluyendo HTTP/HTTPS hacia el proxy web.
- Al trabajar a nivel físico/enlace, se obtiene una copia íntegra de todas las tramas que salen y entran por ese enlace, independientemente de VLANs o protocolos de nivel superior, siempre que el TAP soporte la velocidad y el medio que en este caso es: cobre a 100 Mbps.

Información intercambiada con el fabricante:

- Se podrían identificar todas las conexiones del equipo con servidores externos: dominios/IPs de fabricante, puertos utilizados y patrones de comunicación.
- Si las sesiones no están cifradas, se puede inspeccionar el payload para ver parámetros de actualización, informes de estado, identificadores de dispositivo y otra telemetría; si están cifradas, al menos se obtienen metadatos, como SNI, certificados, tamaños y frecuencia de mensajes.

¿Tiene un impacto mínimo en OT?:

- Una sonda/TAP pasivo bien dimensionada tiene un impacto muy bajo, ya que actúa como un cable inteligente que sólo copia el tráfico sin introducir retardo apreciable ni modificar las tramas.
- Al colocarse en un enlace de 100 Mbps y diseñarse específicamente para esa velocidad, no debería introducir cuellos de botella siempre que sea hardware adecuado y se instale durante la ventana de mantenimiento.

¿Compromete la fiabilidad?:

- Las sondas pasivas se consideran muy fiables: si son realmente pasivas o tienen bypass físico, el enlace entre el equipo y el switch sigue funcionando incluso si la sonda pierde alimentación o la estación de captura se cae.
- El principal riesgo es físico, como un mal conector o una instalación defectuosa, pero una vez desplegada correctamente es una solución estable que no requiere cambios posteriores en la red OT.

Conclusión: ¿Es recomendable en el ámbito de este ejercicio?:

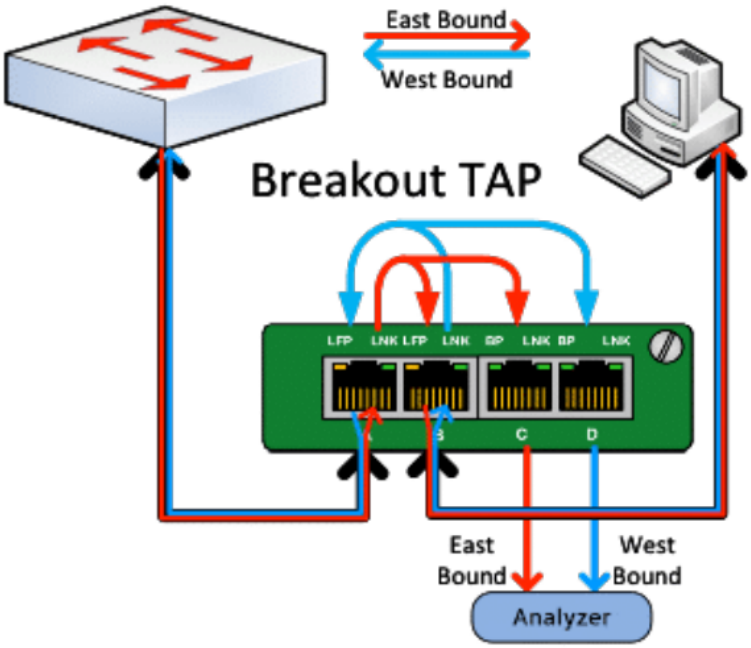
- Sí, es una de las técnicas más recomendables para este caso, porque permite capturar todo el tráfico del nuevo equipo con impacto mínimo y sin tocar su configuración ni la del switch OT, que además no soporta port mirroring.
- Cumple bien los requisitos del cliente, como la cobertura completa del tráfico del equipo, mínimo impacto, alta fiabilidad y posibilidad de dejarlo desplegado tras la ventana de mantenimiento, aunque exige disponer de un TAP físico adecuado y acceso físico al cableado entre el equipo y el switch.

1.2.2 Network TAP - Sonda de Red - Activo

Una sonda/TAP activo es un dispositivo físico que se inserta en línea entre el nuevo equipo y el switch para copiar el tráfico hacia una estación de captura. En enlaces de cobre de 1 Gbps o superiores se suele requerir este tipo de sonda frente a una pasiva; algunos modelos permiten agregar ambos sentidos en un único puerto de monitorización de mayor capacidad, a costa de necesitar alimentación, aunque suelen incluir un bypass físico A–B si se pierde la alimentación.

Cómo se podría usar. Configuración y despliegue:

- Misma configuración que en el TAP pasivo.



- Diferencia práctica frente al activo
  - En el activo, C y D pueden ser opcionales, a veces hay un solo puerto agregado.
  - En el pasivo, normalmente tiene dos salidas independientes, una por sentido, y no hay agregación ni funciones extra: sólo copias de la señal.

Protocolos que podríamos ver:
Se observaría exactamente el mismo tráfico que con un TAP pasivo en ese enlace.

Información intercambiada con el fabricante:
Permitiría identificar las conexiones del equipo con servidores externos, como direcciones, puertos, frecuencia, y si el tráfico no está cifrado, inspeccionar el contenido de las peticiones y respuestas para ver parámetros de actualización, informes de estado, identificadores de dispositivo y otros datos que se envían al fabricante.

Impacto y fiabilidad en OT:

- Es fundamental que el TAP activo disponga de bypass físico entre los puertos A y B para cuando pierda la alimentación, de modo que el enlace equipo–switch siga funcionando aunque el TAP o la estación de captura fallen. Con este bypass el impacto sobre la fiabilidad es muy bajo.

- A diferencia del TAP pasivo, introduce una latencia mínima al regenerar la señal y añade una dependencia de la alimentación y del propio hardware, lo que implica algo más de complejidad operativa y de supervisión, aunque en la práctica la latencia suele ser despreciable en un enlace de 100 Mbps bien dimensionado.

Conclusión: ¿Es recomendable en el ámbito de este ejercicio?:

- Para el enlace de 100 Mbps entre el nuevo equipo y el switch, un TAP pasivo ya sería suficiente y ofrece el menor riesgo posible (no requiere alimentación y puede introducir todavía menos puntos de fallo), por lo que suele considerarse preferible.
- Sin embargo, un TAP activo con bypass también cumpliría los requisitos del ejercicio, por lo que se puede usar como alternativa. Aunque se reserva en general los TAP activos como opción necesaria en enlaces de 1 Gbps o superiores.

1.2.3 Port mirroring (SPAN/RSPAN/ERSPAN)

Esta técnica consiste en configurar un switch o router para que envíe una copia de los paquetes vistos en uno o varios puertos (puertos origen) hacia un puerto específico (puerto destino o monitor) donde se conecta la estación de captura.

Cómo se podría usar. Configuración y despliegue:

- Esta técnico no podemos usarla en el Switch OT porque el enunciado dice que no tiene port mirroring.
- Sí podría aplicarse en la infraestructura IT, incluido el router de interconexión, que sí tiene esta capacidad.
- Despliegue: Se solicitaría al administrador de red que configurase en el router OT-IT una sesión de port mirroring (SPAN) que copie todo el tráfico de la interfaz conectada al uplink del switch OT hacia un puerto monitor, donde se conectaría la estación de captura, o bien lo envíe a otro switch/host remoto mediante RSPAN/ERSPAN, por ejemplo encapsulando el tráfico copiado en un túnel GRE.
- Configuración: La estación de captura se conectaría físicamente a ese puerto monitor para recibir la copia del tráfico
- Las interfaces de red que capturen el tráfico deben estar en modo promiscuo, ya que la mayoría de las tramas, salvo broadcast/multicast, no estarán destinadas a su dirección MAC.
- No se debe configurar una dirección IP en dichas interfaces, de forma que la estación de captura no pueda enviar tráfico a través de ellas.
- Se debe desactivar el reenvío de paquetes IP para evitar que la estación de captura actúe como router.
- No es recomendable utilizar un hub Ethernet para capturar tráfico, porque degrada significativamente el rendimiento de la red.

Protocolos que podríamos ver:

- Protocolos de Internet: Tráfico HTTP dirigido al proxy.
- Configuración de Red: Intercambios de DHCP, ya que el servidor está conectado al router.
- Resolución de Nombres: Consultas y respuestas DNS.
- Pérdida Crítica: Sólo veremos el tráfico que pase por ese el Router IT.

- No veremos:
  - El tráfico OT local entre equipos conectados al mismo switch OT puede no pasar por el router, y además el switch OT no puede espejarlo.
  - El tráfico local entre el "Nuevo equipo" y otros equipos industriales en el mismo switch, ya que este tráfico no llega al router

Información intercambiada con el fabricante:

- Permite identificar a qué servidores externos (dominios/IPs, puertos) se conecta el equipo, si usa el proxy, qué URLs o endpoints HTTP/HTTPS se alcanzan y con qué frecuencia.
- Si alguna comunicación no va cifrada, se podría inspeccionar el contenido para ver parámetros de actualización, informes de estado, identificadores de dispositivo o telemetría; si va cifrada, al menos se obtienen metadatos TLS (SNI, certificados, tamaños de registros).

Impacto y fiabilidad en OT:

- Impacto en la OT: La copia SPAN se hace en dispositivos IT (router/switch IT) sin tocar la configuración del switch OT ni del nuevo equipo, por lo que el impacto directo sobre la red OT es mínimo.
- El mirroring consume recursos del equipo que espeja, porque debe copiar tramas, encolarlas y enviarlas por el puerto destino.
- ¿Compromete la fiabilidad?: No, el uso de port mirroring es una técnica no intrusiva que no interfiere con el flujo de datos original.

Conclusión: ¿Es recomendable en el ámbito de este ejercicio?:

- Como técnica única para cumplir el requisito: “capturar todo el tráfico del nuevo equipo”: No es recomendable.
- Como técnica complementaria: Sí puede ser recomendable. Es útil como complemento para observar todas las comunicaciones del nuevo equipo hacia DNS/proxy/Internet desde la parte IT, aprovechando que la infraestructura IT dispone de port mirroring.
- Posible complemento:
  - TAP en el enlace del equipo = mecanismo principal.
  - SPAN/ERSPAN en router = apoyo/backup y para visibilidad agregada, no para sustituir el TAP.

1.2.4 Prácticas no recomendadas: Hubs Ethenet, Ataques MAC y Robo de puerto

- **Hubs Ethernet - Concentradores:** Aunque un Hub facilita la captura de tráfico al retransmitir todos los paquetes por todos sus puertos, su uso en entornos industriales modernos es contraproducente:
    - Un hub convierte el segmento en medio dúplex compartido: todas las estaciones comparten el mismo dominio de colisión, de modo que si varias estaciones transmiten a la vez se producen colisiones y hay que retransmitir, reduciendo mucho el rendimiento efectivo. - La velocidad máxima de los hubs se quedó en 100 Mbps y degradan seriamente una red moderna, lo que choca frontalmente con el requisito de no afectar la disponibilidad ni el rendimiento de la red OT.
- **Ataques MAC flooding:** Esta técnica consiste en saturar la tabla CAM (Content Addressable Memory) del switch con direcciones MAC falsas para forzarlo a entrar en modo "fail-open", comportándose como un hub.
    - Riesgo de denegación de servicio (DoS): Muchos switches industriales, al ser saturados, pueden bloquearse o reiniciarse en lugar de entrar en modo hub, lo que provocaría una interrupción total de la producción.
    - Inestabilidad del Switch OT: El enunciado prohíbe explícitamente cualquier acción que comprometa la fiabilidad de la red industrial. Un ataque de este tipo es una agresión directa a la infraestructura.
    - Impacto en otros equipos: Al convertir el switch en un hub mediante este ataque, el tráfico de todos los equipos industriales de la planta se vería afectado por colisiones, no solo el del Nuevo equipo.
- **Robo de Puerto:** Esta técnica implica enviar tramas con la dirección MAC de la víctima para "engañar" al switch y que este redirija el tráfico hacia el puerto del atacante.
    - Interrupción de las comunicaciones: Para que esta técnica funcione, se debe competir constantemente con el equipo legítimo por la propiedad de la MAC en la tabla del switch. Esto causa que el equipo original pierda paquetes de forma intermitente, rompiendo la comunicación.
    - Violación de la ventana de mantenimiento: El requisito indica que, una vez en producción, no es posible interrumpir la infraestructura. El robo de puerto es una técnica inestable por naturaleza que requiere ejecución continua y genera "ruido" en la red.
    - Detección y seguridad: Aunque se cuenta con la colaboración de los administradores, realizar ataques de este tipo puede disparar alertas de seguridad en el Router OT-IT o en los sistemas de monitorización de IT, complicando el análisis innecesariamente.

Conclusión: ¿Es recomendable en el ámbito de este ejercicio?:
Ninguna de estas técnicas son recomendables.

- Hub Ethernet: descartado por degradación de rendimiento/colisiones y por fiabilidad (dispositivo en línea).
- Ataques MAC y robo de puerto: descartados por ser ataques activos, ruidosos, poco fiables, con riesgo real de degradar o desestabilizar la LAN OT y contrarios a los requisitos del enunciado.

1.3 Nivel de red

Es una alternativa cuando no es posible acceder al sistema local ni realizar una captura a nivel físico o de enlace, por falta de acceso al hardware o de capacidades de port mirroring en el switch. Esta estrategia se centra en redirigir el tráfico IP para que pase obligatoriamente por la estación de captura.

1.3.1 Modificación de tablas de rutas.

Consiste en cambiar manualmente el "siguiente salto" en el equipo objetivo. No obstante, esto suele requerir permisos de superusuario, lo cual es poco probable si se está recurriendo a este nivel de captura.

Cómo se podría usar. Configuración y Despligue:

- Debido a que el Nuevo equipo no permite la ejecución de comandos para modificar su tabla de rutas local, esta técnica debería implementarse de forma indirecta:
    - Aprovechando el Servidor DHCP: Se configuraría el servidor DHCP que está conectado al router, para que asigne a través de la Opción 3 (Router/Gateway) la dirección IP de nuestra estación de captura en lugar de la dirección IP del Router OT-IT.
    - Estación de Captura: Debe configurarse como un gateway intermedio, habilitando el reenvío de paquetes (IP Forwarding) para recibir el tráfico del equipo y reenviarlo al router real.
- Despliegue: Se realizaría durante la ventana de mantenimiento configurando el servidor DHCP y reiniciando la interfaz de red del equipo para que tome la nueva ruta.

Protocolos que podriamos ver:

- Tráfico hacia Internet: Comunicaciones HTTP dirigidas al Proxy Web.
- Servicios de Red: Consultas DNS.
- Configuración: Intercambios iniciales de DHCP.
- Limitación importante: No se vería el tráfico local entre el nuevo equipo y otros dispositivos del Switch OT. Sólo se observaría el tráfico que efectivamente pase por la estación de captura; el tráfico local dentro de la subred OT o el que no se desvíe por esas rutas no se vería.

Información intercambiada con el fabricante:
Al actuar como intermediario hacia Internet, se capturaría:

- Payloads de comunicación: El contenido íntegro de los mensajes enviados al fabricante para actualizaciones o informes de estado.
- Credenciales: Usuario y contraseña enviados para autenticarse en el Proxy Web.
- Incluso cuando el tráfico vaya cifrado, se obtiene visibilidad de metadatos (IPs, puertos, frecuencia y tamaño de las comunicaciones) similar a la de un router en línea.

Impacto en la OT:
Esta técnico NO tienen un impacto mínimo en la OT. Obliga a cambiar la configuración de encaminamiento del equipo, directamente o vía DHCP, y hace que el tráfico pase “en línea” por la estación de captura que actúa como router.

Fiabilidad en la OT:
Compromete significativamente la fiabilidad: Si la estación de captura se apaga, se bloquea o tiene un fallo de software, el "Nuevo equipo" perderá totalmente la conectividad con el exterior.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable. A pesar de ser técnicamente posible mediante la configuración del servidor DHCP, se descarta por dos razones fundamentales:

- Visibilidad incompleta: No permite cumplir el requisito de capturar el tráfico con "otros equipos de la red industrial" (tráfico local).
- Riesgo operativo: Crea una dependencia crítica de la estación de captura, comprometiendo la fiabilidad de la red OT en caso de fallo.

1.3.2 Ataques AitM - Adversary in the middle

Esta técnica consiste en engañar a los dispositivos de una red local enviando mensajes ARP falsos para que asocien la dirección IP de una víctima (o del gateway) con la dirección MAC de la estación de captura. De este modo, el tráfico fluye a través del analista antes de llegar a su destino real.

Cómo se podría usar. Configuración y Despligue:

- Preparación: Se conectaría una estación de captura a un puerto libre del Switch OT durante la ventana de mantenimiento.
- Configuración: La estación debe tener habilitado el reenvío de paquetes IP (IP forwarding) para no cortar la comunicación.
- Ejecución: Se utilizaría una herramienta como Ettercap o arpspoof para realizar un envenenamiento ARP bidireccional entre el Nuevo equipo y el Router OT-IT.
- Tráfico Local: Para capturar el tráfico con otros equipos industriales, se debería realizar el ataque contra cada uno de esos objetivos específicos dentro del Switch OT.

Protocolos que podriamos ver:
Al situarse en medio de la comunicación, esta técnica permite ver prácticamente todo el tráfico IP del Nuevo equipo hacia fuera de su subred: DNS, HTTP/HTTPS vía proxy, conexiones directas con el fabricante, etc. También las comunicaciones industriales

Información intercambiada con el fabricante:
Al ser una interceptación completa, se tiene acceso a:

- Payloads de mensajes: El contenido íntegro de las comunicaciones con el fabricante, telemetría, estado, etc..
- Credenciales: El usuario y la contraseña enviados para cruzar el Proxy HTTP.
- Actualizaciones: Posibles descargas de archivos o firmware por parte del equipo

Impacto en la OT:
Esta técnica tiene un impacto significativo y negativo:

- Sobrecarga de Red: Genera tráfico adicional constante (mensajes ARP falsos) para mantener el envenenamiento.
- Latencia: Al obligar a que todos los paquetes pasen por el procesador de la estación de captura antes de ser reenviados, se introduce un retardo que puede ser crítico en procesos industriales de tiempo real.

Fiabilidad en la OT:
Compromete la fiabilidad de forma crítica:

- Punto único de fallo: Si la estación de captura sufre un bloqueo, se apaga o simplemente es más lenta que el tráfico original, el Nuevo equipo queda incomunicado (Denegación de Servicio).
- Inestabilidad: Las tablas ARP de los equipos industriales pueden comportarse de forma impredecible ante ataques continuos, provocando desconexiones aleatorias que violan el requisito de fiabilidad del sistema.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable:

- Viola el requisito de fiabilidad: Convierte a la estación de captura en un elemento crítico: un fallo detiene la producción.
- Impacto en el rendimiento: La introducción de latencia mediante esta técnica no es aceptable.

1.3.3 Redirección ICMP

Esta técnica de nivel de red se basa en el envío de mensajes de control ICMP (Internet Control Message Protocol) para informar a un host de que existe una ruta más corta o mejor para alcanzar un destino específico, obligándolo a enviar su tráfico a través de una estación intermedia.

Cómo se podría usar. Configuración y Despligue:

- Conexión: La estación de captura se conecta a un puerto libre del Switch OT.
- Suplantación: La estación de captura envía paquetes ICMP Redirect falsificados dirigidos al Nuevo equipo.
- Contenido del mensaje: El mensaje indicaría al equipo que para llegar a la dirección IP del Router OT-IT (o del Proxy), la mejor ruta es la dirección IP de la estación de captura.
- Reenvío: Es imprescindible que la estación de captura tenga habilitado el reenvío de paquetes (IP Forwarding) para que el tráfico llegue finalmente a su destino original y no se pierda la comunicación.

Protocolos que podriamos ver:

- Tráfico hacia Internet: Todas las peticiones HTTP dirigidas al Proxy Web.
- Resolución de nombres: Consultas DNS si el servidor DNS está fuera de la red local.
- Configuración de red: Tráfico DHCP.
- Limitación crítica: No veríamos el tráfico local entre el nuevo equipo y otros dispositivos del Switch OT, ya que ese tráfico es de Nivel 2 y no consulta la tabla de rutas ni al gateway para entregarse.

Información intercambiada con el fabricante:
Al interceptar el tráfico hacia el proxy, se obtendría:

- Contenido íntegro (Payload): A diferencia de los logs del proxy, aquí veríamos el cuerpo de los mensajes HTTP intercambiados con el fabricante.
- Credenciales: El usuario y contraseña necesarios para autenticarse en el Proxy HTTP.
- Datos de telemetría: Informes de estado y solicitudes de actualización enviados al exterior.

Impacto en la OT:
NO tienen un impacto mínimo en OT. Aunque el envío de mensajes ICMP es ligero, esta técnica:

- Introduce un salto adicional en la red, aumentando la latencia de las comunicaciones hacia el exterior.
- Consume recursos de red de forma innecesaria mediante la inyección de paquetes de control falsificados.

Fiabilidad en la OT:
Compromete la fiabilidad de forma grave:

- Punto único de fallo: Si la estación de captura falla o se apaga, el Nuevo equipo perderá la conectividad con el exterior, violando el requisito de no interrumpir la infraestructura.
- Muchos sistemas operativos modernos y dispositivos industriales tienen desactivada por defecto la aceptación de mensajes ICMP Redirect por motivos de seguridad (para evitar ataques AitM), por lo que la técnica podría simplemente no funcionar.
- Incompatibilidad: Dado que el equipo tiene un SO propietario, no podemos asegurar que acepte este tipo de redirecciones de ruta

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable. Esta técnica se descarta por las siguientes razones:

- Visibilidad incompleta: El cliente exige capturar el tráfico con "otros equipos de la red industrial", y esta técnica solo captura el tráfico que sale hacia el router.
- Inestabilidad: Depender de que un equipo industrial acepte redirecciones de ruta ICMP es muy arriesgado y poco profesional en entornos de misión crítica.
- Riesgo de interrupción: Crea una dependencia crítica de la estación de captura que compromete la fiabilidad de la red OT.

1.3.4 DHCP Spoofing

Esta técnica consiste en introducir un servidor DHCP falso (rogue DHCP) en la red que responda a las solicitudes de configuración de los clientes antes que el servidor legítimo, permitiendo al analista asignar parámetros de red malintencionados para interceptar el tráfico.

Cómo se podría usar. Configuración y Despligue:

- Despliegue: Se conectaría la estación de captura a un puerto libre del Switch OT durante la ventana de mantenimiento.
- Ataque de Carrera: La estación ejecutaría un software (como Ettercap o un script personalizado) para detectar mensajes DHCP Discover del Nuevo equipo y responder con un DHCP Offer más rápido que el servidor legítimo conectado al router.
- Configuración de Parámetros: Se configuraría el servidor falso para asignar al equipo su dirección IPv4, pero estableciendo la IP de la estación de captura como Puerta de Enlace Predeterminada (Gateway) y/o Servidor DNS.
- Reenvío: La estación de captura debe tener activo el IP Forwarding para redirigir el tráfico capturado hacia el router real y evitar que el equipo pierda conexión.
- Replicación de parámetros: Es vital que el servidor falso replique los "parámetros de arranque" personalizados que el equipo requiere del DHCP original para no impedir su inicio.

Protocolos que podriamos ver:

- Tráfico hacia el exterior: Todo el flujo HTTP dirigido al Proxy Web y comunicaciones con Internet. Resolución de nombres: Consultas DNS. Mensajes DHCP.
- Limitación: No capturaría el tráfico local entre el equipo y otros dispositivos industriales en el mismo switch (tráfico de Nivel 2), ya que este no pasa por el gateway.

Información intercambiada con el fabricante:

- Contenido de mensajes (Payload): A diferencia de los logs del proxy, se capturaría el cuerpo completo de los mensajes HTTP enviados al fabricante.
- Credenciales: El usuario y contraseña enviados para la autenticación en el Proxy HTTP.
- Reportes y Actualizaciones: Datos de estado y archivos de actualización descargados.

Impacto en la OT:
NO tiene un impacto mínimo en OT. Esta técnica se considera intrusiva:

- Inestabilidad de red: Introduce una condición de carrera entre dos servidores DHCP, lo que puede causar que el equipo obtenga configuraciones inconsistentes.
- Latencia: Añade un salto intermedio procesado por software, lo que incrementa el retardo en las comunicaciones industriales.

Fiabilidad en la OT:
Compromete la fiabilidad de forma crítica:

- Punto único de fallo: Si la estación de captura falla, se apaga o se desconecta, el equipo pierde su salida a la red y a Internet al no tener un gateway funcional.
- Persistencia: Si el servidor DHCP legítimo "gana" la renovación de la IP más tarde, la captura se detendría repentinamente.

- Arranque del equipo: Si no se replican exactamente los parámetros de arranque especiales mencionados en el enunciado, el equipo podría ni siquiera iniciar correctamente.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable. Aunque permite capturar el tráfico hacia Internet, el cual también podría capturarse mediante port mirroring en el router, se descarta por:

- Incapacidad de ver tráfico local: No cumple con el requisito de capturar comunicaciones con otros equipos de la red industrial.
- Tiene un alto impacto en la OT.
- Riesgo Operativo: Es una técnica "activa" que puede impedir el arranque o funcionamiento del equipo, violando la exigencia de máxima fiabilidad y nula interrupción en la red OT.

1.3.5 ARP/ND Poisoning

Esta técnica de nivel de red consiste en enviar respuestas ARP falsas a uno o varios equipos de la red para que asocien la dirección IP de una víctima, como el router, con la dirección MAC de la estación de captura. De esta forma, el atacante se sitúa en medio de la comunicación (Man-in-the-Middle).

Cómo se podría usar. Configuración y Despligue:

- Despliegue: Se conectaría una estación de captura a un puerto libre del Switch OT.
- Habilitación de Forwarding: Es imprescindible activar el reenvío de paquetes IP (IP forwarding) en la estación de captura para que esta actúe como un puente y no se pierda la comunicación.
- Ejecución: Se utilizarían herramientas como Ettercap, Bettercap o arpspoof para inundar al "Nuevo equipo" y al "Router OT-IT" con mensajes ARP malintencionados.
- Funcionamiento: El "Nuevo equipo" creerá que la estación de captura es el router, y el router creerá que la estación es el nuevo equipo, obligando a que todo el tráfico pase por el analista.

Protocolos que podriamos ver:
Al ser una técnica que intercepta el tráfico antes de que sea conmutado, permitiría ver:

- Tráfico Local: Comunicaciones entre el nuevo equipo y otros dispositivos industriales del mismo fabricante en el Switch OT.
- Servicios de Red: Intercambio de mensajes DHCP (solicitudes y parámetros de arranque) y consultas DNS.
- Tráfico de Aplicación: Todo el flujo HTTP destinado al panel de control web o al proxy.
- Protocolos Propietarios: Cualquier protocolo específico utilizado para la comunicación industrial.

Información intercambiada con el fabricante:
A diferencia de los logs del proxy, esta técnica permite capturar el contenido completo (payload) de los paquetes:

- Cuerpo de mensajes HTTP: Datos exactos de los informes de estado y telemetría enviados al fabricante.
- Actualizaciones: Archivos de firmware o parches descargados por el equipo.
- Credenciales: El usuario y la contraseña enviados para autenticarse en el Proxy HTTP.

Impacto en la OT:
NO tiene un impacto mínimo en OT. Esta técnica es considerada activa e intrusiva:

- Sobrecarga: Genera tráfico adicional constante en la red para mantener "envenenadas" las tablas ARP de los dispositivos.
- Latencia: Al obligar a que el tráfico pase por el software de la estación de captura antes de ser reenviado, se introduce un retardo que puede afectar a la sincronización de los procesos industriales en tiempo real.

Fiabilidad en la OT:
Compromete la fiabilidad de forma crítica:

- Punto Único de Fallo: Si la estación de captura se bloquea, se reinicia o tiene un rendimiento insuficiente, el Nuevo equipo quedará incomunicado, provocando una caída en la producción.
- Inestabilidad: Los sistemas operativos industriales (propietarios) pueden reaccionar de forma impredecible ante el envenenamiento ARP, pudiendo bloquearse o activar mecanismos de defensa que interrumpan la red.
- Fugas de tráfico: Si el ataque cesa, las tablas ARP tardan en recuperarse, lo que puede causar pérdida de paquetes intermitente.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable. Aunque el ARP Poisoning soluciona el problema de la falta de port mirroring en el Switch OT, se debe descartar por las siguientes razones:

- Viola el requisito de fiabilidad: El cliente exige que el sistema no se interrumpa incluso si hay problemas con el mecanismo de captura. Un fallo en la estación de captura bajo esta técnica cortaría la red.
- Impacto en producción: En entornos OT, introducir latencia y tráfico de ataque (aunque sea para auditoría) es una mala práctica que pone en riesgo la infraestructura crítica.

1.3.6 Túneles IP/GRE y VPN

Esta técnica consiste en encapsular el tráfico capturado en un punto de la red (como un switch o router) y enviarlo a través de un túnel IP (comúnmente GRE, utilizado en protocolos como ERSPAN) hacia una estación de captura remota situada en otro segmento de red.

Cómo se podría usar. Configuración y Despligue:

- Limitación en OT: No se puede originar el túnel desde el Switch OT, ya que este no dispone de capacidades de port mirroring ni de funciones de red avanzadas para la creación de túneles.
- Despliegue en el Router: Se configuraría el Router OT-IT, el cual sí permite port mirroring. El administrador configuraría una sesión de ERSPAN que duplique el tráfico de la interfaz conectada a la red industrial, lo encapsule en un túnel GRE y lo envíe a través de la red IT hasta la estación de captura.
- Configuración de la Estación: La estación de captura debe estar preparada para recibir el tráfico encapsulado y disponer de software (como Wireshark) capaz de decodificar el túnel GRE para analizar los paquetes originales en su interior.

Protocolos que podriamos ver:
Al realizarse la captura en el router, solo se vería el tráfico que atraviesa dicho dispositivo:

- Gestión de Red: Intercambios DHCP (solicitudes de IP y parámetros de arranque).
- Resolución de Nombres: Consultas y respuestas DNS.
- Tráfico hacia Internet: Comunicaciones HTTP dirigidas al Proxy Web o directamente a Internet.
- Pérdida Crítica: No se vería el tráfico local entre el equipo y otros dispositivos industriales en el mismo switch, ya que ese tráfico no llega al router y el switch no puede enviarlo al túnel.

Información intercambiada con el fabricante:
A través de este túnel se obtendría:

- Contenido Completo (Payload): El cuerpo íntegro de los mensajes HTTP enviados al fabricante, superando la limitación de los logs del proxy que solo guardan URLs.
- Telemetría y Actualizaciones: Los datos de estado, informes y posibles archivos de firmware intercambiados con los servidores externos.
- Autenticación: Credenciales de usuario y contraseña enviadas hacia el Proxy HTTP.

Impacto en la OT:
Tiene un impacto mínimo en OT. En dispositivos modernos como el router de interconexión, la encapsulación y el espejado se realizan mediante hardware especializado (ASIC), lo que no afecta al rendimiento ni a la latencia del tráfico de producción original. Añade, sin embargo, una ligera carga de tráfico adicional en la red IT por donde viaja el túnel.

Fiabilidad en la OT:
No compromete la fiabilidad. Es una técnica de monitorización pasiva respecto al flujo principal. Si el túnel cae o la estación de captura se desconecta, el tráfico entre la red OT e IT sigue fluyendo normalmente sin interrupciones.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable como solución única porque incumple el requisito de capturar todo el tráfico, ya que no veríamos las comunicaciones locales dentro de la red OT debido a la incapacidad del Switch OT para participar en este tipo de túneles.

Para cumplir con el enunciado, esta técnica debería combinarse con un TAP pasivo en el enlace del equipo, que se encargue de la parte del tráfico local que los túneles IP desde el router no pueden alcanzar.

1.4 Nivel de aplicación

1.4.1 Uso de Proxies - HTTP, SOCKS

Esta técnica se sitúa en el nivel de aplicación y utiliza un equipo intermedio (proxy) que actúa como pasarela para las peticiones de los clientes hacia servicios externos.

Cómo se podría usar. Configuración y Despligue:

- Aprovechamiento de la infraestructura: La red ya cuenta con un Proxy HTTP que es la única vía de salida a Internet.
- Configuración del dispositivo: Se debe acceder al panel de control web del Nuevo equipo para introducir manualmente la dirección IP del proxy, el puerto, el usuario y la contraseña.
- Captura de datos: Para cumplir el objetivo de análisis, se debería configurar el proxy, o interponer uno nuevo como mitmproxy o Burp Suite en la red IT, para que realice una inspección de contenido y guarde los cuerpos (payloads) de los mensajes, ya que el actual solo registra URLs.

Protocolos que podriamos ver:
Al trabajar en la capa de aplicación, esta técnica es muy selectiva:

- Protocolos Web: Únicamente tráfico HTTP y HTTPS.
- Tráfico de salida: Solo las peticiones que el equipo esté diseñado para enviar a través de un proxy.
- Pérdida Crítica: No permite ver ningún protocolo de niveles inferiores como ARP, DHCP, DNS (si se resuelven localmente) ni protocolos industriales propietarios que se intercambien con otros equipos de la red OT.

Información intercambiada con el fabricante:

- Payloads: El cuerpo de los mensajes con informes de estado, telemetría y solicitudes de actualización.
- Autenticación: Las credenciales que el equipo utiliza para validarse ante el proxy.
- URLs: El rastro de todos los dominios y recursos solicitados al fabricante.

Impacto en la OT:
NO tiene un impacto mínimo en OT, el impacto es moderado:

- Requiere intervención directa en la configuración del nuevo equipo.
- Si la configuración del proxy en el equipo es incorrecta, este no podrá comunicarse con el exterior desde el primer momento.
- No monitoriza el tráfico local, por lo que no ofrece visibilidad sobre el comportamiento del equipo dentro de la planta industrial.

Fiabilidad en la OT:
Compromete la fiabilidad, existe un riesgo considerable:

- Dependencia absoluta: Si el servidor proxy cae o se bloquea, el equipo pierde toda capacidad de actualizarse o informar al fabricante, lo que puede ser crítico para su mantenimiento.
- Error de configuración: Al ser un sistema con SO propietario, un error en la gestión de certificados (si se usa HTTPS con inspección) podría provocar que el equipo rechace la conexión y deje de funcionar correctamente.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable como método principal de captura. Aunque su uso es obligatorio para que el equipo tenga salida a Internet en esta red específica, como técnica de análisis presenta deficiencias insalvables para este caso:

- Visibilidad Parcial: Es totalmente ciego al tráfico entre equipos de la red industrial (OT-OT), incumpliendo el requisito de capturar "todo el tráfico".
- Insuficiencia Técnica: El proxy actual no almacena el contenido de los mensajes, que es precisamente lo que se necesita para analizar los protocolos y la información del fabricante.
- Intrusividad: Requiere configurar manualmente el equipo, lo que aumenta el riesgo de error humano frente a técnicas pasivas.

1.4.2 Proxy inverso

Un proxy inverso es un servidor que se sitúa frente a uno o más servidores web, interceptando las solicitudes de los clientes para gestionarlas antes de enviarlas al destino final. En el contexto de captura, permite inspeccionar el tráfico de nivel de aplicación de forma exhaustiva.

Cómo se podría usar. Configuración y Despligue:
Configuración del Equipo: Se debe acceder al panel de control web del Nuevo equipo y configurar la dirección del servidor del fabricante apuntando a la IP de nuestro proxy inverso.

Redirección DNS: Alternativamente, se podría configurar el servidor DNS para que resuelva el dominio del fabricante con la IP de la estación de captura donde corre el proxy inverso.

Despliegue: Se requiere instalar un software de proxy (como Nginx, Apache o herramientas específicas de análisis como Burp Suite o mitmproxy) en una máquina situada entre la Red OT y el Proxy HTTP de salida.

Protocolos que podriamos ver:
Al operar en la capa de aplicación, la visibilidad se limita a protocolos de alto nivel:

- HTTP y HTTPS: Es la técnica ideal para analizar el tráfico web cifrado o plano.
- Protocolos Web-based: Cualquier comunicación basada en API REST o SOAP que el fabricante utilice para la telemetría.
- Limitación: No permite ver tráfico local (ARP, protocolos industriales de Nivel 2) ni otros protocolos de red como DHCP.

Información intercambiada con el fabricante:

- Cuerpo de los mensajes (Payloads): Permite ver el contenido exacto de los reportes enviados (datos de sensores, configuraciones internas).
- Cabeceras: Información sobre el software, versiones y métodos de autenticación.
- Actualizaciones: Permite interceptar y analizar los archivos de firmware que el fabricante envía al equipo.

Impacto en la OT:
NO tiene un impacto mínimo en OT:

- Requiere modificar la configuración original del equipo industrial.
- Introduce latencia adicional al tener que procesar la conexión, terminarla y establecer una nueva hacia el destino real.
- No monitoriza el tráfico entre el equipo y el resto de la planta (comunicaciones este-oeste).

Fiabilidad en la OT:
Compromete la fiabilidad significativamente:

- Punto Único de Fallo: Si el proxy inverso falla o se satura, el equipo pierde completamente la comunicación con el fabricante.
- Incompatibilidad: Al ser un SO propietario, el equipo podría rechazar la conexión si el proxy inverso no gestiona perfectamente los certificados o tiempos de espera, provocando errores en producción.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable como técnica principal. Aunque es excelente para analizar el contenido de los mensajes HTTP que el proxy actual de la empresa ignora, se descarta por las siguientes razones:

- Visibilidad incompleta: El cliente exige capturar el tráfico con otros equipos de la red industrial. El proxy inverso es totalmente ciego al tráfico que no vaya destinado al servidor externo.
- Riesgo Operativo: Incumple el requisito de fiabilidad extrema. Un fallo en la estación de captura cortaría la funcionalidad del equipo.
- Configuración Intrusiva: Obliga a alterar los parámetros del equipo, lo cual no es ideal en una ventana de mantenimiento corta si se busca una solución pasiva y transparente.

1.4.3 Interceptación DNS

Esta técnica consiste en capturar o desviar las consultas de nombres de dominio realizadas por un equipo para identificar a qué servidores intenta conectarse o para redirigir ese tráfico hacia una estación de análisis.

Cómo se podría usar. Configuración y Despligue:

- Vía DHCP (Configuración): Dado que el equipo obtiene su configuración de red por DHCP, se podría modificar el servidor DHCP para que asigne la dirección IP de la estación de captura como servidor DNS primario del equipo.
- Vía DNS Spoofing (Despliegue): Durante la ventana de mantenimiento, se desplegaría una herramienta (como Ettercap o un servidor DNS falso) que responda a las peticiones DNS del "Nuevo equipo" antes que el servidor legítimo, proporcionando direcciones IP controladas por el analista para forzar el paso del tráfico por una sonda.
- Sonda Intermedia: La estación de captura debe estar preparada para resolver las peticiones o actuar como un proxy para no romper la comunicación con el fabricante.

Protocolos que podriamos ver:

- Protocolo DNS: Consultas (Queries) y respuestas (Answers).
- Protocolos de Aplicación Posteriores: Si la interceptación se usa para redirigir el tráfico (haciendo creer al equipo que el servidor del fabricante es la estación de captura), se podrían capturar protocolos como HTTP o HTTPS.
- Limitación Crítica: No veríamos el tráfico local entre el nuevo equipo y otros dispositivos industriales. Los equipos industriales en una misma subred suelen comunicarse mediante direcciones IP directas o protocolos de Nivel 2, por lo que no realizan consultas DNS para hablar entre ellos.

Información intercambiada con el fabricante:

- Destinos de conexión: Lista de dominios y servidores exactos a los que el equipo intenta contactar para actualizaciones o telemetría.
- Payloads (si hay redirección): Si la interceptación DNS se utiliza para derivar el tráfico a un proxy, se capturaría el contenido íntegro de los informes de estado y mensajes que el log del proxy actual no guarda.

Impacto en la OT:
NO tiene un impacto mínimo en OT. Esta técnica es intrusiva por varias razones:

- Introduce latencia en la resolución de nombres, lo que puede afectar a aplicaciones industriales sensibles al tiempo.
- Requiere la manipulación de servicios críticos de infraestructura como el DHCP o el DNS de la organización.

Fiabilidad en la OT:
Compromete la fiabilidad de forma considerable:

- Punto único de fallo: Si la estación de captura que responde a las consultas DNS falla, el equipo no podrá traducir nombres a IPs y perderá toda capacidad de comunicarse con Internet o el fabricante.
- Inestabilidad por Caché: Los sistemas operativos suelen guardar copias (caché) de las respuestas DNS; si la interceptación falla o cambia, el comportamiento del equipo puede volverse errático e impredecible.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable como solución única. Se descarta para este caso particular debido a que:

- Falta de visibilidad local: El cliente exige capturar el tráfico con "otros equipos de la red industrial", y la interceptación DNS es totalmente ciega a ese tráfico interno.
- Riesgo de interrupción: Cualquier fallo en el servidor DNS interceptor cortaría la salida a Internet del equipo, incumpliendo el requisito de fiabilidad absoluta en la red OT.
- Dependencia del Proxy: El enunciado indica que la salida a Internet debe pasar por un Proxy HTTP. Si el equipo ya está configurado para usar un proxy, es probable que ni siquiera realice consultas DNS locales (las delega al proxy), haciendo que esta técnica sea inútil.

1.4.4. Nat destino (DNAT)

Esta técnica consiste en configurar un dispositivo de red (como un router o firewall) para que modifique la dirección IP de destino de los paquetes entrantes, redirigiéndolos de forma transparente hacia una estación de captura o una sonda de análisis en lugar de a su destino original.

Cómo se podría usar. Configuración y Despligue:
Debido a que el Nuevo equipo tiene un SO propietario y no permite cambios internos, la técnica debe aplicarse en el nodo de red que gestiona su salida:

- Punto de aplicación: El Router OT-IT es el lugar adecuado, ya que interconecta la red industrial con el resto de la organización.
- Configuración: Se crearía una regla en el router que intercepte los paquetes provenientes de la IP del "Nuevo equipo" cuyo destino sea el Proxy HTTP o servidores externos, y cambie ese destino por la IP de la estación de captura.
- Despliegue: Se debe realizar durante la ventana de mantenimiento inicial para configurar las tablas de NAT del router y asegurar que la estación de captura esté lista para procesar y reenviar el tráfico.

Protocolos que podriamos ver:
Al ser una técnica aplicada en el router de interconexión, la visibilidad es limitada:

- Tráfico hacia el exterior: Protocolos HTTP y HTTPS dirigidos al fabricante o al proxy.
- Servicios de Red: Peticiones DNS si el destino es externo.
- Limitación Crítica: No veríamos el tráfico local entre el equipo y otros dispositivos del Switch OT. Este tráfico se conmuta internamente en el switch (Capa 2) y nunca llega al router para que se le aplique el DNAT.

Información intercambiada con el fabricante:

- Contenido Completo (Payload): Todo el cuerpo de los mensajes enviados al fabricante (telemetría, reportes de estado), superando la limitación del log actual del proxy.
- Actualizaciones: Identificación de archivos de firmware descargados.
- Credenciales: El usuario y contraseña enviados para autenticarse en el Proxy HTTP.

Impacto en la OT:
NO tiene un impacto mínimo en OT. Aunque muchos routers realizan NAT mediante hardware (ASIC), esta técnica:

- Introduce un proceso de manipulación de paquetes que puede añadir latencia a las comunicaciones industriales.
- Aumenta la complejidad de la red, dificultando el diagnóstico de problemas de conectividad si el equipo falla.

Fiabilidad en la OT:
Compromete la fiabilidad de forma significativa:

- Punto único de fallo: Si la regla de DNAT redirige el tráfico a una estación de captura que se bloquea o apaga, el "Nuevo equipo" perderá totalmente la conexión con el exterior.
- Dependencia: El equipo industrial depende de que la estación de captura reciba, procese y entregue los paquetes correctamente al destino real, lo cual viola el requisito de fiabilidad absoluta en la red OT.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable. Se descarta para este caso particular por las siguientes razones:

- Incumplimiento de Requisitos: El cliente exige capturar todo el tráfico, y el DNAT en el router es ciego al tráfico local entre equipos industriales en el mismo switch.
- Riesgo Operativo: Convierte a la estación de captura en un elemento crítico de la red. Un fallo en la estación cortaría la comunicación del equipo, algo prohibido por el cliente una vez que el equipo entre en producción.
- Complejidad Innecesaria: Teniendo capacidades de port mirroring en el router, es más seguro y sencillo duplicar el tráfico que redirigirlo mediante NAT.

1.4.5 Paneles de desarrollo en navegadores

Cómo se podría usar. Configuración y Despligue:
Esta técnica consiste en utilizar las herramientas de depuración integradas en los navegadores web o interfaces de diagnóstico proporcionadas por el propio fabricante para inspeccionar el tráfico.

Protocolos que podriamos ver:
Al ser una técnica estrictamente limitada a la capa de aplicación del navegador, la visibilidad es muy reducida:

- Protocolos Web: Principalmente HTTP y HTTPS.
- Intercambio de datos: Mensajes en formato JSON, XML o HTML.
- Limitación Crítica: No permite ver ningún protocolo industrial (Nivel 2), ni tráfico de red como ARP, DHCP o DNS. Tampoco permite ver las comunicaciones que el equipo realiza de forma autónoma con el fabricante (como actualizaciones de firmware) si estas no pasan por el panel web.

Información intercambiada con el fabricante:

- APIs de configuración: Las rutas y parámetros que el panel web utiliza para enviar comandos al equipo.
- Payloads: Datos técnicos que se muestran en el panel y que podrían estar siendo replicados hacia el fabricante.
- Credenciales: Es posible capturar el usuario y contraseña que se introducen en el panel web para la gestión.

Impacto en la OT:
Tiene un impacto mínimo en OT. El impacto es prácticamente inexistente sobre la infraestructura, ya que solo se está interactuando con una interfaz que el equipo ya ofrece de serie.

Fiabilidad en la OT:
No compromete la fiabilidad. No existe riesgo de caída de red o del equipo por el simple hecho de inspeccionar el tráfico en el navegador del analista.

Sin embargo, es poco fiable para el análisis, ya que solo ofrece una visión parcial y sesgada del tráfico total que el cliente desea capturar.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
No es recomendable como técnica de captura principal. Aunque es útil para entender cómo funciona la interfaz de gestión, se descarta para cumplir con los objetivos del proyecto por las siguientes razones:

- Incumplimiento de Requisitos: El cliente solicita capturar todo el tráfico (local e Internet). Esta técnica es ciega al tráfico local entre equipos OT y a cualquier comunicación que el equipo realice en segundo plano fuera de la sesión web del analista.

- Invisibilidad Industrial: Al no soportar protocolos de niveles inferiores ni protocolos industriales propietarios, no permite conocer si el equipo se comunica con otros dispositivos del mismo fabricante en la planta.

- Insuficiencia: El enunciado indica que el equipo realiza comunicaciones con el fabricante para informes de estado y actualizaciones; estos procesos suelen ser autónomos y no aparecerán en el panel de desarrollo del navegador.

2 Herramientas de Captura y Análisis de Tráfico

2.1. Captura de tráfico con ‘tcpdump’

La herramiento ‘tcpdump’ es una herramienta de línea de comandos para la captura y análisis de paquetes de red que utiliza la librería libpcap. Es el estándar en sistemas tipo Unix para realizar volcados de tráfico crudo hacia archivos que luego pueden analizarse con herramientas gráficas como Wireshark.

Cómo se podría usar. Configuración y Despligue:
Dado que el "Nuevo equipo" tiene un sistema operativo propietario y no permite ejecutar comandos adicionales, es imposible instalar o ejecutar tcpdump directamente en él. Se podría usar en una estación de captura externa, como un laptop o servidor con Linux.

- Conexión Física: Esta estación se conectaría físicamente al puerto de monitorización de un TAP pasivo (colocado entre el equipo y el Switch OT) o a un puerto configurado con Port Mirroring en el Router OT-IT.
- Comando de Ejecución: Se ejecutaría el comando

  ```
  tcpdump -i [interfaz] -s 0 -w captura.pcap
  ```

  para capturar paquetes completos sin recortar y guardarlos en un archivo para el análisis de reversing.

Protocolos que podriamos ver:
Al ser una herramienta de captura de bajo nivel, tcpdump registra todo lo que circula por el cable:

- Nivel de Enlace y Red: Tráfico ARP, paquetes IP, mensajes de control ICMP e intercambios DHCP (incluyendo parámetros de arranque).
- Nivel de Transporte: Segmentos TCP y UDP que componen las sesiones de comunicación.
- Nivel de Aplicación: Peticiones DNS, tráfico HTTP íntegro y cualquier protocolo industrial propietario del fabricante que se intercambie en la red OT.

Información intercambiada con el fabricante:
A diferencia de los logs del proxy, tcpdump permite inspeccionar el contenido (payload) de los datos:

- Cuerpo de mensajes HTTP: Veríamos los datos exactos enviados en los informes de estado y telemetría.
- Actualizaciones: Podríamos capturar y reconstruir los archivos de firmware o parches descargados.
- Autenticación: Identificación de las credenciales de usuario y contraseña enviadas hacia el Proxy Web.

Impacto en la OT:
Tiene un impacto mínimo en OT:

- Al ejecutarse en una estación independiente conectada a un TAP o puerto espejo, no consume ni un solo ciclo de CPU ni memoria RAM de los equipos industriales de producción.
- No introduce latencia en las comunicaciones industriales originales, cumpliendo con el requisito de impacto mínimo en la planta.

Fiabilidad en la OT:
No compromete la fiabilidad. Al ser una herramienta de escucha pasiva en una estación externa, si el proceso de tcpdump falla o la estación se apaga, el tráfico de producción entre el equipo, el switch y el router sigue fluyendo sin alteraciones.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
Es altamente recomendable como software de captura. Si bien tcpdump no es una técnica de acceso al tráfico por sí sola (requiere un TAP o Mirroring), es la herramienta técnica ideal para este ejercicio porque:

- Fidelidad: Permite capturar el tráfico crudo necesario para el análisis de protocolos que solicita el fabricante.
- Seguridad Industrial: Permite realizar la captura de forma no intrusiva desde una estación externa, respetando la prohibición de ejecutar comandos en el equipo industrial.
- Portabilidad: Los archivos .pcap generados son compatibles con Wireshark para el análisis profundo posterior que requiere la tarea.

2.2. Análisis de tráfico con Wireshark

Wireshark es un analizador de protocolos de red gráfico que permite inspeccionar de forma detallada el tráfico capturado, facilitando la reconstrucción de sesiones y el análisis profundo de las comunicaciones.

Cómo se podría usar. Configuración y Despligue:
Debido a que el "Nuevo equipo" tiene un SO propietario y no permite ejecutar comandos adicionales, Wireshark no puede ejecutarse directamente en el equipo monitorizado. Debe instalarse en una estación de trabajo externa, como un ordenador portátil o un PC de los administradores, que tenga instaladas las librerías libpcap o WinPcap.

- Despliegue Físico: La estación se conectaría al puerto de monitorización de un Network TAP (situado entre el nuevo equipo y el Switch OT) o a un puerto configurado con Port Mirroring en el Router OT-IT.
- Configuración: Se configuraría la interfaz de red de la estación en modo promiscuo para que Wireshark pueda capturar todos los paquetes que circulan por el segmento, no solo los dirigidos a su propia dirección MAC.

Protocolos que podriamos ver:
Wireshark es capaz de decodificar cientos de protocolos, lo que permitiría visualizar:

- Nivel de Red/Enlace: Tráfico ARP, intercambios de DHCP (incluyendo las opciones personalizadas y parámetros de arranque) y consultas DNS.
- Comunicaciones Industriales: Protocolos propietarios del fabricante utilizados para hablar con otros equipos de la red industrial.
- Tráfico Web: Mensajes HTTP completos dirigidos tanto al panel de control web como al Proxy HTTP de salida.

Información intercambiada con el fabricante:
A diferencia del log del proxy, Wireshark permite realizar una inspección profunda de paquetes para extraer:

- Contenido (Payload): Los datos específicos de los informes de estado y telemetría enviados al fabricante.
- Actualizaciones: La identificación y posible extracción de los archivos de firmware descargados.
- Credenciales: El usuario y contraseña empleados por el equipo para autenticarse en el Proxy Web.

Impacto en la OT:
Tiene un impacto mínimo en OT:

- Al ejecutarse en una estación de captura independiente y recibir el tráfico de forma pasiva (vía TAP o Mirroring), Wireshark no consume recursos del equipo industrial ni del resto de la infraestructura de producción.
- No introduce latencia ni modificaciones en las tramas originales de la red OT.

Fiabilidad en la OT:
No compromete la fiabilidad. La fiabilidad de la red industrial se mantiene intacta. Si la estación de trabajo donde corre Wireshark se bloquea o desconecta, el flujo de datos entre el equipo y el switch sigue funcionando sin interrupciones, cumpliendo con el requisito de mantenimiento de la infraestructura en producción.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?
Es la herramienta más recomendable para la fase de análisis. Aunque para la captura de larga duración o en sistemas con pocos recursos se prefiera tcpdump, Wireshark es indispensable en este caso porque:

- Potencia de Análisis: Facilita enormemente el objetivo de "analizar los protocolos y la información intercambiada con el fabricante" gracias a sus filtros y capacidad de seguir flujos TCP.
- Visibilidad Completa: Permite ver los detalles que el proxy oculta, como el contenido de los mensajes y los protocolos industriales no basados en HTTP.
- Seguridad: Permite a los analistas trabajar de forma no intrusiva, respetando las estrictas restricciones de fiabilidad de la red industrialde la empresa.

2.3. Análisis de tráfico a nivel de aplicación con ‘mitmproxy’

La herramienta ‘mitmproxy’ es interactiva de tipo "man-in-the-middle" diseñada específicamente para interceptar, inspeccionar, modificar y reproducir tráfico HTTP y HTTPS.

Cómo se podría usar. Configuración y Despligue:

- Interposición en la red: Dado que el "Nuevo equipo" ya requiere configurar un Proxy HTTP para salir a Internet, se puede situar una estación con mitmproxy entre el equipo industrial y el Proxy corporativo.
- Configuración del equipo: Se accedería al panel web del equipo industrial para cambiar la dirección del proxy por la IP de la estación de captura con mitmproxy.
- Inspección SSL/TLS: Para analizar el tráfico cifrado (HTTPS) con el fabricante, se debería instalar el certificado raíz (CA) de mitmproxy en el equipo industrial. No obstante, al tener un SO propietario que no permite comandos, esta tarea podría ser imposible si el panel web no ofrece una opción de importación de certificados.
- Modo Transparente: También podría configurarse como un proxy transparente mediante reglas de red en el router, evitando modificar la configuración del equipo.

Protocolos que podriamos ver:
Al ser una herramienta de capa de aplicación, su visibilidad es muy específica:

- Protocolos Web: Únicamente HTTP, HTTPS y WebSockets.
- Pérdida de visibilidad local: No permite ver ningún protocolo industrial (como Modbus, Profinet, etc.) que se intercambie con otros equipos del Switch OT, ni protocolos de red como ARP, DHCP o DNS.

Información intercambiada con el fabricante:
Es una de las herramientas más potentes para este objetivo específico:

- Cuerpo de los mensajes (Payload): Permite ver el contenido íntegro de los informes de estado y telemetría que el log del proxy actual de la empresa ignora.
- Flujo de actualización: Facilita el análisis de las peticiones de descarga de firmware y la estructura de las APIs del fabricante.
- Credenciales: Captura de forma clara el usuario y contraseña enviados hacia el exterior.

Impacto en la OT:
NO tiene un impacto mínimo en OT. Es una herramienta activa e intrusiva.

- Introduce latencia en las comunicaciones debido al proceso de interceptación y re-encapsulamiento de los paquetes.
- Requiere cambios en la configuración del equipo o en el enrutamiento de la red IT/OT.

Fiabilidad en la OT:
Compromete la fiabilidad de forma crítica:

- Punto único de fallo: Si la estación con mitmproxy se apaga o el software falla, el equipo industrial pierde toda conectividad con Internet y con el fabricante.
- Riesgo de producción: El enunciado prohíbe interrumpir la infraestructura una vez en producción; el uso de un proxy activo intermedio crea una dependencia que viola esta restricción.

Conclusión: ¿Es recomendable en el ambito de este ejercicio?

No es recomendable como solución única. Aunque mitmproxy es la mejor herramienta para el análisis profundo de los mensajes HTTP/HTTPS que el cliente solicita investigar, presenta fallos de cumplimiento graves para este caso:

- Visibilidad incompleta: El cliente exige capturar "todo el tráfico", incluyendo el intercambio con otros equipos de la red industrial, algo que mitmproxy no puede hacer.
- Riesgo Operativo: Su naturaleza activa compromete la fiabilidad de la red OT de ACME, S.A., la cual no admite interrupciones una vez desplegado el equipo.

II. Solución final

Recapitulamos todas las técnicas y herramientas analizadas anteriormente:

- En el propio equipo
- Network TAP - Sonda de Red - Pasivo
- Network TAP - Sonda de Red - Activo
- Port mirroring (SPAN/RSPAN/ERSPAN)
- Modificación de tablas de rutas.
- Ataques AitM - Adversary in the middle
- Redirección ICMP
- DHCP Spoofing
- ARP/ND Poisoning
- Túneles IP/GRE y VPN
- Uso de Proxies (HTTP, SOCKS)
- Proxy inverso.
- Interceptación DNS
- Nat destino (DNAT)
- Paneles de desarrollo en navegadores
- Captura de tráfico con ‘tcpdump’
- Análisis de tráfico con ‘Wireshark’
- Análisis de tráfico a nivel de aplicación con ‘mitmproxy’

Técnicas Recomendadas

Para garantizar la fiabilidad y capturar tanto el tráfico local como el de Internet, se deben combinar estas dos técnicas:

- **Network TAP (Sonda de Red) - Pasivo:** Es la técnica principal y obligatoria. Debe colocarse físicamente entre el "Nuevo equipo" y el "Switch OT". Al ser pasivo, si la estación de captura falla o pierde energía, el enlace de red del equipo industrial no se interrumpe (así cumple el requisito de fiabilidad). Permite capturar el tráfico local (OT-OT) que el switch no puede duplicar y el tráfico hacia Internet.

- **Port Mirroring (SPAN) en el Router OT-IT:** Se debe usar como técnica complementaria. Aunque el Switch OT no tiene esta capacidad, el Router OT-IT sí. Configurar un espejo en el router permite verificar qué tráfico llega realmente a la red IT, capturar con precisión los mensajes DHCP (configuración inicial) y las peticiones al Proxy HTTP.

Configuración necesaria de la NIC de captura, tanto con TAP como con mirroring:

- NIC en modo promiscuo.
- No asignar IP a la interfaz de captura.
- Desactivar el reenvío IP, para no comportarse como un router.

Herramientas de Captura y Análisis

Una vez que con las técnicas anteriores obtenemos el tráfico de red, se requieren herramientas para procesarlo:

- **Captura de tráfico con tcpdump:** Se debe usar en la estación de captura conectada al TAP. Es ideal para realizar capturas de larga duración de forma ligera, guardando los paquetes en archivos con extensión `.pcap` para su posterior análisis sin sobrecargar la estación de captura.
- **Análisis de tráfico con Wireshark:** Es la herramienta fundamental para el análisis de protocolos. Permite inspeccionar el contenido (payload) de los mensajes intercambiados con el fabricante, reconstruir flujos HTTP y analizar protocolos industriales que tcpdump no muestra de forma amigable.