MÁSTER EN REVERSING, ANÁLISIS DE MALWARE Y BUG HUNTING

MÓDULO 5. REVERSING DE REDES Y PROTOCOLO – TAREA 1 – TÉCNICAS DE CAPTURA DE TRÁFICO

# MÁSTER EN *ANÁLISIS DE MALWARE Y REVERSING*

Campus Internacional CIBERSEGURIDAD

ENIIT INNOVA IT BUSINESS SCHOOL

UCAM UNIVERSIDAD CATÓLICA DE MURCIA

# Actividad 1 – Técnicas de captura de tráfico

En esta actividad individual se analizará un caso teórico, en el que hay que seleccionar las mejores técnicas de captura de tráfico, explicadas en el Capítulo 3, para un caso concreto.

La empresa ACME, S.A. va a desplegar un nuevo equipo en su red industrial, y le ha contratado para que analice las comunicaciones del mismo, porque quiere conocer si se comunica con otros equipos de la red industrial del mismo fabricante, y/o si realiza comunicaciones a través de Internet, así como analizar en la medida que sea posible los protocolos que emplea y la información que se intercambia con el fabricante. El nuevo equipo tiene un sistema operativo propietario que solo ofrece un panel de control web para configurarlo, pero no permite ejecutar ningún comando adicional en el mismo.

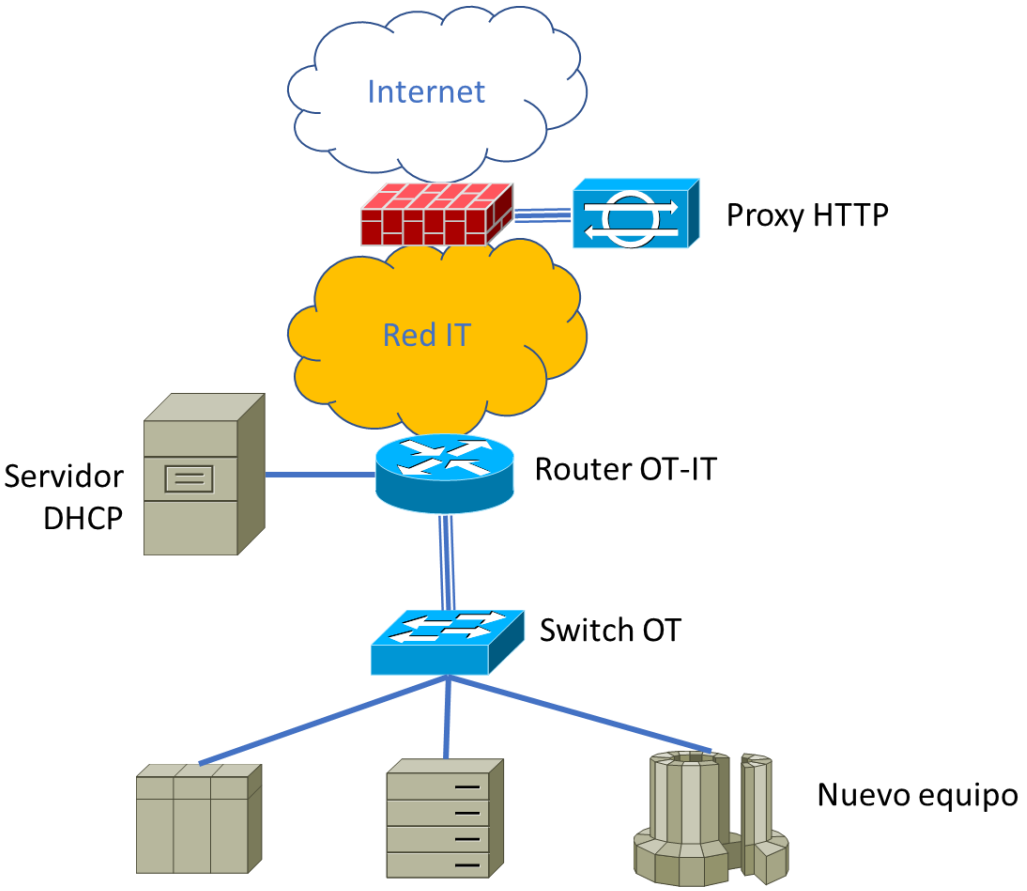


**Figura 1** – Esquema de la red

En particular, el equipo se va a conectar a un *switch* Ethernet industrial a través de un puerto Fast Ethernet de 100 Mbps, que se utiliza para interconectar todos los equipos OT de la planta industrial. Adicionalmente, el *switch* tiene un enlace *uplink*

de 10 Gbps con un *router* que le permite conectarse a la red IT de la organización. Los equipos de la red industrial obtienen su dirección IPv4 y la configuración de red de un servidor DHCP conectado al router, y que permite definir una configuración personalizada a cada uno de los equipos de la red industrial (e.g. algunos equipos requieren que el servidor DHCP les proporcione parámetros de arranque).

Como algunos equipos industriales requieren acceder a Internet para descargarse actualizaciones, y para enviar informes de estado al fabricante, el *router* que interconecta las redes IT y OT de la organización permite que los equipos industriales se comuniquen con un servidor DNS y un *proxy* web que tiene conectividad con Internet, aunque para ello el equipo cliente debe disponer de usuario y contraseña (i.e. el *proxy* debe configurarse explícitamente en el equipo). El *proxy* web es la única forma en la que se puede salir a Internet desde dentro de la organización (i.e. todo el tráfico de salida de la organización que no venga del *proxy* se filtra).

Se desea capturar todo el tráfico que envía o recibe el nuevo equipo, tanto con otros equipos de la red industrial, como con Internet. Pero es esencial que el mecanismo de captura tenga un impacto mínimo en la red OT de la compañía (tanto en el equipo siendo monitorizado como en el resto de la infraestructura). Por ejemplo, al montar el nuevo equipo habrá una pequeña ventana de mantenimiento en la que será posible reconfigurar los equipos o instalar algún dispositivo nuevo, pero una vez que el equipo se ponga en producción, no es posible interrumpir o reconfigurar la infraestructura de la red OT, incluso si existe algún problema con el mecanismo de captura de tráfico. El *switch* industrial no tiene capacidades de *port mirroring*, aunque el resto de la infraestructura IT, incluyendo el *router* de interconexión, sí dispone de esas capacidades. El *proxy* web almacena en un log las URLs a las que se ha conectado cada cliente, aunque no almacena el contenido de los mensajes HTTP intercambiados.

Puede contar con la colaboración de los administradores de la infraestructura de red de la empresa, siempre y cuando no se comprometa la fiabilidad de la red OT.

## 1. Propuesta de captura de tráfico

Debe proponer el mecanismo o mecanismos de captura de tráfico que cumplan con todos los requisitos del cliente. Para ello debe analizar todos y cada uno de los mecanismos y técnicas de captura de tráfico, indicando cómo podrían emplearse, y si serían recomendables o no en este caso.

Una vez revisados todos los mecanismos de captura, debe proponer los que considere necesario para este caso, explicando en detalle en qué consistirían (incluyendo la configuración necesaria en la estación de captura) y cómo se desplegarían.