



Práctica 05.

Star Wars | Rogue One.

Duración: 2 horas

Objetivos de la práctica:

1. Uso de Túneles SSH y explotación de servicios TCP/IP (*port forwarding*)
 2. Certificados SSH
 3. Sondeo de red: `nmap` y `netdiscover`
 4. Uso de cliente FTP de consola
 5. Funciones de dispersión.
 6. Uso de la herramienta `TAR`.
-

Requisitos iniciales

Para esta práctica deberás disponer de un escenario completo facilitado por el profesor en formato OVA llamado '**STAR WARS ESCENARIO.OVA**'. Consta de varias máquinas virtuales configuradas e interconectadas entre sí. Para desarrollar la práctica conocerás sólo parte de los datos de conexión y usuarios (es decir, inicialmente sólo tendrás los datos que tiene la *Alianza Rebelde*). El resto de datos los descubrirás durante el ejercicio.

Introducción

Con la confirmación de los crecientes rumores acerca de la creación de un superarma por parte del Imperio Galáctico y la obtención de los datos de su ubicación en Eadu, Jyn Erso ha armado un plan para infiltrarse en la base militar de Scarif. El propósito: robar los planos técnicos de tal arma y localizar un punto débil colocado intencionadamente por Galen Erso para así lograr destruirla.

El plan presenta un gran inconveniente, y es que el Gobierno Civil de la Alianza rechaza el oponerse abiertamente al Imperio porque teme que se inicie una guerra que no pueden ganar. La mayoría de los rebeldes no le conceden credibilidad alguna al plan propuesto por Jyn. Sin embargo a pesar de la falta de apoyo el pequeño grupo de rebeldes decide desobedecer y llevar a cabo su plan, ya que el autodenominado escuadrón *Rogue One* quiere hacerse a toda costa con los datos técnicos del superarma (conocida como la *Estrella de la Muerte*) alojados en los servidores de archivos del Imperio Galáctico.

La cuadrilla *Rogue One* tiene como miembro de equipo a K-2SO, un androide imperial reprogramado al servicio de la República. El equipo confía en que este droide seguirá pudiendo conectar al servidor BASTIONIMPERIAL con sus antiguas credenciales de acceso que aún conservaba en memoria para poder

realizar las operaciones necesarias de búsqueda y transmisión de la valiosa información. Imaginan que K-S20 no tendrá privilegios de administrador en BASTIONIMPERIAL, pero confían en que con acceder a una consola del Imperio será suficiente para desempeñar la tarea que debe realizar de búsqueda. Una vez localizada la información buscarán la manera de extraerla.

Así pues tras tomar un carguero Clase Z robado en Eadu y usando un viejo código de la nave el escuadrón ha conseguido penetrar y burlar el escudo del planeta Scarif y ha aterrizado. La infiltración ha sido exitosa y tras una dura batalla terrestre los miembros del equipo han conseguido acercarse lo suficiente a las instalaciones que custodian los valiosos planos estructurales del superarma.

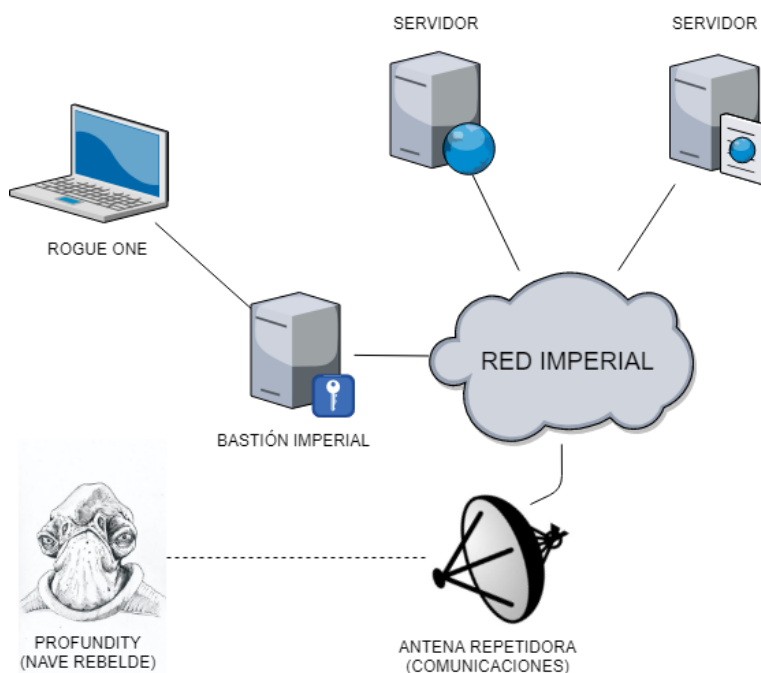
Una vez en las instalaciones K-2SO y Jyn Erso deberán investigar en la red Imperial, localizar los planos estructurales del superarma “*Estrella de la Muerte*” y buscar algún medio para poder transmitirlos a la *Alianza Rebelde* (quizá puedan usar alguna antena de comunicaciones potente para poder transmitirlos a una nave de la flota que orbite el planeta). El acceso a la red Imperial tendrá que realizarse a través de BASTIONIMPERIAL usando las credenciales de K-2SO. Una vez dentro de la red deberán investigar y buscar toda la información posible hasta dar con el objetivo.

¡Que la Fuerza os acompañe Rogue One!

Desarrollo


En esta práctica encarnarás el papel de K-2SO y Jyn Erso en el robo de planos de la Estrella de la Muerte. La Alianza Rebelde usa GNU/Linux en sus sistemas informáticos, así que como miembro del equipo Rogue One dispondrás de una máquina Debian con entorno gráfico (y con permisos de administrador si fueran necesarios).

Observa el diagrama de red del ejercicio, en él se muestra la topología del escenario:




Los pasos del plan a seguir para robar los planos estructurales de la Estrella de la Muerte son:


1. Logra la conexión a la red Imperial abriendo una sesión SSH en BASTIONIMPERIAL y obtén un intérprete de órdenes.

 **Nota:** Probablemente tendrás que utilizar las antiguas credenciales de K-2SO.

2. Sondea la red Imperial en busca de posibles máquinas objetivo. ¿Qué máquinas existen en la red Imperial? ¿Qué direcciones de red tienen? ¿Qué direcciones MAC...? ¿Puedes obtener algo más información?

 **Nota:** K-2SO era un droide de seguridad, así que es posible que todavía tenga acceso a herramientas en BASTIÓNIMPERIAL relacionadas con la auditoría y sondeo de redes, como lo son *netdiscover* y *nmap* (y si no es así siempre podrías usar las herramientas que desees desde tu equipo).

3. Una vez que obtengas algo de información sobre las máquinas de la red Imperial y conozcas sus direcciones IP escanea sus puertos para rastrear los puertos abiertos en busca de posibles servicios. Pregúntate: ¿Dónde está la información? ¿Cómo se presenta a los usuarios de la red? ¿Qué servicios parecen activos? ¿Qué puertos están abiertos?
4. Utiliza tus conocimientos técnicos para obtener toda la información posible de la red Imperial. Por ejemplo, si existe algún servidor web visita la información que ofrece, si existe un servidor de archivos intenta conectarte, consúltalos... investiga y prueba. Lee despacio lo que encuentres, bucea en la información disponible. **La información valiosa que buscas consta de varios planos estructurales.** También tenemos información de que existe un vídeo que muestra cómo atacar el punto débil diseñado por Galen Erso.

 **Nota:** En ocasiones tendrás que crear túneles SSH para explotar desde tu máquina los servicios y así poder investigar. Configura diferentes tipos de túneles (locales, remotos o dinámicos) según tus necesidades. Desde la máquina Rogue One no hay conexión directa a las máquinas del Imperio, pero seguro que puedes canalizar la información a través del Bastión.



5. Cuando logres encontrar la información objetivo no basta con examinarla desde tu puesto, **debes transmitirla a la Alianza Rebelde**. Busca la forma de activar la antena de comunicaciones (tendrás que conectarte de algún modo al REPETIDOR mediante un usuario válido). Tendrás que ingeniártelas para encontrar un nombre de usuario válido y ver cómo poder entrar, pero seguro que en la base de datos Imperial encuentras algo de información que te pueda ayudar. ¿Podrás robar las credenciales de alguien del Imperio y hacerte pasar por él para activar el enlace de comunicaciones?

i Nota: Como tendrás que hacerte pasar por un responsable de comunicaciones del Imperio Galáctico recuerda que si lo necesitas puedes crearte una cuenta de usuario en tu máquina Rogue One con el nombre apropiado, aunque quizá no te sea necesario.

6. La nave rebelde PROFUNDITY tendrá cobertura militar de la *Alianza Rebelde* y estará orbitando el planeta Scarif lo más cercanamente posible esperando a que logres contactar con ellos. Serán los responsables de recibir la información de los planos del superarma, así que no tardes mucho. En cuanto logres establecer la conexión encendiendo la antena de transmisión (REPETIDOR) vuelca la información que hayas encontrado a su servidor de archivos.

Nota: Jyn o K-2SO tendrán que ser las personas que envíen los datos, nadie más podrá hacerlo. Para ello en PROFUNDITY han configurado una cuenta de usuario llamada 'jyn' y un sitio donde poder guardar la información que mandéis desde la base imperial.

Anexo | Datos de conexión.

ROGUE ONE	
usuario / password	<ul style="list-style-type: none">• k2so / k2so• root / toor
Varios	Sistema de escritorio Debian 9.x con entorno gráfico XFCE. Acceso completo al sistema.



PROFUNDITY	
usuario / password	<ul style="list-style-type: none">jyn / jyn
Varios	Servicio FTP en ejecución. Jyn podrá conectarse a su directorio de conexión mediante FTP (con permisos de escritura) pero no tendrá acceso a ningún Shell / intérprete de órdenes.

BASTIONIMPERIAL	
usuario / password	<ul style="list-style-type: none">k2so / <desconocida>
Varios	<ul style="list-style-type: none">Aunque no se conoce la password de acceso del usuario K-2SO en esta máquina el droide debería poder iniciar sesión en el BastiónImperial usando sus antiguas credenciales (certificados). Configura el terminal de Rogue One para usarlas.K-2SO es un droide de seguridad, podrá usar algunas herramientas de sondeo de red instaladas en esta máquina.

MÁQUINAS IMPERIO1, IMPERIO2 Y REPETIDOR	
usuario / password	<ul style="list-style-type: none"><desconocidos>
Varios	Máquinas del Imperio Galáctico. No tendrás usuarios ni información para poder interactuar con estas máquinas, ni siquiera para explorar los archivos de configuración. Sólo ofrecen servicios a la red Imperial. Tendrás que investigar y estudiar para qué pueden servirte en la misión.