Windows Reverse Shell

Claudio Garcia

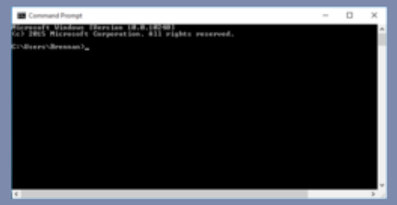
Que es una Shell?

Definicion

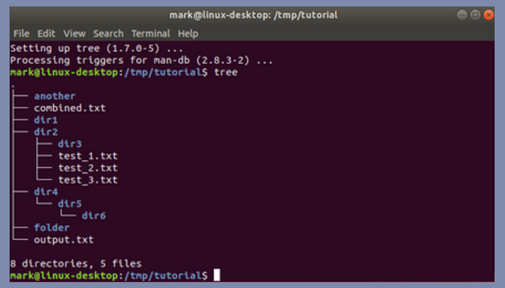
Antes de ver que es una shell inversa (reverse shell) o directa (bind shell), debemos tener claro lo que es una shell; una shell es un software que actúa como una interfaz que nos permite ingresar comandos en un sistema operativo; estos comandos (ingresados a través del teclado) permiten de “cierta forma” que se ejerza un control sobre el sistema operativo, sin la necesidad de utilizar una interfaz gráfica de usuario ¿por qué digo que de “cierta forma”? Porque el hecho de que usted tenga una shell, no significa que posee el control total sobre la máquina, lo anterior, debido a que todo se restringirá a los privilegios del usuario con el que se ejecuta la shell.

Ejemplos

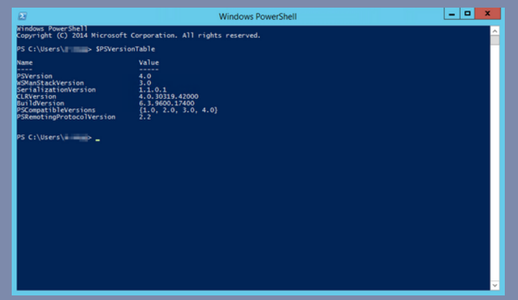
Windows 10 Shell
CMD



Linux Sehll
Bash



Windows 10 Shell
PowerShell



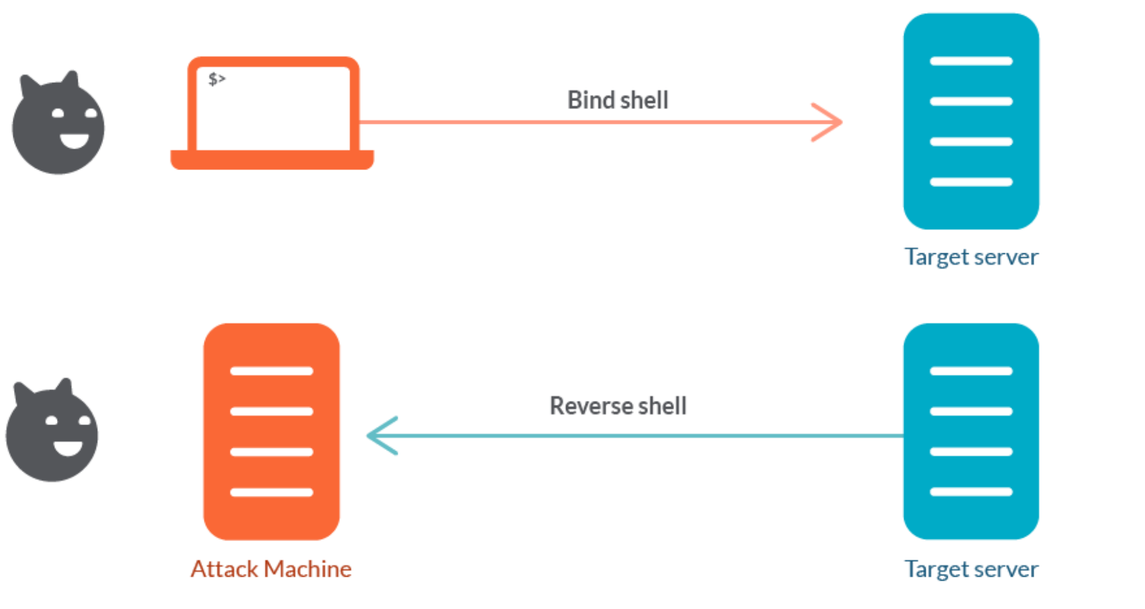
Que es una Reverse Shell?😗

Reverse Shell

La Reverse Shell, se utiliza durante un pentest, como una forma de acceso hacía la máquina objetivo, para iniciar la fase de post explotación; con la shell puede conectarse a la máquina objetivo y, enviarle a esta, a través de la consola, las instrucciones requeridas para continuar con las tareas que va a realizar durante la post explotación.

Como Funciona una Reverse Shell?

Reverse



La shell inversa (reverse shell), funciona de forma inversa a la shell directa; en este caso,el atacante dispone una máquina y, en ella, ejecuta un software que queda a la escucha de solicitudes de conexión, en un puerto determinado; por otro lado, la máquina objetivo (máquina atacada) se conecta hacia el servidor

En conclusión en una shell inversa, el listener se configura y ejecuta en la máquina atacante

Implementacion

01 Nuestra Reverse Shell esta escrita en el lenguaje de programacion GO

02 Es 100% Indetectable en Windows 10 ultima update.

03 Utilizaremos NetCat como listener para ponernos en escucha a una conexion

04 Utilizaremos Ngrok para hacer un port forwarding y poder recibir conexiones fuera de red

05 Utilizaremos CFF explorer para editar el ejecutable cambiar el icono y ocultar la terminal

Estrategia de Infeccion

Ocultar lla consola

Ocultaremos la consola para que al momento que nuestra victima ejecute la shell, para pasar desapersibido

Cambiar nombre e incono

Cambiaremos el y icono y el nombre de binario al de uno comvencional no levante sospechas

Comprimir el Binario

Comprimiremos el binario en un ZIP para enviarlo a nuestra victima por cualquier tipo de plataforma sin que sea detectado

Live Demo!!