M6T2. Tarea 2

Metasploit

Responde a las siguientes preguntas:

• *¿En qué escenarios es más interesante utilizar una Shell o conexión inversa frente a dejar un puerto a la espera de conexiones?*

Siempre que queramos ejecutar comandos, tomar el control, etc es mas interesante utilizar una Shell que dejar un puerto a la espera de conexiones.

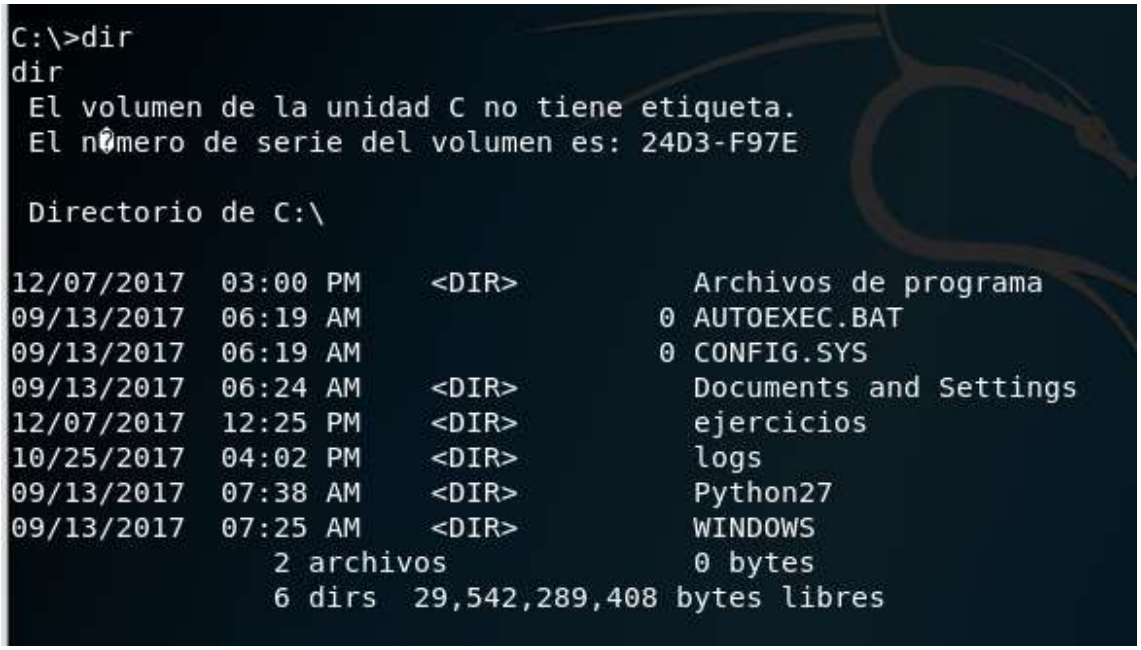
Dejar los puertos a la espera es una manera reactiva de lanzar un exploit, es decir, cuando se conecten por donde estemos escuchando, lanzaremos el exploit.

Usar una Shell es una manera proactiva a la hora de lanzar el exploit, posiblemente también una forma de ataque mas peligrosa, con la cual se pueden generar muchos problemas.

• *En que directorio está ejecutando la sesión obtenida.*

C:\Windows\System32

• *Obtener un pantallazo con el listado de directorios disponibles en C:\ desde la Shell obtenida.*



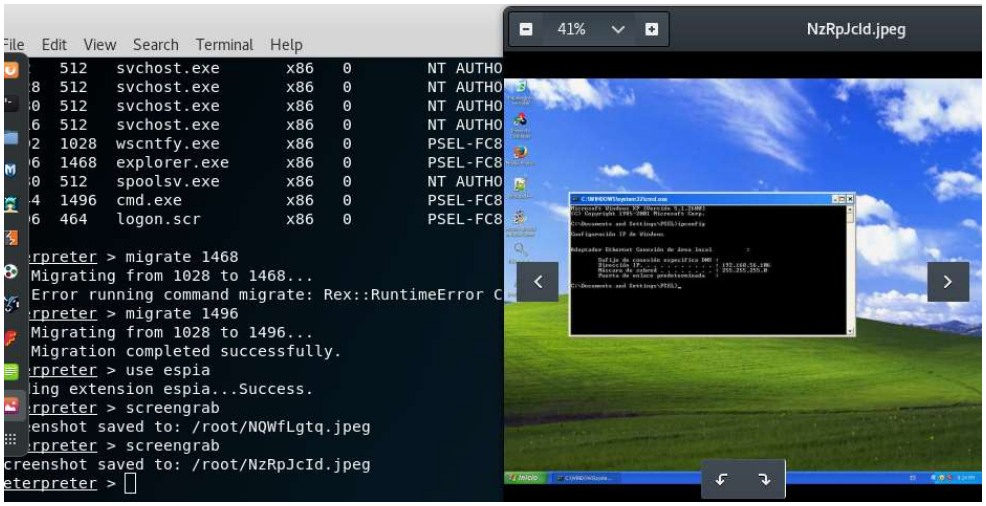
• Modificar el payload y utilizar el payload windwos/meterpreter/reverse_tcp. ¿Cuáles son las diferencias entre el payload utilizado en el primer ejercicio y el utilizado en el utilizado en esta pregunta? Obtener un screenshot del escritorio de la máquina atacada mediante meterpreter y enviarla como resultado.

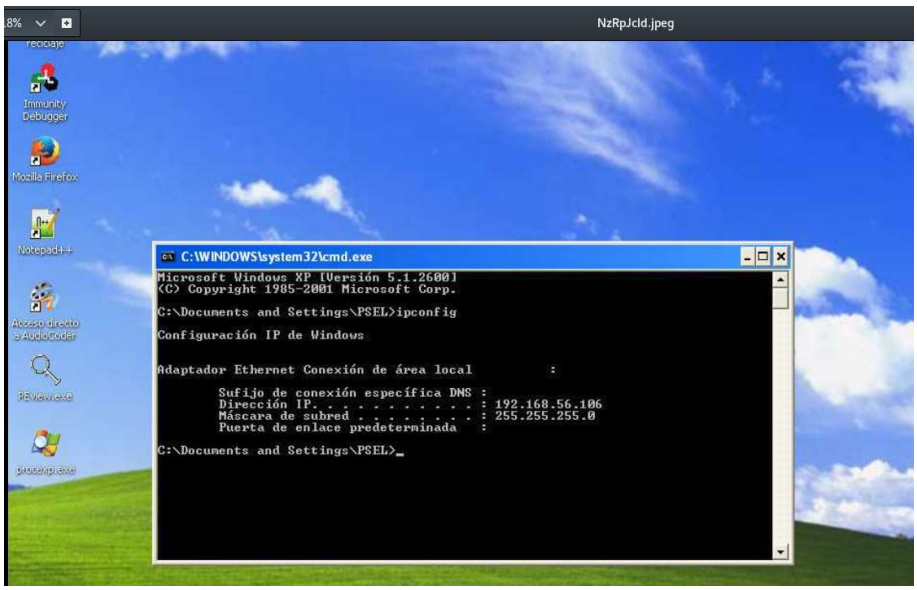
Diferencia:

Se abre la consola de meterpreter en vez de la Shell de Windows, aunque estamos escuchando en la misma carpeta que lo estábamos con la Shell de Windows.

Desde esta consola podemos usar comandos como migrate, espia, etc

Screenshot:





Armitage + nmap

Dado que las dos máquinas son vulnerables y no hemos conseguido explotar la windows 2008 con Armitage, utilizando Metasploit explotar la vulnerabilidad detectada en dicha máquina.

Como podéis observar las dos máquinas son vulnerables y sin embargo en el ejercicio anterior, al lanzar el "Hail Mary" no ha comprometido nada más que una.

PREGUNTA

¿A que puede deberse que sólo comprometiera una de las dos máquinas?

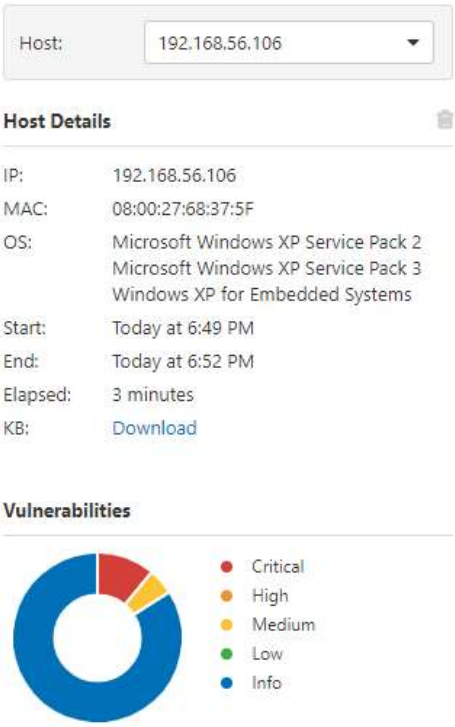
Porque armitage, aunque detecte N exploits sobre M host, usa una única sesión de meterpreter, desde la cual lanza los exploits a un único host.

Al tener esa sesión iniciada lanza todos los exploits disponibles sobre ese host, pero no lo realiza sobre los siguientes.

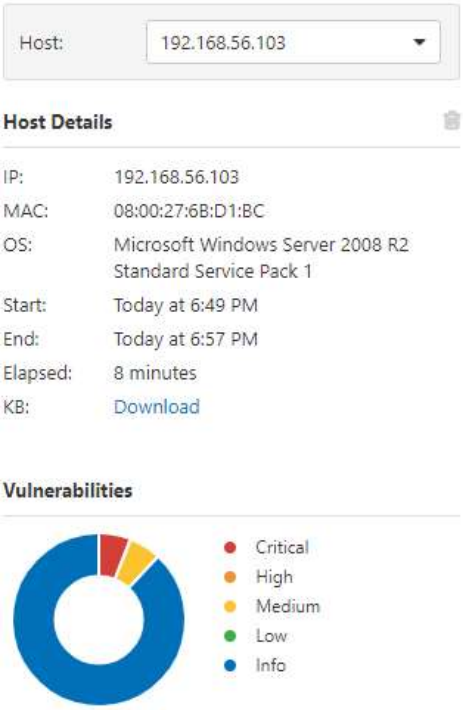
Nessus

Como entregable de esta práctica se deben enviar dos pantallazos de los resulados del escaneo sobre la maquina Windows XP y la maquina Windows 2008.

Windows XP

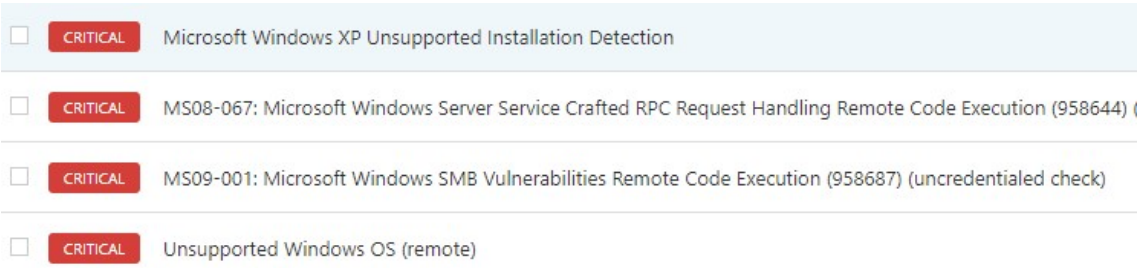


Windows 2008:



Pregunta: Existen exploits dentro de Metasploit para las tres vulnerabilidades criticas que afectan a la máquina Windows XP

Vulnerabilidades de la máquina WXP:

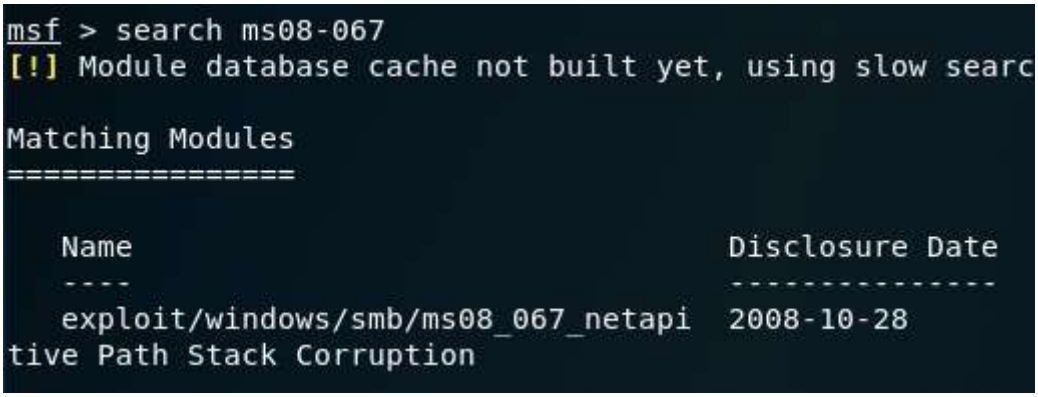


Exploits en metasploit:

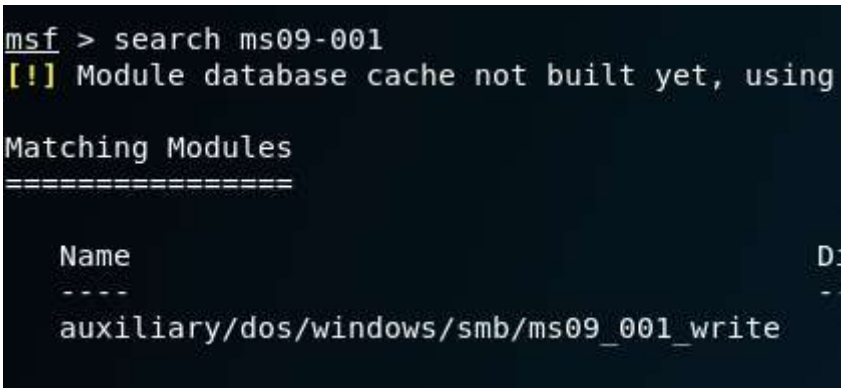
Para la primera y la cuarta vulnerabilidad no hay expliots, ya que indican en la primera que WXP ya no tiene soporte y puede tener vulnerabilidades y en la última que hay un problema con los service pack y puede haber vulnerabilidades.

Para las otras dos si tenemos exploits:

MS08-067:



MS09-001:



Searchexploit

EJERCICIO EXPLOITS

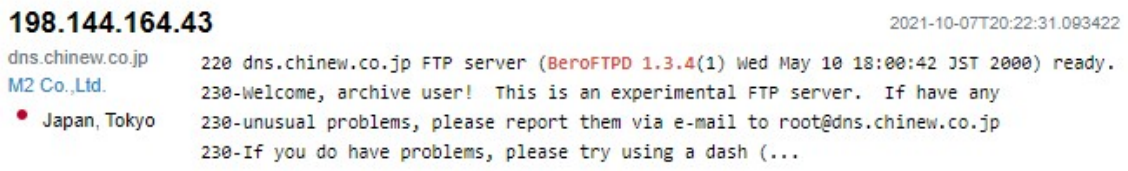
Buscar exploits de ejecución de código remoto sobre servidores Web, de correo o FTP y buscar mediante

Shodan algún posible objetivo para ese exploit. Enviar los resultados como captura de imagen

Sobre servidores FTP:

```
BeroFTPD 1.3.4(1) (Linux x86) - Remote Code Execution
Chilkat Software FTP2 - ActiveX Component Remote Code Execution
```

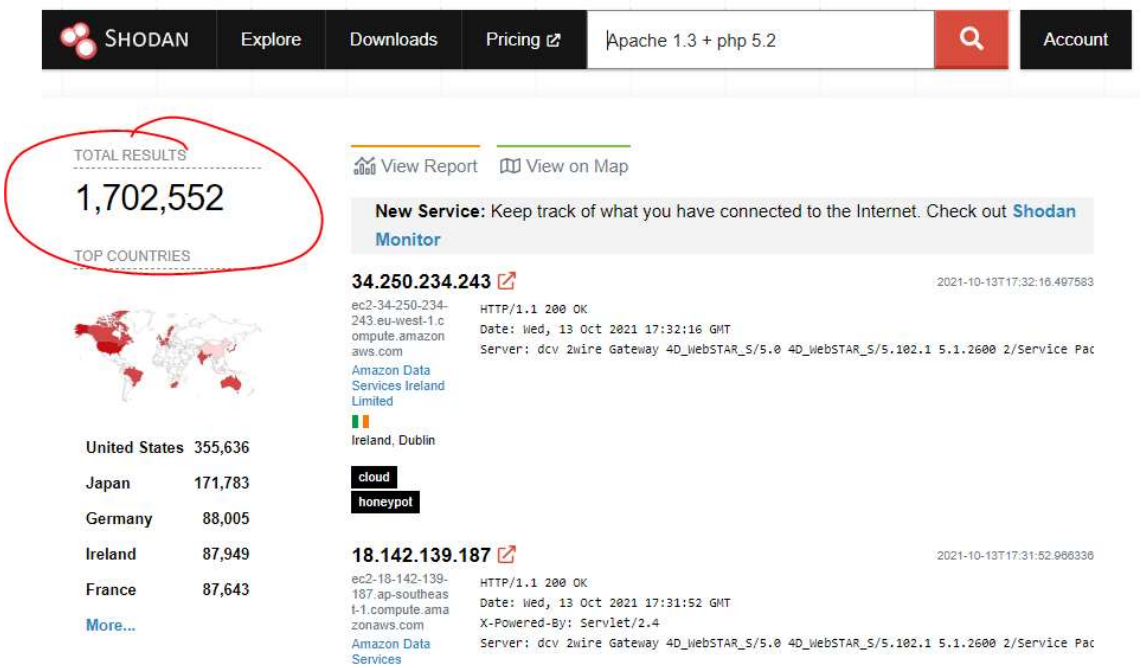
Búsqueda en Shodan:



Sobre servidores Web:

```
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache 1.3.x mod_mylo - Remote Code Execution
```

Búsqueda en Shodan:



Sobre servidores de correo:

```
----------------------------------------------------------------------
Microsoft Exchange Server - Remote Code Execution (MS05-021)
----------------------------------------------------------------------
```