

Forum:[Hack Forums](#)

Thread: [Metasploit Explained A Tutorial For Beginners](#)

Da Judge ® - October 26, 2010, 4:05 pm

[img]http://1.bp.blogspot.com/_fMrF3L8CTmg/TJztUK-r14I/AAAAAAAAA-E/Rz_-t1ZN01A/s1600/Metasploit.jpeg[/img]

Metasploit Framework is a open source penetration tool used for developing and executing exploit code against a remote target machine it, Metasploit frame work has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems.

Its a powerful tool used for penetration testing. Learning to work with metasploit needs a lot of efforts and time. Ofcourse to can learn metasploit overnight, it needs lots of practice and patience
Download here(windows user) <http://www.metasploit.com/releases/framework-3.2.exe>
Download here(linux user) <http://www.metasploit.com/releases/framework-3.2.tar.gz>

Just give a look at following basic steps for beginners to break into a system using metasploit after gathering some information about the target system.

1. Select a right exploit and then set the target. 2. Verify the exploit options to determine whether the target system is vulnerable to the exploit. 3. Select a payload 4. Execute the exploit.

You must be confused !!!!

Now carefully read the following basic terms to get an idea about these four steps mentioned above .I have defined the terms technically and side by side explained in layman language to clarify the things. I have taken an example that an attacker wants to break into a house . I hope my this approach will give you a great idea about these basic terms .

Vulnerability -A weakness which allows an attacker to break into or compromise a system's security.

Like the main gate of house with a weak lock (can be easily opened) , a glass window of house(can be easily broken) etc can be the vulnerabilities in the systems which make it easy for an attacker to break into.

Exploit - Code which allows an attacker to take advantage of a vulnerability system.

The set of different keys which he can try one by one to open the lock , the hammer with him which he can use to break the glass window etc can be the exploits.

Payload- Actual code which runs on the system after exploitation

Now Finally after exploiting the vulnerability and breaking in , he can have different things to do. He

can steal money, destroy the things or just can give a look and come back.. Deciding this is what we mean by setting the Payload.

Credit to author

Unreality - October 26, 2010, 4:20 pm

Nice, a good list of basics for Metasploit.

Night Shade - October 26, 2010, 4:33 pm

Thanks for this, I hear alot of good things about Metasploit but I have never used it.

Derelict22 - October 29, 2010, 2:03 am

FYI, they're up to version 3.5 now...not sure why you'd be posting the link to version 3.2?

Regardless, one can download the latest version of the framework for either Windows or Linux here:

<http://anonym.to/?http://www.metasploit.com/framework/download/>

Go here if you want a much more indepth guide (it's free) on using Metasploit:

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

Cap141Ghost - November 29, 2010, 5:31 am

gud job but thats not fully tutorial about metasploit , please any link to full metasploit tutorial

Sonic Boom - November 29, 2010, 5:41 am

Nice Tutorial.Useful for Everyone.Thanks

Sonic Boom - November 29, 2010, 5:42 am

Nice Tutorial.Useful for Everyone.Thanks

Hack Flavour - November 29, 2010, 6:09 am

-Helpful tutorial .Thanks man.

RadarX - November 29, 2010, 11:54 am

No offense but this absolutely sucks.

The title says "Tutorial For Beginners". Well, I'm a beginner and I don't understand a word you said.

This isn't really a tutorial. :\

andreinescastro - November 29, 2010, 1:22 pm

Very well explained!

I spent lots of time in Metasploit and I didn't get nothing. I tried to get in servers and personal computers but I didn't make it...

Nowadays, the computers are very protected, it's very difficult to exploit :/