

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Metasploit Tutorial Part 1 - INSTALLATION](#)

SIM-2015410 - March 19, 2014, 11:02 pm

Hello Hf,

Welcome to my first hacking tutorial. Hopefully this will not be my last though ?

When you start out in hacking, you will soon run across the word "exploit". An exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders. It can take advantage of both weaknesses in an operating system or vended application programs.

What Is Metasploit?

Metasploit is one of the best, most widely used exploitation tools in both white hat and black hat hacking. It can be used by both beginning n00bs and more advanced hax0rs ?.

Metasploit was developed in 2003 as an open source project by H.D. Moore. Originally developed in PERL, the developer team rewrote Metasploit in Ruby in 2007. This is critical, because you need to have Ruby on your system in order to run Metasploit and to develop your own exploits. Metasploit was then purchased by rapid7 in 2009, which still offers "metasploit community edition" as a free, open source download for anyone to use.

Metasploit is an "exploitation framework". As a framework, it eases the effort to exploit known vulnerabilities in networks, operating systems and applications, and to develop new exploits for new or unknown vulnerabilities. The metasploit framework contains hundreds of exploits and "payloads" and makes it easy to use them. My current version of metasploit contains 1161 exploits and 310 payloads!

In this tutorial, i will be using linux. There are numerous advantages to using linux when hacking. Linux is free, and open source. There is a Windows version of Metasploit, but many of the features such as raw IP packet injection, wireless driver exploitation, SMB relaying attacks, etc. are unavailable on windows. There is also a GUI developed for metasploit by independent developers, but we will be using the command line. All hackers should be familiar and comfortable using the command line.

Download and Installation

First we need to download and install Metasploit (obviously ?).

One of the best distros for hacking is Kali Linux. this distro comes with metasploit framework pre-installed, so if you want to use kali, skip the next few steps. Here, I'll walk you through downloading and installing on one of the most popular Linux distros: Ubuntu.

Spoiler ([Click to View](#))

AS I STATED EARLIER, ENSURE RUBY IS INSTALLED!

Code `sudo apt-get install ruby1.9.1 build-essential`

First open a terminal window and type this for the 32 bit version:

Code `wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-x32-installer.run`

Or this, for the 64 but version:

Code `wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-x64-installer.run`

This uses the wget command to download the latest version of the Metasploit framework.

Next, we need to make the installer executable so we can run it. In the terminal, use the following command to change the mode to execute (x) for Metasploit:

Code `chmod +x metasploit-latest-linux-x*-installer.run`

And now execute the installer (using superuser or root via the sudo command. You will need to enter your root password in order to use this command):

Code `sudo ./metasploit-latest-linux-x*-installer.run`

Follow the prompts in the installer, clicking forward and agreeing to the license agreement. Select yes to allow metasploit to automatically update itself. Accept the default service script, and wait for the installer to finish

After you have metasploit installed, you are ready to run it! To start up the metasploit framework console, type this into terminal:

Code `msfconsole`

NOTE: On kali, you first need to start the metasploit framework service using:

Code `service metasploit start`

You should see the beautiful text art "Metasploit" if it runs correctly, and be prompted for a command. Feel free to experiment and research, or wait loyally for my next tutorial on some basic usage of metasploit.

Now that you have successfully installed Metasploit you can start doing some l33t hacks!

Manual Updates:

Spoiler [\(Click to View\)](#)

Because the exploit databases is always being added to, you should periodically update your version of Metasploit. to do this, simply type:

Code `sudo msfupdate`

LIST OF BASIC COMMANDS:Spoiler [\(Click to View\)](#)

Basic commands

? - help menu

background - moves the current session to the background

bckill - kills a background meterpreter script

bglis - provides a list of all running background scripts

bgrun - runs a script as a background thread

channel - displays active channels

close - closes a channel

exit - terminates a meterpreter session

help - help menu

interact - interacts with a channel

irb - go into Ruby scripting mode

migrate - moves the active process to a designated PID

quit - terminates the meterpreter session

read - reads the data from a channel

run - executes the meterpreter script designated after it

use - loads a meterpreter extension

write - writes data to a channel

File System Commands

cat - read and output to stdout the contents of a file
cd - change directory on the victim
del - delete a file on the victim
download - download a file from the victim system to the attacker system
edit - edit a file with vim
getlwd - print the local directory
getwd - print working directory
lcd - change local directory
lpwd - print local directory
ls - list files in current directory
mkdir - make a directory on the victim system
pwd - print working directory
rm - delete a file
rmdir - remove directory on the victim system
upload - upload a file from the attacker system to the victim

Networking Commands

ipconfig - displays network interfaces with key information including IP address, etc.
portfwd - forwards a port on the victim system to a remote service
route - view or modify the victim routing table

System Commands

clearav - clears the event logs on the victim's computer
drop_token - drops a stolen token
execute - executes a command
getpid - gets the current process ID (PID)
getprivs - gets as many privileges as possible
getuid - get the user that the server is running as
kill - terminate the process designated by the PID
ps - list running processes
reboot - reboots the victim computer
reg - interact with the victim's registry
rev2self - calls RevertToSelf() on the victim machine
shell - opens a command shell on the victim machine
shutdown - shuts down the victim's computer
steal_token - attempts to steal the token of a specified (PID) process
sysinfo - gets the details about the victim computer such as OS and name

User Interface Commands

enumdesktops - lists all accessible desktops
getdesktop - get the current meterpreter desktop
idletime - checks to see how long since the victim system has been idle
keyscan_dump - dumps the contents of the software keylogger
keyscan_start - starts the software keylogger when associated with a process such as Word or browser
keyscan_stop - stops the software keylogger
screenshot - grabs a screenshot of the meterpreter desktop
set_desktop - changes the meterpreter desktop
uictl - enables control of some of the user interface components

Privilege Escalation Commands

getsystem - uses 15 built-in methods to gain sysadmin privileges

Password Dump Commands

hashdump - grabs the hashes in the password (SAM) file

Note that hashdump will often trip AV software, but there are now two scripts that are more stealthy, "run hashdump" and "run smart_hashdump".

Timestamp Commands

timestamp - manipulates the modify, access, and create attributes of a file

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

I am hoping to make another tutorial soon that will teach you how to use Metasploit for a real hack!

Written by MeshCollider ?

The Wizard of Dos - March 19, 2014, 11:07 pm

Pretty neat tutorial ? You might want to change the title to "[TUTORIAL] Metasploit Intallation Tutorial", but other than that it was great.

SIM-2015410 - March 19, 2014, 11:08 pm

(Mar 19, 2014 11:07 PM)The Wizard of Dos Wrote: [\[CITE\]](#) Pretty neat tutorial ? You might want to change the title to "[TUTORIAL] Metasploit Intallation Tutorial", but other than that it was great.

Thanks for your quick reply!

I will change the title now, thanks for that ?

pikachu123 - March 29, 2014, 12:25 pm

hello! thanks for the tut. its awesome ! I just installed kali linux, im trying to run some comands listed up here and every single one says " command not found " (on kali terminal), even ipconfig. should I reinstal it?

SIM-2015410 - March 29, 2014, 2:16 pm

(Mar 29, 2014 12:25 PM)pikachu123 Wrote: [\[CITE\]](#) hello! thanks for the tut. its awesome ! I just installed kali linux, im trying to run some comands listed up here and every single one says " command not found " (on kali terminal), even ipconfig. should I reinstal it?

You should be using ifconfig not ipconfig on Linux. Try running SET from the menu at the top, not from terminal. That will fix it ?

pikachu123 - March 29, 2014, 3:06 pm

sorry but, what you mean by SET? :P

SIM-2015410 - March 29, 2014, 3:07 pm

(Mar 29, 2014 03:06 PM)pikachu123 Wrote: [\[CITE\]](#) sorry but, what you mean by SET? :P
Social engineering toolkit ?

p_h_p - March 29, 2014, 11:48 pm

i wanna use backtrack. Will be that Good One. And i heard a lot's a exploit. as you said in your thread but i also heard exploit about web. what is that..

Thank You for this thread. waiting for the next one.

Anubhavr - March 30, 2014, 12:43 am

Nice TuT man..... i have been waiting for such tutorial since a long time which is noob -friendly like me.....

Cant wait for ur next thread.....

SIM-2015410 - March 30, 2014, 2:35 pm

Hey guys, I have already made a lot more tutorials! check them out, and I'd appreciate it if you could reply to those too ?. Thanks for the great feedback ?.

"An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). "

Basically, it is something we use to get control of their computer.

if not true then false - March 30, 2014, 8:15 pm

(Mar 19, 2014 11:02 PM)m3shc0llid3r Wrote: [\[CITE\]](#) Code chmod +x metasploit-latest-linux-x*-installer.run

And now execute the installer (using superuser or root via the sudo command. You will need to enter your root password in order to use this command):

Should probably fix that typo on chmod to be

Code chmod +x metasploit-latest-linux-x*-installer.run?

Otherwise, nice tutorial.

SIM-2015410 - March 30, 2014, 8:35 pm

(Mar 30, 2014 08:15 PM)if not true then false Wrote: [\[CITE\]](#) Should probably fix that typo on chmod to be

Code chmod +x metasploit-latest-linux-x*-installer.run?

Otherwise, nice tutorial.

Thanks but what is the typo? I can't see anything wrong with it....

if not true then false - March 30, 2014, 8:52 pm

(Mar 30, 2014 08:35 PM)m3shc0llid3r Wrote: [\[CITE\]](#) Thanks but what is the typo? I can't see anything wrong with it....

It didn't put it in the quote for some reason.

SIM-2015410 - March 30, 2014, 10:53 pm

Oh I see, but i cant edit the thread anymore...

Meeko420 - December 20, 2014, 9:20 pm

man ... wheres the rest of the tutorial...i was all excited because i thaught i was gonna be able to use the exploits...damn???

PlayR - December 21, 2014, 5:16 am

Metasploit is nice tool.

Easy to use etc.

Thanks for awesome tutorial.

hahdbwoannniabs - December 21, 2014, 8:34 am

yeah cuz ur not a l33t hacker until u use metasploit!!!!!!

yahoo5000 - March 26, 2015, 2:17 am

i get a problem with this command PHP Code

<?php

chmod +x metasploit-latest-linux-x*-installer.run

after i execute i get and error the command doesnt exist or something like that each time i try ware could be a problem i follow tutorial from first step and stuck hare

zayedfarouk - September 3, 2015, 2:46 pm

Wonderful one, again bro. You are a blessing in disguise

SIM-2015410 - September 3, 2015, 3:03 pm

(Mar 26, 2015 02:17 AM)yahoo5000 Wrote: [\[CITE\]](#) i get a problem with this command PHP Code <?php

chmod +x metasploit-latest-linux-x*-installer.run

after i execute i get and error the command doesnt exist or something like that each time i try ware could be a problem i follow tutorial from first step and stuck hare

You have an extra 'e' in it, should be 'chmod'

Janekkowal - October 29, 2015, 7:56 am

Unfortunatly I use Windows but nice tutorial

32x0LF - June 1, 2016, 9:59 pm

Thank you for this TUT :)

Bad Hero - March 18, 2018, 7:49 am

Help please i dont know where to put the code

CyberStrike - March 18, 2018, 4:46 pm

(Oct 29, 2015 07:56 AM)Janekkowal Wrote: [\[CITE\]](#) Unfortunatly I use Windows but nice tutorial PentestBox is an option it's part of our tool kit when we deploy tools in a network

(Mar 18, 2018 07:49 AM)Bad Hero Wrote: [\[CITE\]](#) Help please i dont know where to put the code Well figuring you are in Linux the terminal would be where you want to place these commands.

98358533 - September 12, 2018, 11:29 am

I appreciate it, did some more research after seeing that thread .

Babayaro - February 2, 2019, 12:09 pm

Well this is an old topic but helped me a lot. I didn't know RUBY is %100 required and got error at installation. This guide let me install it without any error and problem.