

Forum:[Hack Forums](#)

Thread: [Metasploit Helpdesk - Mr. Robot / Shoe](#)

Mr. Robot - October 10, 2016, 2:35 pm

Metasploit Help Desk and Information Thread

Please note, this is far from finished but needing to post right now as my computer is having issues. If you wish to contribute or ask questions, feel free and I will do my best to help you.

If you wish to help run this help desk, and you have knowledge around the 3 primary tools - feel free to help out.

We will also talk about Armitage which is a GUI interface.

What is Metasploit?

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

This thread will hopefully help you with any questions you may have on Metasploit, how to use it and more.

We will also be discussing Setoolkit and The PenTesters Framework(ptf)

The basics on how to use MetaSploit:

- Execute "msfconsole"
- Identify a vulnerability and use an exploit
- Configure the exploit
- Execute the payload against the target.

So let's get started on the basics.

In a fresh install/live boot of Kali Linux, type in
Code msfconsole

The next step is to identify different options that will help you later on when finding exploits.

You can use the following commands to find different payloads and identify which you are after.

The best way to use these commands is to check the parameters needed to identify what you are after. You can use "help search" to see these and the "search payload" to find which you are after.
Code showCode search

Using help on its own provides us with some core commands

Code msf > help

Core Commands

=====

Command	Description
-----	-----
?	Help menu
advanced	Displays advanced options for one or more modules
back	Move back from the current context
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
edit	Edit the current module with \$VISUAL or \$EDITOR
exit	Exit the console
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
info	Displays information about one or more modules
irb	Drop into irb scripting mode
jobs	Displays and manages jobs
kill	Kill a job
load	Load a framework plugin
loadpath	Searches for and loads modules from a path
makerc	Save commands entered since start to a file
options	Displays global options or for one or more modules
popm	Pops the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
quit	Exit the console
reload_all	Reloads all modules from all defined module paths
rename_job	Rename a job
resource	Run the commands stored in a file
route	Route traffic through a session
save	Saves the active datastores
search	Searches module names and descriptions
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
show	Displays modules of a given type, or all modules
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
use	Selects a module by name
version	Show the framework and console library version numbers

Database Backend Commands

=====

Command	Description
-----	-----
creds	List all credentials in the database

db_connect	Connect to an existing database
db_disconnect	Disconnect from the current database instance
db_export	Export a file containing the contents of the database
db_import	Import a scan result file (filetype will be auto-detected)
db_nmap	Executes nmap and records the output automatically
db_rebuild_cache	Rebuilds the database-stored module cache
db_status	Show the current database status
hosts	List all hosts in the database
loot	List all loot in the database
notes	List all notes in the database
services	List all services in the database
vulns	List all vulnerabilities in the database
workspace	Switch between database workspaces

So we are going to search for an exploit for android, but we are going to search for .apk. In msfconsole, we type the following.
Code search .apk

We would then choose our exploit from the list, and run
Code use exploit/path/to/exploit

Once we have selected our exploit, we need to choose which payload to use. We can type in
Code show payloadsWhich will give us a list of payloads for that exploit.

Now we need to configure it so we get the connection on our end. To do that, we need to enter
Code show options

And for each option that displays, we use the set "optionname" "settings"
For example.

Code Set LHOST 192.168.1.54

Where LHOST is the localhost on your LAN network(ipv4) you can type ifconfig into another terminal to identify your inet_address.

?now - October 10, 2016, 2:40 pm

High quality post, loving the explanations keep it up :D

M5DD - October 10, 2016, 3:20 pm

HQ post from hq user, excellent

Solvaxus-Kun - October 10, 2016, 4:16 pm

It's only half finished! Where's the rest?!

THC - October 10, 2016, 5:03 pm

Great thread so far, looking forward to updates. Glad to see you collaborating with Shoe, my personal bae <3