Summer Metasploit Package

Commands

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

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

history       Show command history

irb           Drop into irb scripting mode

load          Load a framework plugin

quit          Exit the console

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

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

edit          Edit the current module with the preferred editor

info          Displays information about one or more modules

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

previous      Sets the previously loaded module as the current module

pushm         Pushes the active or list of modules onto the module stack

reload\_all    Reloads all modules from all defined module paths

search        Searches module names and descriptions

show          Displays modules of a given type, or all modules

use           Selects a module by name

Job Commands

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

Command       Description

--------------       ---------------

handler       Start a payload handler as job

jobs          Displays and manages jobs

kill          Kill a job

rename\_job    Rename a job

Resource Script Commands

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

Command       Description

--------------       ---------------

makerc        Save commands entered since start to a file

resource      Run the commands stored in a file

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\_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

Credentials Backend Commands

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

Command       Description

--------------       ---------------

creds         List all credentials in the database

Module Type:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Module | encoders | nops | exploits | payloads | auxiliary | post |

Information Gathering Using Metasploit

Think like a hacker

1. Passive Information Gathering

Discover information about targets without touching their systems, identify network boundaries, operating systems, open ports and web server software.

1. Active Information Gathering

Interact directly with a system, port scan, service scan

IDS: intrusion detection system

IPS: intrusion prevention system

Points:

1. Import nmap results into metasploit

nmap –Pn –sS –A –oX [save\_file\_name] 192.168.20.0/24

db\_import [fileNamePath]

hosts : check all alive devices

1. Running nmap from MSFconsole

db\_nmap –sS –A [IP address]

services: check all open services on all alive hosts

1. Port scanning with metasploit

search portscan: check all available scan tools

use [module name]

show options: check all options for the module

set RHOSTS [IP address]/[mask bit]

set THREADS [number]

1. Gathering MySQL server information

use scanner/mssql/mssql\_ping

set options

1. Gathering SSH Server information

use scanner/ssh/ssh\_version

set options

1. Scanning FTP Version

use scanner/ftp/ftp\_version

set options

use auxiliary/scanner/ftp/anonymous

Bruteforce SSH

Module: auxiliary/scanner/ssh/ssh\_login

Core options: PASSWORD, PASS\_FILE, RHOSTS, THREADS, USERNAME, USERPASS\_FILE, USER\_FILE

Loading External Modules

1. Create correct path and module name $HOME/.msf4/..
2. Reload\_all in msf

Backdoor Instructions