Assignment-2:

Rohan Idiculla Abraham
21BEC1080

In this lets explore Metasploit tool in kali Linux OS and scan the own computer and find the vulnerabilities and exploits in it.

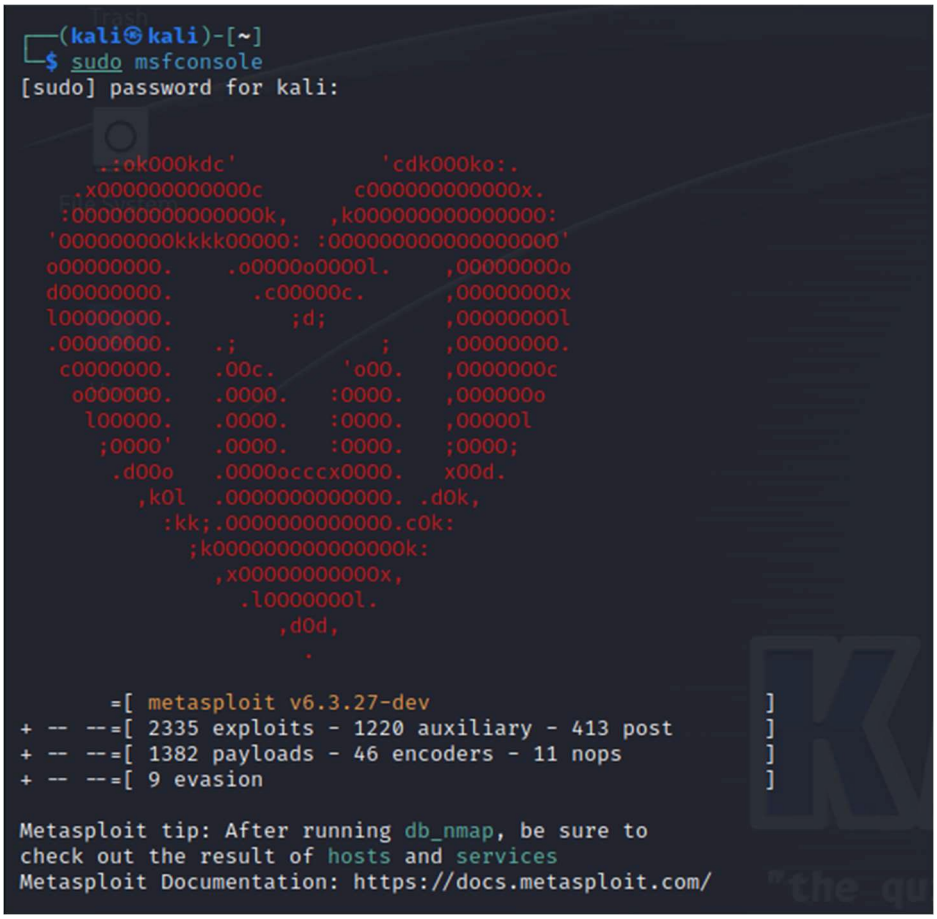
- First we have to get the systems ipv4 address of the system we are checking and then scan the system using nmap.

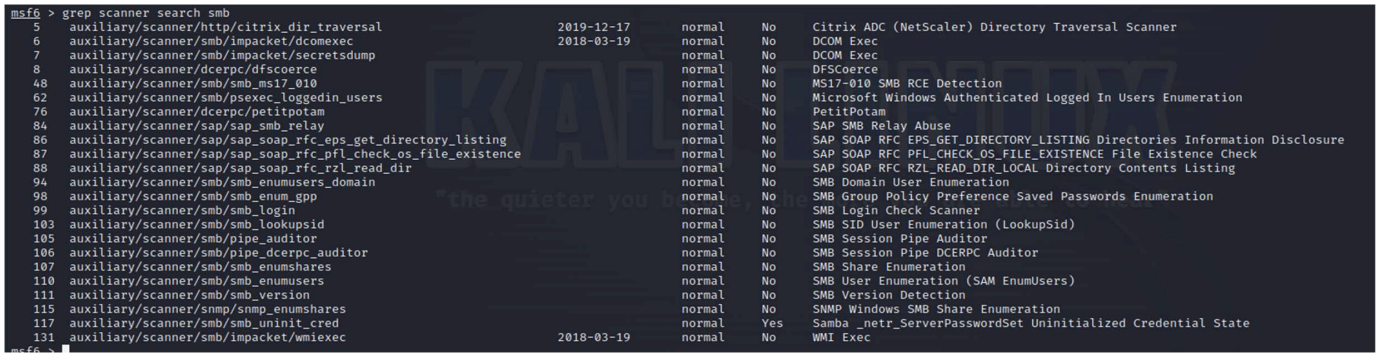
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.35 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 10:43 IST
Nmap scan report for VISHNU-PC (192.168.10.35)
Host is up (0.014s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
```

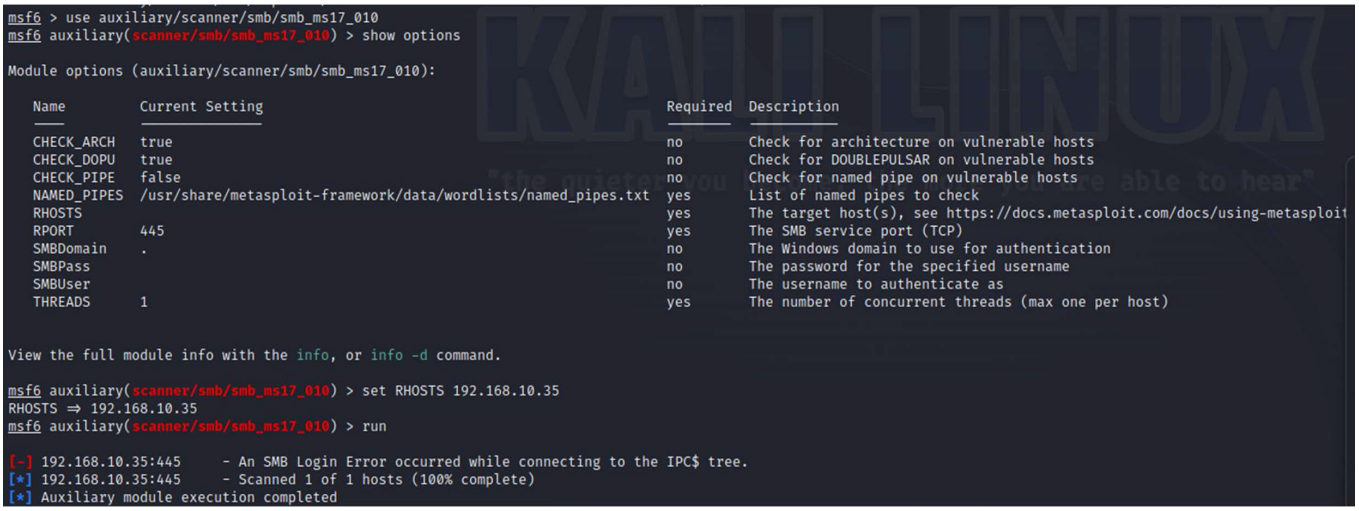
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.35 -Pn -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 10:45 IST
Nmap scan report for VISHNU-PC (192.168.10.35)
Host is up (0.0087s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port3306-TCP:V=7.94%I=7%D=9/5%Time=64F6B975%P=x86_64-pc-linux-gnu%r(NUL
SF:L,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\
SF:x20connect\x20to\x20this\x20MySQL\x20server")%r(GenericLines,45,"\0\0\0
SF:\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x20connect\x
SF:20to\x20this\x20MySQL\x20server")%r(GetRequest,45,"\0\0\0\xffj\x04Host\
SF:x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x
SF:20MySQL\x20server")%r(HTTPOptions,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC
SF:'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20se
SF:rver")%r(RTSPRequest,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20no
SF:t\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20server")%r(RPCC
SF:heck,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20
SF:to\x20connect\x20to\x20this\x20MySQL\x20server")%r(DNSVersionBindReqTCP
SF:,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x
SF:20connect\x20to\x20this\x20MySQL\x20server")%r(DNSStatusRequestTCP,45,"
SF:\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x20con
SF:nect\x20to\x20this\x20MySQL\x20server")%r(Help,45,"\0\0\0\xffj\x04Host\
SF:x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x
SF:20MySQL\x20server")%r(SSLSessionReq,45,"\0\0\0\xffj\x04Host\x20'VISHNU-
SF:PC'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20
SF:server")%r(TerminalServerCookie,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\
SF:x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20serv
SF:er")%r(TLSSessionReq,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20no
SF:t\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20server")%r(Kerb
SF:eros,45,"\0\0\0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20
SF:to\x20connect\x20to\x20this\x20MySQL\x20server")%r(SMBProgNeg,45,"\0\0\
SF:0\xffj\x04Host\x20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x20connect\
SF:x20to\x20this\x20MySQL\x20server")%r(X11Probe,45,"\0\0\0\xffj\x04Host\x
SF:20'VISHNU-PC'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x2
SF:0MySQL\x20server")%r(FourOhFourRequest,45,"\0\0\0\xffj\x04Host\x20'VISH
SF:NU-PC'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\
SF:x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.60 seconds
```

- We can see port no 139 and 445 resembles SMB. So we have to explore for exploits in smb.
- Now lets open Metasploit in our kali Linux which is exploitation framework that gives access to entire system.

- We can enter “search smb” or “grep scanner search smb”.







In this way we can run a scan on any system we can gain the access of the system too if it is we find the vulnerabilities in that auxiliary scan.