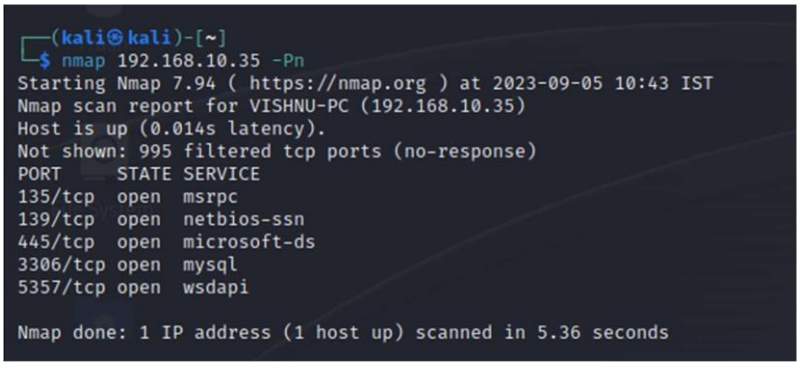
Assignment-2:

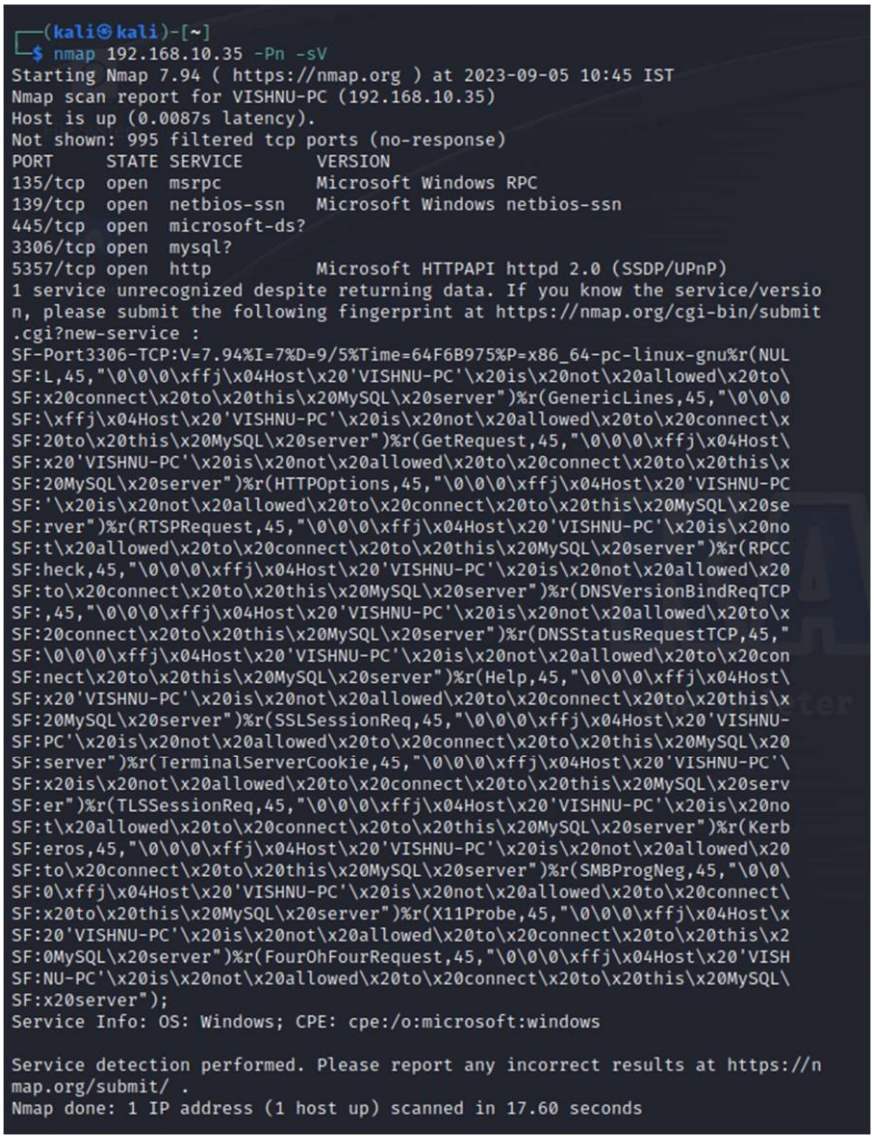
In this lets explore Metasploit tool in kali Linux OS and scan the own computer and find the vulnerabili es and exploits in it.

- 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
```

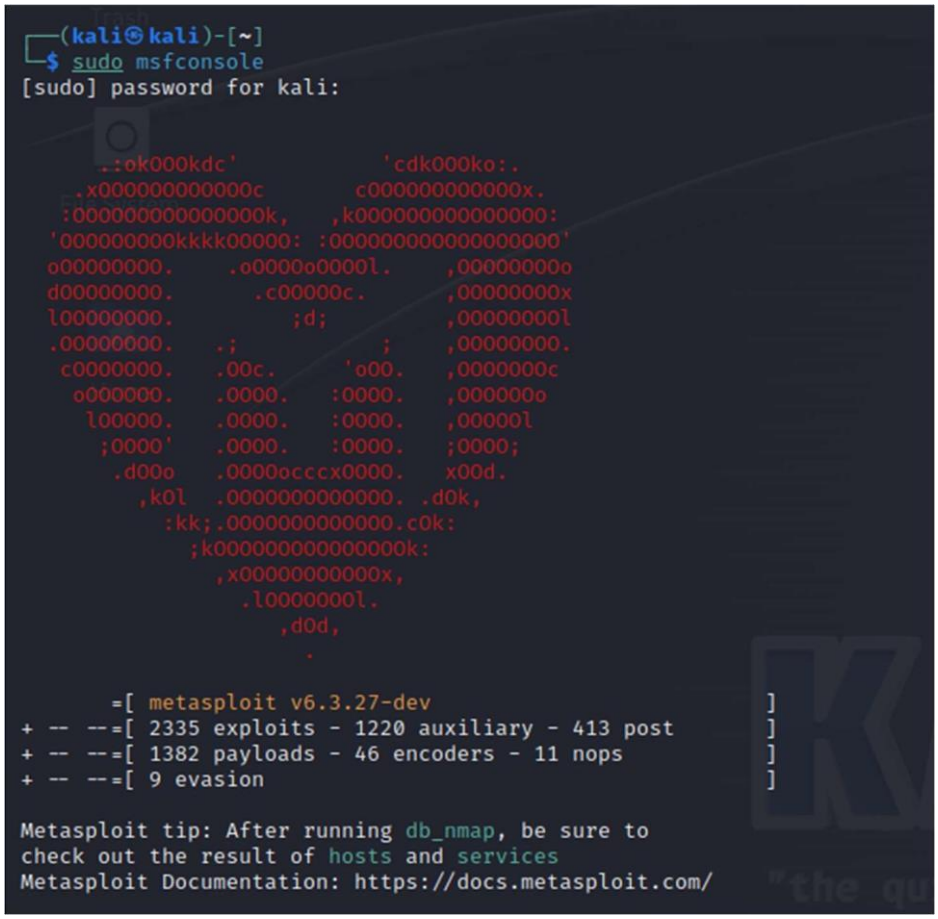


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.35 -Pn -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 10:45 IST
Nmap scan report for VISHNU-PC (192.168.10.35)
Host is up (0.0087s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         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
```

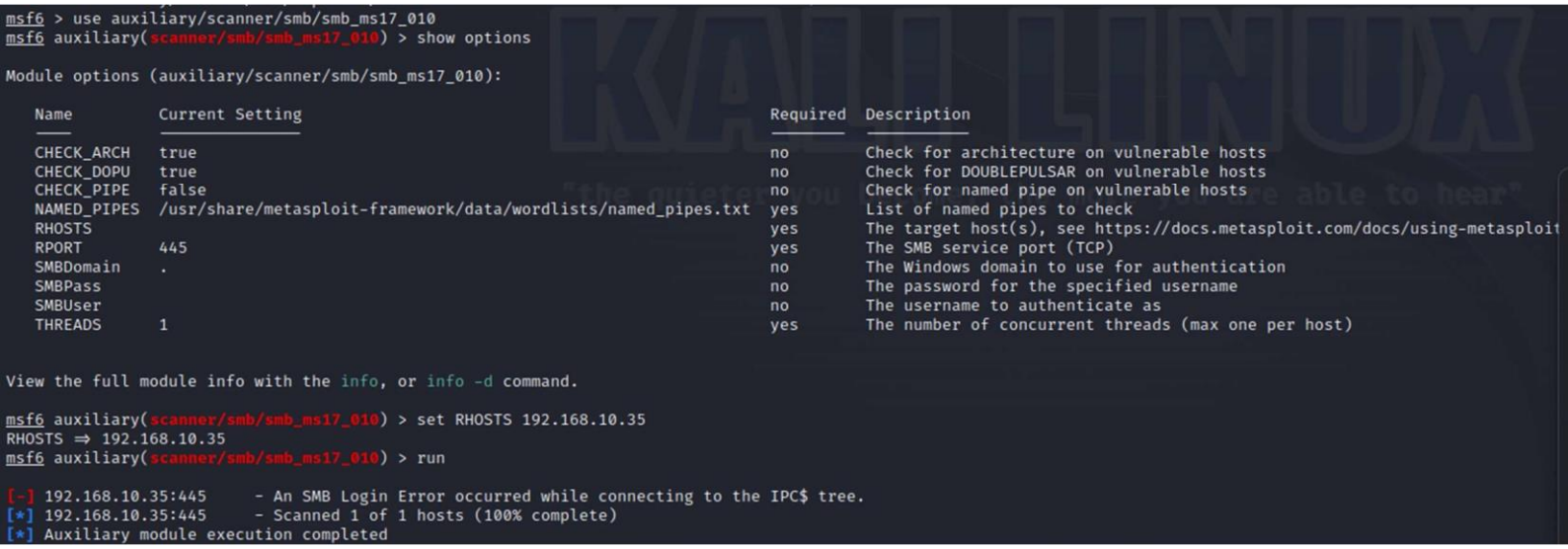
- We can see port no 139 and 445 resembles SMB. So we have to explore for exploits in smb.

- Now lets open Metasploit in our kali Linux which is exploita on framework that gives access to en re system.



- We can enter "search smb" or "grep scanner search smb".

```
msf6 > grep scanner search smb
   5    auxiliary/scanner/http/citrix_dir_traversal                          2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   6    auxiliary/scanner/smb/impacket/dcomexec                              2018-03-19       normal     No     DCOM Exec
   7    auxiliary/scanner/smb/impacket/secretsdump                                            normal     No     DCOM Exec
   8    auxiliary/scanner/dcerpc/dfscoerce                                                    normal     No     DFSCoerce
   48   auxiliary/scanner/smb/smb_ms17_010                                                    normal     No     MS17-010 SMB RCE Detection
   62   auxiliary/scanner/smb/psexec_loggedin_users                                           normal     No     Microsoft Windows Authenticated Logged In Users Enumeration
   76   auxiliary/scanner/dcerpc/petitpotam                                                   normal     No     PetitPotam
   84   auxiliary/scanner/sap/sap_smb_relay                                                   normal     No     SAP SMB Relay Abuse
   86   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing                          normal     No     SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Directories Information Disclosure
   87   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence                        normal     No     SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE File Existence Check
   88   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                                       normal     No     SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Contents Listing
   94   auxiliary/scanner/smb/smb_enumusers_domain                                            normal     No     SMB Domain User Enumeration
   98   auxiliary/scanner/smb/smb_enum_gpp                                                    normal     No     SMB Group Policy Preference Saved Passwords Enumeration
   99   auxiliary/scanner/smb/smb_login                                                       normal     No     SMB Login Check Scanner
   103  auxiliary/scanner/smb/smb_lookupsid                                                   normal     No     SMB SID User Enumeration (LookupSid)
   105  auxiliary/scanner/smb/pipe_auditor                                                    normal     No     SMB Session Pipe Auditor
   106  auxiliary/scanner/smb/pipe_dcerpc_auditor                                             normal     No     SMB Session Pipe DCERPC Auditor
   107  auxiliary/scanner/smb/smb_enumshares                                                  normal     No     SMB Share Enumeration
   110  auxiliary/scanner/smb/smb_enumusers                                                   normal     No     SMB User Enumeration (SAM EnumUsers)
   111  auxiliary/scanner/smb/smb_version                                                     normal     No     SMB Version Detection
   115  auxiliary/scanner/snmp/snmp_enumshares                                                normal     No     SNMP Windows SMB Share Enumeration
   117  auxiliary/scanner/smb/smb_uninit_cred                                                 normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   131  auxiliary/scanner/smb/impacket/wmiexec                               2018-03-19       normal     No     WMI Exec
msf6 >
```



```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                 Required  Description
   ----         ---------------                                                 --------  -----------
   CHECK_ARCH   true                                                            no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                            no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                           no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
   RPORT        445                                                             yes       The SMB service port (TCP)
   SMBDomain    .                                                               no        The Windows domain to use for authentication
   SMBPass                                                                      no        The password for the specified username
   SMBUser                                                                      no        The username to authenticate as
   THREADS      1                                                               yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.10.35
RHOSTS => 192.168.10.35
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.10.35:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.10.35:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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 vulnerabili es in that auxiliary scan.