Assignment-2:
Name: Gadey Sathwik
Reg.no: 21bce8137

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.

- 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.


```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:


      .:ok000kdc'              'cdk000ko:.
    .x0000000000000c          c0000000000000x.
    :0000000000000000k,     ,k0000000000000000:
   '00000000kkkk00000: :00000000000000000'
   o00000000.    .o0000o00000l.    ,00000000o
   d00000000.      .c00000c.       ,00000000x
   l00000000.           ;d;         ,00000000l
   .00000000.     .;        ;        ,00000000.
    c0000000.    .00c.     'o00.    ,0000000c
     o000000.    .0000.    :0000.    ,000000o
      l00000.    .0000.    :0000.    ,00000l
       ;0000'    .0000.    :0000.    ;0000;
        .d00o    .0000occcx0000.    x00d.
          ,k0l  .0000000x0000.  .d0k,
           :kk;.00000000000.c0k:
             ;k000000000000000k:
              ,x00000000000x,
                .l0000000l.
                  ,d0d,
                    .


        =[ metasploit v6.3.27-dev                      ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post    ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops        ]
+ -- --=[ 9 evasion                                    ]


Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/
```

- 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.