Name : Ahmed Alzahrani **|| Email** : You-187@hotmail.com

SMB Enumeration

Frist Step

```
└─# nmblookup -A 10.0.2.7
Looking up status of 10.0.2.7
        METASPLOITABLE3 <00> -         B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        METASPLOITABLE3 <20> -         B <ACTIVE>

        MAC Address = 08-00-27-67-4D-D1
```

Second Step

```
└─# sudo nmap --script=smb-enum-shares 10.0.2.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-30 09:43 ED
Nmap scan report for 10.0.2.7
Host is up (0.00026s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
```

Third Step

```
Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENI
|   account_used: <blank>
|   \\10.0.2.7\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.0.2.7\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.0.2.7\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds
```

Fourth Step

```
└─# smbclient -U vagrant%vagrant -L 10.0.2.7

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

```
└─# smbclient //10.0.2.7/ADMIN$ -c 'ls' vagrant -U vagrant
  .                                   D        0  Sat Oct 30 09:47:48 2021
  ..                                  D        0  Sat Oct 30 09:47:48 2021
  AppCompat                           D        0  Mon Jul 13 23:20:08 2009
  AppPatch                            D        0  Sat Nov 20 22:31:48 2010
  assembly                          DSR        0  Sun Sep 19 14:12:06 2021
  bfsvc.exe                           A    71168  Sat Nov 20 22:24:24 2010
  Boot                                D        0  Mon Jul 13 23:20:09 2009
  bootstat.dat                       AS    67584  Sat Oct 30 16:33:56 2021
  Branding                            D        0  Tue Jul 14 01:37:10 2009
  Cursors                             D        0  Mon Jul 13 23:20:09 2009
  debug                               D        0  Tue Jul 14 00:56:52 2009
  diagerr.xml                         A     1908  Sun Sep 19 13:42:54 2021
  diagnostics                         D        0  Tue Jul 14 01:37:10 2009
  diagwrn.xml                         A     1908  Sun Sep 19 13:42:54 2021
  DigitalLocker                       D        0  Tue Jul 14 01:41:18 2009
  Downloaded Program Files            D        0  Tue Jul 14 01:37:10 2009
  DtcInstall.log                      A     2790  Sun Sep 19 13:42:48 2021
  en-US                               D        0  Sun Nov 21 00:56:54 2010
  explorer.exe                        A  2872320  Sat Nov 20 22:24:14 2010
  Fonts                             DSR        0  Sat Nov 20 22:31:50 2010
  fveupdate.exe                       A    15360  Mon Jul 13 21:39:10 2009
  Globalization                       D        0  Mon Jul 13 23:20:09 2009
  Help                                D        0  Sun Nov 21 00:56:53 2010
  HelpPane.exe                        A   733696  Mon Jul 13 21:39:12 2009
  hh.exe                              A    16896  Mon Jul 13 21:39:12 2009
```

Fifth Step

```
└─# smbclient //10.0.2.7/C$ -c 'ls' vagrant -U vagrant
  $Recycle.Bin                       DHS        0  Mon Jul 13 22:34:39 2009
  Boot                               DHS        0  Sun Sep 19 14:41:59 2021
  bootmgr                           AHSR   383786  Sat Nov 20 22:24:02 2010
  BOOTSECT.BAK                      AHSR     8192  Sun Sep 19 14:42:00 2021
  Documents and Settings          DHSrn        0  Tue Jul 14 01:06:44 2009
  glassfish                           D        0  Sun Sep 19 13:58:16 2021
  inetpub                             D        0  Sun Sep 19 13:52:59 2021
  jack_of_diamonds.png                A        0  Sun Sep 19 14:16:45 2021
  java0.log                           A      103  Sun Sep 19 14:15:36 2021
  java1.log                           A      103  Sun Sep 19 14:15:36 2021
  java2.log                           A      103  Sun Sep 19 14:15:36 2021
  ManageEngine                        D        0  Sun Sep 19 14:13:58 2021
  openjdk6                            D        0  Sun Sep 19 14:00:07 2021
  pagefile.sys                      AHS 2147016704  Sat Oct 30 16:33:56 202
  PerfLogs                            D        0  Mon Jul 13 23:20:08 2009
  Program Files                      DR        0  Sun Sep 19 14:16:51 2021
  Program Files (x86)                DR        0  Sun Sep 19 14:13:58 2021
  ProgramData                       DHn        0  Sun Sep 19 13:55:01 2021
  Recovery                        DHSn        0  Sun Sep 19 13:43:21 2021
  RubyDevKit                          D        0  Sun Sep 19 14:00:35 2021
  startup                             D        0  Sat Oct 23 02:46:41 2021
  System Volume Information         DHS        0  Sun Sep 19 13:42:32 2021
  tmp                                 D        0  Sat Oct 23 02:46:17 2021
  tools                               D        0  Sun Sep 19 14:00:22 2021
  Users                              DR        0  Sun Sep 19 13:53:21 2021
  wamp                                D        0  Sun Sep 19 13:59:50 2021
  Windows                             D        0  Sat Oct 30 09:47:48 2021
    Argon  .tmp                       A      226  Wed Oct  7 21:22:24 2015
```

LAst Step

```
└─# echo "enumdomusers"|sudo rpcclient -I 10.0.2.7 querydominfo -U vagrant%vagrant
user:[Administrator] rid:[0x1f4]
user:[anakin_skywalker] rid:[0x3f3]
user:[artoo_detoo] rid:[0x3ef]
user:[ben_kenobi] rid:[0x3f1]
user:[boba_fett] rid:[0x3f6]
user:[chewbacca] rid:[0x3f9]
user:[c_three_pio] rid:[0x3f0]
user:[darth_vader] rid:[0x3f2]
user:[greedo] rid:[0x3f8]
user:[Guest] rid:[0x1f5]
user:[han_solo] rid:[0x3ee]
user:[jabba_hutt] rid:[0x3f7]
user:[jarjar_binks] rid:[0x3f4]
user:[kylo_ren] rid:[0x3fa]
user:[lando_calrissian] rid:[0x3f5]
user:[leia_organa] rid:[0x3ec]
user:[luke_skywalker] rid:[0x3ed]
user:[sshd] rid:[0x3e9]
user:[sshd_server] rid:[0x3ea]
user:[vagrant] rid:[0x3e8]
```