Using CrackmapExec

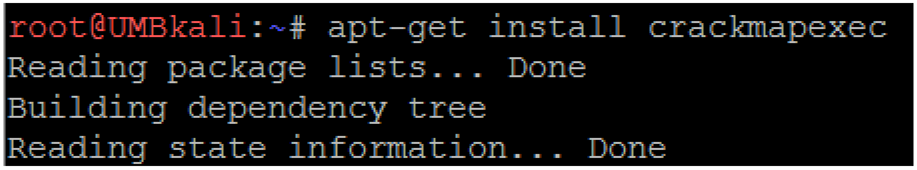
In the previous lab, where you used **NetBios** and **LLMNR** to find the username and password hash, you were able to find and extract the password of a regular user (may not be an administrator). Our lab uses **Win7** in workgroup, but in a corporate environment, what you find is the user ID in the domain. Given that you have a domain *user ID* and *password*, use this lab to understand more about the corporate domain.

1. Pre-requisite:

    a. Your **Kali** needs internet connection for additional file. Make sure your VM is set the networking to NAT. Download and install the tool as instructed.

    b. A **Windows 7** and **Windows 2012** VM provided by the instructor

2. Logon to you Kali, and install the tool as following. **Take a screenshot** of the completion

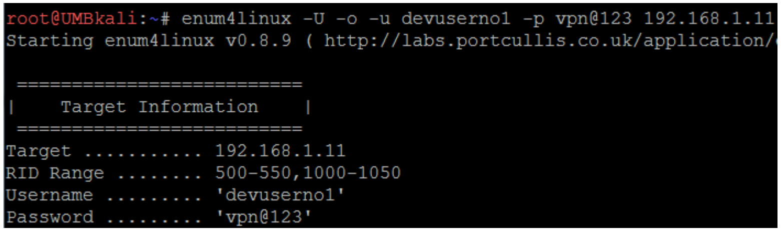


```
root@UMBkali:~# apt-get install crackmapexec
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

3. Follow the steps, and finish the tool installation

4. The ID you found in the **LLMNR** lab is **`devuserNo1`**, the password is **`vpn@123`** or whatever you set it to.

5. At your Kali terminal, use the following command, and replace the IP with your Windows 2012 IP address. **Take a screenshot of user IDs you can find from this tool**



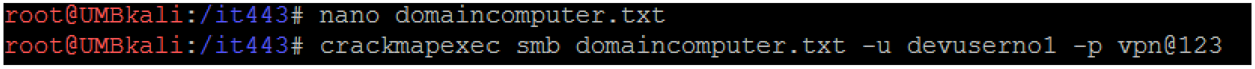
```
root@UMBkali:~# enum4linux -U -o -u devuserno1 -p vpn@123 192.168.1.11
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.1.11
RID Range ........ 500-550,1000-1050
Username ......... 'devuserno1'
Password ......... 'vpn@123'
```

6. When you get the list of user id, filter out the User ID only, and save it to a file on your Kali Linux (remember the directory where you save the file). In corporate environment, you may have a list of thousands of IDs (user ID, service account ID…)

7. Assuming you already got the list of domain servers when you gained access to a Windows7 using PowerShell Empire (previous lab). As a reminder, on PowerShell prompt of any Window 7, you can execute the command **`get-adcomputer -filter * | select dnsname`** and receive the full list of computers in the domain.

8. Use **nano** to create a file in a directory on your Kali Linux and insert the IP address of your Windows7, and Windows 2012 into the file and save it.

9. Run the following command and see if the ID can be authenticated to any of the device. **Take a screenshot of your result.**

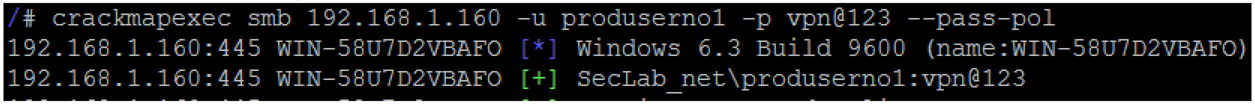


```
root@UMBkali:/it443# nano domaincomputer.txt
root@UMBkali:/it443# crackmapexec smb domaincomputer.txt -u devuserno1 -p vpn@123
```

In corporate environment, you use this to check how many workstations and servers this ID has access to. If the tool says the ID can logon to a server, you can logon to that server and expand your search more.

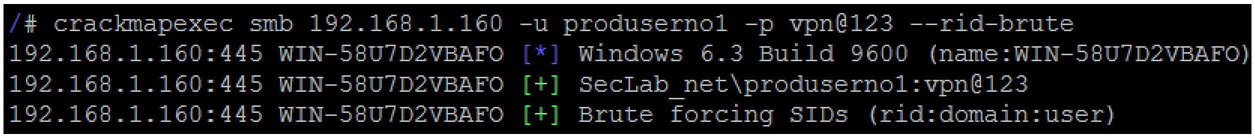
10. Logon to your Windows 7, create the same ID devuserno1 with the mentioned password. Re-run the **crackmapexec** tool again and **take a screenshot** of the result. It should say that logon to the Win7 is green

11. Now run the following command against your Windows 2012 to find the domain policy. **Take a screenshot of your result**



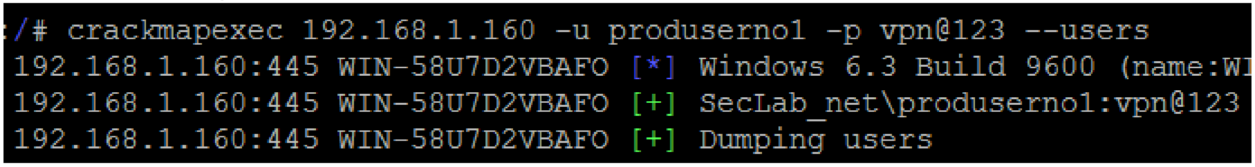
```
/# crackmapexec smb 192.168.1.160 -u produserno1 -p vpn@123 --pass-pol
192.168.1.160:445 WIN-58U7D2VBAFO [*] Windows 6.3 Build 9600 (name:WIN-58U7D2VBAFO)
192.168.1.160:445 WIN-58U7D2VBAFO [+] SecLab_net\produserno1:vpn@123
```

12. Run the following command to enumerate all groups and user IDs in the domain. **Take a screenshot of the first 20 lines**



```
/# crackmapexec smb 192.168.1.160 -u produserno1 -p vpn@123 --rid-brute
192.168.1.160:445 WIN-58U7D2VBAFO [*] Windows 6.3 Build 9600 (name:WIN-58U7D2VBAFO)
192.168.1.160:445 WIN-58U7D2VBAFO [+] SecLab_net\produserno1:vpn@123
192.168.1.160:445 WIN-58U7D2VBAFO [+] Brute forcing SIDs (rid:domain:user)
```

13. Run the following command to enumerate all user IDs in the domain. **take a screenshot**



```
/# crackmapexec 192.168.1.160 -u produserno1 -p vpn@123 --users
192.168.1.160:445 WIN-58U7D2VBAFO [*] Windows 6.3 Build 9600 (name:WI
192.168.1.160:445 WIN-58U7D2VBAFO [+] SecLab_net\produserno1:vpn@123
192.168.1.160:445 WIN-58U7D2VBAFO [+] Dumping users
```