fel-hita

(https://profile.intra.42.fr)

(https://profile.intra.42.fr/searches)

SCALE FOR PROJECT INIT (/PROJECTS/INIT)

You should evaluate 1 student in this team

★

Git repository

vogsphere@vogsphere.13

Introduction

Please respect the following rules:

- Remain polite, courteous, respectful and constructive throughout the evaluation process. The well-being of the community depends on it.

- Identify with the person (or the group) graded the eventual dysfunctions of the work. Take the time to discuss and debate the problems you have identified.

- You must consider that there might be some difference in how your peers might have understood the project's instructions and the scope of its functionalities. Always keep an open mind and grade him/her as honestly as possible. The pedagogy is valid only if the peer-evaluation is conducted seriously.

Guidelines

- Only grade the work that is in the student or group's GiT repository.

- Double-check that the GiT repository belongs to the student or the group. Ensure that the work is for the relevant project and also check that "git clone" is used in an empty folder.

- Check carefully that no malicious aliases was used to fool you and make you evaluate something other than the content of the official repository.

- To avoid any surprises, carefully check that both the evaluator

and the evaluated students have reviewed the possible scripts used to facilitate the grading.

- If the evaluated student has not completed that particular project yet, it is mandatory for this student to read the entire subject prior to starting the defence.

- Use the flags available on this scale to signal an empty repository, non-functioning program, a norm error, cheating etc. In these cases, the grading is over and the final grade is 0 (or -42 in case of cheating). However, with the exception of cheating, you are encouraged to continue to discuss your work (even if you have not finished it) in order to identify any issues that may have caused this failure and avoid repeating the same mistake in the future.

Attachments

Sujet (https://cdn.intra.42.fr/pdf/pdf/1381/init.fr.pdf)

Subject (https://cdn.intra.42.fr/pdf/pdf/1308/init.uk.pdf)

Subject (https://cdn.intra.42.fr/pdf/pdf/1281/init.en.pdf)

Part 1 - Follow Slash16 around the world

You have to follow us in the whole world

The student has followed Slash16 on Linkedin, Facebook and Twitter

The student has followed Slash16 on Linkedin, Facebook and Twitter

Yes No

Part 2 - Network

Evaluation of Part 2 - Network

Get the list of the network interfaces of the machine without displaying any detail

Check that the answer file contains the command which lists the names of the interfaces of the machine and no other information. For instance:

```
$>`cat 01`
lo0 gif0 stf0 en0 en1 en2 en3 p2p0 awdl0 bridge0
$>
```

☑ Yes ☒ No

Identify and display the Ethernet interface characteristics

Check that the answer file contains the command which
identifies and displays the specifications of the Ethernet interface.
For instance:

```
$>`cat 02`
en0: flags=XXXX
mtu 1500
options=10b
ether 00:00:00:00:00:00
inet 42.42.42.42 netmask 0xffffff00 broadcast 42.42.42.255
nd6 options=1
media: autoselect (1000baseT )
status: active
$>
```

☑ Yes ☒ No

Identify the MAC address of the Wi-Fi card

Check that the answer file contains the command which
identifies and diplays the MAC address of the wi-fi board. For instance:

```
$>`cat 03`
xxn: flags=XXXX
ether 00:00:00:00:00:00
$>
```

☑ Yes ☒ No

Identifiy the default gateway in the routing table

Check that the answer file contains the command which
identifies and displays the default gateway in the routing table. For instance:

```
$>sh 04
default 42.42.42.42 UGSc 19 16 en0
$>
```

☑ Yes ☒ No

Identify the IP address of the DNS server which answers to slash16.org

Check that the answer file contains the command which
identifies and displays the IP address of the DNS server. For instance:

```
$>`cat 05`
Server:10.51.1.42
Address:10.51.1.42

Non-authoritative answer:
Name:slash16.org
Address: 195.154.52.157
Name:slash16.org
Address: 195.154.52.158
$>
```

☑ Yes ☒ No

Get the complete path of the file that contains the IP address of the DNS server you're using

Check that the answer file contains the complete path of the file in
which the IP address of the used DNS server is written.

```
$>cat 05
/etc/resolv.conf
$>
```

☑ Yes ☒ No

Query an external DNS server on the same domain name (ex, google 8.8.8.8)

Check that the answer file contains the command which
use another DNS server to solve the same domain name. For instance:

```
$>`cat 07`
Server:8.8.8.8
Address:8.8.8.8
```

Non-authoritative answer:
Name:slash16.org
Address: 195.154.52.157
Name:slash16.org
Address: 195.154.52.158
$>

Yes No

Find the provider of slash16.org

Check that student's answer in the file is AWS (Amazon Web Services).

Yes No

Find the external IP of 42.fr

Ask the student to show you his approach and explain it.
Check that student's answer in the file is 163.172.250.12 and/or 163.172.250.11.

Yes No

Identify the network devices between your computer and the slash16.org domain

Check that the answer file contains the command which
identifies and displays the different network devices between
your computer and slash16.org.
For instance:

$>`cat 10`
traceroute to slash16.org (195.154.52.158), 64 hops max, 52 byte packets
1 10.8.0.1 (10.8.0.1) 5.809 ms 6.087 ms 3.124 ms
2 10.42.1.254 (10.42.1.254) 6.005 ms 13.668 ms 7.037 ms
3 nat-1.42.fr (10.60.1.11) 7.530 ms 3.379 ms 9.966 ms
4 dc3.42.fr (62.210.35.1) 7.100 ms 7.587 ms 5.160 ms
5 195.154.1.174 (195.154.1.174) 57.350 ms 168.093 ms 8.906 ms
6 a9k2-45x-s44-2.dc3.poneytelecom.eu (195.154.1.106) 6.590 ms 3.910 ms 5.525 ms
7 195.154.1.179 (195.154.1.179) 4.077 ms 46.904 ms 3.883 ms
8 pub-1.slash16.org (195.154.52.158) 5.699 ms 6.034 ms 7.632 ms
$>

Yes No

Use the output of the previous command to find the name and the IP address of the device that makes the link between you (local network) and the outside world.

Check that student's answer in the file is the NAT server.

☑ Yes ☒ No

Check that the server with the 10.51.1.253 IP address is reachable from your computer.

Check that the answer file contains the command which
displays if the IP address is reachable or not. For instance:

```
$>`cat 12`
64 bytes from 10.51.1.253: icmp_seq=0 ttl=62 time=40.663 ms
64 bytes from 10.51.1.253: icmp_seq=1 ttl=62 time=5.024 ms
$>
```

☑ Yes ☒ No

Use the Reverse DNS to find out the name of the server linked to the 10.51.1.81 IP address

Check that student's answer in the file is ldap-proxy.42.fr

☑ Yes ☒ No

What file contains the local DNS entries?

Check that student's answer in the file is /etc/hosts.

☑ Yes ☒ No

Make the intra.42.fr address reroute to 46.19.122.85

Ask the student to show you his approach and explain it.
Check that student's answer in the file is '46.19.122.85 intra.42.fr'.

☑ Yes ☒ No

Part 3 - System

Evaluation of Part 3 - System

In what file can you find the installed version of your Debian?

Check that student's answer in the file is /etc/debian_version.

☑ Yes ☒ No

What command can you use to rename your system?

Check that the answer file contains the command which
rename the system. For instance:

$>`cat 02`
machine.old.name.local
$>

☑ Yes ☒ No

What file has to be modified to make it permanent?

Check that student's answer in the file is /etc/hostname.

☑ Yes ☒ No

What command gives your system was last booted?

Check that the answer file contains the command which
gives the time since the last boot of the system. For instance:

$>`cat 04`
17:44 up 1 day, 6:45, 4 users, load averages: 1.33 1.42 1.40
$>

☑ Yes ☒ No

Name the command that determines the state of the SSH service?

Check that the answer file contains the command which
determines the state of the SSH service. For instance with init.d :

$>`cat 05`

openssh-daemon (pid 22405) is running...
$>

Or with service:

$>`cat 05`
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled)
Active: active (running) since Fri 2016-12-02 18:42:05 CET; 1 months 0 days ago
Main PID: 13106 (sshd)
CGroup: /system.slice/ssh.service
├─ 2461 ssh-agent -s
├─13106 /usr/sbin/sshd -D
├─27517 sshd: skyline [priv]
├─27519 sshd: skyline@pts/0
├─27520 -zsh
├─27561 sudo su
├─27562 su
├─27563 zsh
└─27589 systemctl status sshd.service
$>

☑ Yes ☒ No

Name the command that reboots it.

Check that the answer file contains the command which
reboot the SSH service. For instance with init.d:

$>`cat 06`
Stopping sshd: [OK]
Starting sshd: [OK]
$>

Or with service:

$>`cat 06`
$> service sshd status
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled)
Active: active (running) since Fri 2016-12-02 18:42:05 CET; 10s ago
Main PID: 13106 (sshd)
CGroup: /system.slice/ssh.service
├─ 2461 ssh-agent -s
├─13106 /usr/sbin/sshd -D
├─27517 sshd: skyline [priv]
├─27519 sshd: skyline@pts/0

```
├──27520 -zsh
├──27561 sudo su
├──27562 su
├──27563 zsh
└──27589 systemctl status sshd.service
$>
```

The displayed time in Active has to be in seconds because of the reboot of sshd.

☑ Yes ☒ No

Figure out the PID of the SSHD service

Check that the answer file contains the command which
figure out the PID of the ssh service. For instance:

```
$>`cat 07`
root 22405 0.0 0.0 66224 1184 ? Ss 17:46 0:00 /usr/sbin/sshd
$>
```

☑ Yes ☒ No

What file contains the RSA keys authorized to connect via SSH?

Check that student's answer in the file is .ssh/authorized_keys

☑ Yes ☒ No

What command lets you know who is connected to the System?

Check that the answer file contains the command which
lets you know who is connected to the system. For instance:

```
$>`cat 09`
skyline console Mar 23 10:59
skyline ttys000 Mar 24 17:04
$>
```

☑ Yes ☒ No

Name the command that lists the partition tables of drives?

Check that the answer file contains the command which
lists the partition tables of drives. For instance:

$>`cat 10`
Disk /dev/sdb: 2000.4 GB, 2000398934016 bytes
255 heads, 63 sectors/track, 243201 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
$>

☑ Yes ☒ No

Name the command that displays the available the space left and used on the system in an humanly understandable way

Check that the answer file contains the command which
displays the available space left and used on the system in an humanly understandable way.
For instance:

$>`cat 11`
Filesystem Size Used Avail Use% Mounted on
/dev/xvda2 7.8G 1.2G 6.3G 16% /
udev 10M 0 10M 0% /dev
tmpfs 200M 4.2M 196M 3% /run
tmpfs 500M 0 500M 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 500M 0 500M 0% /sys/fs/cgroup
$>

☑ Yes ☒ No

Figure out the exact size of each folder of /var in a humanly understandable way followed by the path of it.

Check that the answer file contains the command which
displays the exact size of each folders of /var in a humanly understandable way followed by the path of it.
For instance:

$>`cat 12`
4.0K /var/opt
864K /var/spool
1.3M /var/log
111M /var/lib

124M /var/cache
4.0K /var/local
8.0K /var/mail
1.1M /var/backups
4.0K /var/tmp
238M /var
$>

☑ Yes ☒ No

Name the command that find, in real time, currently running processes

Check that the answer file contains the command which
displays running processes in real time.
For instance:

$>`cat 13`
Tasks: 58 total, 1 running, 57 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 1022952 total, 359176 used, 663776 free, 168200 buffers
KiB Swap: 0 total, 0 used, 0 free. 86924 cached Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1 root 20 0 28740 4760 3064 S 0.0 0.5 0:03.28 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
3 root 20 0 0 0 0 S 0.0 0.0 0:00.02 ksoftirqd/0
5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
$>

☑ Yes ☒ No

Run the tail -f /var/log/syslog command in background

Check that the answer file contains the command which
runs the command `tail -f /var/log/syslog` in background
For instance:

$>`cat 14`
[1] 2660
Mar 25 06:25:03 rsyslogd: [origin software="rsyslogd" swVersion="8.4.2" x-pid="330" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
Mar 25 07:17:01 CRON[2601]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
Mar 25 08:17:01 CRON[2656]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
$>

Yes No

Find the command that kills the background command's process

Check that the answer file contains the command which
kills the process of the tail -f /var/log/syslog command.
For instance:

$>`cat 15`
[1]+ Terminated tail -f /var/log/syslog
$>

Yes No

Find the service which makes it possible to run specific tasks following a regular schedule

Check that student's answer in the file is cron.

Yes No

Find the command which gives the list of firewall rules

Check that the answer file contains the command which
gives the list of firewall rules.
For instance:

$>`cat 17`
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
$>

Yes No

With the previous command, authorize only IP addresses from 10.0.0.0/8 to connect to your system

Check that the answer file contains the command which
authorize only IP addresses from 10.0.0.0/8 to connect to your system.

For instance:

$>`cat 18`
$>
$> iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 10.0.0.0/8 anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
$>

☑ Yes ☒ No

With the previous command, forbid all others IP

Check that the answer file contains the command which
forbids all others to connect to your system.
For instance:

$>`cat 19`
$>
$> iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- 10.0.0.0/8 anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
$>

☑ Yes ☒ No

Part 4 - Scripting

Evalution of the part 3 - Scripting

Write a script which displays only the login, UID and Path of each entry of the /etc/passwd file

Check that the script displays only the login, UID and
Path of each entry of the /etc/passwd file.
For instance:

$>sh 1
root:0:/bin/bash
daemon:1:/usr/sbin/nologin
bin:2:/usr/sbin/nologin
sys:3:/usr/sbin/nologin
sync:4:/bin/sync
games:5:/usr/sbin/nologin
man:6:/usr/sbin/nologin
lp:7:/usr/sbin/nologin
mail:8:/usr/sbin/nologin
news:9:/usr/sbin/nologin
uucp:10:/usr/sbin/nologin
proxy:13:/usr/sbin/nologin
www-data:33:/usr/sbin/nologin
backup:34:/usr/sbin/nologin
list:38:/usr/sbin/nologin
irc:39:/usr/sbin/nologin
gnats:41:/usr/sbin/nologin
nobody:65534:/usr/sbin/nologin
systemd-timesync:100:/bin/false
systemd-network:101:/bin/false
systemd-resolve:102:/bin/false
systemd-bus-proxy:103:/bin/false
sshd:104:/usr/sbin/nologin
Debian-exim:105:/bin/false
postfix:106:/bin/false
skyline:1000:/bin/bash
$>

Yes No

Write a script which updates all the package sources, then all pachages and then logs everything in a file named /var/log/update_script.log. Create a scheduled task for this script, once per week at 4 AM.

Check that the script updates all the package sources and
logs everything in the good file and check if it is cron.
For instance:

$>sh script/2
$>cat /var/log/update_script.log
Hit http://cloudfront.debian.net jessie-backports InRelease
Hit http://security.debian.org jessie/updates InRelease

```
Hit http://security.debian.org jessie/updates/main Sources
Hit http://security.debian.org jessie/updates/contrib Sources
Hit http://security.debian.org jessie/updates/non-free Sources
Hit http://security.debian.org jessie/updates/main amd64 Packages
Hit http://security.debian.org jessie/updates/contrib amd64 Packages
Hit http://security.debian.org jessie/updates/non-free amd64 Packages
Hit http://security.debian.org jessie/updates/contrib Translation-en
Ign http://httpredir.debian.org jessie InRelease
Hit http://security.debian.org jessie/updates/main Translation-en
Get:1 http://httpredir.debian.org jessie-updates InRelease [142 kB]
Hit http://security.debian.org jessie/updates/non-free Translation-en
Get:2 http://cloudfront.debian.net jessie-backports/main Sources/DiffIndex [27.8 kB]
Get:3 http://httpredir.debian.org jessie Release.gpg [2,373 B]
Get:4 http://cloudfront.debian.net jessie-backports/main amd64 Packages/DiffIndex [27.8 kB]
Get:5 http://cloudfront.debian.net jessie-backports/main Translation-en/DiffIndex [27.8 kB]
Hit http://httpredir.debian.org jessie-updates/main Sources
Hit http://httpredir.debian.org jessie-updates/contrib Sources
Hit http://httpredir.debian.org jessie-updates/non-free Sources
Get:6 http://httpredir.debian.org jessie-updates/main amd64 Packages/DiffIndex [1,012 B]
Hit http://httpredir.debian.org jessie-updates/contrib amd64 Packages
Get:7 http://httpredir.debian.org jessie-updates/non-free amd64 Packages/DiffIndex [736 B]
Get:8 http://httpredir.debian.org jessie-updates/contrib Translation-en [14 B]
Get:9 http://httpredir.debian.org jessie-updates/main Translation-en/DiffIndex [736 B]
Get:10 http://httpredir.debian.org jessie-updates/non-free Translation-en/DiffIndex [736 B]
Get:11 http://httpredir.debian.org jessie Release [148 kB]
Hit http://httpredir.debian.org jessie/main Sources
Hit http://httpredir.debian.org jessie/contrib Sources
Hit http://httpredir.debian.org jessie/non-free Sources
Hit http://httpredir.debian.org jessie/main amd64 Packages
Hit http://httpredir.debian.org jessie/contrib amd64 Packages
Hit http://httpredir.debian.org jessie/non-free amd64 Packages
Get:12 http://httpredir.debian.org jessie/contrib Translation-en [38.5 kB]
Get:13 http://httpredir.debian.org jessie/main Translation-en [4,582 kB]
Get:14 http://httpredir.debian.org jessie/non-free Translation-en [72.5 kB]
Fetched 5,073 kB in 4s (1,143 kB/s)
Reading package lists...
Reading package lists...
Building dependency tree...
Reading state information...
The following packages will be upgraded:
git git-man
2 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,530 kB of archives.
After this operation, 30.7 kB of additional disk space will be used.
Get:1 http://security.debian.org/ jessie/updates/main git-man all 1:2.1.4-2.1+deb8u2 [1,267 kB]
Get:2 http://security.debian.org/ jessie/updates/main git amd64 1:2.1.4-2.1+deb8u2 [3,262 kB]
Fetched 4,530 kB in 0s (14.5 MB/s)
(Reading database ... 41091 files and directories currently installed.)
Preparing to unpack .../git-man_1%3a2.1.4-2.1+deb8u2_all.deb ...
```

```
Unpacking git-man (1:2.1.4-2.1+deb8u2) over (1:2.1.4-2.1+deb8u1) ...
Preparing to unpack .../git_1%3a2.1.4-2.1+deb8u2_amd64.deb ...
Unpacking git (1:2.1.4-2.1+deb8u2) over (1:2.1.4-2.1+deb8u1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up git-man (1:2.1.4-2.1+deb8u2) ...
Setting up git (1:2.1.4-2.1+deb8u2) ...
$>
```

Pour vérifier que ce script est en cron :

```
$>crontab -l
00 4 * * 1 /bin/sh /usr/local/bin/01.sh
$>
```

☑ Yes ☒ No

Write a script which displays the list of files from the folder given as parameter, sorted by size.

Check that the script diplays the list of files in the folder given as
parameter, sorted by size.
For instance:

```
$>sh script/3 /var
248736 /var
131080 /var/cache
125012 /var/cache/apt
113992 /var/lib
97572 /var/lib/apt
97544 /var/lib/apt/lists
75024 /var/cache/apt/archives
33016 /var/cache/apt/archives/linux-image-3.16.0-4-amd64_3.16.7-ckt20-1+deb8u4_amd64.deb
33012 /var/lib/apt/lists/httpredir.debian.org_debian_dists_jessie_main_binary-amd64_Packages
31764 /var/lib/apt/lists/httpredir.debian.org_debian_dists_jessie_main_source_Sources
$>
```

☑ Yes ☒ No

Make a script which monitors the modifications of the /etc/crontab file and sends an e-mail to root if the file is modified. Create a scheduled task to run this script everyday at midnight.

Check that the script monitors the modifications of the
/etc/crontab file and sends an e-mail to root ONLY if the file is modified.
So you should receive an email showing the changes on the file,
either in local with the mail command or in your own mailbox.

Further, you have to check the crontab:

```
$>crontab -l
00 0 * * * /bin/sh /usr/local/bin/04.sh 2>&1
$>
```

☑ Yes ☒ No

Make a script which displays 42.

42 Obviously ;)

☑ Yes ☒ No

Ratings

Don't forget to check the flag corresponding to the defense

✔ Ok

Empty work Cheat Forbidden function

Conclusion

Leave a comment on this evaluation

Finish evaluation