Turkcell Bootcamp Linux Bitirme Odevi
mailto: kaanavsarasan@outlook.com
SUBJECT: Turkcell Bootcamp – name/surname

Steps

1. Configure the time zone to GMT.

2. Allow password-less login for the root user using SSH.

3. Create a user (named *user*) that can connect to the machine without a password.

4. The user `user` should change their password every week, with 2 days' warning and 1 day of usage once expired.

5. The root user must be able to SSH as *user* without a password so that nobody can connect remotely as root using a password.

6. The user *user* should be able to become root user without a password, and also execute commands without a password.

7. When a user tries to log in over SSH, display a legal message about not allowing unauthorized access to this system.

8. SSH must listen on port *22222*, instead of the default one (*22*).

9. Create a group named `devel`.

10. Make `user` a member of `devel`.

11. Store user membership in a file named `userids` in the home folder for *user.*

12. The user *user*, and *root* user, should be able to connect to localhost via SSH without specifying the port, and default to compression for the connection.

13. Find all man page names in the system, and put the names into a file named *manpages.txt*.

14. Print usernames for users without logins permitted to the system. For each username, print the user ID and groups for that user.

15. Monitor available system resources every 5 minutes. Do not use cron. Store as */root/resources.log*.

16. Add a per-minute job to report the available percentage of free disk space, and store it in */root/freespace.log* so that it shows both the filesystem and free space.

17. Configure the system to only leave 3 days of logs.

18. Configure the log rotation for */root/freespace.log* and */root/resources.log*.

19. Configure the time synchronization against *pool.ntp.org*, using fast sync.

20. Provide NTP server services for the subnet *172.22.0.1/24*.

21. Configure system stats for collection every minute.

22. Configure the password length for users in the system to be 12 characters long.

23. Create a bot user named *privacy,* which will keep its files only visible to itself by default.

24. Create a folder in *shared* that can be accessed by all users, and that defaults new files and directories to still be accessible to users of the *devel* group.

25. Configure a network connection with IPv4 and IPv6 addresses named *mynic,* using the following data:

```
Ip6: 2001:db8:0:1::c000:207/64 g
gateway 2001:db8:0:1::1
Ipv4 192.0.1.3/24
gateway 192.0.1.1
```

26. Allow the host to use a *google* hostname to reach `www.google.com`, and a *redhat* hostname to reach `www.redhat.com`.

27. Report the files modified from those that the vendor distributed, and store them in */root/altered.txt*.

28. Make our system installation media packages available via HTTP under the */mirror path* for other systems to use as a mirror, configuring the repository in our system. Remove the kernel packages from that mirror, so that other systems (even ours) can't find new kernels. Prevent the glibc packages from being installed from this repo without removing them.

29. While being *user*, make a copy of the */root* folder in */home/user/root/* folder, and keep it in sync every day, synchronizing additions and deletions.

30. Check that our system conforms to the PCI-DSS standard.

31. Add a second hard drive of 30 GB to the system. However, use only 15 GB to move the mirror to it, making it available at boot using compression and deduplication. Make it available under */mirror/mirror*.

32. As we plan to mirror custom sets of packages based on the same data, configure the filesystem to report at least 1,500 GB to be used by our mirrors.

33. Create a second copy of the mirror under */mirror/mytailormirror*, removing all packages starting with the letter *k**.

34. Create a new volume in the remaining space of the added hard drive (15 GB), and use it to extend the root filesystem.

35. Create a boot entry that allows you to boot into emergency mode, in order to change the root password.

36. Create a custom tuning profile that defines the readahead to be *4096* for the first drive and *1024* for the second drive. This profile should also crash the system should an OOM event occur.

37. Disable and remove the installed HTTP package. Then, set up the HTTP server using the *registry.redhat.io/rhel8/httpd-24* image.