REPORT FOR TEAM NUMBER 10.134.178.10 on 2023-04-17

USER MANAGEMENT

> - This is the list of users on server 10.134.178.10
> - (If the list starts with the 'team' user, than that user has not been deleted)
>   - 1005 Vasil
>   - 1006 Jasper
>   - 1007 Vlad
>   - 1008 Panagiotis
>   - 1009 team1

Check sudoers.d drop-in directory

> - This is/are the file(s) in the folder and the permissions:
> - (root should have read/write perms)

```
-rw-------. 1 root root 26 Feb 13 14:04 /etc/sudoers.d/team10
```

> - And this is the content:

```
%team10 ALL=(ALL:ALL) ALL
```

SSH KEY MANAGEMENT

> - Checking if every user on the system has an authorized-keys file in their .ssh folder
> - There should be at least as many lines as there are users on the system.
> - Additionally, every line should start with 'ssh-ed25519'
> - If it doesn't, then you didn't create ssh keys of the required type.

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMJvSrOD4MrbfiTXZPwEowN2vHg4sYIqw/van/RxPu0p twan@kdgmint
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMJvSrOD4MrbfiTXZPwEowN2vHg4sYIqw/van/RxPu0p twan@kdgmint
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHTilsYWatPXbqXYkN5KwL39b5Zbp1TpfqPcFguaHkAg vasil@HP-V-Dragon
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDeZxR2HqH21IplYUfUZ5K9/LgNo+gVS3BDfI99ne1PR jasper_school@Laptop-JM
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDunC5ql0V3KccQa448Hv3Rs5NeYhPjX5rG5fwYbr8D9 vladbuinceanu@Vlads-MacBook-
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPtFQwEYSl9a/TwO8aB+sNX+wjjyqJzOh2ARaRR+8ftF panagiotis@DESKTOP-G05CN35
```

> - (Every user should know how to log in passwordlessly on the server.)

NETWORK CONFIGURATION

> - The additional connection is ok
> - The additional IP address should be in the range of 192.168.1.0/24;
> - with the last octet the same as your team number:

```
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 46:a0:b4:4e:fe:8a brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.1.10/24 brd 192.168.1.255 scope global noprefixroute ens19
       valid_lft forever preferred_lft forever
    inet 10.134.177.24/21 brd 10.134.183.255 scope global dynamic noprefixroute ens19
       valid_lft 9908sec preferred_lft 9908sec
    inet6 fe80::dfda:269c:c79d:47b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- To be able to reach the back end server, there should be a route displayed by ip route:
- (The route should be to the 192.168.1.0/24 network)

```
default via 10.134.176.1 dev ens18 proto dhcp src 10.134.178.10 metric 100
default via 10.134.176.1 dev ens19 proto dhcp src 10.134.177.24 metric 101
10.134.176.0/21 dev ens18 proto kernel scope link src 10.134.178.10 metric 100
10.134.176.0/21 dev ens19 proto kernel scope link src 10.134.177.24 metric 101
192.168.1.0/24 dev ens19 proto kernel scope link src 192.168.1.10 metric 101
```

DATABASE CONFIGURATION

- Check if postgresql server is installed, active and enabled :
  - Installed? Yes
  - Enabled? enabled
  - Active? active

- Looking for database 'game'

```
                                 List of databases
   Name    |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
-----------+----------+----------+-------------+-------------+-----------------------
 game      | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =Tc/postgres         +
           |          |          |             |             | postgres=CTc/postgres+
           |          |          |             |             | game=CTc/postgres
 postgres  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
 template1 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
(4 rows)
```

- This is the list of users:
- (Look for user 'game')

```
                                 List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 game      |                                                            | {}
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
```

Is network 10.0.0.0/8 added to pg_hba.conf : **Yes, added.**

Which addresses is postgresql listening on?

`listen_addresses = '10.134.178.10'` **(OK)**

WEBSERVER CONFIGURATION

- Check if apache2 server is installed, active and enabled.
  - Installed? Yes
  - Enabled? enabled
  - Active? active

- Check if there is a .htaccess redirecting .git access to 404 : **No, '.htaccess' is not present**

- Checking presence of index.html
  - Checking file and folder permissions :

```
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (   48/  apache)
```

- Perms should be 0644, Uid should be root and Gid should be apache

- Checking permissions of folder /var/www/html

```
Access: (0755/drwxr-xr-x)  Uid: (    0/    root)   Gid: (   48/  apache)
```

- Perms should be 0755, Uid should be root and Gid should be apache.

RSYSLOG CONFIGURATION

- Check for the existence of a file /var/log/team.log : **(OK)**

Checking content of files in rsyslog.d drop-in directory :

- /etc/rsyslog.d/local6.conf

```
    local6.* /var/log/team.log
```

Checking persistence of system journal database : **(Not OK)**

DETECTING PRESENCE OF SCRIPT

- Only detecting presence of a script.
- Review of the script will follow in a separate feedback.

- The script is present in /opt/script/ : **(OK)**

CRON JOB FOR BACKUP SCRIPT

- Checking presence of a cron job for root : **(OK)**
- This is the cronjob:

```
0 0 */2 * * /opt/script/newpicture.sh
0 0 * * 0 /opt/script/backup.sh
```