Nintendo Debian 11 README

Please read the entire README thoroughly before modifying anything on this computer.

Forensic Questions

There are "Forensic Questions" on your Desktop; you will receive points for answering these questions correctly. Valid (scored) "Forensic Questions" will only be located directly on your Desktop. Please read all "Forensic Questions" thoroughly before modifying this computer, as you may change something that prevents you from answering the question correctly.

Competition Scenario

You have been tasked with a mission of great importance from Nintendo HQ.

Hello! Nintendo HQ has recently been attacked by the evil wizards and they need your help in taking the system back over for them. It seems like many artifacts and backdoors have also been left for the evil wizards to come back and easily take the system back over. Please take care of our security maintenance as well as other issues you find along the way.

Along with the many security issues that Nintendo HQ have learned about, they also noticed that they couldn't get back in the system themselves! Something was said about privileges being messed up and even after fixing those, they still couldn't get their root access back! More about this in the first forensics question, but please help Nintendo HQ get all their belongings back.

Nintendo HQ's security policies require that all user accounts be password protected. Everyone is required to choose secure passwords; however, this policy may not be currently enforced on this computer. It is very important to **write down all passwords you change**. The presence of any non-work related media files and "hacking tools" is strictly prohibited. We currently do not use any centralized maintenance or polling tools to manage our IT equipment. This system is for official business use only by authorized users. Your job is to secure this computer, within the guidelines of the scenario, while ensuring the availability of authorized business-critical software and services.

Super Mario Land

Super Mario Land is a beautiful world, filled to the brim with characters trying to find the true Mario Dream while being able to laugh and play with their friends.

All residents of Super Mario Land should be part of the "sml" group.

Bowser
Bowser Jr.
Daisy
Diddy Kong
Donkey Kong
Luigi
Mario
Peach
Rosalina
Toad
Waluigi
Wario
Yoshi

Super Wizard Land

Alongside Super Mario Land lies an evil underground world, holding anyone and everyone who comes in hostage.

The residents of Super Wizard Land are in the "wizards" group. Due to the state of the nation please quickly remove this group from Nintendo Land.

Hyrule

The Kingdom of Hyrule is a medieval-based fantasy land, filled with characters who love exploration and adventure. They are always on the lookout for vulnerabilities lying in the system and are the first to notify any problems.

All residents of Hyrule should be part of the "koh" group.

> Ganondorf
> Link
> Zelda

Archanea

Archanea contains several nations, all trying to fight to become the best nation. They all compete with each other to see who can last the longest getting attacked and by finding vulnerabilities.

All residents of Hyrule should be part of the "fireemblem" group.

> Alear
> Byleth
> Chrom
> Corrin
> Ike
> Lucina
> Marth
> Robin
> roy

Pokeland

Lastly, the Pokemon World is a place filled with danger, where trainers get to have fun and battle monsters and each other at the same time.

All residents of Pokeland should be part of the "pokemon" group.

> Ash
> Pikachu

Misty
Brock
Meowth
Jessie
James

Debian 11

We have also decided to use only Debian 11 on this system. It is also a Nintendo policy to use only the latest, official, stable Debian 11 packages available for required software and services on this computer. Nintendo HQ has decided that the default web browser for all users on this computer should be the latest stable version of Firefox. They have also decided on a policy to never let users log in as root. If administrators need to run commands as root, they are required to use the "sudo" command.

Nintendo HQ has also reported some strange events happening every 30 minutes after they start the system. They said something about their progress being lost and the system going down?

Nintendo World

Nintendo HQ has decided to implement a LAMP Stack with a wordpress instance to help them post about their activities and progress with the system. Please help them make sure all components of the LAMP stack are secure.

All their wordpress data is stored at /var/www/wordpress/

They also wanted their wordpress instance to be configured with SSL, so their communications could be secure. Please help them configure this and update the firewall properly.

Mariadb Root User: root;N1nt3nd0R0cks!
Mariadb nintendoadmin User: nintendoadmin;N1nt3nd0bl0gs!
Wordrpess msakurai User: msakurai;password

Nintendo HQ also wanted to implement Phpmyadmin for their database management purposes. It seems like they haven't changed the password for the phpmyadmin user from the default one though, so please make sure to fix it along with all the other components!

Phpmyadmin phpmyadmin User: phpmyadmin;password

Critical Services:

- LAMP (All Components + wordpress)
- phpmyadmin

Authorized Administrators and Users

Authorized Administrators:
msakurai (you)
        password: password
mario
        password: 1tsAm3M@r1o!
link
        password: Th3L3g3nd0fZ3ld4#
chrom
        password: SurrenderNow!
ash
        password: G0tt@c@tch3m4ll!

Authorized Users (Minions):
bowser
bowserjr
daisy
kingboo
foureyes
mysteryman
kingkrool
diddykong
donkeykong
luigi
peach
rosalina
toad
waluigi
wario
yoshi
ganondorf
zelda
kirby

```
metaknight
corrin
ike
lucina
marth
robin
roy
alear
byleth
pikachu
misty
brock
meowth
jessie
james
```

Competition Guidelines

- In order to provide a better competition experience, you are **NOT** required to change the password of the primary, auto-login, user account. Changing the password of a user that is set to automatically log in may lock you out of your computer.
- Authorized administrator passwords were correct the last time you did a password audit, but are not guaranteed to be currently accurate.
- Do not remove any files from /opt/aeacus.
- Do not remove any authorized users or their home directories.
- The time zone of this image is set to PDT. Please do not change the time zone, date, or time on this image.
- This image was created for the sole purpose of training cyber students at Troy High School. This image should not be redistributed outside of Troy High School unless given proper authorization to do so.

Created by Jaden Wijata in collaboration with Derek Peng and Ian Tseng