ImaginaryCTF 2025 - Syshardening 11

OS: Mint 22

Made with <3 by @shubuntu && @prilasey, w/ help from @eth007, @c.bass., @syossu

Challenge Guidelines (How to get the flag)

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 tamper with the scoring engine and its helper files, as doing so can destroy the scoring for this image, and therefore make it impossible to get the flag. **THIS IS NOT A REV CHALL. THERE IS A REASON THIS IS IN MISC. IF YOU SCORE 80 YOU GET THE FLAG.** Do not remove any authorized users or their home directories. **Make a ticket when you get 80 points, and you will receive the flag.** **ANY VULNERABILITY ADDRESSED IN THE FORENSICS QUESTION WILL (GENERALLY) NOT SCORE IF PATCHED.** This is just a way to keep vulnerabilities largely unique. If you are unsure about something not scoring, send us a DM. DM @shubuntu or @prilasey on Discord. Good luck and have fun!

Forensics Questions

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

Company Policy

This company's security policies require that all user accounts be password protected. Employees are required to choose secure passwords, however this policy may not be currently enforced on this computer. The presence of any non-work related media files

and "hacking tools" on any computers is strictly prohibited. This company currently does not use any centralized maintenance or polling tools to manage their IT equipment. This computer is for official business use only by authorized users. This is a critical computer in a production environment. Please do NOT attempt to upgrade the operating system on this Mint 22 machine if prompted to do so. Management has decided that the default web browser for all users on this computer should be the latest stable version of Firefox. Company policy is to never let users log in as root.

Scenario Layout

Welcome to the official Studio Ghibli SMB server! This server is set up a bit unconventionally as it will act as both a development workspace but will utilize SMB file share. Samba will be used to serve important source code files (anonymous enabled, read only) with simultaneous SSH access to let users connect and use the Python development space.

Company Policy

Company policy is to prohibit hacking tools, games, media files, malware, backdoors, or generally unwanted software but last week Howl already used his magic to keep this policy in check after the events of our last breach. Your mission will be mainly targeted more toward system hardening and workspace setup to close off any vulnerabilities and ensure this server acts as a functional SMB server and development workspace. The users of this machine will primarily be using both pip and apt package managers, so please keep the workspace policy in mind when managing these package managers. For apt management, please use the configuration file /etc/apt/apt.conf.d/99custom for ANY CONFIGURATION. Make sure SSH uses pubkey based authentication. Samba file share (code) is at /srv/samba/public, default credentials for Samba are used. Additionally, please make sure the latest stable version of (standard) opencv is

installed only for the user totoro. Chutotoro needs it to code a new Limelight CV pipeline for FTC DECODE™ (And also to detect horrible AI ghibli pfps). Make sure this is installed for Lastly, please ensure that system passwords are hashed with YESCRYPT.

Critical Services

Samba (SMB)
OpenSSH (SSH)

Administrators

totoro (you)	Password: password
kiki	Password: D3l1v3ry$$$
howl	Password: C@5tle123
chihiro	Password: Yubab@5ucks

Authorized Users

marco
jiro
nahoko
jiji
chutotoro
chibitotoro
sophie
haku
satsuki
catbus
calcifer
sosuke
ponyo
mononoke
mahito

Corrections/Critical Info

- FQ2: Answer with full path, not filename.
- FQ5: Please make a ticket about Forensics Question 5; it's not scored correctly but we will give you the scorable answer if you give us the correct answer.
- FQ8: All lowercase.
- OpenCV: Totoro account, using pip. DM me if this does not work. It may be grounds for appeal.