System Administration Challenge

»»———— Windows 10 ————««

Dear competitor,

You've been hired as a system administrator for the company **Skills Canada**. Nine (9) tasks have been assigned to you in this document. Upon starting your virtual machine, immediately create a file named `player.txt` on the desktop with the code identifier that will be provided to you.

The scoring engine (`scoring.exe`) runs automatically every minute, but you can also run it manually to update your score. Your progress will be reflected in the `report.txt` document, as well as the live scoreboard. VMware 14 or higher is required.

Please feel free to use any system administration tools and resources available at your disposal. Open source tools (eg. scripts and programs from GitHub) and network-based tools (eg. Google, Google Lens) are all permitted. Some programs are installed for you, but you may use any tools you like. You may not receive scripting assistance from LLMs like ChatGPT and GitHub Copilot.

You may reset the VM by extracting from the zip file again. You will not be penalized and will eventually receive points for the challenges you already solved. Please let your supervisor know if you plan on restarting.

Tampering with the scoring engine is considered cheating and will result in severe penalties. Examples of prohibited actions include reverse engineering, modifying, and network interception on/of the scoring engine.

The challenge weights are as follows:

Challenge	1	2	3	4	5	6	7	8		**Total**
Points	10	10	5	10	10	5	10	10		/70

Good luck!

An online version of this document is available at https://skillscanada.yegyouth.tech/README.pdf

Hard Medium Easy

1. **Wallpaper Recovery**
   We used to keep our password on the desktop wallpaper, but an intern (correctly) thought that this was unsafe and deleted the wallpaper without approval. Please recover and restore the old wallpaper using the official tool `winfr` or otherwise.
   Note: If you download large files or software to the VM prior to recovering the images, this could override the deleted files! If this happens, you may have to restart the image.
   Topics: File recovery

2. **Phishy Google**
   An employee reported that the URL http://google.ca redirects to another website. Web browser activity is highly sensitive and unexpected redirects are a major security concern. Please identify the source of the redirect and remediate this vulnerability as soon as possible.
   Topics: Malware, browsers / web technologies, network configuration

3. **Weird Web Font**
   Your boss has sent you this secret message, but it's in a really weird language or font I can't read! If you understand it, please follow the instructions provided in the message.
   Attachments: https://skillscanada.yegyouth.tech/secret_message/
   Topics: Web technologies

4. **Firefox Update**
   Firefox update is not working. Can you find the installer for v112 and update Firefox to v112? (Note: v112 is **NOT** the latest version) Firefox must remain installed at `C:\Program Files (x86)\Mozilla Firefox\firefox.exe`.
   Topics: Application updates, registry configuration, filesystem features

5. **Google Docs IP Logger** — Hints may be released
   Our employee has just been sent a malicious Google Docs IP Logger, and someone was able to grab our company's IP! Please see if you can find any information about this individual.
   Tip: Log in with a Google account. Check Google Apps Script.
   https://docs.google.com/document/d/1e16h5Xo7f8xfHKIPSrsA6HPu3fFmH1VkCW1Mbe9U-wo/edit
   Topics: Google Apps Script, reverse engineering, IPv6 networking, SSH

6. **Basic System Hardening**
   "Brute force password attacks can use automated methods to try millions of password combinations for any user account." Take measures to mitigate this risk.
   Topics: Windows hardening, Google

7. **No Screenshots of Code** — Hints may be released

   Senior programmers find it annoying when they're sent screenshots of code instead of the code in text format. A fellow employee in your company sent you this hex screenshot of an image, presumably just to annoy you. However, as the amazing sysadmin you are, you refuse to let this minor inconvenience get to you. Please recover the screenshotted file and save it as `small.jpg` on the desktop. As a sanity check, the image should be a heavily-compressed JPEG containing the Skills Canada logo.

   Attachments: https://skillscanada.yegyouth.tech/Screenshot_20230517_094042.png

   Topics: OCR

8. **Database Migration**

   An employee is requesting that you make some images available to customers. You've been sent an URL to access these images and you're tasked with making it available on the desktop in a folder named `images`. They need to be split into three subfolders: `Portrait`, `Landscape`, and `Square`. To classify the images, we use the following definitions:

Square	`0.8 ≤ aspect_ratio ≤ 1.2`
Portrait	`aspect_ratio < 0.8`
Landscape	`aspect_ratio > 1.2`

   where `aspect_ratio = width / height`. The folders must be empty except for these images.

   Attachments: https://skillscanada.yegyouth.tech/imagegallery/

   Topics: Automation, recursive download, website mirroring, scripting