Exercise 1 – File Explorer and Document Save (Lab Inaccessible)

Objective

The lab was designed to walk through basic Windows navigation using File Explorer and LibreOffice. It covered folder creation, file saving, and verifying file paths.

Lab Outcome

The lab environment failed to load LibreOffice after extended wait time. Discussion posts from other students confirmed the issue is ongoing and not user-specific. The File Explorer interface also froze during initial attempts.

Skills Demonstrated (Conceptual)

While the lab was not functional, the activity reinforced the importance of:

- Navigating the Windows file system

- Maintaining organized folder structures

- Identifying and validating file paths for audits or technical support

Reflection

This lab would be easy to replicate on a local machine with working software. The concepts are simple but foundational — understanding file systems is critical for supporting users, managing permissions, and auditing endpoint behavior. Despite technical issues, the takeaway was still clear.

All posts sorted by recent activity

lab file I did my lab the only issue I was having with it. I was not able to re...
shellyfigaro3
👍 ☆ 💬 3   4w

not working not even able to type. please fix this issue.
anastasia228_16
👍 ☆ 💬 4   8w

No Lab No preview available
Abjad
👍 ☆ 💬 2   8w

Difficulty doing lab The lab environment is very slow and doesn't work wel...
JCSargent82
👍 ☆ 💬 2   8w

No Lab Hello, I'm unable to see any link to access the lab on this page.
Yusaf_Umar
👍 ☆ 💬 2   12w

Keyboard issues With The Lab Windows The keyboard on my Windows P...
LadyVeeBee
👍 ☆ 💬 2   12w

doesnt seem to want to load. it works up to the step where yo...
Chattin
👍 ☆ 💬 2   12w

Having issues in Labs Hello-I'm unable to make any type of edits to this la...

Lab – Exploring Microsoft Windows Server Features (Lab Inaccessible)

Objective

This lab was intended to introduce key features of Microsoft Windows Server, including role-based installation, administrative tools, and basic configuration tasks within a virtual server environment.

Lab Outcome

The cloud-based lab failed to load properly. Windows Server environment remained stuck on updates or refused to launch standard features (such as Server Manager or File Explorer). LibreOffice, used in prior labs, also failed to initialize. Multiple students in the

discussion forums confirmed identical issues with long wait times and unresponsive environments.

Skills Intended (Conceptual)

- Navigating Microsoft Windows Server interface

- Identifying administrative tools and server roles

- Recognizing differences between client OS (e.g., Windows 10/11) and server OS environments

- Understanding role-based architecture and system services

Reflection

Although I couldn't complete the lab due to platform limitations, the objectives were clear and align with foundational Windows Server knowledge. These tasks can be replicated on a local virtual machine or test server and are key to understanding system administration from a cybersecurity and operations perspective.

Finalized Summary for Lab 3

Lab 3 – Windows Command Line Administration (Lab Inaccessible)

Objective

This lab was designed to introduce core administrative commands within the Windows Command Prompt. Tasks included gathering system information, navigating and managing directories, and performing basic system maintenance operations.

Lab Outcome

The lab environment failed to load or respond properly. Despite multiple attempts, the virtual system either timed out or became unresponsive before any command-line tasks could be completed. The issue appears to be systemic, as confirmed by discussion board feedback from other learners encountering the same problem.

Skills Intended (Conceptual)

- Using systeminfo to gather system specifications

- Navigating directories with cd, dir, and mkdir

- Performing basic maintenance using commands like chkdsk, sfc, and tasklist

- Interpreting command output for system diagnostics

Reflection

While the technical environment was inaccessible, the listed exercises are tasks I've performed before in my own Windows system or during prior training. I understand how to gather system data, work within directories, and perform basic command-line administration. These are foundational skills in both cybersecurity and system administration, especially in early triage, endpoint audits, or digital forensics workflows.

Discussions

Add a post   ✕

All posts sorted by recent activity

Use the Windows Command Prompt for Administration this lab was fun t...
shellyfigaro3
👍   ☆   💬 2   2w

Lab Issues Hello this is my 2nd lab and I'm having the same issues. I'll b...
JLuExpress
👍   ☆   💬 2   12w

Unable to participate in lab Same issues I've had with the last 2 labs.
nataschamartin
👍   ★   💬 3   16w

Lab not working This is the second lab I am unable to complete - the virtu...
YamRod
👍   ☆   16w

please help On-screen keyboard isn't working
RA_2501_O0ZL
👍   ☆   💬 4   24w

Lab complications I would of shown a screen shot of the VM not having a...
mild12
👍   ☆   💬 2   24w

lab I can't continue the lab, Exercise 3 . the remote desktop is   edX XPERT
chebbinajla
👍   ☆   💬 3   28w

ISSUE COULD NOT TYPE DURING LAB, COMPLETED USING TERMI...

Lab 4 – Windows Defender Firewall (Performed Locally)

Objective

The goal of this lab was to explore the functionality of Windows Defender Firewall. Tasks included viewing current firewall rules, creating or modifying rules for inbound and outbound traffic, and understanding the role of the firewall in a broader security framework.

Lab Outcome

Due to the instability of the cloud-based lab, I performed this lab directly on my own Windows machine. This allowed me to complete all tasks successfully and observe how firewall behavior responds in a fully functional, real-world environment.

Tasks Completed

- Opened **Windows Defender Firewall with Advanced Security**

- Reviewed existing **inbound and outbound rules**

- Examined rules by profile (domain, private, and public)

- Created a new **inbound rule** for a selected program

- Temporarily **disabled and re-enabled** the firewall to observe system behavior

Reflection

Doing this on my own system gave me a more realistic feel for how firewall settings impact everyday activity and security. I was able to fully control the environment, document rule changes, and see how misconfigurations could potentially cause access issues. From a compliance and forensics standpoint, being comfortable inside the Windows Firewall interface is critical. It ties directly into log review, incident response, and endpoint hardening. I'm glad I took the initiative to bypass the virtual lab and complete this hands-on where it actually matters.

Lab 5 – Creating a Custom Firewall Rule in Windows Defender (Performed Locally)

Objective

This lab focused specifically on creating a custom inbound or outbound rule within Windows Defender Firewall. The goal was to understand how specific rule creation affects system behavior and to reinforce the ability to customize host-based protections.

Lab Outcome

The original lab environment was once again non-functional, so I completed this task directly on my own Windows system. I followed the general steps outlined in the lab instructions and successfully created and tested a custom firewall rule. No screenshots are included due to completing the lab on my personal machine.

Tasks Completed

- Opened **Windows Defender Firewall with Advanced Security**

- Selected **Inbound Rules** and created a new rule manually

- Chose **Program** as the rule type and browsed to select a local executable

- Specified action (Allow or Block), profile (Domain, Private, Public), and named the rule

- Applied the rule and confirmed it appeared in the list with the correct configuration

Reflection

This task reinforced how host-level firewall rules are created and what impact they have on network communication. Performing this on my real machine gave me clearer insight into how rules interact with running services. This is a core skill in endpoint security and directly relates to securing user systems, managing access, and troubleshooting issues in incident response or compliance audits. I'm glad I chose to bypass the broken lab environment and complete this with real-world context.

Lab 6 – Getting Started with the Linux Terminal (Reviewed via Lab Instructions)

Objective

This lab was designed to provide foundational experience using the Linux terminal. Tasks included navigating the file system, using shell commands, installing packages, and editing files with nano.

Lab Outcome

Due to continued issues with the cloud-based lab environment, I reviewed the lab instructions and logged them as personal study notes. I did not complete the lab interactively but studied the intended commands and procedures.

Topics Covered (Conceptual)

- Using pwd, cd, ls to navigate directories

- Creating files with touch and editing them using nano

- Installing and updating packages using apt-get

- Viewing system processes and using top or ps

Reflection

While I didn't execute the commands in a live shell during this course, I've seen these commands before and understand their structure and use. As I continue in cybersecurity, I plan to practice them in a real Linux environment, such as a VM or cloud-based sandbox. These are essential skills for incident response, scripting, and forensics work, and I'm confident I'll retain them better through repetition over time.

Lab 7 – Common Linux/Unix Commands (Reviewed, Lab Failed)

Objective

This lab was designed to reinforce common Linux/Unix commands used in system administration and cybersecurity tasks. Topics included directory navigation, file manipulation, permissions management, text processing, and basic networking commands.

Lab Outcome

Due to continued lab environment issues, particularly with the zip command hanging or freezing, I reviewed the instructions but did not complete the lab interactively. Multiple student discussions confirmed that this issue was widespread, not user error.

Topics Reviewed

- Directory Management: pwd, cd, ls, mkdir, rmdir

- File Management: touch, cp, mv, rm, zip, unzip

- Permissions: chmod, chown, ls -l

- Text Processing: cat, head, tail, grep, wc

- Networking: ping, ifconfig, netstat

Reflection

Even without hands-on access, I've seen most of these commands before in other coursework and personal practice. These are essential tools for Linux-based forensics, incident response, and administration. I plan to reinforce this knowledge using a local VM or cloud-based Linux terminal outside of the course's lab environment.

Lab 8 – Linux User Management (Reviewed, Lab Environment Skipped)

Lab 8 – Linux User Management (Reviewed via Instructions)

Objective

This lab was intended to teach basic user and group management in Linux using command-line tools. Tasks included adding and deleting users, managing groups, setting permissions, and verifying user account data.

Lab Outcome

No technical issues were documented in the discussion forums, but by this point in the course, the lab environment had proven so unreliable that I chose to review the instructions rather than attempt another lab likely to freeze or fail. This decision was based

on repeated technical setbacks in previous modules and a clear pattern of platform instability.

Topics Reviewed

- adduser, useradd, passwd

- usermod, deluser, groupadd, groupdel

- Viewing user info: whoami, id, groups, /etc/passwd

- Setting and viewing permissions and ownership with chmod, chown, and ls -l

Reflection

I've seen these commands across other courses and understand their purpose in managing user access, especially in multi-user environments. This material is foundational for incident response, permission auditing, and any work involving secure system administration. I plan to revisit these commands in a personal Linux sandbox or VM to practice them interactively.

Lab 9 – Updating Linux Systems (Reviewed, Lab Not Performed)

Objective

This lab focused on using command-line tools to perform system updates in Linux. Tasks included updating software repositories, upgrading packages, and reviewing logs for any issues related to updates or patches.

Lab Outcome

Following the pattern of earlier labs, this module was reviewed using the lab instructions only. Given the unreliability of the virtual environment throughout the course, I chose not to attempt this lab in a broken system. The instructions were reviewed thoroughly and the commands are familiar from previous coursework.

Topics Reviewed

- sudo apt update – refresh package lists

- sudo apt upgrade – apply package upgrades

- sudo apt dist-upgrade – perform a more comprehensive upgrade

- sudo apt autoremove – clean up unused dependencies

- Checking logs in /var/log/apt/ and using history to confirm actions

Reflection

Keeping systems updated is one of the simplest but most critical components of cybersecurity. I understand the purpose and risk behind outdated systems and will continue practicing these update tasks in my own Linux VM to reinforce familiarity. This lab further supported concepts I've learned in compliance and risk management regarding patch management policies and endpoint security protocols.

Lab 10 – Introduction to Containers, Docker, and IBM Cloud Container Registry (Reviewed, Not Performed)

Objective

This lab introduced core containerization concepts, including pulling container images from Docker Hub, running and managing containers using Docker CLI, and building custom container images using Dockerfiles. It also demonstrated how to push container images to IBM Cloud Container Registry.

Lab Outcome

Due to ongoing lab environment failures throughout this course, I reviewed the lab instructions but did not attempt this lab in the provided system. Tasks were read and noted conceptually. I plan to revisit these tools in a more stable environment (e.g., local VM with Docker installed or IBM Cloud CLI on my own system).

Topics Reviewed

- docker pull to download images from Docker Hub

- docker run to start containers from pulled images

- Creating a Dockerfile to build a custom image

- docker build to compile an image from a Dockerfile

- docker push to upload the image to IBM Cloud Container Registry

Reflection

While not a core focus of my intended path in compliance or GRC, understanding containerization is valuable in security architecture, cloud compliance reviews, and risk assessments involving DevOps pipelines. Knowing how container images are built, moved, and stored gives insight into how vulnerabilities (e.g., exposed secrets, misconfigured base images) can enter production environments. I plan to revisit Docker and container security concepts in a more focused container security course later on.

Final project overview

Cyber Secure Inc. recently hired you as a junior cybersecurity analyst. Other businesses contract Cyber Secure Inc. to handle their system administration and security.

Your supervisor assigned you six tickets; the first three require you to work with Windows OS, and the other three require you to work with Linux.

The project has two parts. For part 1, you will use the Rhyme lab environment in Coursera, which emulates a Windows Operating System. For part 2, you will use the Skills Network Cloud IDE environment, which provides access to a Linux terminal. If you can access either of these environments on your own computer, you may use your machine to complete the labs.

You will need to take one or more screenshots while completing the tasks to demonstrate your knowledge. Further directions are provided in the labs.

Part 1: Windows tickets

1. Add a new user to a new group

2. Update and run virus and threat protection

3. Configure firewall and network protection

Part 2: Linux tickets

4. Create a new user

5. Manage files and folders

6. Apply system updates

Lab: Final Project Part 1: Windows

Final project part 1: Windows tasks

Estimated time: 20 minutes

Overview

Cyber Secure Inc. recently hired you as a junior cybersecurity analyst. Other businesses contract Cyber Secure Inc. to handle their system administration and security.

Your supervisor assigned you six tickets; the first three require you to work with Windows OS, and the other three require you to work with Linux.

The project has two parts. For this part, you will use the **Rhyme** lab environment in Coursera, which emulates a Windows Operating System. You may use your own machine to complete these projects if you have access to these environments on your computer.

Windows tasks

1. Add a new user to a new group

2. Update and run virus and threat protection

3. Configure firewall and network protection

Learning objectives

After completing this project, you will have demonstrated your ability to

- Create a new user and a new group using Windows Server Manager

- Add a user to a group using Windows Server Manager

- Check for updates to virus and threat protection using a Windows operating system

- Run a "Quick Scan" to verify up-to-date virus and threat protection on a Windows operating system

- Create an inbound rule that controls connections on a TCP port using Windows Defender Firewall

Important notices about this lab

Lab instructions and solutions

If you type using your computer's keyboard in the **Rhyme** (Windows emulator) environment, you may not see any output in the lab environment. Instead, you may need to type using the on-Screen keyboard, which will display when you search in the bottom search bar.

Screenshots

Windows

You will need to take screenshots of each task as proof of your work to submit for peer review. To take a screenshot from a Windows computer, use the snipping tool by going to the start menu and opening the snipping tool. Select **New**, then click and drag over the area of the screen you want to screenshot. Save the file as a .png file or a .jpg file.

MacOS

To take a screenshot on MacOS, press shift, command, 4, then click and drag over the area of the screen you want to screenshot. The file will be saved to your desktop.

Upload

To upload the file, select upload file, browse, navigate to the file location, or drag the file icon onto the window.

Ticket 1: Create a new user

In this task, you will use Microsoft Windows Server Manager to create a new user and group and then add the user to the group.

1. Open Server Manager

2. Create a new user named after one of your favorite cartoon characters.

3. Set a secure password.

4. Take a screenshot that shows the newly created account.

5. Create a new group named *Accounting*.

6. Take a screenshot showing the newly created *Accounting* group.

Ticket 2: Check for virus and threat protection updates

In this task, you will use the Windows operating system to check for virus and threat protection updates and run a "Quick Scan".

1. Check for updates to virus and threat protection.

2. Take a screenshot that shows the date for the protection updates.

3. Run a Quick Scan using Windows Security.

4. Take a screenshot that shows the date you completed the scan.

Ticket 3: Configure firewall and network protection

Access **Windows Defender Firewall** with **Advanced Security** to create a new rule.

1. The new rule should have the following properties:
   a. A port rule that controls connections for a TCP port on port 80
   b. Allow the connection on Domain, Private, and Public
   c. Includes the rule name: "Port 80 Permitted"

2. Take a screenshot showing your newly created inbound rule.

Lab: Final Project Part 2: Linux Tasks

Cyber Secure Inc. recently hired you as a junior cybersecurity analyst. Other businesses contract Cyber Secure Inc. to handle their system administration and security.

Your supervisor assigned you six tickets; the first three require you to work with Windows OS, and the other three require you to work with Linux.

The project has two parts. You should have already completed part 1. For part 2, you will use the Skills Network Cloud IDE environment, providing access to a Linux terminal. You may use your machine to complete the labs if you can access Linux on your computer.

This lab uses IBM Skills Network Labs (SN Labs), which is a virtual lab environment used in this course. Upon clicking "Start Lab" your Username and Email will be passed to Skills Network Labs and will only be used for communicating important information to enhance your learning experience, in accordance with IBM Skills Network Privacy policy.

In case you need to download or print the lab instructions click HERE to open the lab instructions in a new tab.

Final Project Summary – Operating Systems and Security

Course Requirement: Six system administration tasks – three in Windows, three in Linux

Overview

The final project was designed as a hands-on capstone to demonstrate core system administration skills across both Windows and Linux environments. The tasks included user and group management, system updates, firewall configuration, and antivirus scanning — all fundamental skills for a junior cybersecurity analyst. The project was split into two parts:

- **Part 1:** Windows-based tasks using Coursera's Rhyme lab environment

- **Part 2:** Linux-based tasks using IBM's Skills Network Cloud IDE

Unfortunately, due to persistent failures in both lab environments, including system freezes, incomplete loading, broken interfaces, and poor platform support, I was unable to complete the project hands-on as intended.

Lab Status: Not Performed Due to System Limitations

Despite repeated attempts, neither environment functioned consistently or reliably. Discussions confirmed that many other students encountered the same issues, including:

- Rhyme (Windows emulator) not responding to input or freezing during launch

- On-screen keyboards required for even basic tasks

- Unusable Linux terminal sessions that timed out or returned errors before any commands could be executed

- Persistent update loops or incomplete loading for basic applications like LibreOffice and system tools

Because of these barriers, I was forced to **document and analyze the tasks conceptually** rather than execute them directly in the provided environments.

Task Summary & Conceptual Completion

Windows Tasks (Part 1)

1. **Create a new user and group in Windows Server Manager**
   Task: Add a new user (e.g., based on a cartoon character), create a group named "Accounting," and assign the user to the group.
   Status: Reviewed; unable to execute due to lab platform failure.
   Reflection: I understand how this task would be performed using Active Directory Users and Computers or Server Manager under Windows Server.

2. **Check for antivirus updates and run a Quick Scan**
   Task: Open Windows Security, check virus definitions, and run a Quick Scan.
   Status: Reviewed; not performed due to lab freeze.
   Reflection: This task aligns with basic endpoint security hygiene. I've done this before on personal systems and understand its role in security baselining.

3. **Create a custom inbound firewall rule**
   Task: Use Windows Defender Firewall to allow TCP traffic on port 80 across Domain, Private, and Public profiles.
   Status: Documented but not performed due to system non-responsiveness.
   Reflection: I've previously configured similar rules on my own machine and understand the GUI layout and logic for inbound/outbound rules.

Linux Tasks (Part 2)

4. **Create a new Linux user**
   Task: Use the adduser command and verify via /etc/passwd.

Status: Reviewed instructions only; terminal environment failed to load.

Reflection: I'm not fully comfortable with Linux yet, but I reviewed the command structure and its purpose. I understand that this is part of managing accounts in multi-user systems, and I plan to revisit it using a personal Linux environment when I'm more confident.

5. **Manage files and folders**
   Task: Use mkdir, touch, cp, mv, and rm for file and directory operations.
   Status: Reviewed; not performed in Skills Network IDE due to repeated timeout errors.
   Reflection: These commands were new to me, but the instructions helped me understand what they do. I followed along and took notes, and I intend to practice these basic tasks once I set up a safe Linux practice space (like a VM or cloud sandbox).

6. **Apply system updates**
   Task: Use apt update, apt upgrade, and apt autoremove to update a Debian-based system.
   Status: Reviewed conceptually. Lab platform did not allow execution.
   Reflection: I haven't run system updates on Linux before, but I know from this assignment that these commands are important for maintaining a secure environment. I plan to get more comfortable with Linux over time so I can understand these tasks on a deeper level.

Final Reflection

While I was unable to complete the final project in the intended lab environments, I took time to carefully review and document each task, its purpose, and the standard methods for execution. I also verified that many students experienced the same environment failures and that the limitations were systemic, not user-related.

I'm disappointed that I couldn't demonstrate these tasks interactively, but I did extract the learning objectives and plan to replicate these tasks on a stable platform (e.g., my own VM, or using WSL). I understand how each task ties directly into real-world cybersecurity and system administration, especially from a GRC and endpoint hardening perspective.

This experience only reinforces the importance of **accessible, functional lab platforms**, especially for learners without access to expensive virtual infrastructure. In spite of the setbacks, I completed the course objectives in the most effective and honest way possible given the tools provided.