Rapid Ascent Assignments

Rubric

	4	3	2	1
Meets Task Requirements	All	Most	Some	Very Few or None
Frequency	Always	Usually	Some of the Time	Rarely or None
Accuracy	No Errors	Few Errors	Some Errors	Frequent Errors
Comprehensibility	Always Comprehensible	Almost Always Comprehensible	Gist and Main Ideas Comprehensible	Isolated Bits are Comprehensible
Content Coverage	Fully Developed	Adequately Developed	Partially Developed	Minimally Developed
Cybersecurity Vocabulary	Broad and Varied	Adequate and Varied	Limited / Lacks Variety	Basic / Highly Repetitive

Assignment #1 – Windows Concepts

Tasks

- Explain the Windows Firewall and Advanced Security.

Purpose

- **Clarify** – Understand the functionalities and importance of Windows Firewall with Advanced Security.
- **Summarize** – Be able to describe how to configure firewall rules and monitor network traffic for security purposes.

Assignment

- **In a text box**
  - o Describe the role of Windows Firewall with Advanced Security in protecting Windows Server environments. Explain how to create inbound and outbound rules, and the significance of configuring security settings tailored to different network profiles.
- **Screenshots**
  - o Provide screenshots showing the interface for Windows Firewall with Advanced Security, steps to create and modify firewall rules, and how to view current network connections and security settings.

Assignment #2 – Windows Concepts

Tasks

- Explain how to configure a proxy server in Windows Server networking.

Purpose

- **Clarify** – Understand the steps involved in setting up a proxy server networking configuration on a Windows Server system.
- **Summarize** – Be able to describe the configuration process, including the necessary settings and considerations for effective proxy deployment.

Assignment

- **In a text box**

- o Describe the process of configuring a proxy server in Windows Server, including the roles and features that need to be installed and the configurations that must be set within the server environment. Discuss the purpose of using a proxy, such as enhancing security, managing internet access, or caching content to improve network efficiency.
- **Screenshots**
  - o Provide screenshots showing the installation of the necessary roles and features, the setup of the proxy settings, and any relevant configurations within the Windows Server Management Console.

Assignment #3 – Web Browser Configuration – Split Proxy

Tasks

- Explain how to configure split proxying in the Firefox browser.

Purpose

- **Clarify** – Understand the concept of split proxying and how it can be set up in the Firefox browser.
- **Summarize** – Be able to describe the steps to configure split proxying, highlighting the scenarios where it might be particularly useful.

Assignment

- **In a text box**
  - o Describe what split proxying involves and why it might be used, such as directing some traffic directly to the internet while routing other traffic through a proxy server based on URL patterns or other criteria. Explain how to configure these settings in the Firefox browser, including accessing the necessary menus and entering the correct configurations.
- **Screenshots**
  - o Provide screenshots that show navigating the Firefox settings to configure proxy settings, including detailed steps to set up different proxy rules for different types of traffic.

Assignment #4 – Network Security Concepts

Tasks

- What is the purpose of VPNs (Virtual Private Networks)?

Purpose

- **Clarify** – Understand the fundamental purposes of VPNs in a network security context.
- **Summarize** – Be able to explain the benefits and typical uses of VPNs, including how they enhance security and privacy.

Assignment

- **In a text box**
  - Describe the primary purposes of using a Virtual Private Network (VPN), such as securing internet connections, encrypting data transfers, and masking user identity and location. Explain how VPNs provide these benefits by creating a secure and private tunnel for data exchange over public networks.
- **Screenshots**
  - Include diagrams or illustrations that visually explain the concept of a VPN tunnel and how it protects data privacy and security.

Assignment #5 – Network Configuration Techniques

Tasks

- Explain how to create a SOCKS5 proxy via the CLI in the Windows Command Prompt to a Linux server.

Purpose

- **Clarify** – Understand the process of setting up a SOCKS5 proxy server using command line tools.
- **Summarize** – Be able to describe each step involved in configuring a SOCKS5 proxy connection from a Windows machine to a Linux server.

Assignment

- **In a text box**
  - Describe the steps required to establish a SOCKS5 proxy from a Windows machine to a Linux server using command-line tools, including the installation of necessary software, configuration of the proxy settings, and verification of the

proxy operation. Explain why someone might use a SOCKS5 proxy and the advantages it offers over other types of proxies.
- **Screenshots**
  - o Provide screenshots or command line output examples showing the commands used at each step, such as setting up SSH on the Windows machine, configuring the SOCKS5 proxy via SSH, and testing the connection.

Assignment #6 – Home Network Management

Tasks

- Explain the process of port forwarding in a home router.

Purpose

- **Clarify** – Understand what port forwarding is and why it is used in home networking.
- **Summarize** – Be able to describe the steps involved in setting up port forwarding on a home router, including the reasons for using it.

Assignment

- **In a text box**
  - o Describe port forwarding, its purpose, and how it works within the context of home networking. Explain how to configure port forwarding on a home router to allow external devices to access services running on devices within your home network, such as private game servers, web servers, or remote desktop applications.
- **Screenshots**
  - o Provide screenshots that guide through the router's web interface, showing how to access the port forwarding section, enter the necessary port numbers, and specify the internal IP addresses to which traffic should be directed.