Lab Report – Using Windows PowerShell

Objective

The purpose of this lab was to explore the functions of PowerShell for task automation, configuration management, and system administration.

Tasks Performed

Part 1: Accessing PowerShell Console

Opened and worked with the Windows PowerShell console. Compared PowerShell with the Command Prompt.

Part 2: Exploring Commands

Used basic commands like dir, ping, cd, and ipconfig. Observed differences in output between Command Prompt and PowerShell.

Part 3: Exploring Cmdlets

Learned that PowerShell uses cmdlets in the format Verb-Noun. Identified dir as an alias for the cmdlet Get-ChildItem.

Part 4: Exploring Netstat Command

Executed netstat -h and netstat -r to view routing tables and active connections. Retrieved the IPv4 gateway information. Mapped PIDs from netstat -abno with processes in Task Manager to analyze system activity.

Part 5: Managing Recycle Bin

Used the Clear-RecycleBin command to permanently delete files. Learned how automation can simplify network-wide tasks like cleanup and security enforcement.

Reflection (Security Analyst Perspective)

As part of this lab, I researched useful PowerShell commands that would simplify tasks for a security analyst:
• Get-Process – Detects unusual or malicious processes.
• Get-Service – Monitors unauthorized or suspicious services.
• Get-EventLog -LogName Security -Newest 50 – Reviews recent login and security events.
• Get-LocalUser – Identifies unauthorized local accounts.
• Test-NetConnection – Troubleshoots connectivity and potential attacks.
• Get-FileHash – Ensures file integrity and detects tampering.
• Set-ExecutionPolicy RemoteSigned – Improves script execution security.

Key Learning

This lab enhanced my skills in system monitoring, task automation, and security analysis using PowerShell. I gained hands-on experience with cmdlets, network analysis, and process investigation.

Resume-ready Achievement Example:

“Completed lab on Windows PowerShell, gaining hands-on experience with cmdlets, system monitoring, process investigation, and automation for security tasks. Applied commands such as Get-Process, Get-EventLog, and Clear-RecycleBin to enhance system administration and security analysis.”