**Group Work C1W2: Network Security Log Analysis**

**Total Points:** 100

**Assignment Overview**

**Scenario:** You are a network security analyst who has just received suspicious log files from your organization's network infrastructure. Multiple security incidents may have occurred over the past week, and you need to analyze the logs to identify threats, document findings, and provide recommendations.

**Your Mission:** Use Linux command-line tools to analyze network logs, identify security incidents, and create a comprehensive security report.

**Skills Focus:** grep, awk, sed, sort, uniq, wc, file operations, text processing, cross-referencing data

**Provided Files**

Download the security-logs.zip file from Canvas and extract it to your DEVASC VM. You may place these files in /home/devasc/security-logs/:

1. **firewall.log** - Firewall connection attempts and blocks
2. **ssh-auth.log** - SSH authentication attempts
3. **network-scan.log** - Network scanning detection logs

**Setup Instructions:**

# In your Ubuntu VM:

Browse to folder of choice

unzip security-logs.zip

ls -la security-logs/

**Investigation Tasks**

**Task 1: Brute Force Attack Detection (30 points)**

**Objective:** Find evidence of SSH brute force attacks

**Requirements:**

* Identify IP addresses with more than 20 failed SSH login attempts
* Find the top 5 most aggressive attackers by failed login count
* Determine the time period of the most intense attack activity
* Create a summary report showing attacker IPs and attempt counts

**Commands you'll need (suggestions):** grep, awk, sort, uniq -c, head

**Deliverable:** Screenshot of commands and a text summary in a section named 1. Brute-force-report in your final response document.

**Task 2: Port Scanning Analysis (30 points)**

**Objective:** Identify port scanning activities and their targets

**Requirements:**

* Find IP addresses that scanned more than 40 different ports
* Identify which internal servers were most heavily scanned
* List the most commonly targeted ports

**Commands you'll need:** grep, awk, sort, uniq, wc -l

**Deliverable:** Screenshot of commands and a text summary in a section named 2. Port-scan-analysis in your final response document.

**Task 3: Correlation Analysis (40 points)**

**Objective:** Connect incidents across multiple log sources

**Requirements:**

* Find IP addresses that appear in multiple log files (cross-reference attackers)
* Create a timeline of coordinated attack activities

**Commands you'll need:** grep -f, comm, join, sort, file redirection, awk

**Deliverable:** Screenshot of commands and a text summary in a section named 3. Correlation-report

**Grading Rubric**

| **Task** | **Excellent (90-100%)** | **Good (80-89%)** | **Satisfactory (70-79%)** | **Needs Work (<70%)** |
| --- | --- | --- | --- | --- |
| **Command Usage** | Uses advanced command combinations efficiently | Uses appropriate commands correctly | Uses basic commands with some errors | Commands don't work or are inappropriate |
| **Analysis Accuracy** | Finds all security incidents correctly | Finds most incidents with minor errors | Finds some incidents but misses key ones | Analysis is largely incorrect |
| **Documentation** | Clear, professional reports with insights | Good reports with adequate detail | Basic reports meeting requirements | Poor or incomplete documentation |

**Point Distribution:**

* Task 1: 30 points
* Task 2: 30 points
* Task 3: 40 points
* **Total: 100 points**

**Submission Requirements**

**What to Submit:**

1. One word file containing three sections: 1. brute-force-report, 2. port-scan-analysis, 3. correlation-report
2. Screenshots showing command execution and textual interpretation for each task

**Submission Method:**

1. Create a single word file containing all your work
2. Submit the file through Canvas

**Getting Help**

**Common Linux Commands Reference:**

* grep -i "pattern" file - Case-insensitive search
* awk '{print $1}' file - Print first field
* sort file | uniq -c - Count unique occurrences
* wc -l file - Count lines in file
* head -n 10 file - Show first 10 lines
* comm file1 file2 - Compare sorted files

**Tips:**

* Start with simple grep commands to understand log formats
* Use head and tail to examine files before full analysis
* Test commands on small file sections first
* Save intermediate results to files for correlation analysis

**Success Criteria**

By completing this assignment, you will demonstrate:

**Linux Command Proficiency:** Effective use of text processing tools for data analysis

**Security Analysis Skills:** Ability to identify and correlate network security incidents

**Problem-Solving Approach:** Systematic investigation of complex log data

**Professional Documentation:** Clear, organized reporting of technical findings

**Network Operations Understanding:** Practical experience with real network security scenarios

**Technical Requirements**

* Work must be completed in the Linux terminal
* Screenshots must be clear and show clear command execution