**CIS195 – Net Lab 13 – Secure Network Administration Principles Log Analysis**

**Lab Worksheet**

**Name: Marco Zuniga**

**Date:**

1. **Define grep and gawk commands and how they can be used for log analysis.**

**Grep and gawk are powerful command-line tools used for text processing and pattern matching in Unix-like operating systems. They are commonly used for log analysis tasks. Let me explain each of them in more detail:**

**grep:**

**The grep command (which stands for "global regular expression print") is primarily used to search for specific patterns or regular expressions within files or streams of text.**

**It scans input line by line and prints any lines that match the specified pattern.**

**It supports various options and flags to modify its behavior, such as case-insensitive searches (-i), printing line numbers (-n), displaying surrounding lines (-A, -B, -C), and more.**

**For log analysis, grep is often used to filter log files based on specific criteria, extract relevant information, or find occurrences of certain events or error messages.**

**gawk (GNU Awk):**

**Gawk is an enhanced version of the Awk programming language, primarily used for text processing and data extraction.**

**It operates on a line-by-line basis, splitting input lines into fields based on a specified delimiter (by default, whitespace), and allows you to perform operations on those fields.**

**It provides a rich set of built-in functions, variables, and control structures, making it a powerful tool for log analysis and data manipulation tasks.**

**With gawk, you can filter and transform log data, perform calculations, aggregate statistics, and generate custom reports.**

**gawk scripts can be written in separate files or executed directly from the command line using the -f option.**

**It supports regular expressions, making it convenient for matching patterns and extracting specific information from log files.**

**In log analysis workflows, grep is commonly used for initial filtering and identification of relevant log entries, while gawk is often employed for more complex data extraction, transformation, and analysis tasks.**

1. **When using the ‘cut’ command, what is the significance of adding the -d option?**

**The -d option in the cut command is used to specify the delimiter character that separates the fields in the input.**

**Field Delimiter:**

**By default, cut treats the tab character (\t) as the delimiter.**

**With the -d option, you can specify a different delimiter character that separates the fields in the input.**

**The delimiter can be a single character, such as a space or a comma, or even a multi-character string.**

**Separating Fields:**

**The -d option allows cut to recognize and split the input lines into fields based on the specified delimiter.**

**Each field is treated as a separate column, and you can select and extract specific columns using other options like -f.**

1. **Define some use cases of the curl command:**

**The curl command is a versatile tool used to interact with various network protocols and transfer data to or from a URL. It supports a wide range of functionalities and can be used for several use cases. Here are some common use cases of the curl command:**

**Downloading Files:**

**curl can be used to download files from a remote server or website. It supports various protocols like HTTP, FTP, SFTP, and more.**

**You can specify the URL of the file you want to download, and curl will retrieve and save it to your local machine.**

**Uploading Files:**

**curl allows you to upload files to a remote server using protocols like FTP, SFTP, or HTTP(S).**

**You can use the -T option to specify the local file to be uploaded and the destination URL.**

**Making HTTP Requests:**

**curl can send HTTP requests to web servers and retrieve the responses.**

**You can specify different HTTP methods like GET, POST, PUT, DELETE, etc., and include request headers or data.**

**This can be useful for testing APIs, debugging web applications, or automating tasks that involve interacting with web servers.**

1. **On a Linux machine, which location and file stores all SSH login attempts?**

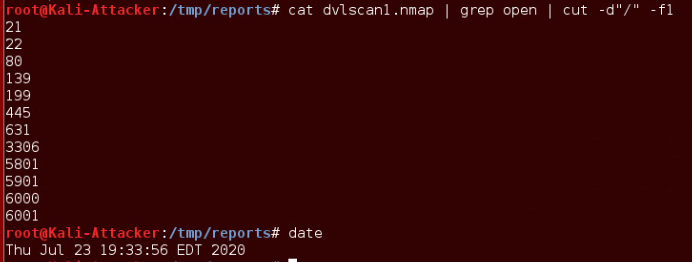
**On a Linux machine, the SSH login attempts are typically logged and stored in the /var/log/auth.log file. This file contains system authentication-related logs, including SSH login attempts, successful logins, authentication failures, and other related events.**

**You can view the content of the auth.log file using various commands, such as cat, less, or tail.**

1. **Describe the Hydra tool. What type of password cracking do we utilize in this lab?**

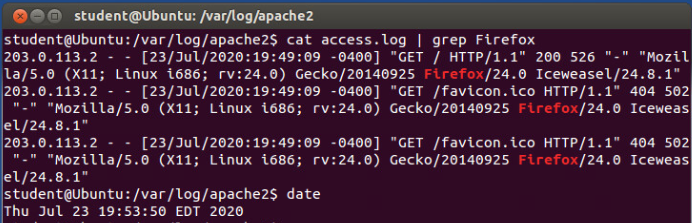
**Hydra is a powerful and popular password cracking tool used for performing brute-force and dictionary-based attacks on various network services and protocols. It is designed to automate the process of guessing passwords by trying different combinations until the correct one is found.**

On page 10, import the snapshot equivalent to Figure 7 followed by the **date** command. See the example below:



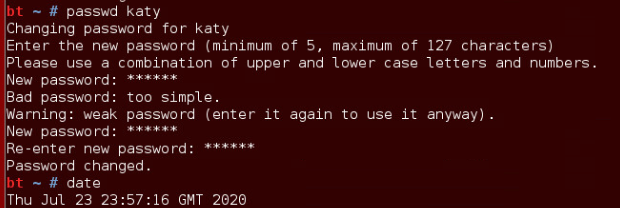
1. **Import your snapshot (similar to example above) here:**

On page 18, import the snapshot equivalent to Figure 7 followed by the **date** command. See the example below:



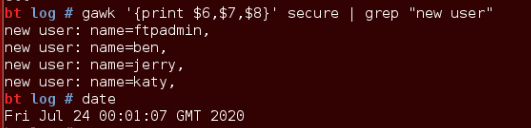
1. **Import your snapshot (similar to example above) here:**

On page 20, import the snapshot equivalent to Figure 7 followed by the **date** command. See the example below:



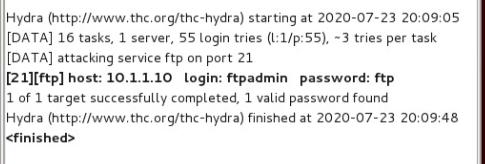
1. **Import your snapshot (similar to example above) here:**

On page 21, import the snapshot equivalent to Figure 4 followed by the **date** command. See the example below:



1. **Import your snapshot (similar to example above) here:**

On page 26, import the snapshot equivalent to Figure 13. See the example below:



1. **Import your snapshot (similar to example above) here:**
2. **Summarize this lab by including the following keywords (purpose of this lab, log analysis, DVL machine, HTTP and FTP servers, dvlscan1.xml, dvlscan1.gnmap, grep-able, parse output, grep, cut, livehosts.txt, dvlscan1.nmap, livehostscan.txt, scanreport.sh script, second part of lab, curl command, find an email address, intense Nmap scan, /var/log/apache2, access.log, (example: cat access.log | Firefox), third part of lab, Kali, ssh 10.1.1.10, groupadd anongroup, useradd ben -g anongroup, passwd pen, /var/log, secure, gawk, fourth part of lab, Hydra, dictionary attack, GUI, set target, protocol, ftpadmin, /tmp/wordlists/passlist, successfully cracked, DVL server, /var/log, tail -50 proftpd.log, grep for “Incorrect”):**