|  |
| --- |
|  |
| Capstone Experience IST 894  Carl Laneave |
| Lab 12 Report |

Table of Contents

[1.0 Introduction – CySA+ Infrastructure Management 3](#_Toc152536431)

[1.1 Lab Results – CySA+ Infrastructure Management 4](#_Toc152536432)

[2.0 Introduction – CySA+ Log, SIEM, and Email Analysis 11](#_Toc152536433)

[2.1 Lab Results – CySA+ Log, SIEM, and Email Analysis 12](#_Toc152536434)

[3.0 References: 18](#_Toc152536435)

[4.0 Activity Log 19](#_Toc152536436)

# Introduction – CySA+ Infrastructure Management

In this lab, we evaluate the usage of capturing logs of a potential attacker through the usage of a honey pot. Attacker and attacker patterns can be tracked into logs using a fake website, server, etc. known as a honey pot. These honey pots are separate and isolated away from an actual server and allow blue team and security teams to watch and analyze potential attacker methods.

Once these logs are captured, they will need to be stored in a way that protects them from being removed, read, or stolen. This is done through the usage of encryption. In the first method, the files are encrypted using an SHA1 key, that once completed, is stored in the application KeePass. KeePass is a local password manager client that can be used to store important information, including hash and encryption keys, to prevent attackers from accessing our log files.

The last method of protection was through the usage of a hash key. Hash keys are another way to encrypt log files and prevent them from being intercepted or read by potential attackers. Any security engineer or blue team member must understand how to protect, transport, and work with logs.

# Lab Results – CySA+ Infrastructure Management

A computer screen shot of a program

Description automatically generated

Figure 1.0 – Scan the range to see output from running system.

A computer screen with a black background

Description automatically generated

Figure 1.1 – Attempt to connect to the honeypot through FTP.

A screenshot of a computer

Description automatically generatedFigure 1.2 – Attempt to connect to port 80 of the honey pot to see if exploitable.

A computer screen shot of a computer screen

Description automatically generated

Figure 1.3 – View the logs on the honey pot of the attackers attempted actions.

A computer screen shot of a computer program

Description automatically generated

Figure 1.4 – Tee out the logs to watch the traffic as it does a while loop through attackers actions on the honeypot.

A computer screen with white text

Description automatically generated

Figure 1.5 – Zip up the log file and securely send them to through SCP.

A computer screen with white text

Description automatically generated

Figure 1.6 – Encryption on the backup logs from the honey pot are created.

A screen shot of a computer

Description automatically generated

Figure 1.7 – Run Keepass password authentication system and password manager.

A screenshot of a computer program

Description automatically generated

Figure 1.8 – Add the encryption key and information into KeePass.

A black screen with white text

Description automatically generated

Figure 1.9 – Hash the log file using SHA1 algorithm.

A computer screen with white text and yellow text

Description automatically generated

Figure 1.10 – Update with the hash key, delete to end the lab.

A black screen with white text and a check mark

Description automatically generated

Figure 1.11 – Lab is complete.

# 2.0 Introduction – CySA+ Log, SIEM, and Email Analysis

In this lab, we evaluate different tools for logging and log analysis. The first evaluation starts by capturing log information and feeding it into Splunk. Splunk is one of the most popular SIEM tools currently available to security engineers. It allows security professionals to feed large amounts of log data and easily parse it through Splunk querying language to identify and capture important information. This information can include attacker information, patterns of potential threats, vulnerability assessments, and even potential future attack patterns.

Secondly, the lab evaluates how to review and analyze potential threats in email. In this case, we reviewed first the headers of a sender to validate if the sender was legit from the host, it was saying it was coming from. Then, we looked at potential threatening files through the usage of binwalk.

Binwalk is a client tool that allows to review of different types of files to determine if they are actual file extensions as listed or executables hiding as non-threatening. It is critical to understand the different methods of potential attacks, especially in email phishing, as it is one of the most popular types of attacks in business today.

# 2.1 Lab Results – CySA+ Log, SIEM, and Email Analysis

A screenshot of a computer

Description automatically generated

Figure 2.0 – Run an output of our syslog, remove the cron job that is running a backdoor shell file.

A screenshot of a computer

Description automatically generated

Figure 2.1 – Log into splunk enterprise.

A screenshot of a computer

Description automatically generated

Figure 2.2 – Once in splunk, run a query against our access log file to see the useragent in order of count.

A screenshot of a computer

Description automatically generated

Figure 2.3 – Search by client Ip and sort by count in Splunk.

A screenshot of a computer

Description automatically generated

Figure 2.4 – Search by useragent WPScan and client IP.

A screenshot of a computer

Description automatically generated

Figure 2.5 – Download the suspicious phishing email and rename it to a readable file.

A screenshot of a computer screen

Description automatically generated

Figure 2.6 – Download the file and examine it with binwalk. It shows that the file is not a png but an actual executable.

A white circle with a check mark in it

Description automatically generated

Figure 2.7 – Lab is now complete.

# 3.0 References:

[1] *KeePass*. (2022, July 13). Wikipedia. <https://en.wikipedia.org/wiki/KeePass>

‌[2] *What is splunk? key benefits and features of Splunk.* Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/what-is-splunk

[3] *What is Splunk & What does it do? an introduction to splunk*. Splunk. (2022, November 18). https://www.splunk.com/en\_us/blog/learn/what-splunk-does.html

[4] *Binwalk: Kali linux tools*. Kali Linux. (2023, March 8). https://www.kali.org/tools/binwalk/

‌

‌

‌

‌

# 4.0 Activity Log

| **Member Name** | **Task Date** | **Task Details** |
| --- | --- | --- |
| Carl Laneave | 12/2/2023 | Created Template, executed all labs, took screenshots, and completed report |
|  |  |  |
|  |  |  |