IS-4543: Cyber Attack and Defend

Project Milestone Report for Milestone 4

Name: Delton Robinson

Section: IS-4543-001

Date: 11/19/2024

Milestone Report

This report includes the approved project proposal (included for easy reference), a summary of what was done during this project milestone, a description of what I learned during this milestone, and documentation of the work completed during this milestone.

Project Proposal

Project Idea 3: Honeypot Deployment for Network Intrusion Detection

Description: This project focuses on setting up an internal honeypot within a virtualized environment to lure and log simulated internal attack attempts. Using tools like Cowrie, an SSH honeypot, I will create a fake, "enticing" system for simulated internal attacks. The goal is to analyze common attack vectors in a controlled environment, without exposing the honeypot to external networks.

Milestones:

1. **Virtualized Environment Setup**
    - I'll begin by setting up a completely isolated virtual environment using VMware. This environment will contain multiple virtual machines, including the honeypot (potentially running Cowrie on a Linux VM) and at least one attacker machine (Kali Linux). The network will be fully internal, ensuring no exposure to external traffic, and configured to simulate a typical corporate or home network.
2. **Honeypot Configuration**
    - I'll install and configure a honeypot on a Linux VM, setting it up as an SSH honeypot. The system will be designed to look like a valuable internal server, with fake services, decoy files, and user accounts to entice attackers. I'll configure the system to log all actions in detail, including commands typed and files accessed.
3. **Simulated Attack Scenarios**
    - Using the attacker VM (Kali Linux), I'll simulate multiple types of attacks typically seen in an internal network scenario. This will include brute-force SSH login attempts, privilege escalation attempts, and file exploration. Each attack will be executed in a controlled manner, allowing the honeypot to capture detailed logs of the process.
4. **Analyzing Logs and Attack Patterns**
    - After completing the attack simulations, I'll dive into analyzing the logs captured by Cowrie. I'll look for patterns that could indicate specific attacker behavior, such as

common commands used after gaining access or file manipulation strategies. I'll use these insights to build a report on the attack patterns observed.

5. **Reporting and Future Implementations**
    - Finally, I'll create a detailed report summarizing the findings from the honeypot logs, describing the effectiveness of the honeypot in detecting and logging internal attacks. I'll also propose potential enhancements for internal network security, such as improved monitoring or stricter access control policies to mitigate the risks demonstrated during the simulation.

Summary of Activities

In this milestone, I analyzed logs generated from the Cowrie SSH honeypot and the vsftpd FTP service during previous brute-force attack simulations. Using tools like grep, I filtered and examined key events such as failed login attempts, successful logins, and commands executed by attackers. For Cowrie, I identified multiple failed login attempts with weak credentials like 123456 and password, as well as successful logins using **user:root** with **password:123456789**. After gaining access, the "attacker" executed several commands, including ls to list directory contents, cd to navigate directories, and attempted unusual inputs such as **“;s”** and **“c;ear”.** These commands revealed typical attacker reconnaissance behavior and missteps (in reality I was just inputting commands too quickly and typo’d).

For the vsftpd FTP service, I reviewed logs showing numerous failed login attempts for the user ftpuser, followed by a successful login. After gaining access, the "attacker" downloaded sensitive files such as **passwords.txt** and **ssn.txt**, demonstrating the potential impact of weak password security. Through this process, I observed clear patterns of brute-force attack behavior and the corresponding log entries generated by each service.

I was able to identify that the attacker downloaded sensitive data from an unsecured directory after the brute force attack, and I can report this information to the appropriate team in order to secure and recover any data loss from the attack.

Description of Learning Completed

Throughout this milestone, I deepened my understanding of log analysis for detecting and analyzing attacker behavior. By reviewing Cowrie logs, I learned how detailed event logging captures every interaction, from failed login attempts to commands executed during a session. For example, Cowrie logged both unsuccessful brute-force attempts and the specific commands entered after successful logins, such as directory listing (**ls**) and would have logged user identification (**whoami)** (if I ran the command within the attack scenario). I better learned how to proficiently use grep in order to search for specific logs within the larger log file, and I practiced matching timestamps in order to verify the timing of the attacks to distinguish one burst of brute force attempts from another. These logs provided insight into the typical reconnaissance phase of an attack, as well as the (extremely simplified) response on behalf of a cybersecurity analyst after a breach.

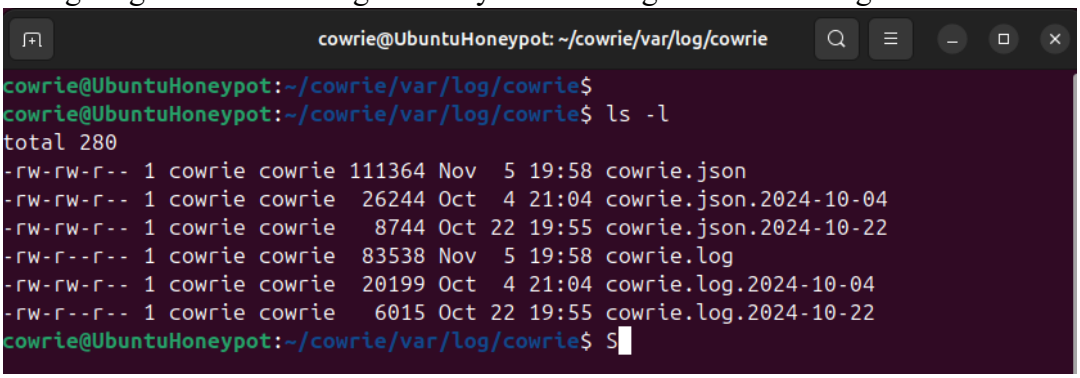
The vsftpd logs emphasized the danger of successful brute-force attacks on FTP services. By analyzing failed and successful login attempts, I recognized patterns in brute-force behavior, including repeated attempts with common weak passwords. Additionally, I observed how logs recorded file downloads, highlighting the risk of data theft when services are not properly secured. The **ssn.txt and passwords.txt** files were stolen by the fictional attacker, and if this were a real data breach, an extreme level of negligence would’ve allowed this to occur.

This milestone enhanced my ability to analyze service logs, identify attack patterns, and understand the importance of securing exposed services with strong passwords and proper configurations. The experience also reinforced the value of honeypots like Cowrie for studying attacker behavior in a controlled environment.

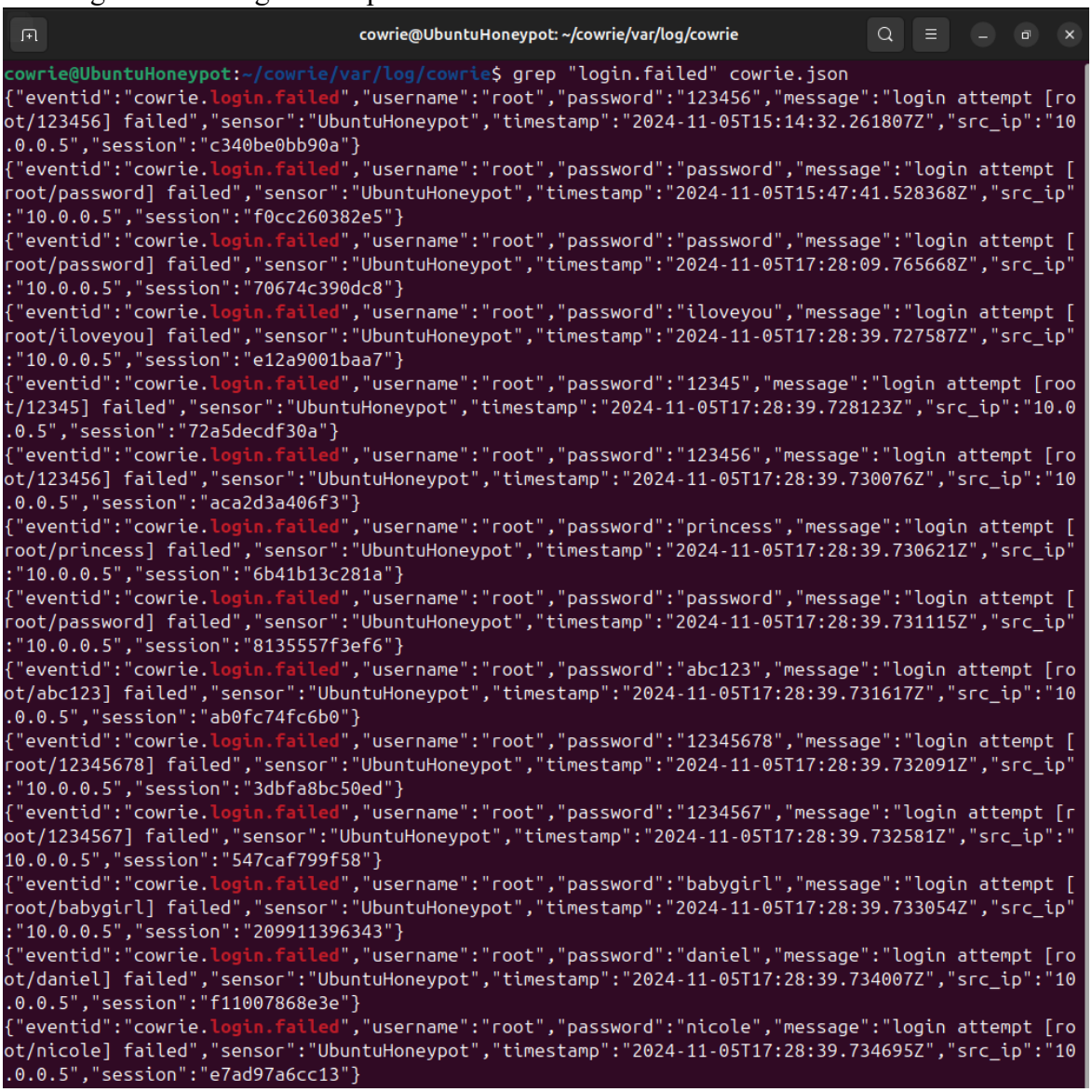
Documentation of Work Completed

1. Cowrie Log Analysis

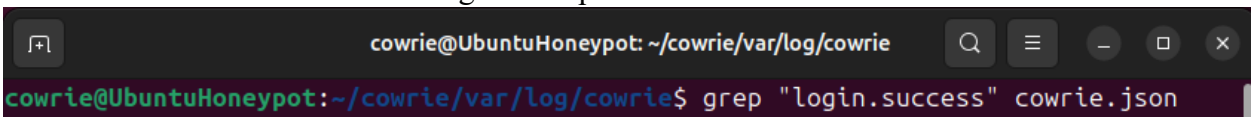
a. Navigating to the cowrie log directory and viewing the different logs



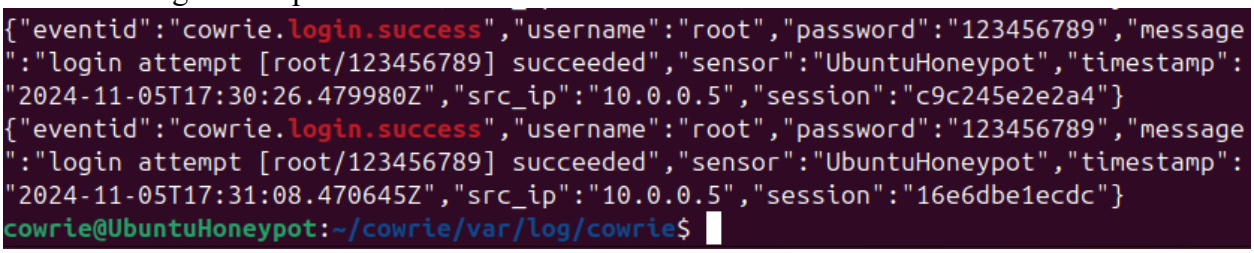
b. Viewing the failed login attempts on the cowrie machine.



c. Command to view the successful login attempts

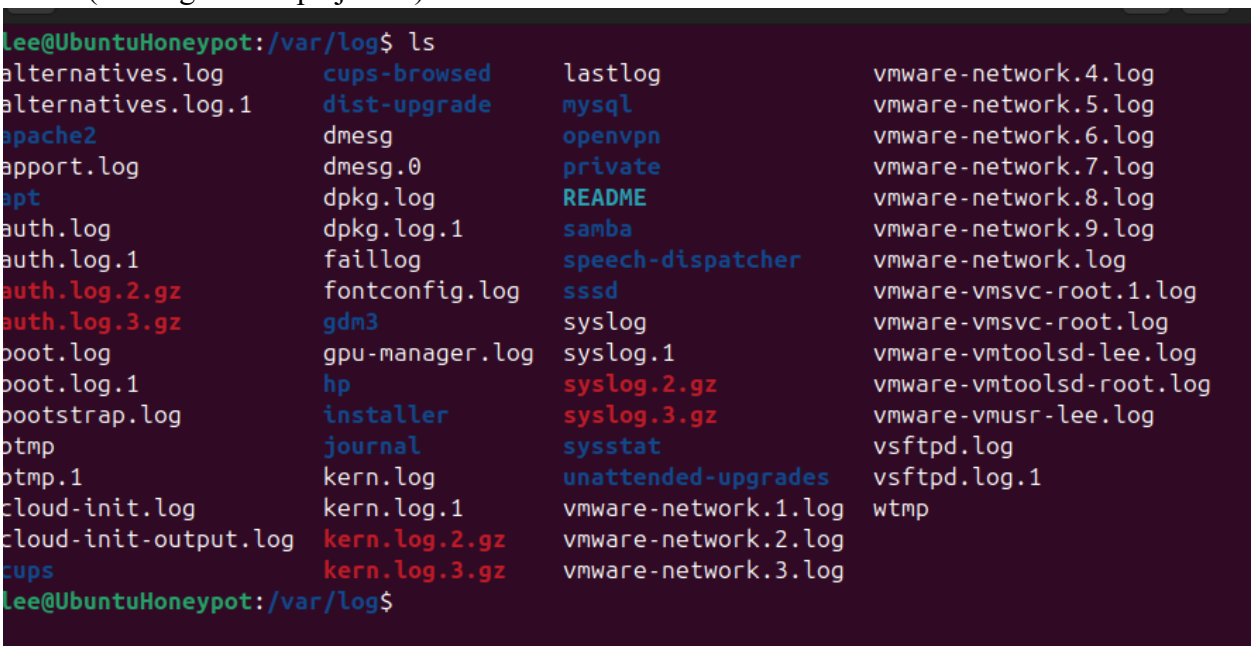


d. Successful login attempts

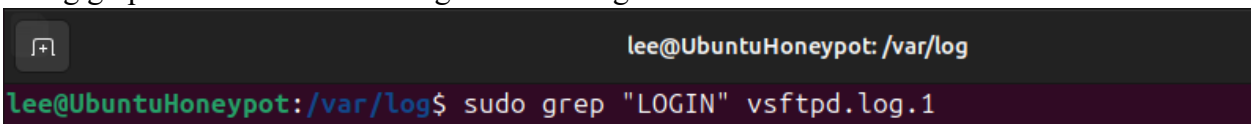


2. VSFTP Log Analysis

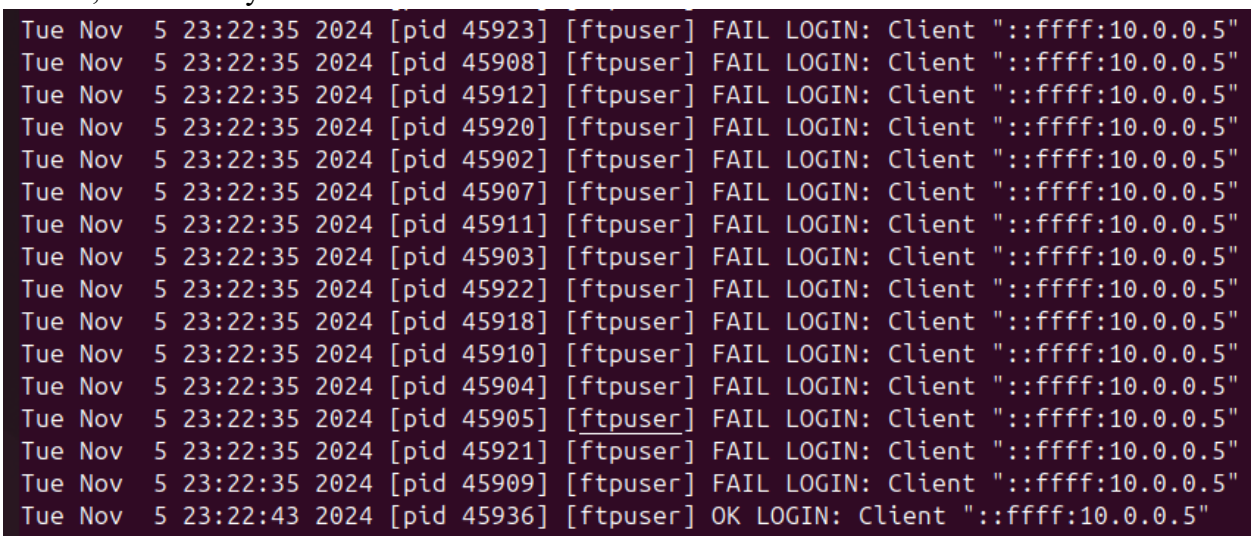
a. After navigating to /var/log, running the ls command to view the files within the log folder (looking for vsftpd.json.1)



b. Using grep to view the LOGIN logs from the log file



c. A successful brute force attack within the logs. Multiple failed logins within the same minute, followed by a successful one.



d. The vsftpd.json.1 log file displaying that the attacker downloaded **passwords.txt** and **ssn.txt** from */home/ftpuser/important_files*