

IS-4543: Cyber Attack and Defend

Project Milestone Report for Milestone 5

Name: Delton Robinson

Section: IS-4543-001

Date: 12/3/2024

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

During this milestone, I prepared a comprehensive report analyzing the findings from previous honeypot log analyses. The report focused on evaluating the effectiveness of the Cowrie SSH honeypot and the vsftpd FTP service in capturing and logging attack patterns during simulated internal attack scenarios. It included details such as failed and successful login attempts, commands executed post-login, and file exfiltration activities. Additionally, I outlined recommendations for improving internal network security, including stronger password policies, centralized log monitoring, and enhanced service configurations. This report synthesized the observed vulnerabilities and provided actionable steps to mitigate the risks demonstrated during the simulations.

Description of Learning Completed

Honeypot Effectiveness: The Cowrie SSH honeypot effectively simulated a real-world attack environment while ensuring no system compromise. Its logs captured failed brute-force attempts, successful logins, and post-login commands, providing insights into attacker behavior. The vsftpd FTP service logs revealed vulnerabilities from weak credentials, such as successful brute-force attacks and file downloads. Together, these tools offered a thorough analysis of attacker activity and exposed critical security risks in internal services.

Reporting Skills: Writing the report strengthened my ability to analyze technical data and present it in a clear, professional format. Translating log details into actionable recommendations improved my skills in communicating findings to both technical and non-technical audiences. This experience reinforced my ability to propose practical solutions, such as password policies, centralized monitoring, and service hardening, to address observed vulnerabilities.

Critical Analysis and Documentation: Analyzing and documenting the honeypot logs improved my ability to identify patterns in attacker behavior, such as brute-force attempts and data exfiltration. Summarizing these observations honed my attention to detail and emphasized the importance of clear, actionable reporting in driving security improvements within an organization.

Documentation of Work Completed for Milestone 5

➤ Introduction

This report focuses on analyzing the logs generated by the **Cowrie** SSH honeypot and the **vsftpd** FTP service during simulated internal attack scenarios.

The analysis identified common attacker behaviors, such as:

- Brute-Force login attempts
- System Reconnaissance
- Data Exfiltration.

Weak credentials were exploited to gain unauthorized access to both services, with sensitive decoy files downloaded via the FTP service after a successful breach. These files were:

- passwords.txt
- ssn.txt

These findings highlight the critical risks posed by insecure configurations and weak password policies. To mitigate such threats, this report recommends implementing the following:

- Stronger access controls
- Centralized log monitoring
- Network segmentation to enhance internal network security

➤ Analysis

a. Cowrie Log Analysis

- i. **Navigating to the Cowrie Log Directory:** I started by navigating to the `~/cowrie/var/log/cowrie/` directory, which contains all activity logs generated by the Cowrie SSH honeypot. From here, I accessed and filtered the `cowrie.json` file to isolate relevant events such as failed login attempts and commands executed by attackers.

```
cowrie@UbuntuHoneypot: ~/cowrie/var/log/cowrie
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$ ls -l
total 280
-rw-rw-r-- 1 cowrie cowrie 111364 Nov  5 19:58 cowrie.json
-rw-rw-r-- 1 cowrie cowrie 26244 Oct  4 21:04 cowrie.json.2024-10-04
-rw-rw-r-- 1 cowrie cowrie  8744 Oct 22 19:55 cowrie.json.2024-10-22
-rw-r--r-- 1 cowrie cowrie  83538 Nov  5 19:58 cowrie.log
-rw-rw-r-- 1 cowrie cowrie 20199 Oct  4 21:04 cowrie.log.2024-10-04
-rw-r--r-- 1 cowrie cowrie  6015 Oct 22 19:55 cowrie.log.2024-10-22
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$
```

- ii. **Viewing Failed Login Attempts:** Using the `grep` command, I extracted failed login attempts from the `cowrie.json` file. This allowed me to identify brute-force patterns where attackers repeatedly tried weak credentials like `root` and `123456`. This log provided insight into how common weak passwords are exploited in brute-force scenarios.

```
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$ grep "login.failed" cowrie.json
{"eventid":"cowrie.login.failed","username":"root","password":"123456","message":"login attempt [root/123456] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T15:14:32.261807Z","src_ip":"10.0.0.5","session":"c340be0bb90a"}
{"eventid":"cowrie.login.failed","username":"root","password":"password","message":"login attempt [root/password] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T15:47:41.528368Z","src_ip":"10.0.0.5","session":"f0cc260382e5"}
{"eventid":"cowrie.login.failed","username":"root","password":"password","message":"login attempt [root/password] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:09.765668Z","src_ip":"10.0.0.5","session":"70674c390dc8"}
{"eventid":"cowrie.login.failed","username":"root","password":"iloveyou","message":"login attempt [root/iloveyou] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.727587Z","src_ip":"10.0.0.5","session":"e12a9001baa7"}
{"eventid":"cowrie.login.failed","username":"root","password":"12345","message":"login attempt [root/12345] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.728123Z","src_ip":"10.0.0.5","session":"72a5decdf30a"}
{"eventid":"cowrie.login.failed","username":"root","password":"123456","message":"login attempt [root/123456] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.730076Z","src_ip":"10.0.0.5","session":"aca2d3a406f3"}
{"eventid":"cowrie.login.failed","username":"root","password":"princess","message":"login attempt [root/princess] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.730621Z","src_ip":"10.0.0.5","session":"6b41b13c281a"}
{"eventid":"cowrie.login.failed","username":"root","password":"password","message":"login attempt [root/password] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.731115Z","src_ip":"10.0.0.5","session":"8135557f3ef6"}
{"eventid":"cowrie.login.failed","username":"root","password":"abc123","message":"login attempt [root/abc123] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.731617Z","src_ip":"10.0.0.5","session":"ab0fc74fc6b0"}
{"eventid":"cowrie.login.failed","username":"root","password":"12345678","message":"login attempt [root/12345678] failed","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:28:39.732091Z","src_ip":"10.0.0.5","session":"3dbfa8bc50ed"}
```

- iii. **Filtering for Successful Login Attempts:** I searched for login.success events within the cowrie.json file to identify successful brute-force attacks. These entries confirmed that an attacker gained access using the credentials root:123456789

```
cowrie@UbuntuHoneypot: ~/cowrie/var/log/cowrie
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$ grep "login.success" cowrie.json
{"eventid":"cowrie.login.success","username":"root","password":"123456789","message":"login attempt [root/123456789] succeeded","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:26.479980Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.login.success","username":"root","password":"123456789","message":"login attempt [root/123456789] succeeded","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:31:08.470645Z","src_ip":"10.0.0.5","session":"16e6dbe1ecdc"}
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$
```

- iv. **Commands Executed Post-Login:** Once inside the honeypot, the attacker executed reconnaissance commands such as **ls** and **cd** to explore the system. Additional mistyped commands like **;s** and **c;ear** were also logged, showcasing typical errors during manual interaction. These commands reflect an initial exploration phase of an attacker after gaining access.

```
cowrie@UbuntuHoneypot: ~/cowrie/var/log/cowrie
cowrie@UbuntuHoneypot:/var/log$ cd ~/cowrie/var/log/cowrie/
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$ ls
cowrie.json          cowrie.json.2024-10-22  cowrie.log.2024-10-04
cowrie.json.2024-10-04 cowrie.log              cowrie.log.2024-10-22
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$ grep "cowrie.command.input" cowrie.json
{"eventid":"cowrie.command.input","input":"exit","message":"CMD: exit","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T15:47:49.691917Z","src_ip":"10.0.0.5","session":"f0cc260382e5"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:27.903568Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"cd ~","message":"CMD: cd ~","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:36.986856Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":";s","message":"CMD: ;s","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:37.700436Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:38.692255Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"cd /home","message":"CMD: cd /home","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:40.205223Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:41.083569Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"cd phil","message":"CMD: cd phil","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:51.072368Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:52.361625Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"c;ear","message":"CMD: c;ear","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:30:59.114734Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"exit","message":"CMD: exit","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:31:01.153682Z","src_ip":"10.0.0.5","session":"c9c245e2e2a4"}
{"eventid":"cowrie.command.input","input":"cd /home/phil/","message":"CMD: cd /home/phil/","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:32:02.983226Z","src_ip":"10.0.0.5","session":"16e6dbe1ecdc"}
{"eventid":"cowrie.command.input","input":"exit","message":"CMD: exit","sensor":"UbuntuHoneypot","timestamp":"2024-11-05T17:32:24.583570Z","src_ip":"10.0.0.5","session":"16e6dbe1ecdc"}
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$
```

b. VSFTP Log Analysis

- i. **Navigating to the FTP Log Directory:** I accessed `/var/log/` to locate the `vsftpd.log` file, which records all FTP activity. This directory contains essential logs for analyzing login attempts and file transfers.

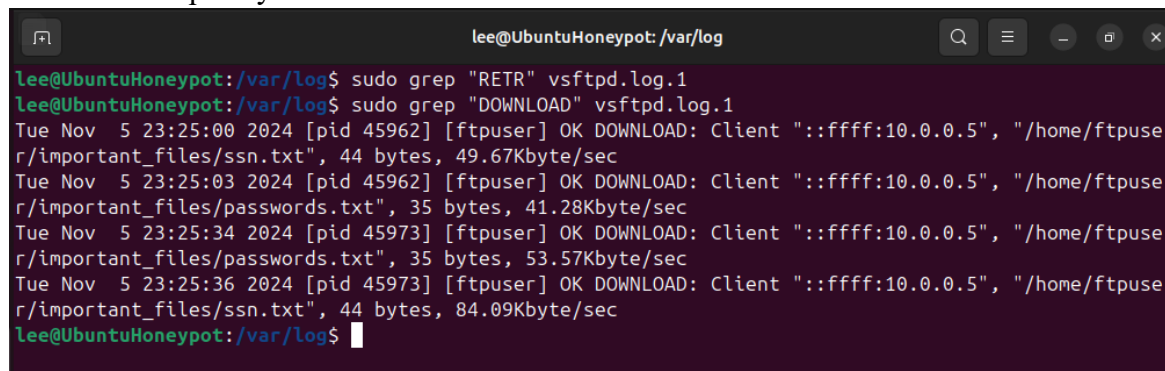
```
lee@UbuntuHoneypot:/var/log$ ls
alternatives.log      cups-browsed          lastlog               vmware-network.4.log
alternatives.log.1    dist-upgrade          mysql                vmware-network.5.log
apache2              dmesg                 openvpn              vmware-network.6.log
appport.log          dmesg.0              private              vmware-network.7.log
apt                 dpkg.log              README               vmware-network.8.log
auth.log             dpkg.log.1            samba                vmware-network.9.log
auth.log.1           faillog               speech-dispatcher    vmware-network.log
auth.log.2.gz        fontconfig.log        sssd                 vmware-vmsvc-root.1.log
auth.log.3.gz        gdm3                  syslog               vmware-vmsvc-root.log
boot.log             gpu-manager.log       syslog.1             vmware-vmtoolsd-lee.log
boot.log.1           hp                    syslog.2.gz          vmware-vmtoolsd-root.log
bootstrap.log        installer             syslog.3.gz          vmware-vmusr-lee.log
btmtp                journal              sysstat              vsftpd.log
btmtp.1              kern.log              unattended-upgrades vsftpd.log.1
cloud-init.log        kern.log.1            vmware-network.1.log wtmp
cloud-init-output.log kern.log.2.gz          vmware-network.2.log
cups                 kern.log.3.gz          vmware-network.3.log
lee@UbuntuHoneypot:/var/log$
```

- ii. **Viewing FTP Login Attempts:** Using `grep`, I filtered the log file for **LOGIN** events to distinguish successful and failed login attempts. Multiple failed attempts indicated a brute-force attack targeting the **ftppuser** account.

```
lee@UbuntuHoneypot:/var/log$ sudo grep "LOGIN" vsftpd.log.1
Tue Nov 5 23:22:35 2024 [pid 45923] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45908] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45912] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45920] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45902] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45907] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45911] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45903] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45922] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45918] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45910] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45904] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45905] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45921] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:35 2024 [pid 45909] [ftppuser] FAIL LOGIN: Client "::ffff:10.0.0.5"
Tue Nov 5 23:22:43 2024 [pid 45936] [ftppuser] OK LOGIN: Client "::ffff:10.0.0.5"
```

- iii. **Analyzing File Downloads:** The attacker successfully accessed and downloaded sensitive decoy files (**passwords.txt** and **ssn.txt**) as recorded in the **vsftpd** logs. Each download event was logged with the **DOWNLOAD** command, including details such as file size and transfer speed. These logs highlight the potential severity of a successful brute-force attack

on an unsecured FTP service, where sensitive data can be exfiltrated quickly and without detection in a poorly monitored environment.



```
lee@UbuntuHoneypot: /var/log
lee@UbuntuHoneypot:/var/log$ sudo grep "RETR" vsftpd.log.1
lee@UbuntuHoneypot:/var/log$ sudo grep "DOWNLOAD" vsftpd.log.1
Tue Nov  5 23:25:00 2024 [pid 45962] [ftpuser] OK DOWNLOAD: Client "::ffff:10.0.0.5", "/home/ftpuser/important_files/ssn.txt", 44 bytes, 49.67Kbyte/sec
Tue Nov  5 23:25:03 2024 [pid 45962] [ftpuser] OK DOWNLOAD: Client "::ffff:10.0.0.5", "/home/ftpuser/important_files/passwords.txt", 35 bytes, 41.28Kbyte/sec
Tue Nov  5 23:25:34 2024 [pid 45973] [ftpuser] OK DOWNLOAD: Client "::ffff:10.0.0.5", "/home/ftpuser/important_files/passwords.txt", 35 bytes, 53.57Kbyte/sec
Tue Nov  5 23:25:36 2024 [pid 45973] [ftpuser] OK DOWNLOAD: Client "::ffff:10.0.0.5", "/home/ftpuser/important_files/ssn.txt", 44 bytes, 84.09Kbyte/sec
lee@UbuntuHoneypot:/var/log$
```

➤ Overview

- c. **Failed Login Attempts (Cowrie SSH and FTP Services):** The logs captured multiple failed login attempts for both the Cowrie SSH honeypot and the vsftpd FTP service. These failed attempts reflect typical brute-force attack patterns where attackers rely on weak or common credentials to gain unauthorized access. The Cowrie logs, for instance, recorded repeated attempts using usernames like root and passwords such as 123456, while the vsftpd logs revealed sustained brute-force attempts targeting the ftpuser account.
- d. **Identifying Successful Logins (FTP Service):** Within the FTP logs, I identified a successful brute-force attempt where the attacker gained access using the credentials ftpuser:ftpuser. The logs show a series of failed login attempts within the same minute, followed by a successful login. This sequence confirms the vulnerability of weak credentials and emphasizes the need for better credential management practices to mitigate such risks.
- e. **Identifying Successful Logins & Post-Login Activity (Cowrie SSH):** After successful brute-force attempts, attackers executed several reconnaissance commands on the Cowrie honeypot. Commands like ls and cd were used to explore the file system and navigate directories, demonstrating a typical attacker's behavior upon gaining access. The logs also captured mistyped or nonsensical commands such as ;s and c;ear, indicating manual interactions that may be characteristic of less experienced attackers or human error. This level of logging provides critical insights into attacker behavior and potential missteps during post-compromise activity.
- f. **Identifying Successful Logins (FTP Service):** Within the FTP logs, I identified a successful brute-force attempt where the attacker gained access using the credentials ftpuser:ftpuser. The logs show a series of failed login attempts within the same minute, followed by a successful login. This sequence confirms the vulnerability of weak credentials and emphasizes the need for better credential management practices to mitigate such risks.

➤ Recommendations

I recommend several enhancements to internal network security to address the risks observed.

- g. First, **implementing centralized log management systems and real-time alerting** will enable faster detection and response to suspicious activity.

- h. **Strengthening access control policies**, such as enforcing strong password requirements, enabling account lockout mechanisms, and deploying multi-factor authentication (MFA), is crucial to preventing successful brute-force attacks.
- i. Furthermore, **securing services like FTP by restricting access to sensitive files** and applying **network segmentation** to **isolate critical assets** will significantly reduce the risk of unauthorized access.
- j. Finally, **conducting regular audits** and providing **employee training on cybersecurity** best practices will reinforce these technical measures, ensuring a more secure and resilient internal network.