Delton Robinson
12/3/2024
IS-4543-001

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:

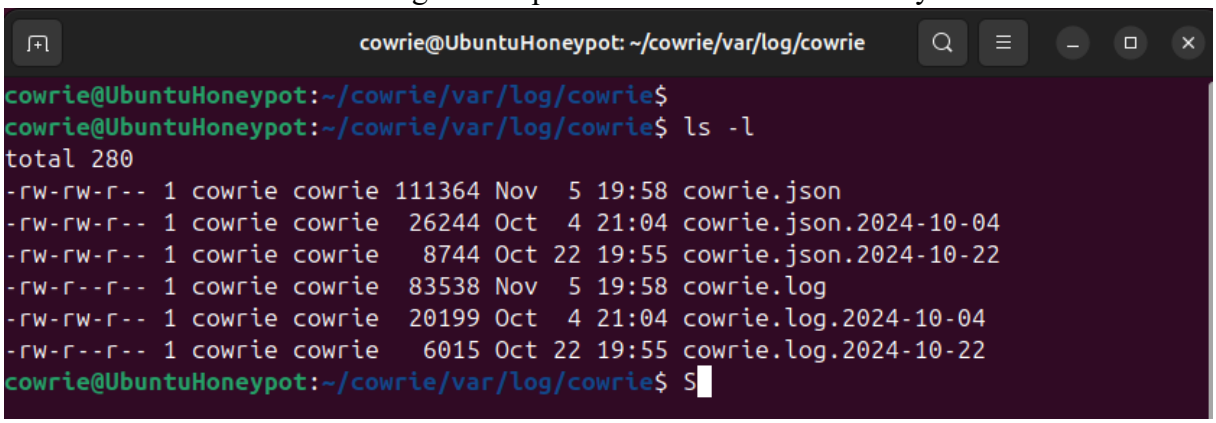
- Stronger access controls
- Centralized log monitoring
- Network segmentation to enhance internal network security

Delton Robinson
12/3/2024
IS-4543-001

➢ Analysis

❖ 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.



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

Delton Robinson
12/3/2024
IS-4543-001

into how common weak passwords are exploited in brute-force scenarios.

```
cowrie@UbuntuHoneypot: ~/cowrie/var/log/cowrie
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$ grep "login.failed" cowrie.json
{"eventid":"cowrie.login.failed","username":"root","password":"123456","message":"login attempt [ro
ot/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 [roo
t/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 [ro
ot/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 [ro
ot/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

Delton Robinson
12/3/2024
IS-4543-001

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","t
imestamp":"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","times
tamp":"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","t
imestamp":"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","times
tamp":"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","times
tamp":"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":"UbuntuHone
ypot","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","times
tamp":"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":"UbuntuHoneyp
ot","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","times
tamp":"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","t
imestamp":"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":"16e6dbe1
ecdc"}
{"eventid":"cowrie.command.input","input":"exit","message":"CMD: exit","sensor":"UbuntuHoneypot","t
imestamp":"2024-11-05T17:32:24.583570Z","src_ip":"10.0.0.5","session":"16e6dbe1ecdc"}
cowrie@UbuntuHoneypot:~/cowrie/var/log/cowrie$
```

- **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

Delton Robinson
12/3/2024
IS-4543-001

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
apport.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
btmp                    journal           sysstat                vsftpd.log
btmp.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$
```

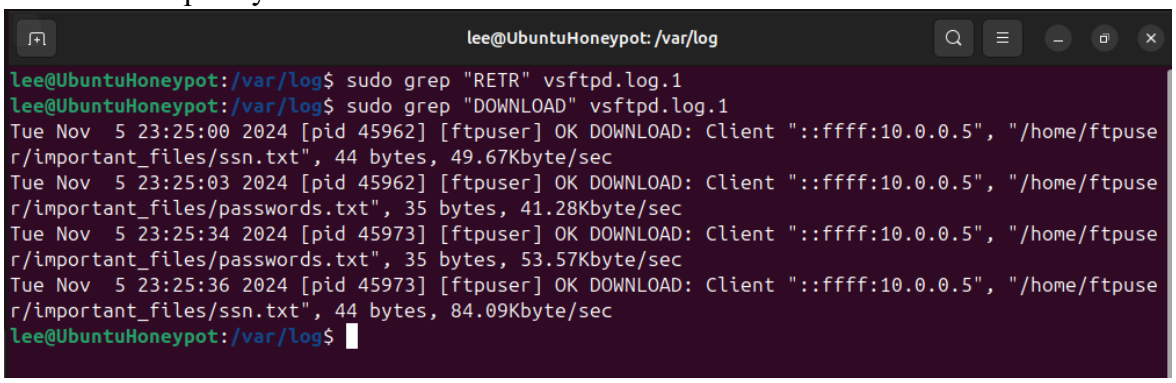
II. **Viewing FTP Login Attempts:** Using grep, I filtered the log file for **LOGIN** events to distinguish successful and failed login attempts. Multiple failed attempts indicated a brute-force attack targeting the **ftpuser** account.

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

Delton Robinson
12/3/2024
IS-4543-001

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.



➢ Overview

- **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.
- **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.
- **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.
- **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

Delton Robinson
12/3/2024
IS-4543-001

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

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