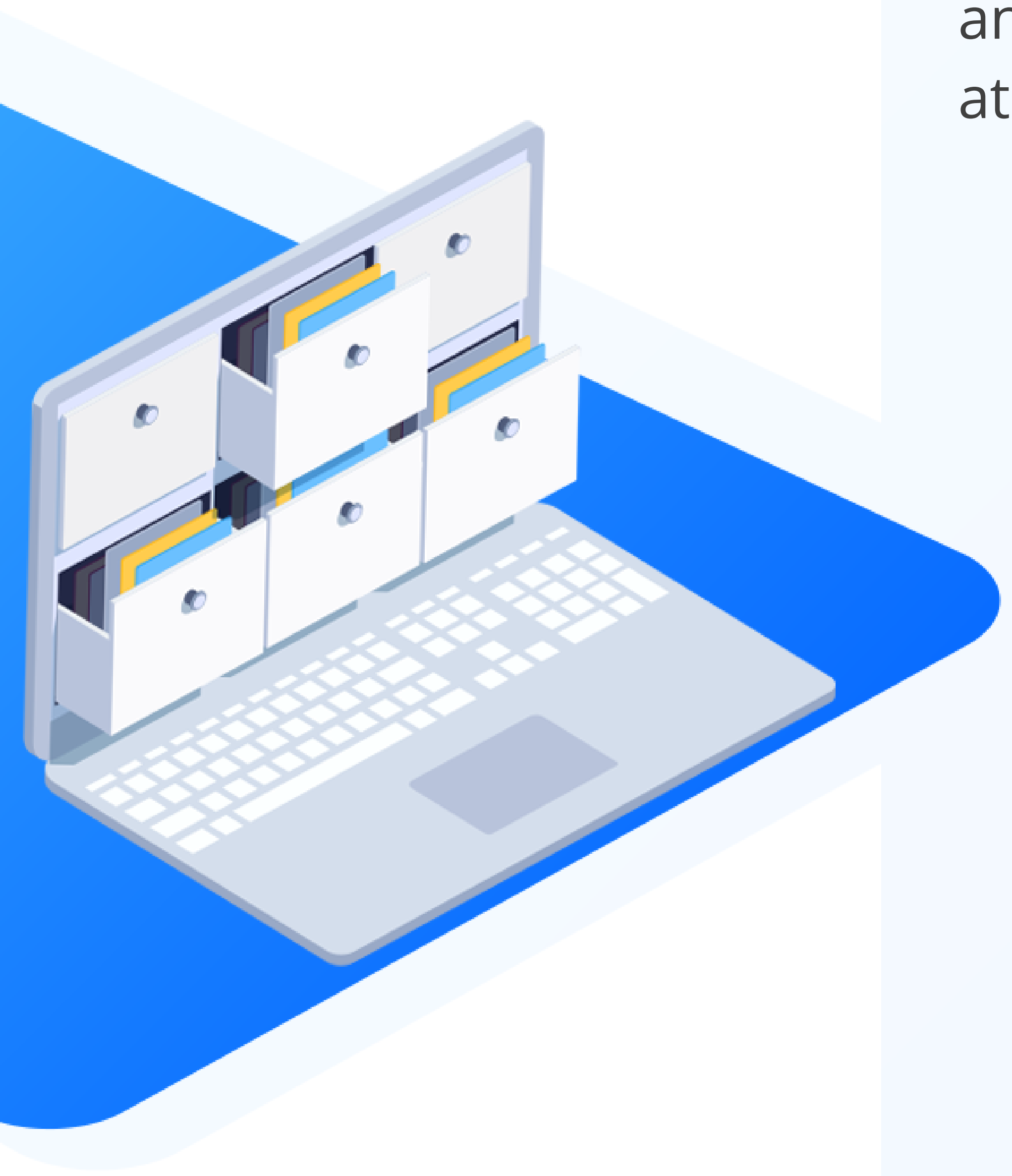
Cybersecurity

Course-End Project

Securing Linux Servers Using Honeypots and IP Blocking

Objective



To deploy a honeypot and configure defensive mechanisms like SSH hardening and automated IP blocking to detect, analyze, and mitigate SSH brute-force attacks on public-facing Linux servers

Problem Statement and Motivation

Real-time scenario:

SecureDefense, a cybersecurity firm managing Linux servers with public IPs, faces frequent SSH brute-force attacks that exploit weak credentials. To combat these threats, SecureDefense deploys honeypots to mimic real servers, capturing attack data to analyze patterns and attacker behaviors.

They enhance security by automating IP blocking using fail2ban, which monitors failed SSH login attempts and blocks attackers after repeated failures. Additionally, they harden SSH configurations by using non-standard ports and limiting login attempts to reduce attack surfaces.

This strategy not only protects client servers but also provides actionable insights to improve intrusion detection systems. By demonstrating proactive cybersecurity measures, SecureDefense strengthens its reputation as a trusted provider, attracting new enterprise clients.

Industry Relevance

The following tools used in this project serve specific purposes within the industry:

1. **Honeypots (vsftpd, smbd, httpd, mysql)**: Decoy systems that mimic real servers to attract attackers, gather data on attack patterns, and improve intrusion detection systems

2. **Fail2ban:** Automates IP blocking after failed login attempts, effectively reducing brute-force attacks and maintaining server security

3. **TCP Wrappers:** Controls access by blocking or allowing specific IPs, adding an extra security layer to Linux servers

4. **Firewalld:** Manages dynamic firewall rules, restricting access to sensitive ports and mitigating brute-force attacks

Industry Relevance

The following tools used in this project serve specific purposes within the industry:

5. **Splunk:** Analyzes server logs to identify attack trends and improve threat detection and response

6. **OpenSSH:** Secures remote access with custom configurations like non-standard ports and login attempt limits to reduce vulnerabilities

Tasks

The following tasks outline the process of deploying a honeypot and configuring SSH hardening and IP blocking to detect and mitigate brute-force attacks on Linux servers:

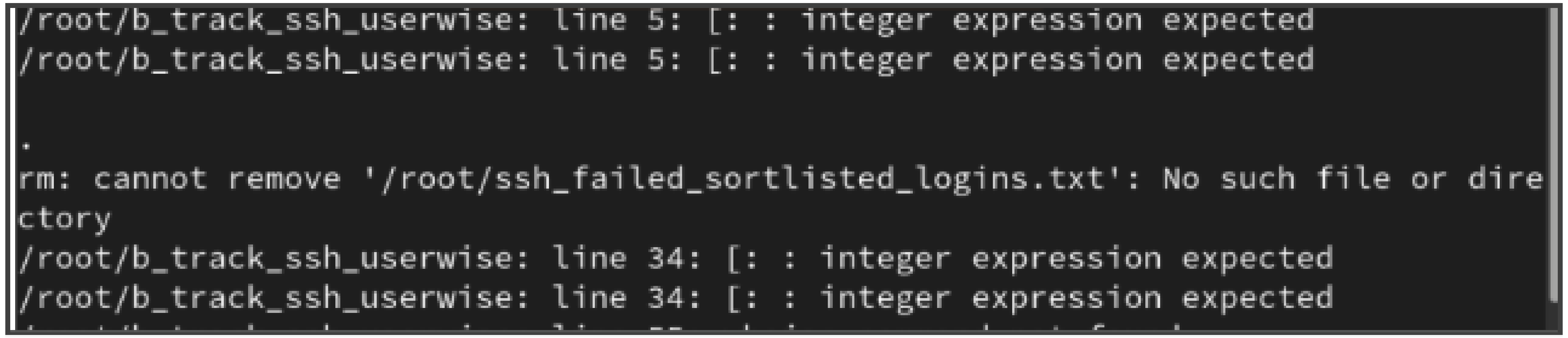
1. Deploy Honeypot to simulate SSH attacks and collect data
2. Harden SSH configuration to secure the server
3. Implement IP blocking to mitigate repeated attacks

Project References

- **Task 1:** Lesson 06
- **Task 2:** Lesson 02
- **Task 3:** Lesson 02
- **Task 4:** Lesson 07

Output Screenshots

It shows that the SSH protection script encountered errors during execution, including missing files and invalid integer expressions.



```
/root/b_track_ssh_userwise: line 5: [: : integer expression expected
/root/b_track_ssh_userwise: line 5: [: : integer expression expected


.
rm: cannot remove '/root/ssh_failed_sortlisted_logins.txt': No such file or dire
ctory
/root/b_track_ssh_userwise: line 34: [: : integer expression expected
/root/b_track_ssh_userwise: line 34: [: : integer expression expected
```

Thank you