MAJOR PROJECT REPORT

Title: Securing SSH Services Against Brute-Force Attacks in a Cloud Environment

1. Introduction
This project demonstrates how insecure SSH configurations in cloud-based Linux servers can lead to brute-force attacks. The project follows a Red Team and Blue Team approach to simulate, detect, and prevent such attacks using AWS EC2.

2. Problem Statement
Weak SSH configurations such as password-based authentication and unrestricted access expose cloud servers to brute-force attacks. This project addresses how such vulnerabilities can be exploited and secured.

3. Objectives
• Identify insecure SSH configurations
• Simulate an SSH brute-force attack
• Detect the attack using log analysis
• Apply SSH security hardening
• Validate security by re-attacking

4. System Architecture
Two EC2 instances were used: an attacker machine and a victim server within AWS. The attacker executed brute-force attempts, while the victim server logs and security settings were monitored.

5. Tools & Technologies
AWS EC2, Ubuntu Linux, OpenSSH, Hydra, Linux Authentication Logs

6. Methodology
The project involved setting up a vulnerable server, performing an SSH brute-force attack, analyzing authentication logs, applying SSH hardening measures, and validating security by ensuring attacks fail.

7. Results
Before hardening, SSH brute-force attacks were successful. After disabling password authentication, reducing login attempts, and enforcing key-based login, all attacks failed.

8. Conclusion
This project proves that proper SSH security configuration is critical for protecting cloud servers from unauthorized access and brute-force attacks.

9. Future Scope
Further enhancements include Fail2Ban, intrusion detection systems, and multi-factor authentication.

10. References
AWS Documentation, OpenSSH Manuals, Hydra Documentation, Ubuntu Security Guides