# Glossary

## Apache HTTP Server (httpd).

Open-source software that serves web content using HTTP/HTTPS protocols; used here to simulate website hosting and serve reports.

## Brute-Force Attack.

A method of attack where many username/password combinations are tried rapidly to gain unauthorized access.

## CentOS.

Stable, free Linux distribution based on Red Hat Enterprise Linux, commonly used in servers.

## Chroot Jail.

A security mechanism restricting a process to a specific directory subtree to limit filesystem access.

## Cowrie.

An interactive SSH honeypot designed to capture detailed attacker behavior for research and analysis.

## ELK Stack.

Open-source log management platform composed of Elasticsearch, Logstash, and Kibana for aggregation and visualization.

## Fail2ban.

An intrusion prevention software that scans logs for repeated failed login attempts and blocks malicious IPs.

## Firewalld.

Dynamic Linux firewall management tool that uses zones for network traffic control.

## Hydra.

Automated password-cracking tool that performs brute-force attacks on various network services including SSH.

## HTTP Response Codes.

Standardized codes like 200 (OK), 403 (Forbidden), 404 (Not Found) indicating the status of an HTTP request.

## Intrusion Detection System (IDS).

A monitoring system that detects suspicious or malicious activity on networks or hosts.

## Intrusion Prevention System (IPS).

A proactive system that blocks or mitigates detected security threats.

## jail.conf / jail.local (Fail2ban).

Fail2ban configuration files; jail.local contains user customizations that persist after updates.

## Key-Based SSH Authentication.

A method of authenticating SSH sessions using cryptographic key pairs instead of passwords.

## Linux Systemd Journald.

Logging daemon responsible for collecting and managing logs in systemd-based Linux systems.

## MFA (Multi-Factor Authentication).

Authentication method requiring two or more verification factors to improve security.

## OpenSSH.

An implementation of the SSH protocol for encrypted and secure remote connections.

## Proxychains.

A utility that routes network connections through proxy servers to maintain anonymity or simulate different conditions.

## SELinux (Security-Enhanced Linux).

A kernel security module enforcing mandatory access controls for improved system security.

## SELinux Port Labeling.

Assigning SELinux types to network ports to regulate service access securely.

## Shell Script.

A text file containing a series of commands executed by a command-line interpreter.

## SIEM (Security Information and Event Management).

Platforms that collect and analyze security event data to correlate threats and support incident response.

## SSH (Secure Shell).

A protocol that enables secure encrypted remote login and command execution.

## SSH Daemon (sshd).

The server component that listens for and manages incoming SSH connections.

## Syslog.

A standard protocol and facility for sending, receiving, and storing log messages.

## TCP Wrappers.

Host-based network access control system using hosts.allow and hosts.deny files to restrict service access.

## Tor.

An anonymity network that routes internet traffic through relays to conceal user location.

## vsftpd (Very Secure FTP Daemon).

A secure and efficient FTP server widely used on Unix/Linux systems.

## Log Rotation.

Automated process that manages log file sizes by archiving or deleting older entries.

## Intrusion Prevention System (IPS).

Software or hardware that actively prevents malicious activity detected by an IDS.

## Jail (Fail2ban Terminology).

A specific Fail2ban configuration that defines rules to monitor logs and ban IPs upon detected malicious activity.

## Password Authentication.

A login method requiring a secret password; less secure than key-based authentication.

## Cron Job.

A scheduled command or script executed automatically at specified intervals on Unix-like systems.

## Log Parsing.

The automated process of extracting structured data from unstructured log files.

## Firewall Rule.

A configuration directive that permits or denies network traffic based on criteria like IP address or port.