Glossary

Apache HTTP Server (httpd).

Open-source software that serves web content using HTTP/HTTPS protocols. Used here to simulate web services and serve reports.

Brute-Force Attack.

An attack method where numerous username/password combinations are tried rapidly to gain unauthorized access.

CentOS.

A stable, free Linux distribution derived from Red Hat Enterprise Linux, widely used for servers.

Chroot Jail.

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

Cowrie.

An interactive SSH honeypot capturing detailed attacker behavior for research.

ELK Stack.

Open-source logging platform consisting of Elasticsearch, Logstash, and Kibana for log aggregation and visualization.

Fail2ban.

Intrusion prevention tool monitoring logs for failed login attempts and banning malicious IP addresses.

FirewallD.

Dynamic Linux firewall management tool using zones to control network traffic.

Hydra.

An automated tool for performing brute-force password attacks on network services.

HTTP Response Codes.

Standard codes sent by servers indicating the status of HTTP requests (e.g., 200 OK, 403 Forbidden).

Intrusion Detection System (IDS).

A system that monitors network or host activity for malicious actions or policy violations.

Intrusion Prevention System (IPS).

A system that actively blocks or prevents detected security threats.

jail.conf / jail.local (Fail2ban).
Configuration files for Fail2ban; jail.local is for user customizations that persist through updates.

Key-Based SSH Authentication.

SSH login method using cryptographic key pairs instead of passwords, enhancing security.

Linux Systemd Journald.

A logging service in Linux that collects and manages system and application logs.

MFA (Multi-Factor Authentication).

An authentication method requiring more than one type of credential to grant access.

OpenSSH.

A suite of secure networking utilities implementing SSH protocol for encrypted communication.

Proxychains.

Software forcing application's network traffic through proxies, used for anonymity or simulation.

SELinux (Security-Enhanced Linux).

Kernel security module enforcing mandatory access controls on programs and processes.

SELinux Port Labeling.

Configuring SELinux to allow services to bind securely to non-default network ports.

Shell Script.

A script written for a command-line interpreter, automating tasks like log parsing or IP blocking.

SIEM (Security Information and Event Management).

Platform that aggregates and analyzes security data to detect and respond to threats.

SSH (Secure Shell).

Network protocol for secure remote login and command execution over an unsecured network.

SSH Daemon (sshd).

The server component of SSH, handling incoming connections and authentication.

Syslog.

Standardized logging protocol used to send event messages in IP networks.

TCP Wrappers.

A host-based access control mechanism to allow or deny network access to services.

Tor.

An anonymity network routing traffic through multiple relays to protect user privacy.

vsftpd (Very Secure FTP Daemon).

A secure FTP server known for stability and performance, sometimes used as a honeypot.