--Acunetix SOP---

Windows

Download Acunetix

- Go to the official site: https://www.acunetix.com/download/
- Download the installer (Premium / On-Prem).

Run Installer

- Double-click the .exe installer.
- Follow the wizard → accept license → choose install directory.

Install Dependencies (auto-handled)

- The installer sets up required components (local web server, services).

Start Acunetix Services

- Services are installed as **Acunetix** and auto-start.
- If not running, open **Services.msc** → start *Acunetix*.

Access Web UI

- Open browser:
- https://localhost:13443/
- Accept certificate warning (self-signed cert).

1. **Login & Activate**

- Create first admin account during setup.
- Enter license/activation key if required.

Linux (Debian/Ubuntu/Kali)

Download Acunetix Package

- From official site: https://www.acunetix.com/download/
- Example: **wget https://download.acunetix.com/acunetix_trial.sh**

Install Dependencies

- sudo apt-get update
- sudo apt-get install libxss1 libayatana-appindicator3-1 libgtk-3-0

Install Acunetix

- chmod +x acunetix_trial.sh
- sudo ./acunetix_trial.sh

Start Service

- sudo systemctl start acunetix
- sudo systemctl enable acunetix

Access Web UI

- Open browser: https://localhost:13443/
- from another PC: https://<server-ip>:13443/

Login & Activate

- Create admin account during first login.
- Enter license key / trial key.

Scan setup for pentesting

1. Target Configuration Target URL → the exact site/app you're testing.

- *Business Criticality* → set this (High/Medium/Low) so findings are prioritized in reports.
- *Login Details (if required):*
  - Use Login Sequence Recorder → record how you log in.
  - Save credentials/session cookies for authenticated scans.
- *Excluded Paths* → if there are areas you don't want to scan (e.g., logout pages, admin reset endpoints).

2. Scan Profiles

- *Full Scan* → for comprehensive testing (default for pentests).
- *High Risk Vulnerabilities Only* → for quick checks.
- *Custom Profile* → recommended for pentesting:
  - Enable OWASP Top 10 + All Web Vulnerability Checks.
  - Disable Denial of Service (DoS) and brute force attacks unless explicitly allowed by client.

3. Scan Speed & Options

- *Scan Speed* → set to Moderate to balance depth & avoid overloading the target.
- *Crawl & Attack* → enable (so Acunetix discovers hidden pages and input fields).
- *Maximum Concurrent Connections* → don't max out; keep default unless scanning staging servers.

4. Authentication Settings

- Use Recorded Login (preferred) or username/password form-based auth.
- For multi-factor auth, generate session cookies manually and configure them.

5. Exclusions & Restrictions

- *Excluded Hosts* → add domains/IPs out of scope.
- *Excluded File Extensions* → e.g., .jpg, .png, .css, .js (saves time).
- *Excluded Paths* → avoid logout endpoints or destructive actions.

6. Notifications & Reports

- *Enable Email Alerts* → get notified when scan finishes or if critical issues found.
- Set Report Type depending on audience:
  - OWASP Top 10 → for devs.
  - Executive Summary → for management.
  - Developer Report → step-by-step remediation.

7. Advanced (Optional)

- *Custom Headers* → if app uses tokens or special headers.
- *Crawling Depth* → increase for apps with deep navigation.
- *SSL/TLS Testing* → keep enabled.
- *Integration* → connect Acunetix with JIRA, GitLab, Jenkins if part of CI/CD.