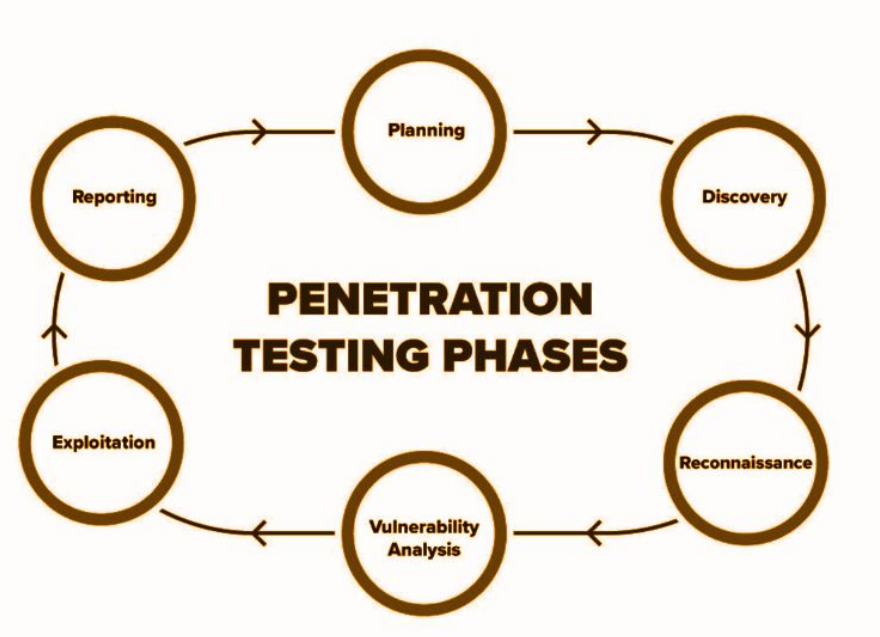
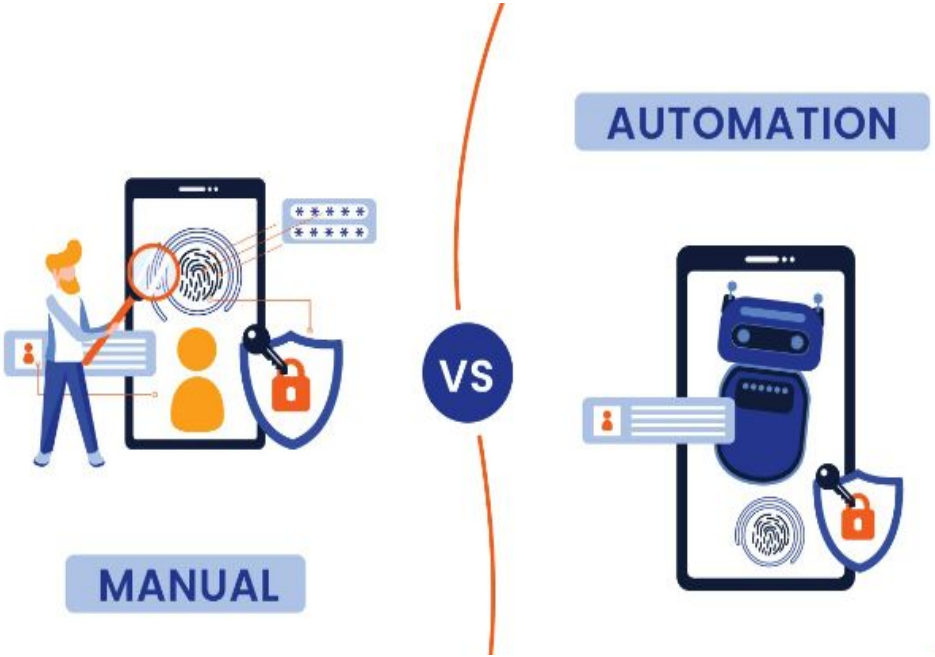
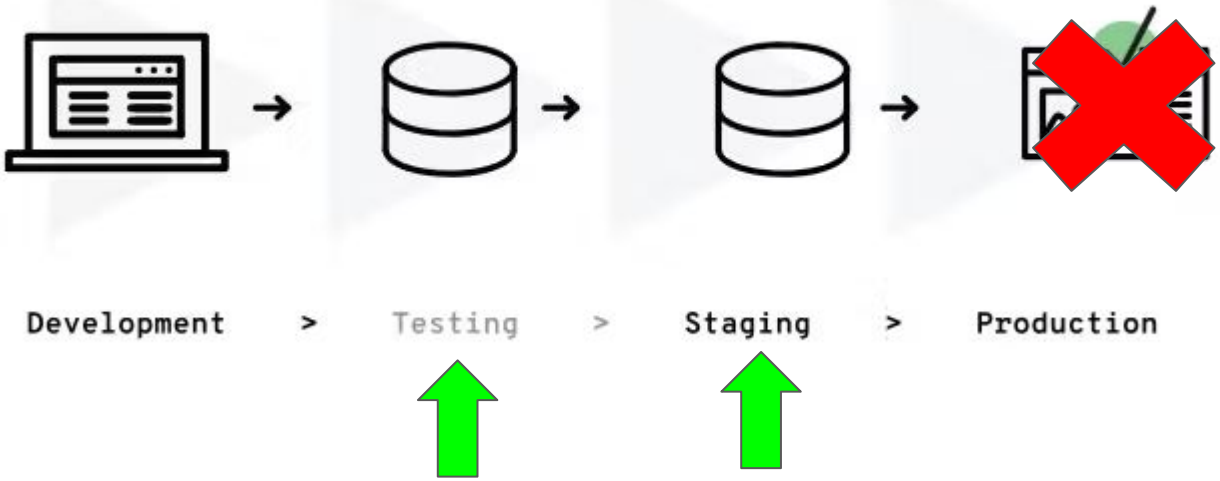


Penetration Testing, also known as **pen testing**, is a form of security testing that involves simulating a real-world attack on a system to identify vulnerabilities and potential exploits.

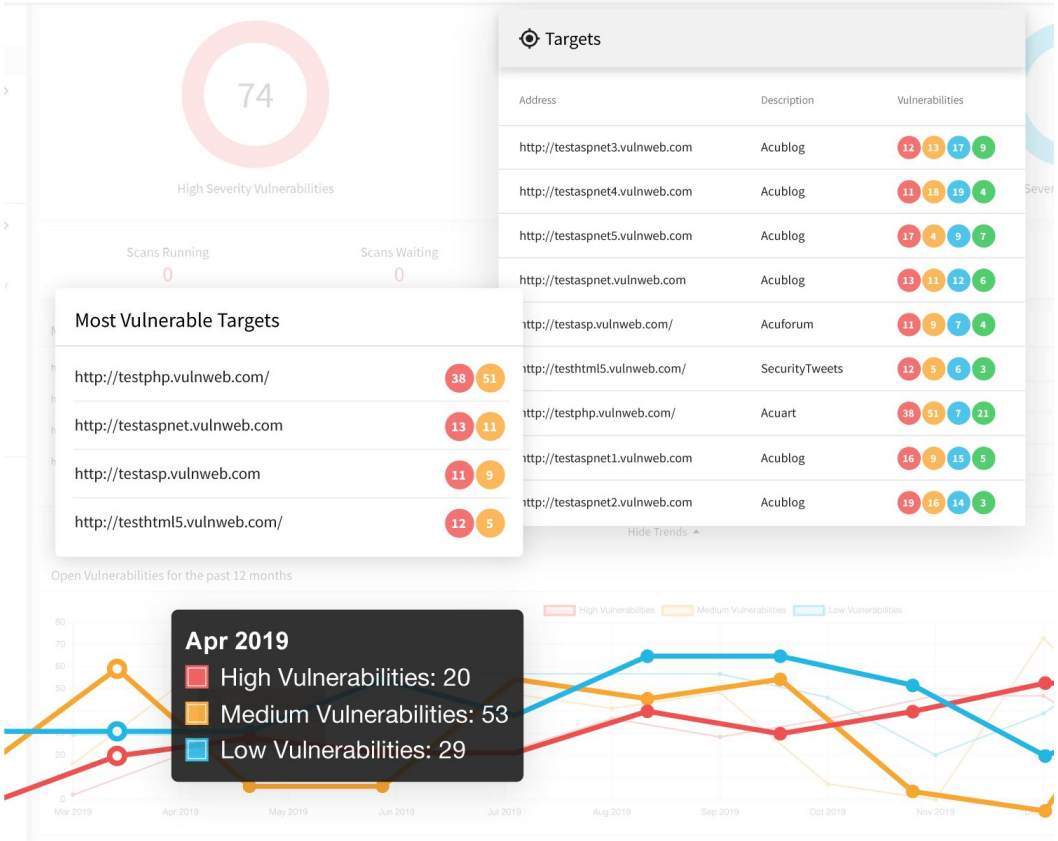


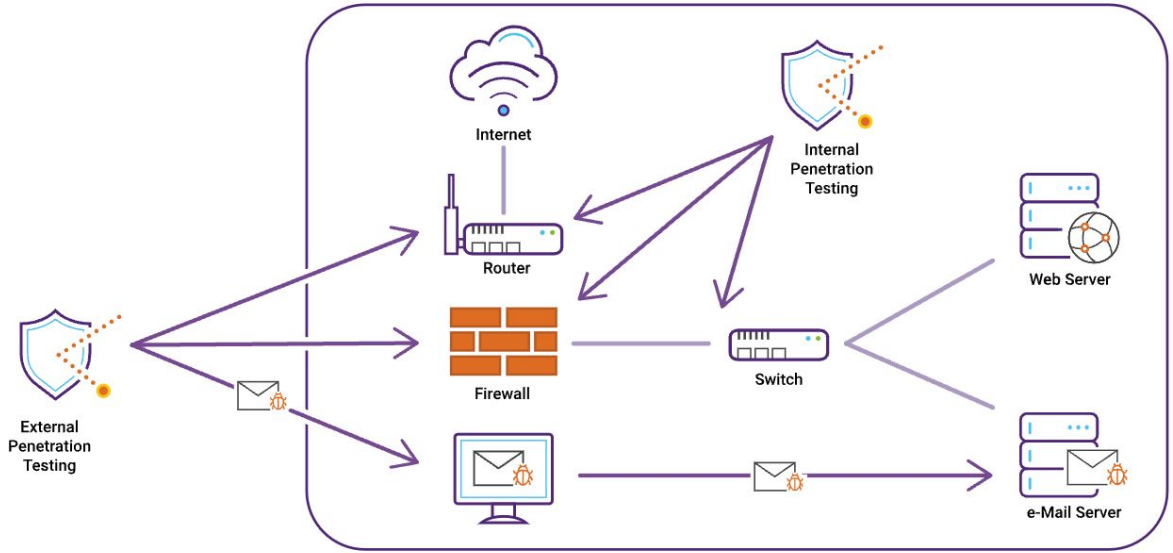
The pen tester attempts to exploit vulnerabilities, typically using a combination of **manual** and **automated** techniques, to gain access to sensitive data or functionality



The testing is typically conducted in a controlled environment, such as a test or staging environment, to prevent any unintended impact on the production system.

During a pen test, the tester attempts to identify and exploit vulnerabilities, using a range of techniques including automated scanning, manual testing, and social engineering.





The testing can be performed from various perspectives, such as an **external** attacker or an **internal** threat, to identify vulnerabilities from different angles.

Free and Open-Source Pen Testing Tools

- **Nmap**: For reconnaissance - it can quickly scan large networks
- **Zed Attack Proxy** scans web applications for vulnerabilities
- **Nikto2** can identify the most common faults found in web servers
- **Jok3r** compilation of more than 50 open source tools and scripts
- **OpenSCAP** offers automated configuration, vulnerability and patch checking, and continuous infrastructure evaluation for security compliance
- **Metasploit** robust testing framework backed by more than 200,000 contributors
- **Burp Suite** intercept all requests and responses between the browser and the target for cross-site request forgery (CSRF) attacks