Automated Scanners

What are automated scanners?

- Automated scanners are software tools designed to detect and assess security vulnerabilities and weaknesses in various components of an organization's IT infrastructure.
- The primary focus of the scanners is to identify vulnerabilities and assist in strengthening an organization's overall security posture.
- Automated Scanners can significantly impact the organizations operations by reducing errors which cost valuable time and resources.

Different automated scanners

Automated scanners can be categorized into several types:

- **Vulnerability Scanners**: These scanners focus on identifying known vulnerabilities in systems, applications, and networks. They check for outdated software, missing security patches, misconfigurations, default credentials, and other weaknesses that could be exploited by attackers.
- **Web Application Scanners**: Web application scanners are specialized tools that assess the security of web applications, including websites and web services. They look for common vulnerabilities like SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF).
- **Network Scanners**: Network scanners examine the network infrastructure to identify open ports, services running on them, and potential misconfigurations that might leave the network exposed to attacks.
- **Malware Scanners**: These scanners search for malware, viruses, and other malicious software on systems and devices, helping organizations detect and remove infections.

Uses

- Identifying known vulnerabilities in networks, systems, and applications.
- Prioritizing vulnerabilities based on severity and impact to focus on critical issues.
- Identifying and mitigating security vulnerabilities in web applications and websites.
- Scanning and mapping network infrastructure to identify open ports and services running on them.
- Scanning and mapping network infrastructure to identify open ports and services running on them.

Automated Scanners

1. **Vulnerability Scanners:**
    - Nessus is a widely-used vulnerability scanner that identifies security issues in networks, systems, and applications.

    - OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner known for its comprehensive coverage of network-related vulnerabilities. It includes a constantly updated database of known vulnerabilities.

- Qualys Vulnerability Management is a cloud-based vulnerability scanner that offers continuous monitoring, risk assessment, and prioritization of vulnerabilities for efficient security management.

2. **Web Application Scanners:**

- Acunetix is a web application scanner that detects and helps remediate common web vulnerabilities like SQL injection, XSS, and more.

- Burp Suite is a popular web vulnerability testing tool. It allows manual and automated scanning

- OWASP ZAP (Zed Attack Proxy) is an open-source tool designed for identifying vulnerabilities in web applications.

3. **Network Scanners:**

   - Nmap (Network Mapper) is a network scanner used for network discovery and security assessments. It detects open ports, running services, and provides OS fingerprinting.

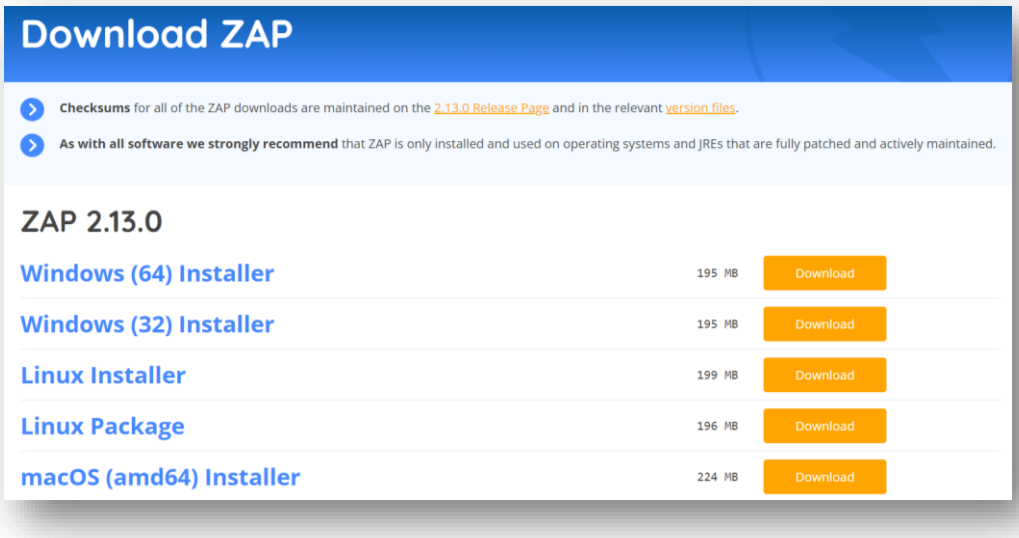
   - Advanced IP Scanner is a user-friendly network scanner that quickly identifies devices connected to a network, helping administrators monitor network assets and detect potential security risks.

- Angry IP Scanner is a network scanner that scans IP addresses and ports, allowing administrators to identify active hosts and troubleshoot network issues.

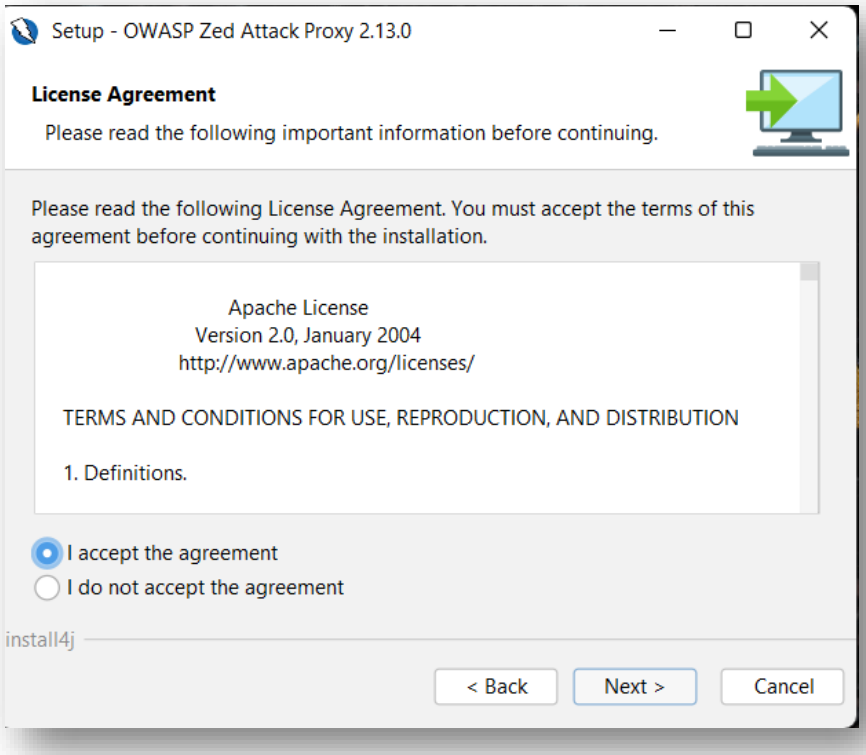
4. **Malware Scanners:**
   - Malwarebytes is an anti-malware tool that scans and removes malware from systems, offering real-time protection against known threats.

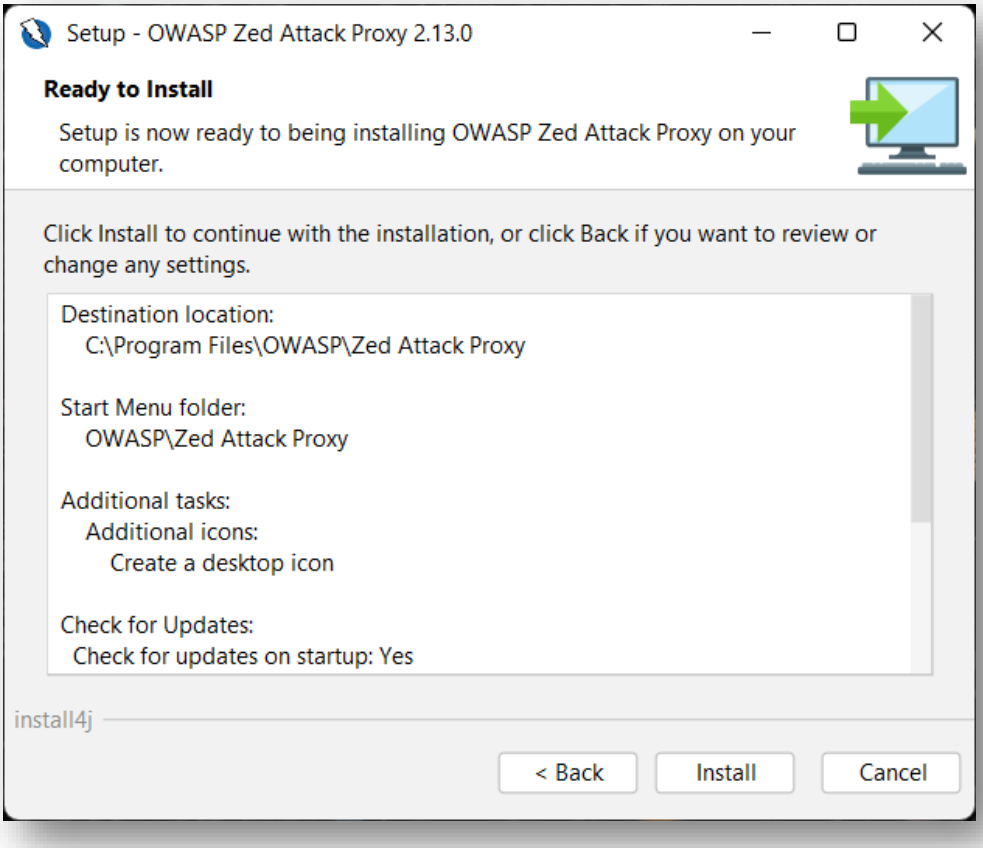
OWASP ZAP

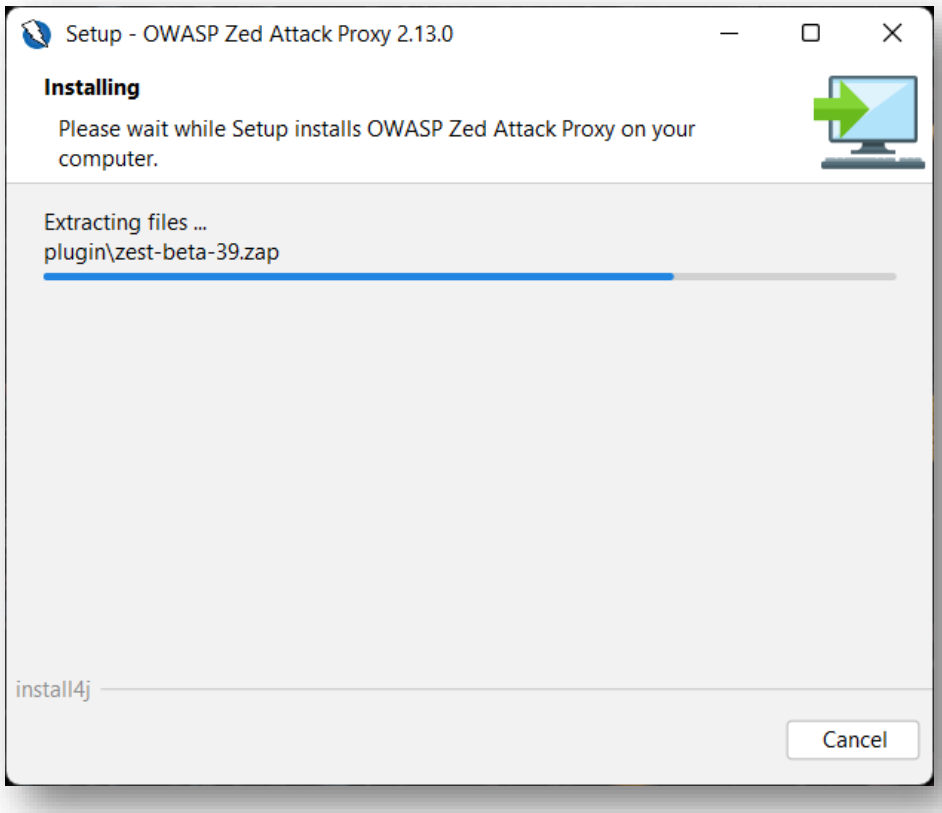
1. First download the appropriate installer based on operating system requirements from official page: https://www.zaproxy.org/download/



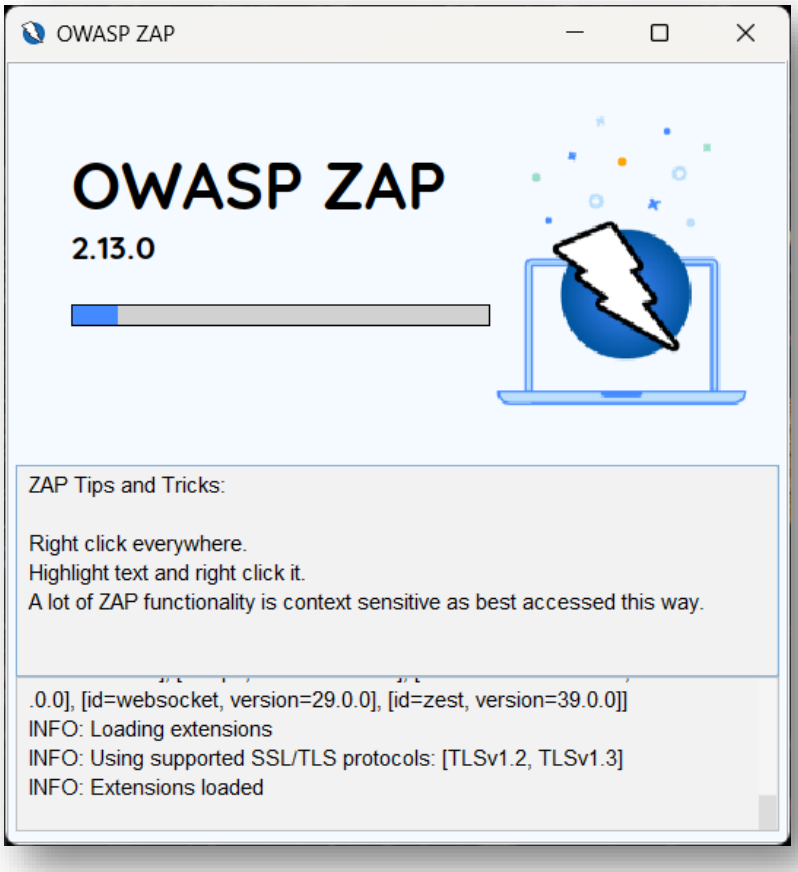
2. After installation is completed launch the ZAP and agree the license terms by clicking the check box.



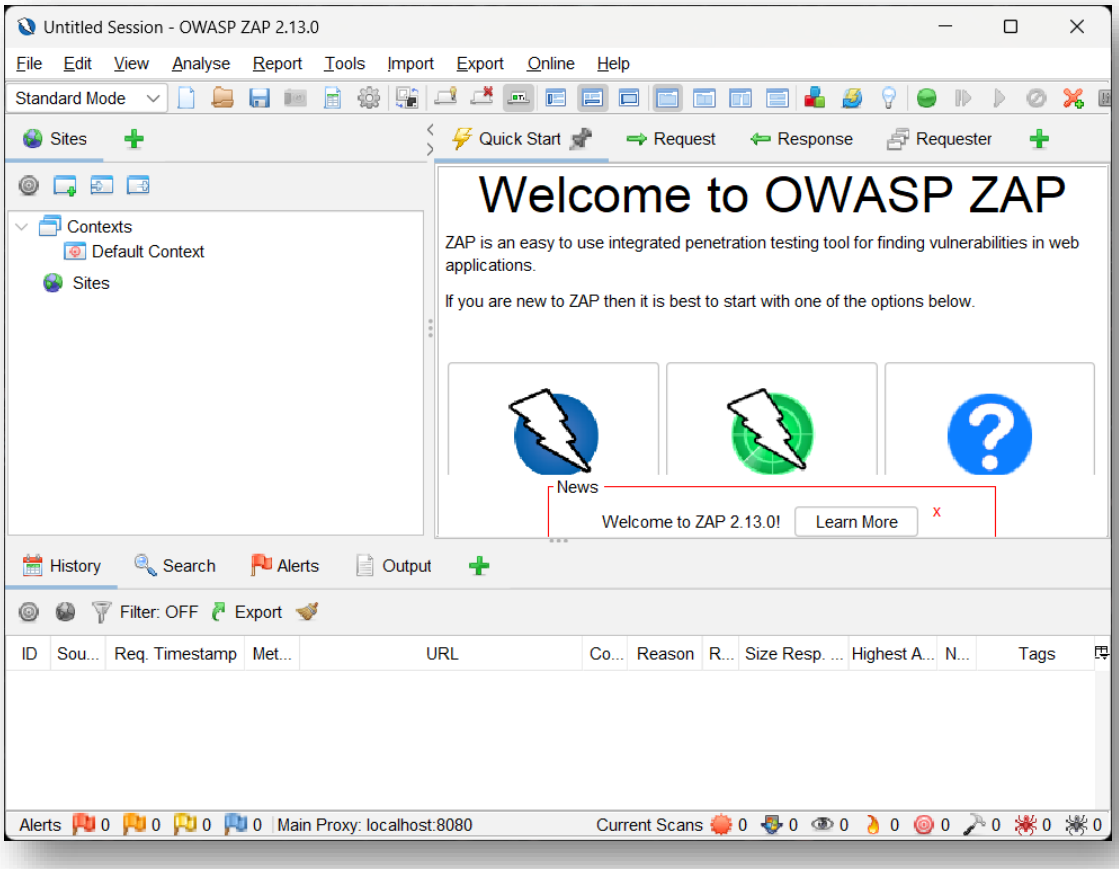

Setup - OWASP Zed Attack Proxy 2.13.0
Ready to Install
Setup is now ready to being installing OWASP Zed Attack Proxy on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\OWASP\Zed Attack Proxy
Start Menu folder:
OWASP\Zed Attack Proxy
Additional tasks:
Additional icons:
Create a desktop icon
Check for Updates:
Check for updates on startup: Yes
install4j
< Back
Install
Cancel


Setup - OWASP Zed Attack Proxy 2.13.0
Installing
Please wait while Setup installs OWASP Zed Attack Proxy on your computer.
Extracting files ...
plugin\zest-beta-39.zap
install4j
Cancel


Setup - OWASP Zed Attack Proxy 2.13.0
Completing the OWASP Zed Attack Proxy Setup Wizard
Setup has finished installing OWASP Zed Attack Proxy on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Finish


OWASP ZAP
OWASP ZAP
2.13.0
ZAP Tips and Tricks:
Right click everywhere.
Highlight text and right click it.
A lot of ZAP functionality is context sensitive as best accessed this way.
.0.0], [id=websocket, version=29.0.0], [id=zest, version=39.0.0]]
INFO: Loading extensions
INFO: Using supported SSL/TLS protocols: [TLSv1.2, TLSv1.3]
INFO: Extensions loaded

3. ZAP desktop UI will open after installation is finished.



References

1. https://solutionnetsystems.com/solutions/automated-scanning/
2. https://www.coresecurity.com/blog/top-14-vulnerability-scanners-cybersecurity-professionals
3. https://www.getastra.com/blog/security-audit/web-application-vulnerability-scanner/
4. https://snyk.io/learn/vulnerability-scanner/
5. https://blog.rsisecurity.com/7-types-of-vulnerability-scanners/