Web Application Vulnerability Scanning using OWASP ZAP LAB

1. Start and login to your Kali Linux virtual machine as user kali with a password of **kali**.

2. In Kali Linux, click the menu in the upper left, then choose **03 – Web Application Analysis**, then choose **ZAP**. This the OWASP Zed Attack Proxy (ZAP) web app proxy and vulnerability scanning tool. When prompted to persist the session, choose **No, I do not want to persist this session at this moment in time** and then click **Start.** If you are prompted to update ZAP, click **Update All** then click **Close**. Always ensure that vulnerability scanning tools are kept up to date.

3. Start and login to your Metasploitable2 virtual machine as user msfadmin with a password of **msfadmin**.

4. Type ifconfig and take note of the IP address.

5. Switch back to Kali Linux where the ZAP tool is running

6. Click Automated Scan.

7. In the URL To Attack field, enter **http://IP_Address_From_4**.

8. Next to **Use Ajax Spider**, ensure the checkmark is enabled and choose **Firefox** from the dropdown list. Click **Attack**. This will spawn a Firefox instance that will test all aspects of the Metasploitable2 web application.

9. Switch back to OWASP Zap. Notice the items appearing down under the **Ajax Spider** tab.

10. Click the **Alerts** tab at the bottom and notice some of the discovered web application vulnerabilities. In OWASP Zap, click the **Stop** button.