Task 7: Identify and Remove Suspicious Browser Extensions

In this task, the objective was to review the installed browser extensions, identify any suspicious or unused ones, and remove them to improve security and performance. This process is crucial in preventing potential cyber threats that may originate from malicious browser add-ons.

Steps Taken:

- Opened the browser’s extension/add-ons manager.
- Reviewed all installed extensions carefully to identify their purpose.
- Checked permissions and online reviews for each extension.
- Identified an unused extension named 'Wappalyzer', which was removed.
- Retained only trusted extensions: Google Docs Offline and McAfee WebAdvisor.
- Restarted the browser to apply the changes and ensure smooth performance.
- Verified that no suspicious or unnecessary extensions remained.

How Malicious Extensions Can Harm Users:

- Stealing sensitive information such as passwords and browsing history.
- Injecting malicious advertisements or redirecting to phishing sites.
- Tracking user activity without consent.
- Slowing down browser performance or causing crashes.
- Installing additional unwanted software in the background.

By removing unused or suspicious extensions, the browser becomes more secure and efficient. This proactive step reduces the risk of data theft, privacy breaches, and system performance issues.