**CHECKLIST**

**MOZILLA FIREFOX**

1 Configure Locked Preferences

2 Updating Firefox

3 Network Settings

4 Encryption Settings

5 JavaScript Settings

6 Privacy Settings

7 Extensions and Add-ons

8 Malware Settings

* 1. ***(L1) Create local-settings.js file***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type app.update in the filter

3. Ensure the preferences listed are set to the values specified below

**general.config.obscure\_value=0**

**general.config.filename=mozilla.cfg**

**Remediation:**

Perform the following procedure:

1. Navigate to the defaults/pref directory inside the Firefox installation directory and create a file called local-settings.js.

2. Include the following lines in local-settings.js:

pref("general.config.obscure\_value", 0); pref("general.config.filename", "mozilla.cfg");

***1.3 (L1) Create mozilla.cfg file***

**Audit:**

Perform the following procedure:

1. Navigate to the Firefox installation directory and ensure there is a file called mozilla.cfg.

2. Ensure the first line of the file is a comment: **//**

**Remediation:**

Perform the following procedure:

1. Navigate to the Firefox installation directory and create a file called mozilla.cfg.

2. The first line of the file must be a comment**: //**

***2.1 (L1) Enable Automatic Updates***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type app.update.auto in the filter

3. Ensure the preferences listed are set to the values specified below:

**app.update.enabled=true app.update.auto=true app.update.staging.enabled=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("app.update.enabled", true); lockPref("app.update.auto", true); lockPref("app.update.staging.enabled", true);**

***2.2 (L1) Enable Auto-Notification of Outdated Plugins***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type plugins.update.notifyUser in the filter

3. Ensure the preferences listed are set to the values specified below:

plugins.update.notifyUser=true

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

lockPref("plugins.update.notifyUser", true);

***2.3 (L1) Enable Information Bar for Outdated Plugins***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type plugins.hide\_infobar\_for\_outdated\_plugin in the filter

3. Ensure the preferences listed are set to the values specified below:

**plugins.hide\_infobar\_for\_outdated\_plugin=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("plugins.hide\_infobar\_for\_outdated\_plugin", false);**

***2.4 (L1) Set Update Interval Time Checks***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type app.update.interval in the filter

3. Ensure the preferences listed are set to the values specified below:

**app.update.interval=43200**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("app.update.interval", 43200);**

***2.5 (L1) Set Update Wait Time Prompt***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type app.update.promptWaitTime in the filter

3. Ensure the preferences listed are set to the values specified below:

app.update.promptWaitTime=172800

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

lockPref("app.update.promptWaitTime", 172800)

***2.6 (L1) Ensure Update-related UI Components are Displayed***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type app.update.silent in the filter

3. Ensure the preferences listed are set to the values specified below:

**app.update.silent=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("app.update.silent", false);**

***2.7 (L1) Set Search Provider Update Behavior***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.search.update in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.search.update=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.search.update", true);**

***3.2 (L2) Do Not Send Cross SSL/TLS Referrer Header***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.http.sendSecureXSiteReferrer in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.http.sendSecureXSiteReferrer=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.http.sendSecureXSiteReferrer", false);**

***3.3 (L1) Disable NTLM v1***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.auth.force-generic-ntlm-v1 in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.auth.force-generic-ntlm-v1=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.auth.force-generic-ntlm-v1", false);**

***3.4 (L1) Enable Warning For "Phishy" URLs***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.http.phishy-userpass-length in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.http.phishy-userpass-length=1**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.http.phishy-userpass-length", 1);**

***3.5 (L2) Enable IDN Show Punycode***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.IDN\_show\_punycode in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.IDN\_show\_punycode=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.IDN\_show\_punycode", true);**

***3.6 (L1) Set File URI Origin Policy***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.fileuri.strict\_origin\_policy in the filter

3. Ensure the preferences listed are set to the values specified:

**security.fileuri.strict\_origin\_policy=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.fileuri.strict\_origin\_policy", true)**

***3.7 (L1) Disable Cloud Sync***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type services.sync.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**services.sync.enabled=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("services.sync.enabled", false);**

***3.8 (L1) Disable WebRTC***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type media.peerconnection in the filter

3. Ensure the preferences listed are set to the values specified below:

**media.peerconnection.enabled=false media.peerconnection.use\_document\_iceservers=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("media.peerconnection.enabled", false); lockPref("media.peerconnection.use\_document\_iceservers", false);**

***4.1 (L2) Set SSL Override Behavior***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.ssl\_override\_behavior in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.ssl\_override\_behavior=0**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.ssl\_override\_behavior", 0);**

***4.2 (L1) Set Security TLS Version Maximum***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.tls.version.max in the filter

3. Ensure the preferences listed are set to the values specified below:

**security.tls.version.max=3**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.tls.version.max", 3**

***4.3 (L1) Set Security TLS Version Minimum***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.tls.version.min in the filter

3. Ensure the preferences listed are set to the values specified below:

**security.tls.version.min=1**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.tls.version.min", 1)**

***4.4 (L2) Set OCSP Use Policy***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.OCSP.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**security.OCSP.enabled=1**

Note: Configuring this setting to 2 also conforms with this benchmark.

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.OCSP.enabled", 1)**

***4.5 (L1) Block Mixed Active Content***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.mixed\_content.block\_active\_content in the filter

3. Ensure the preferences listed are set to the values specified below:

**security.mixed\_content.block\_active\_content=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.mixed\_content.block\_active\_content", true)**

***4.6 (L2) Set OCSP Response Policy***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.ocsp.require in the filter

3. Ensure the preferences listed are set to the values specified below:

**security.ocsp.require=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.ocsp.require", true);**

***5.1 (L1) Disallow JavaScript's Ability to Change the Status Bar Text***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type dom.disable\_window\_status\_change in the filter

3. Ensure the preferences listed are set to the values specified below:

**dom.disable\_window\_status\_change=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("dom.disable\_window\_status\_change", true);**

***5.2 (L1) Disable Scripting of Plugins by JavaScript***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.xpconnect.plugin.unrestricted in the filter

3. Set the preference listed with the values specified below:

**security.xpconnect.plugin.unrestricted=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.xpconnect.plugin.unrestricted", false);**

***5.3 (L1) Disallow JavaScript's Ability to Hide the Address Bar***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type dom.disable\_window\_open\_feature.location in the filter

3. Ensure the preferences listed are set to the values specified below:

**dom.disable\_window\_open\_feature.location=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("dom.disable\_window\_open\_feature.location", true);**

***5.4 (L1) Disallow JavaScript's Ability to Hide the Status Bar***

**Audit:**

Perform the following procedure:

1. Type about.config in the address bar

2. Type dom.disable\_window\_open\_feature.status in the filter

3. Ensure the preferences listed are set to the values specified below:

**dom.disable\_window\_open\_feature.status=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("dom.disable\_window\_open\_feature.status", true)**

***5.5 (L1) Disable Closing of Windows via Scripts***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type dom.allow\_scripts\_to\_close\_windows in the filter

3. Ensure the preferences listed are set to the values specified below:

**dom.allow\_scripts\_to\_close\_windows=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("dom.allow\_scripts\_to\_close\_windows", false);**

***5.6 (L1) Block Pop-up Windows***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type privacy.popups.policy in the filter

3. Ensure the preferences listed are set to the values specified below:

**privacy.popups.policy=1**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("privacy.popups.policy", 1);**

***5.7 (L1) Disable Displaying JavaScript in History URLs***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.urlbar.filter.javascript in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.urlbar.filter.javascript=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.urlbar.filter.javascript", true);**

***6.1 (L1) Disallow Credential Storage***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type signon.rememberSignons in the filter

3. Ensure the preferences listed are set to the values specified below:

**signon.rememberSignons=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

49 | P a g e

**lockPref("signon.rememberSignons", false);**

***6.2 (L1) Do Not Accept Third Party Cookies***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.cookie.cookieBehavior in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.cookie.cookieBehavior=1**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.cookie.cookieBehavior", 1);**

***6.4 (L1) Set Delay for Enabling Security Sensitive Dialog Boxes***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type security.dialog\_enable\_delay in the filter

3. Ensure the preferences listed are set to the values specified below:

**security.dialog\_enable\_delay=2000**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("security.dialog\_enable\_delay", 2000);**

***6.5 (L1) Disable Geolocation Serivces***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type geo.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**geo.enabled=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("geo.enabled", false);**

***7.1 (L1) Secure Application Plug-ins***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.helperApps.alwaysAsk.force in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.helperApps.alwaysAsk.force=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.helperApps.alwaysAsk.force", true);**

**7.2 (L1) Disabling Auto-Install of Add-ons**

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type xpinstall.whitelist.required in the filter

3. Ensure the preferences listed are set to the values specified below:

**xpinstall.whitelist.required=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("xpinstall.whitelist.required", true);**

***7.3 (L1) Enable Extension Block List***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type extensions.blocklist.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**extensions.blocklist.enabled=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("extensions.blocklist.enabled", true);**

***7.4 (L1) Set Extension Block List Interval***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type extension.blocklist.interval in the filter

3. Ensure the preferences listed are set to the values specified below:

**extensions.blocklist.interval=86400**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("extensions.blocklist.interval", 86400);**

***7.5 (L1) Enable Warning for External Protocol Handler***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.protocol-handler.warn-external-default in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.protocol-handler.warn-external-default=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.protocol-handler.warn-external-default", true);**

***7.6 (L1) Disable Popups Initiated by Plugins***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type privacy.popups.disable\_from\_plugins in the filter

3. Ensure the preferences listed are set to the values specified below:

**privacy.popups.disable\_from\_plugins=2**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("privacy.popups.disable\_from\_plugins", 2)**

***7.7 (L1) Enable Extension Auto Update***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type extensions.update.autoUpdateDefault in the filter

3. Ensure the preferences listed are set to the values specified below:

**extensions.update.autoUpdateDefault=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("extensions.update.autoUpdateDefault", true)**

***7.8 (L1) Enable Extension Update***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type extensions.update.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**extensions.update.enabled=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("extensions.update.enabled", true)**

***7.9 (L1) Set Extension Update Interval Time Checks***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type extensions.update.interval in the filter

3. Ensure the preferences listed are set to the values specified below:

**extensions.update.interval=86400**

Note: A value less than 86400 is in conformance with this benchmark.

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("extensions.update.interval", 86400)**

***8.1 (L1) Enable Virus Scanning for Downloads***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.download.manager.scanWhenDone in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.download.manager.scanWhenDone=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.download.manager.scanWhenDone", true);**

***8.2 (L1) Disable JAR from Opening Unsafe File Types***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type network.jar.open-unsafe-types in the filter

3. Ensure the preferences listed are set to the values specified below:

**network.jar.open-unsafe-types=false**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("network.jar.open-unsafe-types", false);**

***8.3 (L1) Block Reported Web Forgeries***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.safebrowsing.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.safebrowsing.enabled=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.safebrowsing.enabled", true);**

***8.4 (L1) Block Reported Attack Sites***

**Audit:**

Perform the following procedure:

1. Type about:config in the address bar

2. Type browser.safebrowsing.malware.enabled in the filter

3. Ensure the preferences listed are set to the values specified below:

**browser.safebrowsing.malware.enabled=true**

**Remediation:**

Perform the following procedure:

1. Open the mozilla.cfg file in the installation directory with a text editor

2. Add the following lines to mozilla.cfg:

**lockPref("browser.safebrowsing.malware.enabled", true);**