FIREFOX SETUP

Extract from book “Open Source Intelligence Techniques written by Michael Bazzell

If we want to do OSINT properly, we need a good browser. Statistics show us that most people use Chrome. It is an excellent browser that is known for being very fast and responsive. Chrome is also very secure by nature, but compromises privacy since Google receives a lot of data about our internet usage.
Ubuntu offers us a valid alternative because it offers Firefox by default. There are many reasons for choosing Firefox. Some of the most important are as follows

- Firefox uses less memory compared to Chrome.
- Firefox Adopts Mindset Open-Source.
- Firefox looks out for your privacy.
- Firefox is more customizable.
- Firefox provides unique extensions.

Downloading and installing Firefox is no different than any other application. However, pay attention when installing and executing, choose not to import any settings from other browser. This will keep your browser clean from unwanted data.

We can download firefox on this page. We suggest choosing the English us version. https://www.mozilla.org/it/firefox/all/#product-desktop-release

We now are ready changing the following settings within Firefox

1. Click on the menu in the upper right and select “Setting”, “Options”, or Preferences
2. In the “General” options, uncheck both “Recommend extensions as you browse” and Recommend features as you browse”. This prevents some interest usage information from being sent to Firefox

3. In the “Home” options, change “Homepage and new windows” and “New Tabs” to “Blank page”. This prevents Firefox from loading their services in new pages and tabs
4. Disable all Firefox “Home Content” options
5. In the “Privacy & Security” options, enable “Delete cookies and site data when Firefox is closed”. This cleans things up when you exit the browser
6. Uncheck all options under “Logins and Passwords”
7. Change the History setting to “Firefox will use custom settings for history”
8. Uncheck the box titled “Remember browsing and download history
9. Uncheck the box titled “Remember search and form history”
10. Check the box titled “Clear history when Firefox closes”
11. Do NOT check the box titled “Always use private browsing mode”, as this will break Firefox Containers
12. Uncheck “Browsing history” from the “Address Bar” menu
13. In the “Permission” menu click “Setting” next to Location, Camera, Microphone, and notifications. Check the box titled “Block new requests…” for each of these options
14. Uncheck all options under “Firefox Data Collection and use”
15. Uncheck all options under “Deceptive Content and Dangerous Software Protection”. This will prevent Firefox from sharing potential malicious site visits with third-party services. This leaves us more exposed to undesired software attacks (we are however into the VM), but protects our history from being shared with Google
16. Enable “HTTPS-Only Mode in all windows

Because the list of about:config settings contains hundres of entries, you should search for all of these through the search bar in the about:config tab. The settings in the following examples are desired options. We would want the first example to be changed to FALSE

- geo.enabled: FALSE: this disable Firefox from sharing your location
- dom.battery.enabled: FALSE: this setting blocks sending battery level information

- extensions.pocket.enabled: FALSE: this disables the proprietary Pocket service
- browser.newtabpage.activity-stream.section.highlights.includePocket: FALSE
- services.sync.prefs.sync.browser.newtabpage.activity-stream.section.highlights.includePocket: FALSE
- browser.newtabpage.activity-stream.feeds.telemetry: FALSE: disable Telemetry
- browser.ping-centre.telemetry: FALSE: Disables Telemetry
- toolkit.telemetry.server: (delete URL): Disable Telemetry
- toolkit.telemetry.unified: FALSE: Disable Telemetry
- media.autoplay.default: 5: Disables audio and video from playing automatically
- down.webnotifications.enabled: FALSE: disables embedded notifications
- privacy.resistFingerprinting: TRUE:Disables some fingerprinting
- webgl.disabled: TRUE: Disable some fingerprinting
- network.http.sendRefererHeader: 0: Disables referring website notifications
- identity.fxaccounts.enabled:FALSE: Disables any embedded Firefox accounts
- Browser.tabs.crashReporting.sendReport: FALSE: Disables crash reporting
- Pdfjs.enableScripting:FALSE: prevents some malicious PDF actions
- Network.dns.disablePrefetch: TRUE: Disables prefetching
- Network.dns.disablePrefetchFromHTTPS: FALSE: Disables prefetching
- Network.prefetch-next:FALSE: Disables prefetching