Network and Web Security

Chrome and Burp in Kali *

February 8, 2021

1 Installing Google Chrome

Google Chrome is the reference browser for the web security segment of this course. Unfortunately, it isn't available in the Kali Linux repositories, so if you want to use it during the labs, you'll have to install its dependencies and then install Chrome manually from Google's website.

1. In a terminal in `kali-vm`, type `apt-get install libappindicator1` to manually install `libappindicator` from the Kali repositories. Confirm the installation when prompted by entering `y`.
2. Download Chrome from `https://www.google.com/chrome/`. Choose the **64 bit .deb (For Debian/Ubuntu)** version.
3. Run `dpkg -i /root/Downloads/google-chrome-stable_current_amd64.deb` to install the package after it finishes downloading.
4. Chrome won't run as `root` for security reasons, so you'll need to create a separate, unprivileged user account just for Chrome: type `adduser chrome`, and enter a new password for this account twice when prompted. The other information is optional; you don't have to enter anything except the password. The account will be created when you confirm that the information is correct (type `y`).
5. Start Chrome either by running it as the `chrome` user as `root` (e.g. `gksu -lu chrome google-chrome` — check **Do not display this message again** and click **Close**), or by logging in to Kali as the newly-created `chrome` user and selecting **Google Chrome** from the *Applications* menu.

After installing Chrome like this, you'll receive updates for it via Kali's normal package-updating mechanism.

2 Setting up Burb

Although it's possible to find vulnerabilities in web applications using just a web browser, a good intercepting proxy makes it easier. The free version of Burp Suite is pre-installed on Kali. It offers, amongst other tools, an *intercepting web proxy*. After configuring your web browser to use Burp's proxy as its HTTP proxy, it logs all HTTP requests and responses that pass between your browser and web servers. Two of its most useful features are the ability to *tamper* with requests and responses in-flight, and the ability to *replay* earlier requests.

To use Burp Suite's intercepting proxy in `kali-vm`:

1. Open Burp Suite from the **Applications** → **03 – Web Application Analysis** menu.
2. Choose **Temporary project**, and click **Next**.

*Based on material prepared by Chris Novakovic `c.novakovic@imperial.ac.uk` in 2017. Some links and commands may have changed slightly.

3. Choose **Use Burp defaults**, check **Default to this option in future**, and click **Start Burp**.
4. In the main Burp Suite window, click on the **Proxy** tab, then the **Options** sub-tab.
5. Under **Proxy Listeners**, make a note of the IP address and port number that Burp's proxy is listening on. It'll probably be `127.0.0.1:8080`. Make sure the **Running** box next to the IP address is checked.

Refer to the online documentation of Chrome and/or Firefox for how to tell your browser of choice to use Burp (at the address above) as an *HTTP proxy*.

2.1 The proxy as a MITM

We have seen in Module 9 that the use of TLS would hinder the operation of a MITM, and therefore also of an intercepting proxy such as Burp. In order to intercept HTTPS requests and responses, as shown in the "Certificate trust" slide, Burp needs to present its own certificates for communication between itself and the browser, and behave like a regular HTTPS client when communicating with the real HTTPS server that the browser was trying to communicate with. For this to work, the browser will need to trust the root CA certificate that Burp uses to sign its own certificates ("Portswigger CA"); you'll need to import it into each browser's certificate store. Don't do this "at home": you don't want to import custom CAs on the browser that you use for emails, banking, work, and other sensitive activities, as a rogue CA could sign spoofed certificates!

1. In your Kali browser (Firefox or Chrome), set Burp as the active proxy and download its root CA certificate from `http://burp/cert`. Save it to `/tmp/cacert.der`.
2. In Firefox, click the **Open menu** icon in the main toolbar and click **Preferences**.
3. On the *Advanced* pane, open the **Certificates** tab and click **View Certificates**.
4. On the *Authorities* tab, click **Import…**.
5. Browse to `/tmp/cacert.der`, then click **Open**.
6. Check **Trust this CA to identify websites**, then click **OK**. The certificate will now be imported into Firefox's certificate store, and will not show a warning message when you use Burp to intercept HTTPS traffic in Firefox.
7. Click **OK**, and close Firefox's *Preferences* tab.
8. In Chrome, visit `chrome://settings/certificates`.
9. On the *Authorities* tab, click **Import…**.
10. In the file format filter dropdown box, select **All Files**. Browse to `/tmp/cacert.der`, then click **Open**.
11. Check **Trust this certificate for identifying websites**, then click **OK**. The certificate will now be imported into Chrome's certificate store, and will not show a warning message when you use Burp to intercept HTTPS traffic in Chrome.
12. Click **Finished**, and close Chrome's *Settings* tab.