Network and Web Security

Chrome and Burp in Kali *

February 5, 2024

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 it manually. Alternatively, you can just skip this step and happily use the preinstalled Firefox, which is a perfectly fine alternative.

1. In a terminal in `kali-vm`, download the right package:
   `curl -O https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb`
2. Let's update `apt`, just in case: `sudo apt update`
3. Next, install it: `sudo apt install ./google-chrome-stable_current_amd64.deb`
   Confirm the installation when prompted by entering `y`

After installing Chrome like this, you can run it from the command line using the command `google-chrome`.

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**.
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 **Proxy settings** 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. Close the settings tab.
6. In Firefox, go to Settings, scroll down to Network Settings and select the manual proxy configuration, using the address and port above for both HTTP proxy and HTTPs proxy.

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

7. For Chrome, we need to set the proxy settings via command line parameters.

   i Create a file called `chrome` with the content:

   ```
   #!/bin/bash
   echo "Starting Chrome in interceptor mode..."
   google-chrome \
   --proxy-server="http=127.0.0.1:8080;https=127.0.0.1:8080" \
   > /dev/null 2> /dev/null & # run in the background and be quiet
   ```

   ii Give yourself permission to execute it: `chmod u+x chrome`

   iii You can now run Chrome with Burp using the command: `./chrome`

   iv If Chrome seems to ignore the directive to use the proxy, try repeating the step 1 above using:

   ```
   --proxy-server="http://127.0.0.1:8080" \
   --proxy-server="https://127.0.0.1:8080" \
   ```

   instead of the corresponding line above.

8. Now experiment with using the **Proxy/Intercept** sub-tab of Burb: you can toggle intercept on or off, and when a request is intercepted, you can modify it, forward it, drop it as desired.

2.1 The proxy as a MITM

We have seen in Module 11 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, open the settings and search for "certificates" in the settings search bar.

   i Click on the **View Certificates...** suggestion.

   ii On the *Authorities* tab, click **Import...**.

   iii Browse to `/tmp/cacert.der`, then click **Open**.

   iv 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.

   v Click **OK**, and close Firefox's *Preferences* tab.

3. In Chrome, visit `chrome://settings/certificates`.

   i On the *Authorities* tab, click **Import**.

   ii In the file format filter dropdown box, select **All Files**. Browse to `/tmp/cacert.der`, then click **Select**.

   iii 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.

   iv Close Chrome's *Settings* tab.