Non-SSL & SSL Interception

Table of Contents

[Requirements 1](#_Toc494028780)

[Server Setup 1](#_Toc494028781)

[Client Setup (Non-SSL) 2](#_Toc494028782)

[Chromium 2](#_Toc494028783)

[FireFox 2](#_Toc494028784)

[Demos (Non-SSL) 2](#_Toc494028785)

[Client Setup (SSL) 2](#_Toc494028786)

[Demos (SSL) 2](#_Toc494028787)

# Requirements

* Linux VM – My recommendation is LUbuntu
* Burp 1.7.03

# Server Setup

Download the last version of Burp that is both x64 and x86: [burpsuite\_free\_v1.7.03.jar](https://portswigger.net/burp/releases/download?product=free&version=1.7.03&type=jar) from <https://portswigger.net/burp/releasesarchive/free>

Launch Burp by using the following command:

sudo java -jar -Xmx2G ./burpsuite\_free\_v1.7.03.jar

Set it up as follows:

1. Temporary Project -> Next
2. Use Burp Defaults -> Start Burp
3. Select the “Proxy” tab
4. Select the “Options” subtab
5. Under “Proxy Listeners”
   1. Select the first element in the list and click edit
      1. Under the binding subtab
      2. Bind to Address -> Bind to All Interfaces
      3. Under “Request Handling”
      4. Check “Support invisible proxying”
6. Under “Intercept Server Responses”
   1. Check “Intercept Responses”

# Client Setup (Non-SSL)

After setting up the browsers below have each client browse to an unencrypted site such as Dell.com. Burp should trap those requests.

## Chromium

chromium-browser --proxy-server="192.168.168.100:8080"

Make sure no other instance is running

## FireFox

Firefox -proxy-server proxy.example.com

## Google Chrome

google-chrome --proxy-server="192.168.168.100:8080"

## Neither Working?

If any of these cases don’t work then go through the browser’s specific proxy settings. Set it up using your IP and proxy for all proxy settings.

# Demos (Non-SSL Interception)

## Demo 1 Dynamically Replacing Content

Add Match and Replace Rule as Follows

* Type: Reponse Body
* Match “Product”
* Replace “Prof\_Clark”

Browse Dell.com from the clients

Show them what Dell’s certificate chain looks like:

* Using Firefox click on the lock and select the right arrow next to the domain you are on. Select “More Information”. Another way to get to this same information is hitting Alt+T and selecting Page Info -> Security
* Click “View Certificate”
* Click “Details”

This will display the chain of certificates. Look through those. Note the root certificate. Now go to the Certificate store and find it.

* Using Firefox hit the menu button and select “Preferences”
* Select “Advanced” -> Certificate Tab -> “View Certificates”

Look through the certificate store and see which ones look interesting.

# Client Setup (SSL Interception)

1. Have the clients browse the IP and port of the proxy
2. Click CA Certificate
3. This will download the certificate. You can’t directly import it
4. Manually import it using the browser certificate manager. Check all certificate options at import

# Demos (SSL Interception)

1. Under “Intercept Client Requests”
2. Add
3. Operator “Add”
4. Type: “Body”
5. Relationship: “Matches”
6. Condition: “Password”
7. Under “Intercept”
8. Click the Intercept button so that is shows “Intercept is On”
9. Have a client try to log into Dell.com. You will see the response get intercepted

Show them what Dell’s certificate chain looks like:

* Using Firefox click on the lock and select the right arrow next to the domain you are on. Select “More Information”. Another way to get to this same information is hitting Alt+T and selecting Page Info -> Security
* Click “View Certificate”
* Click “Details”
* You will now see that it is signed by PortSwigger