NEST Kali Linux Tutorial: Burp Suite

"Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun."

Catherine Zittlosen

Ruth Karkiewicz

November 2013

http://www.portswigger.net/burp/

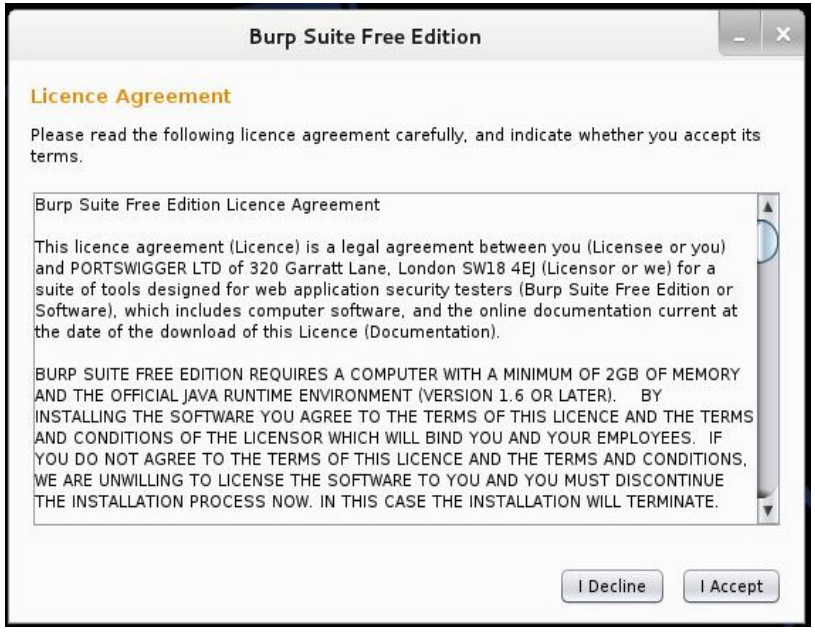
UNM CENTER for INFORMATION ASSURANCE RESEARCH and EDUCATION (CIARE)

Introduction

- Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Launch Burp Suite

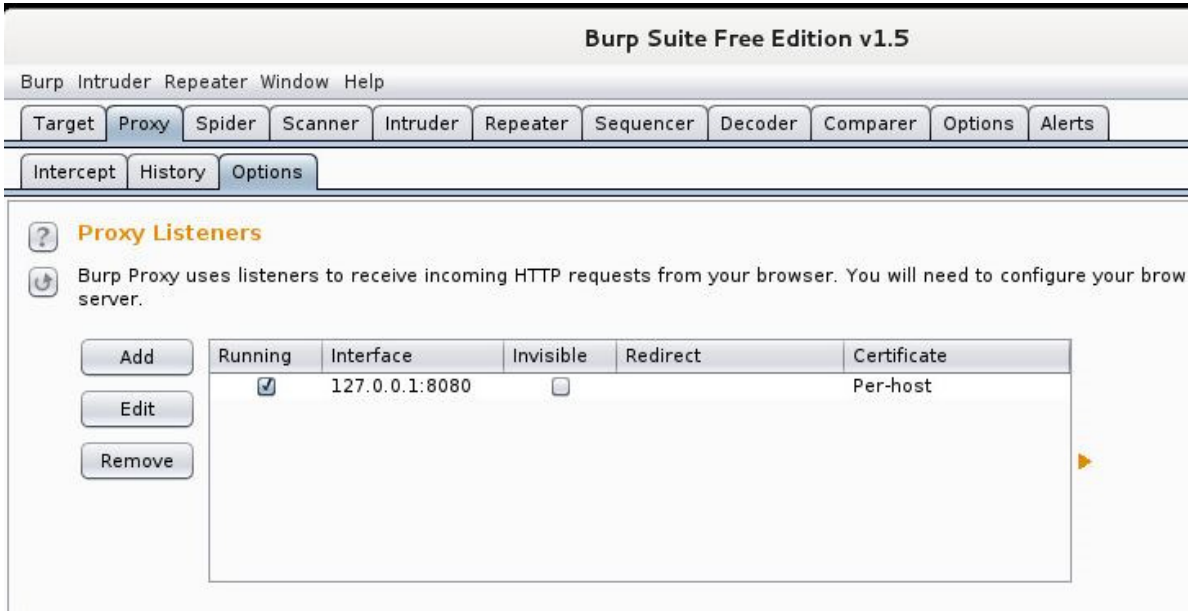
- Applications > Kali Linux > Top 10 Security Tools > burpsuite
- Accept the license agreement.



- The program will launch after a few seconds.

Start Proxy

- Check that the proxy is running by clicking on
  - Proxy > Options
- There should be a check box under the "Running" column to indicate that the proxy is running.

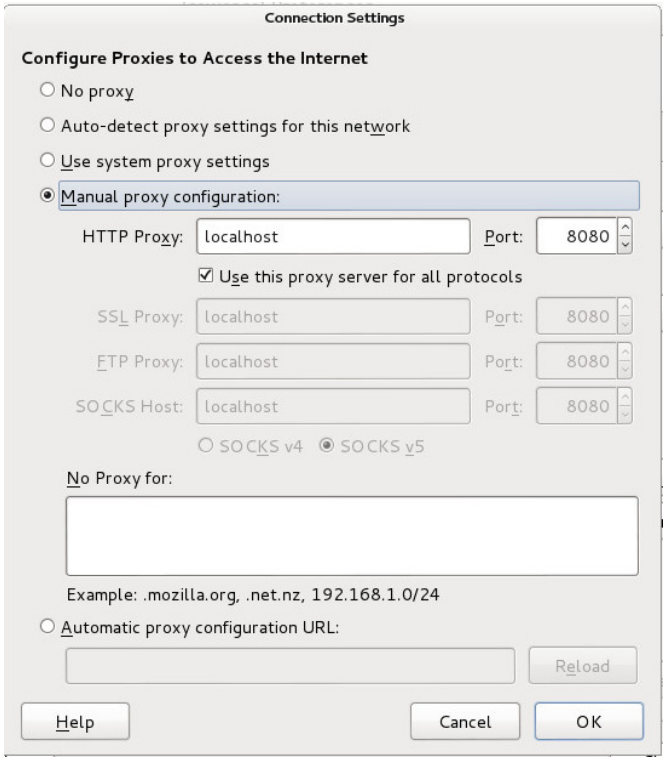


Configure Browser

- Launch Iceweasel Internet browser
  - Applications > Internet > Iceweasel Web Browser
- In Iceweasel Web Browser go to
  - Edit > Preferences > Advanced > Network > Settings…

Proxy Settings

- Select “Manual proxy configuration”
- Enter “localhost” in “HTTP Proxy” and set it to port “8080”
- Check “Use this proxy server for all protocols”
- Delete everything in the “No Proxy for” box.
- Select “OK” and then “Close”.

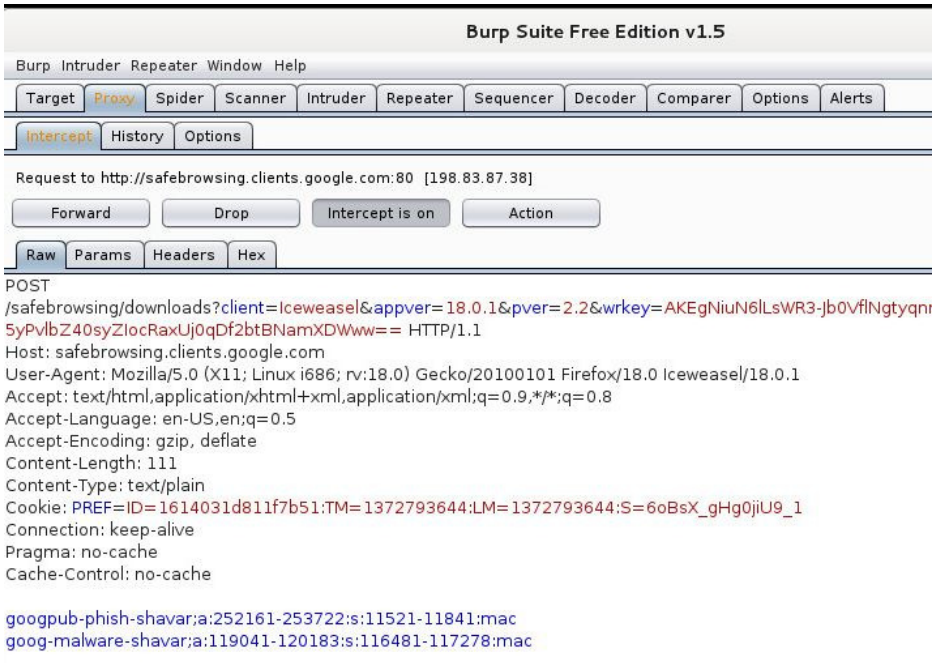


Test Browser

- With Burp running, in your browser go to any HTTP URL.
  - You can use “www.thinkgeek.com” if you want
- Your browser should sit waiting for the request to complete.

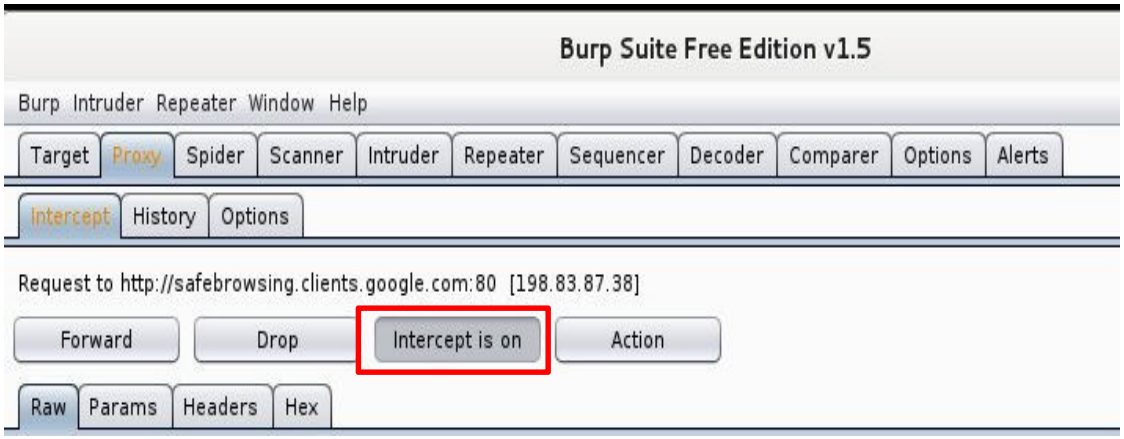
Test Browser Cont.

- In Burp, go to Proxy > Intercept
- These tabs should be highlighted, and there should be an HTTP request showing in the main panel.



Test Browser Cont.

- Click on the "Intercept is on" button so that it says "Intercept is off".
- Go back to your browser, and you should (shortly) see the URL you requested being loaded in the normal way.



Using Burp Proxy

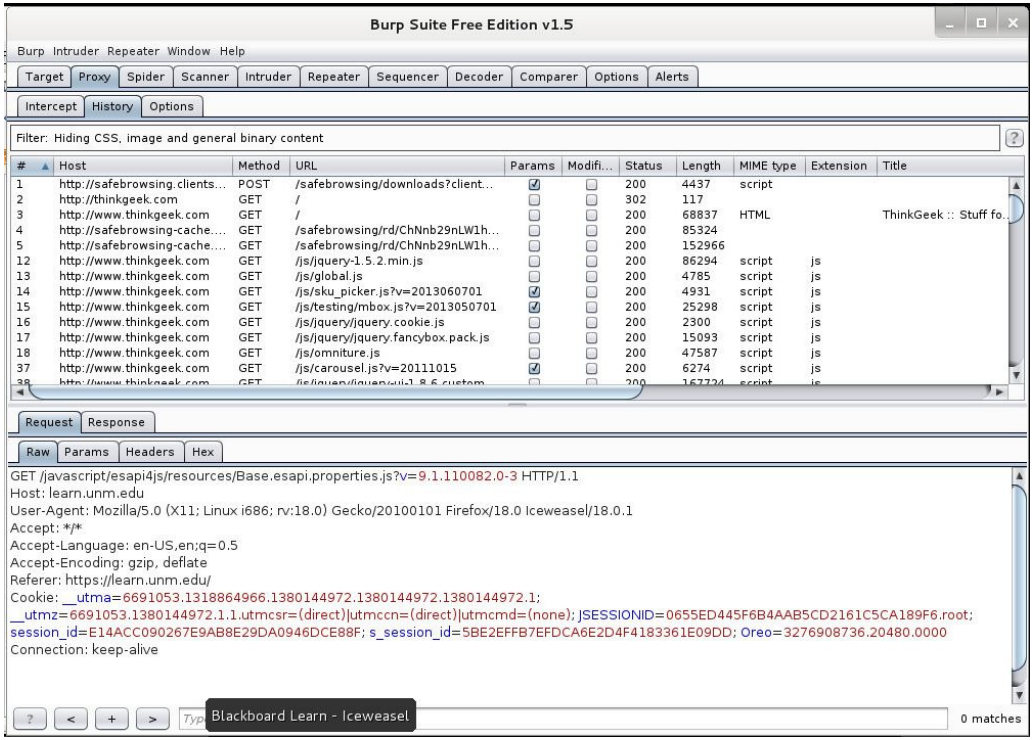
- Each HTTP request made by your browser is displayed in the Intercept tab. You can view each message, and edit it.
- Click on the “Intercept is on” button in Burp Suite
- Browse to “nest.unm.edu” in Iceweasel
- You can view the request in Burp Suite.
- Click through each of the message editor tabs (Raw, Headers, etc.) to see the different ways of analyzing the message.

Forward Request

- Click the "Forward" button to send the request on to the destination web server (repeat if necessary).
- In most cases, your browser will make more than one request in order to display the page (for images, etc.). Look at each subsequent request and then forward it to the server. When there are no more requests to forward, your browser should have finished loading the URL you requested.
- You can toggle the "Intercept is on / off" button in order to browse normally without any interception.

History

- As you browse via Burp, the Proxy history keeps a record of all requests and responses.
- Go to Proxy > History

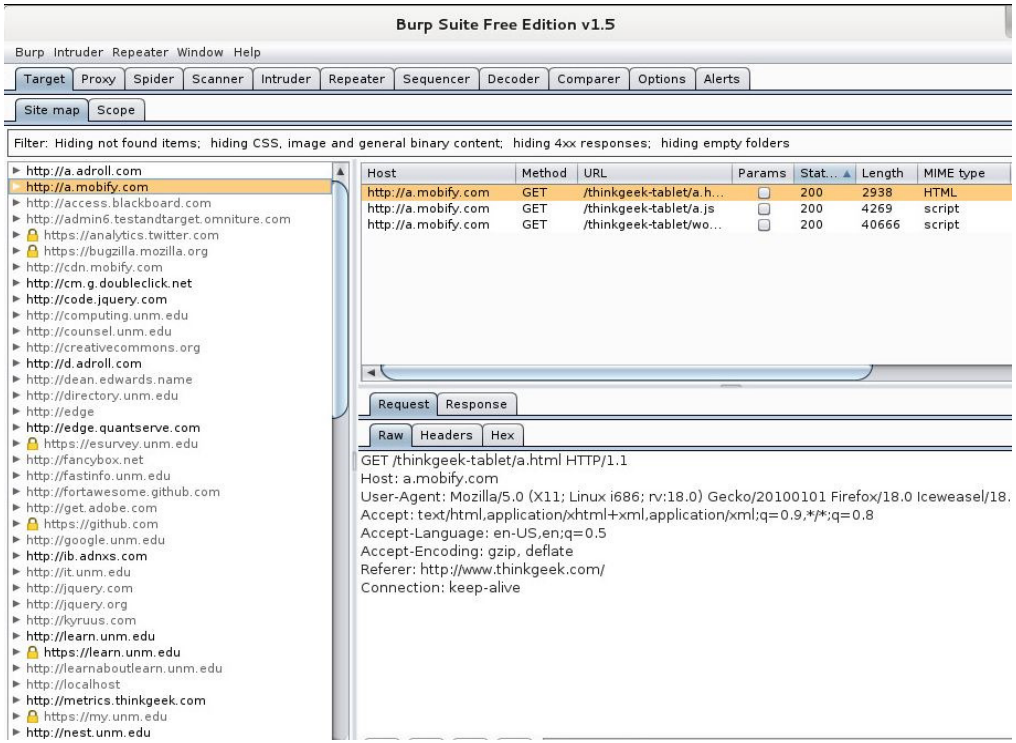


History Cont.

- You can review the series of requests you have made.
- Click on a column header in the Proxy history to sort.
- Select an item in the table and view the full messages in the Request and Response tabs.

Site Map

- Also, as you browse, Burp builds up a site map of the target application.
- Go to Target > Site map



Site Map Cont.

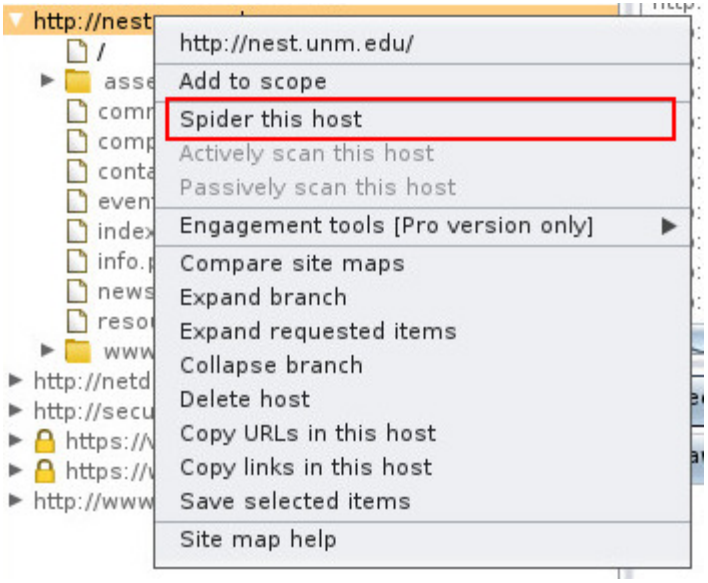
- The site map contains all of the URLs you have visited in your browser, and also all of the content that Burp has inferred from responses to your requests (e.g. by parsing links from HTML responses).
- Items that have been requested are shown in black, and other items are shown in gray.
- You can expand branches in the tree, select individual items, and view the full requests and responses (where available).

Burp Spider

- Burp Spider uses various techniques to crawl application content, and by default it will follow all in-scope links, submit forms with dummy data, and make additional requests (for robots.txt, directory roots, etc.).

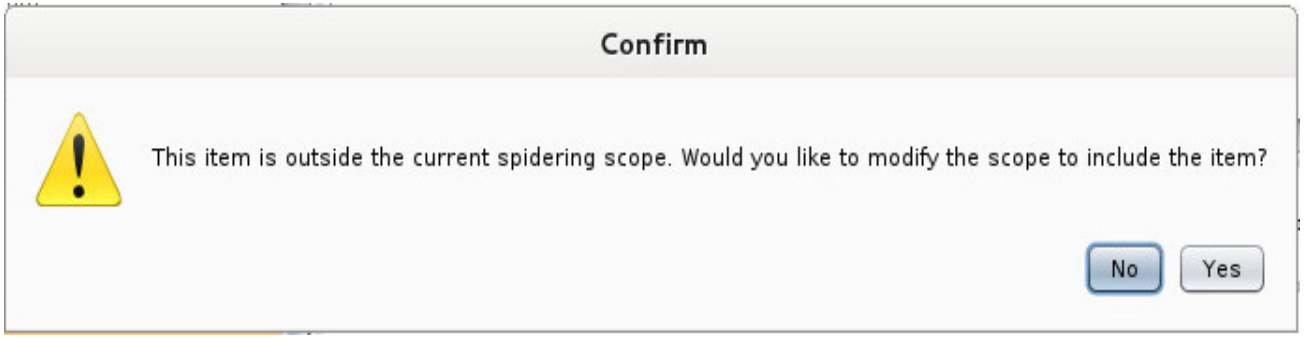
Initiating the Spider Cont.

- In the Site Map, find ‘http://nest.unm.edu/’
- Right click and select ‘Spider this host’



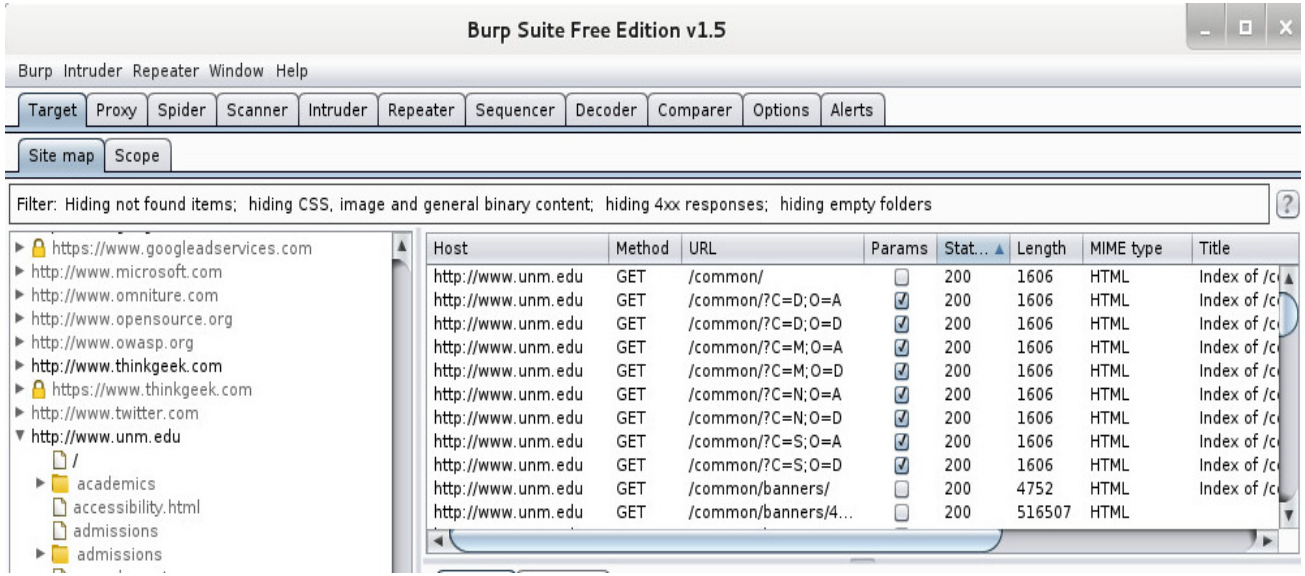
Confirm Scope

- If you get the following message
  - Click “Yes”



Spider Results

- Once the spider starts, it will display all the pages. You will see them in the main window to the right.



References

- http://geekyshow.blogspot.com/2013/07/how-to-use-maltego-in-kali-linux.html
- http://portswigger.net/burp/help/proxy_gettingstarted.html
- http://portswigger.net/burp/help/spider_using.html