Loi Tran
MIS5211.001

Burp Suite Assignment

Burp Suite is a suite of products that can be used to perform security testing of web applications. Some of the tools available are proxy server, web spider, scanner, intruder, repeater, sequencer, decoder, collaborator and extender. In this assignment, we are using Burp suite as an intercepting proxy, which acts a server that sits between the web browser and the internet. An intercepting proxy allows the user to intercept, inspect, and modify raw traffic passing between the browser and the internet. Testers may use it to review what their browsers are sending or receiving to/from the internet. Hackers, if successful at creating am intercepting proxies in front of a website, will be able to harness a lot of personal information (i.e., username, passwords, session cookies) that can be used to attack either the website or the user.

For this assignment, I used the proxy between my Kali virtual machine and Ookla.com to intercept the traffic between my browser and the website. Ookla is a popular web service that provides free analysis of internet access performance metrics, such as connection data rate and latency. Since its existence, Ookla has provided over nine billion speed tests.

The initial traffic between my browser and Ookla was normal. A cookie and session ID was created between my machine and the website. The website responded with an HTML document for the browser to render. The header information on my request was more specific (operating system and browser versions) than the response from Ookla (only specify the type of server without the version), When I looked at the HTTP history, it revealed some troubling details of what Ookla was loading onto the browser.

Investigation of the HTTP history reviewed that Ookla was also sending over two hundred and fifty different adware and external contents for the browser to load. Some were used to track users and others were questionable on exactly what it does. For example, research of b.scorecardresearch.com (https://www.malwarekillers.com/how-to-remove-b-scorecardresearch-com-pop-up-ads-redirects/) revealed that the ads presented by this host can infect PC with "very dangerous malware." According to the source, security analysis concluded that the pop-up ads were fake and the primary goal is to infiltrate computer systems without owner's permission to steal private data such as usernames, emails, SSNs, birthday, passwords, credit card information, and/or other financial information.

Since I was on a virtual machine, I decided to proceed with the speed test. Ookla continued to load hundreds of adware and potentially some spyware onto the browser. Further investigation of some of the hosts (pi.pardot.com, pxl.jivox.com, wtp101.com, among others) shows that some are classified as malicious, according to my anti-virus software.

Finally, the results of the test were rendered through basic scripting language. Although the speed test itself is free, the user is potentially giving up a lot of their privacy to see the result. They are also exposing themselves to hundreds of adware that can make them vulnerable to browser high jacking, unwanted pop-ups and potentially malicious software being installed on their computer without consent.

This assignment made me realize that nothing is really free on the internet. The intercepting proxy showed me what my computer is sending out and what it's receiving. By reviewing this information, I was able to see 'under the hood' of all the traffic my computer receives from the internet. This made me more aware of the risks associated with traversing through the internet without properly reviewing what you click on.