**Burp Suite Analysis**

Burp Suite is a java-based software that functions as an interception proxy to analyze web traffic. While it also has other tools available, Kali only includes the free version to use. In the full version, Burp Suite has tools such as the spider, the sequencer, the decoder, and the intruder. Luckily, the free tool has enough power to find out a lot about a website by acting as a man-in-the-middle to analyze the traffic over a connection. We are going to look at the results found on Xfinity, the website for the Comcast company.

Initial viewing of the burp suite when connecting to the website lists almost 80 connections. Some are for page resources like CSS, while a large number are for advertising services or background tracking of users. What is interesting is how it tries to give you the weather by using a cookie with your zip code.

One of their advertising sites was internal, named oascenral.comcast.net. Further searching found little information on Oascentral, except for a description describing it as a company focusing on SEO internet marketing. Another site was called rubiconproject.com which is for a large advertising company based in Los Angeles, California. They also use Demdex, an audience analysis firm owned by Adobe.

Moving to the login page, I saw that the system uses OAuth, which can be useful information if there are any known flaws in that SSO protocol. I used a username and password to sign into the site, and found out that Burp Suite was able to pick up the username and passwd fields that were being sent. This worried me as it means that they could have been intercepted by someone else using similar analyzers on the traffic.

Preventing your account from being compromised by someone conducting man-in-the-middle attacks or simply using Burp suite risk is lower now that the browsers warn you that the connection is unsecure. Preferably they could encrypt the connection and send hashed versions of the username and password and compare that to their hashes internally. When software is telling you that connecting is a bad idea, you should listen.