Ex110 Submission

Gary Jones

Contents

Executive Summary

Goals

The goal of this exercise was to use BeEf to capture browser information.

Attack Narrative

To begin I started apache2 and then initiated wireshark (see figures 1 and 2). After turning on all the name resolution options in wireshark I was then able to identify a Get request to kali.pr0b3.com/coins/collection.html (see figure 3).

At this point I started up BeEF and logged into the system (see figure 4). Noticing the settings I identified that there already existed a hook URL for 172.24.0.10 which is the same host that my target was using.

In order to start up the necessary website I created the directory 'coins' in the filepath /var/www/html. From here I then created a collection.html script that has an exertnal link to the hook js script. By doing this the program automatically executes when the page loads (see figure 5).

Once this was set up I made sure to check that the site was working (see figure 6). From here I was able to confirm that I hooked the target through the UI interface on BeEF through the online kali.pr0b3.com hooked browser and also under the zombies tab (see figures 7, 8, and 9).

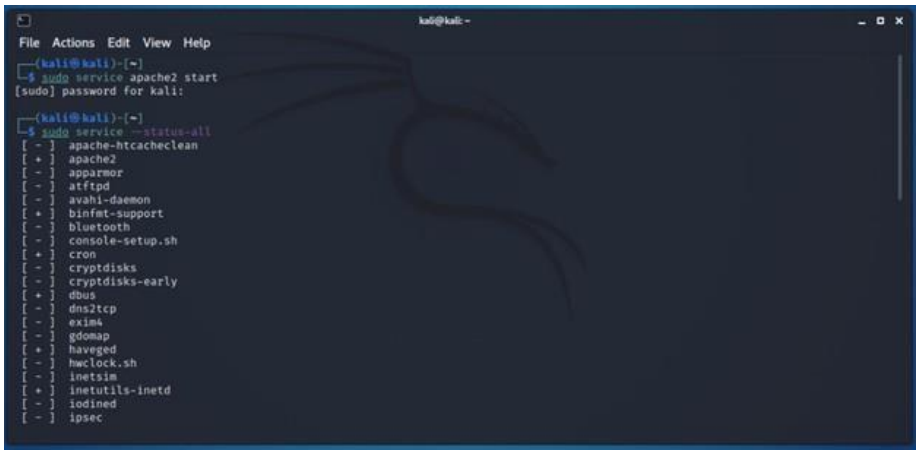

Figure 1:

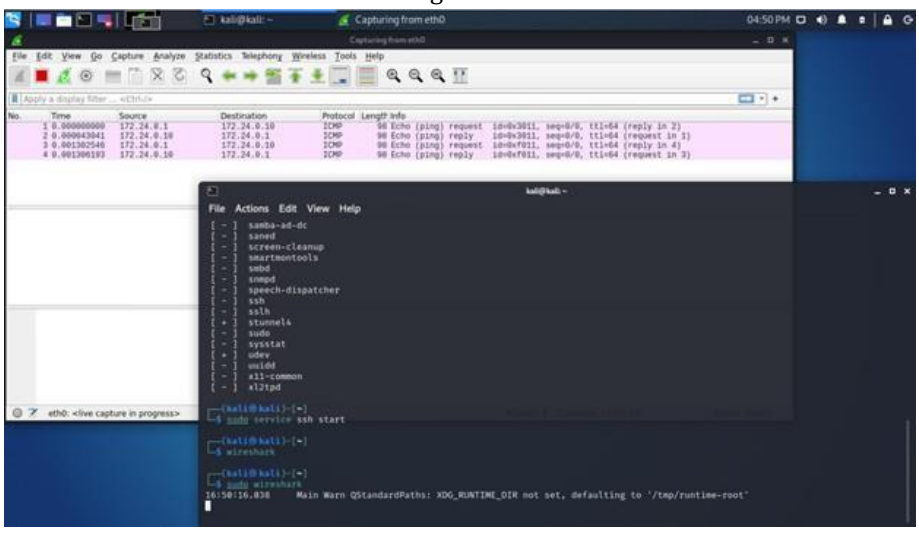

Figure 2:

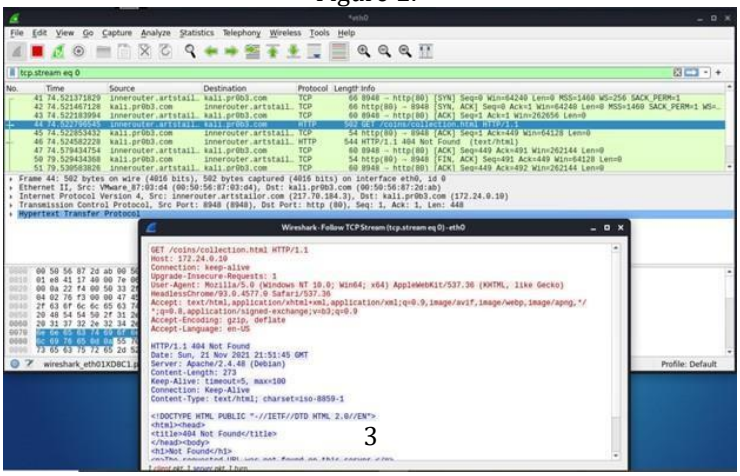

Figure 3:

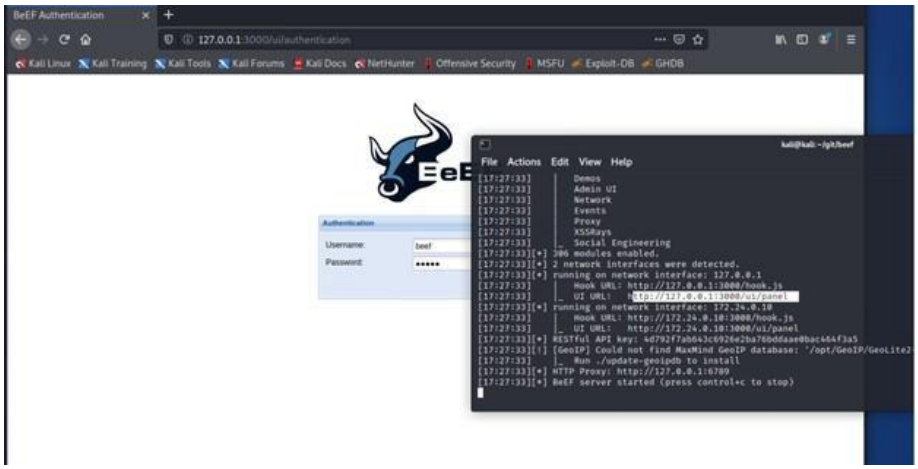

Figure 4:

Figure 5:

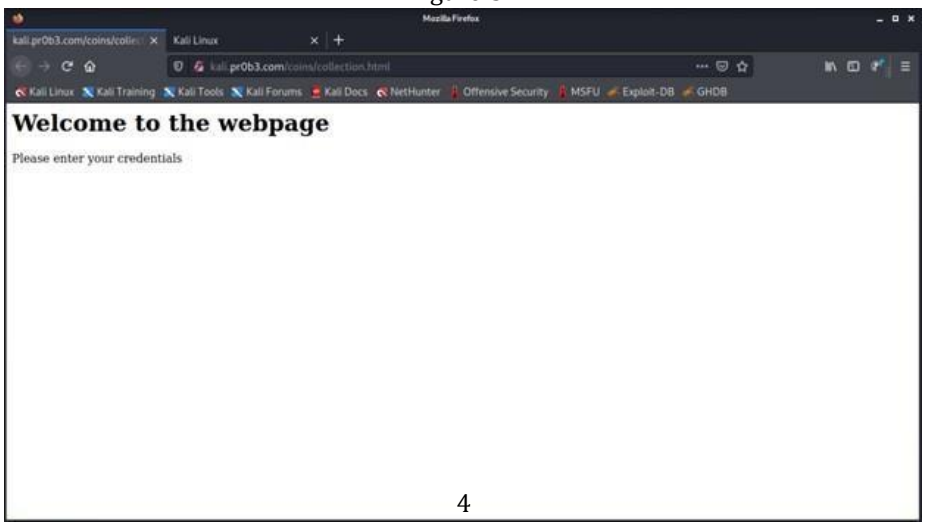

Figure 6:

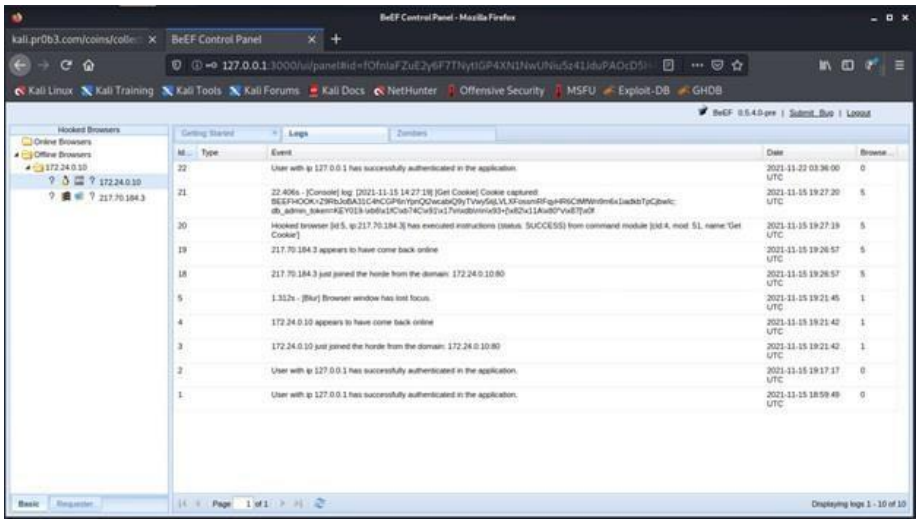

Figure 7:

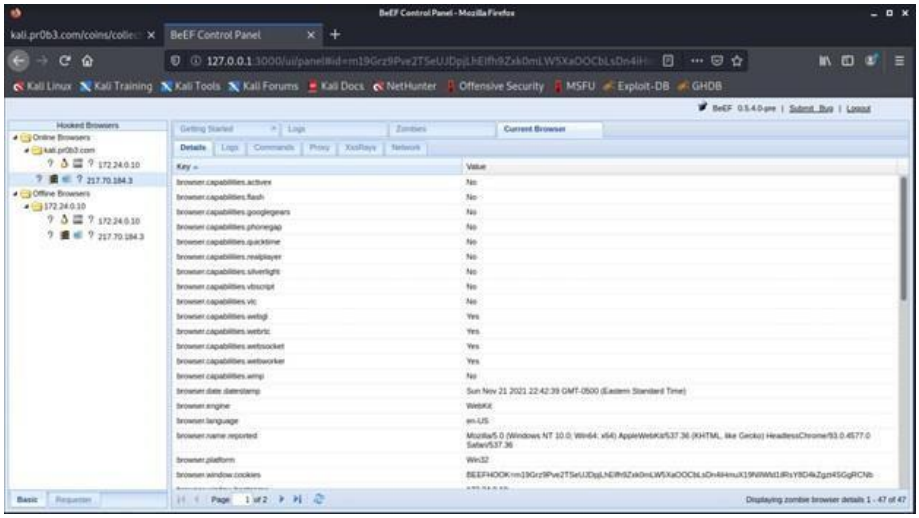

Figure 8:

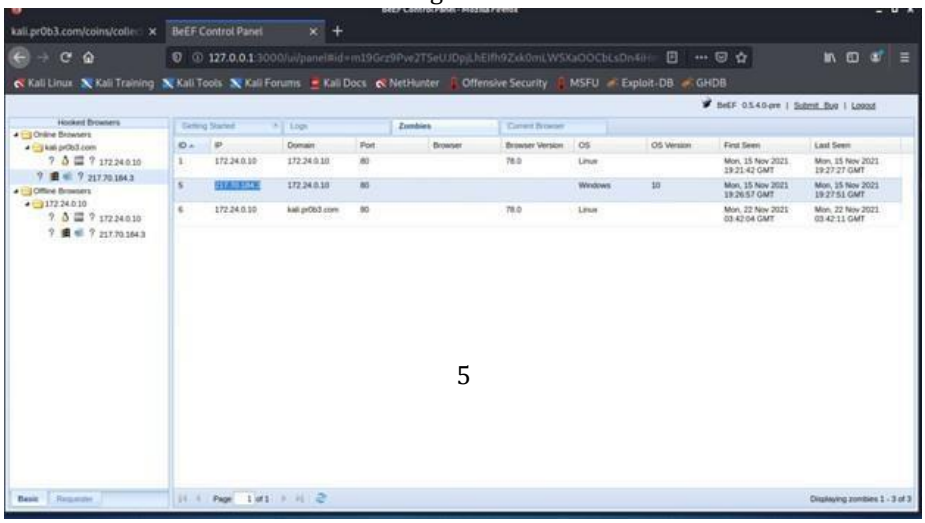

Figure 9: