PenTest Lab Exercise Ex110 – BeEFHooking

Goal

Use `BeEF` to capture browser information.

Tasks

1. Log in to the ndg box and schedule an Ex110 lab.

2. Hank Hacker previously arranged with Art for Tina Tester, the FNG (fairly new grunt) at Pr0b3, to social engineer one of Art's employees. They did so by identifying an employee, Nuri Numismatist, who is a fanatic stamp collector. Nuri is a part-time employee who is working on developing a database for Art and Otto. Tina told Nuri that they have a valuable collection that contains an 1873 U.S. $20 Double Eagle coin, one that Nuri does not have and has been asking about this on a local coin club chat site. Tina told Nuri that a web site is being brought online soon and Tina can check out this and other coins there.

   Unfortunately, after mounting the social engineering campaign, Tina immediately left Pr0b3 to join a Zen monastery and now, living somewhere in remote southeast Asia, cannot be contacted for the details of the social engineering campaign.

   We believe Nuri is actively attempting to contact the supposed web site at `kali.pr0b3.com` (`172.24.0.10`), but we don't know anything else about Nuri's activity. We don't even know the URL of the web page that Tina was supposed to be constructing.

   Identify what web page or pages Nuri is attempting to grab. (They may only be checking on an occasional basis.) You can do this using any method you choose. Some methods require attention others don't. All will require some level of patience.

3. After you have identified the web page that Nuri is attempting to get, construct a page that will satisfy Nuri's request and also use `BeEF` to hook their browser. See if you can capture any useful information by doing that.

   You can find the `BeEF` project's Git repo in `/homes/kali/git/beef` on `Kali`. It has been installed but has yet to be executed. `BeEF` explains

some of the details of its use when you start it up. Make sure to *pay attention* and customize any elements you need to in order to get it to function correctly. This can be a little tricky.

4. Before leaving, Tina mentioned something about a special administrative session token that Nuri may use for some kind of access to the database which will be coming online for the public soon. Even if that system can't be identified, having the token could prove to be valuable in the future.

5. Write a partial penetration test report about the incremental progress you have made and turn it in via Canvas.