CIS 76 Ethical Hacking Lab Exercise

Lab X8 - Using BeEF
Fall 2017

Lab X8 - Using BeEF

This lab provides practice using BeEF to “hook” browsers and carry out client exploitation.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab, you have authorization to hack the VMs in the associated Netlab+ pod.

Preparation

1) Reserve a Netlab+ pod for the maximum amount of time for this lab:
   NDG Lab 12: Client Side Exploitations
   You can always release it if you finish early.

NDG Lab Part 1 – Hooking Browsers with BeEF Framework

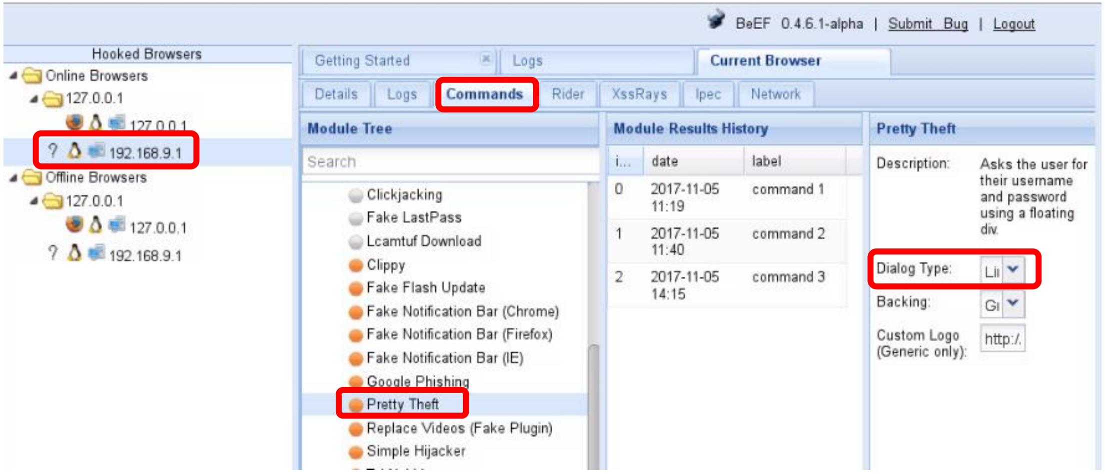
1) Complete steps 1-16 of the NDG lab.
2) On step 17 use “XXXX was here!” as your secret (where XXXX is your first name) then take a screenshot showing it.
3) Complete steps 18-21 then take a screenshot of showing the captured keystrokes in the BeEF log.

NDG Lab Part 2 – Client Exploitation with BeEF Framework

1) Complete steps 1-24 of the NDG lab.
2) For step 25 enter this data instead:
   `Name:` **`first last`** *(use your real name)*
   `Phone:` **`Pod xx`** *(where xx is your pod number)*
   `Address:` **`CIS Lab`**
   `Credit Card:` **`10.76.xx.0/24`** *(where xx is your pod number)*
3) Complete steps 25 to 30 then take a screenshot showing the captured keystrokes in the BeEF log.
4) Ignore step 31.

NDG Lab Post lab custom steps

1) On Kali select and execute the command to display a fake expired LinkedIn session:



i...	date	label
0	2017-11-05 11:19	command 1
1	2017-11-05 11:40	command 2
2	2017-11-05 14:15	command 3

Description: Asks the user for their username and password using a floating div.

Dialog Type: Li

Backing: Gi

Custom Logo (Generic only): http:/.

2) On OpenSuse file in the fake Session Timeout Popup as follows:
   `Email:` **`first@podxx.edu`** *(your real first name and xx is your pod number)*
   `Password:` **`xxxxxxxxx`** *(whatever you want)*
   Then take a screenshot for your report.
3) On Kali take a screenshot showing the captured keystrokes in the BeEF log.

Submit your work

1) Prepare a report using the word processor and formatting of your choice. Your report should contain the following:
   - Course name, lab assignment name, your name, and date.
   - Labelled or captioned screenshots for:
     - Part 1 OpenSUSE Entering secret in web form (Step 17)
     - Part 1 Kali showing captured keystrokes (Step 21)
     - Part 2 OpenSUSE web food order (Step 25)
     - Part 2 Kali showing captured keystrokes (Step 30)
     - Post lab fake LinkedIn expired session popup (Step 2)
     - Part lab Kali showing captured keystrokes (Step 3)

As an example you can see Benji Simms' report here: https://simms-teach.com/docs/cis76/cis76-labX8-simben76.pdf

2) Email your report to: **`risimms@cabrillo.edu`**

Remember **late work is not accepted.** If you run out of time submit what you have completed for partial credit.

Grading Rubric (6 points)
2 points for the Part 1 screenshots.
2 points for the Part 2 screenshots.
2 points for the Post lab screenshots.