Cabrillo College

CIS 76 Ethical Hacking Lab Exercise

Lab 4: Footprinting and Social Engineering
Fall 2017

Lab 4: Footprinting and Social Engineering

This lab details a specific browser vulnerability and how the related exploit can be used in a social engineering attack known as phishing.

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 VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.

- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Part 1 – Pod configuration

1) If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 2 – CVE-2009-0075 vulnerability and exploit

1) Review this vulnerability on cvedetails.com and take a screen shot of the details page. http://www.cvedetails.com/
2) On your EH-Kali VM examine the actual Ruby code of the exploit in `/usr/share/metasploit-framework/modules/exploits/windows/browser/ms09_002_memory_corruption.rb` Include the Ruby code in your report. We will use this vulnerability in Part 3 to exploit a victim's browser.

Part 3 – [Netlab+] NISGTC Lab 9: Using Spear Phishing to Target an Organization

Lab errata:

- Page 10, step 8, use exploit/windows/browser/ms09_002_memory_corruption
- Page 12, step 14, set LHOST 216.6.1.100

Lab additions:

- Page 16, step 5: Add your name, as the commissioner, at the end of the phishing email.
- Page 29, after step 7, create a new directory on the victim's computer, change into it and use pwd command to show you are in it.

Screen shots to capture:

- [Windows 7] Outlook Sent Items folder, showing successfully sent phishing email with your name as the IRS commissioner.
- [Windows XP] Outlook Express Inbox, showing received phishing email that has your name as the commissioner.
- [BackTrack 5] meterpreter session showing captured hashdump account/encrypted passwords plus the pwd command output showing the new directory created with your name.

Submit your work

a) 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.
- For Part 2 include:
  - Screen shot of cvedetails.com showing the vulnerability.
  - Ruby code of the related exploit for the vulnerability.
- For Part 3 include:
  - [Windows 7] Screen shot showing attacker view of sent email with your name as commissioner.
  - [Windows XP] Screen shot showing victim view of received email showing your name as the commissioner.
  - [BavkTrack 5] Screen shot of meterpreter session showing captured accounts and pwd output of directory named after you.

As an example you can see Benji Simms' report here:
https://simms-teach.com/docs/cis76/cis76-lab04-simben76.pdf

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

Remember **late work is not accepted.** If you can't finish the lab by the deadline submit what you have completed for partial credit.

Grading Rubric (30 points)

6 points for CVE details.
6 points for Ruby exploit code.
6 points for attacker view of personalized phishing email.
6 points for victim view of personalized phishing email.
6 points for exfiltrated accounts and making custom directory.