Cabrillo College

CIS 76 Ethical Hacking Lab Exercise

Lab 7: Programming for Security Professionals
Fall 2017

Lab 7: Programming for Security Professionals

This lab introduces an IRC bot. The student will add a new Bot command to their Bot on EH-Kali-xx. This will enable an attacker on Opus-II to instruct the Bot on EH-Kali-xx to exfiltrate a file. The Bot will respond by emailing the contents of the EH-Kali-xx /etc/passwd file to the attacker on Opus-II.

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.
- 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 1 – Add a new command to your Bot named after yourself

1) On your EH-Kali-xx vm, if needed, add this line to your /etc/resolv.conf file:

```
search cis.cabrillo.edu
```

This will let you use short hostnames like "opus-ii" rather than typing out all of "opus-ii.cis.cabrillo.edu".

2) Review and do the corresponding Bot module activities in Lesson 8:
   a. "Setting up email on Kali" module.
   b. "Using IRSSI"
   c. "Installing IRC Bot" module.
   d. "Adding more commands to your bot" module.
   e. "/etc/resolv.conf exfiltration script" module.
   f. [Optional] "Flood script" module.
3) Extend your bot to steal /etc/passwd with a command named after yourself:
   a. Make a new copy of **mailer.py** named **mailer_L7.py** that steals *\/etc/passwd*.
   b. Make a new copy of **bot_example01_script** named **bot_script_L7**.
   c. Modify **bot_script_L7** to run your new **mailer_L7.py** program.
   d. Make sure **bot_script_L7** has execute permissions.
   e. Make backup copy of your **bot_commands.py** file.
   f. Add a new command to **bot_commands.py**, named after your first name, that runs your new **bot_script_L7** file.

Part 2 – Test your bot

1) On Opus-II run the Irssi chat client.
2) Connect to eh-irc and join #cis76.
3) Run the **!runscript** command and check you that get an email containing */etc/resolv.conf*.
4) Run the **!***firstname* command and check that you get an email containing */etc/passwd*.

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.
- Your modified **bot_data.py** file
- Your modified **bot_commands.py** file.
- Your new **bot_script_L7** file
- Your new **mailer_L7.py** file.
- Screenshot of chat session showing **!runscript** and **!*firstname*** commands where first name is your real first name.
- A copy of the full email from the Bot showing the **/etc/resolv.conf** file.
- A copy of the full email from the Bot showing the **/etc/passwd** file.

- As an example you can see Benji Simms' report here: https://simms-teach.com/docs/cis76/cis76-lab07-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 (30 points)

4 points for correctly modified bot_data.py file.
4 points for correctly modified bot_commands.py file.
4 points for correctly modified bot_script_L7 file.
4 Points for correctly modified mailer_L7.py file.
4 points for chat session showing both added commands.
5 Points for your received email with */etc/resolv.conf*.
5 Points for your received email with */etc/passwd*.