Hack the web servers and protocols

Lab Manual

Objectives

- Apply socket library urllib2
- Map open source web applications
- Evaluate brute-forcing directories and file locations
- Evaluate brute-forcing HTML form authentication

Table of Contents

1.

Background Reading

Textbook:

Black Hat Python, chapter 5

Notes common to all lab and home assignment problems

For every lab and home assignment, all work should go into your personal repository, subdirectory named python/mMM, where MM stands for the module number. For each problem, carefully name the program as described. If the name for the program is not mentioned in the problem, name it mMMpPP.py, or mMMpPP.c, etc. (MM is the module number, PP is the problem number, and then add the proper extension) The programs are extracted from your repository by a Python script, and errors in the program name will result in the instructor never seeing your program, and your mark for it will be ZERO!

Anything to record and report in this lab is to be written in plain text files, one file per problem (Word document is not a plain text file). The files MUST be named mMMpPP.txt (again, MM is the module number, PP is the problem number, e.g. m03p12.txt would be a report for module 3, problem 12). Mis-naming this file, or not having it in the proper location will result in mark ZERO for anything to be recorded or reported.

There are always many ways how to solve a programming problem, and usually one or two ways which are fast, compact and elegant.

Make sure to push your work to the server often, and have pushed the working version of the program by the deadline specified. The script extracting your programs from your repository will be run at any time after the deadline.

Lab specific intro

We will learn how to analyze web applications. This is one of the more important tasks for penetration tester or an attacker, as web applications present the most possibilities for an attack, and are the most common path to obtain access. We will explore the basics of interacting with the web using Python by utilizing the urllib2 library.

Problem 1

Write script **`m13p01.py`**, which will fetch and print the page at http://itss.biomea.com/index.html utilizing the urllib2 library. Report the output.

Problem 2

Review the “Mapping Open Source Web App Installations” within chapter 5 in the Black Hat Python textbook. Install the open source blogging platform Joomla on one of your virtual machines. Using this

installation, write script **`m13p02.py`**, which will attempt to access every file on the server. Submit log of the script run, listing the files attempted, and files accessed.

Problem 3

Write python script **`m13p03.py`**, which will try to get directories and files, as described in “Brute-Forcing Directories and File Locations” part of chapter 5 of the textbook. Point the script at your joomla installation. Report the results.

Problem 4

Study the “Brute Forcing HTML Form Authentication” in chapter 5 of the textbook. Describe the technique in 300 words and submit.