

Hacking Web Servers and Protocols

Offensive and Defensive Tool Construction

Table of Contents

[Objectives 4](#_Toc477858191)

[Background Reading 4](#_Toc477858192)

[Important Information 4](#_Toc477858193)

[Introduction 5](#_Toc477858194)

[Problem 1 5](#_Toc477858195)

[Problem 2 5](#_Toc477858196)

[Problem 3 5](#_Toc477858197)

[Problem 4 6](#_Toc477858198)

Offensive and Defensive Tool Construction

Hacking Web Servers and Protocols

Objectives

This lab focuses on the following objectives:

* Apply socket library urllib2.
* Map open source web applications.
* Evaluate brute force attacks on directories and file locations.
* Evaluate brute force attacks on HTML form authentication.

Background Reading

Read Chapter 5 in the *Black Hat Python* textbook.

# Important Information

* For *every* lab and home assignment, store all your work in your personal repository in a subdirectory named **mXX**, where XX is the module number. Carefully name the program as described in each problem.
* Your programs are extracted from your repository by a Python script. If there are any errors in the program name, then your instructor will never see your program, and you will receive a mark of zero.
* Push your work to the server often, and ensure that you push the final version of a program by the deadline specified, because the script extracting them can be run at any time after the deadline.

# Introduction

In this lab, we will learn how to analyze web applications. This is one of the more important tasks for a penetration tester or an attacker, because web applications present the greatest possibility 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

1. Write a script named **m13p01.py** that fetches and prints the page located at http://itss.itc.sait.ca/index.html using the urllib2 library.
2. Report the output.

# Problem 2

1. Review the “Mapping Open Source Web App Installations” section in chapter 5 of the *Black Hat Python* textbook.
2. Install the open source blogging platform Joomla on one of your virtual machines.
3. Using this installation, write a script named **m13p02.py** that attempts to access every file on the server.
4. Submit a log of the script run, listing the files attempted and the files accessed.

# Problem 3

1. Write a Python script named **m13p03.py** that attempts to get directories and files, as described in the “Brute-Forcing Directories and File Locations” section in chapter 5 of the textbook.
2. Point the script at your Joomla installation and report the results.
3. Point the script at itss.ict.sait.ca and report the results.

# Problem 4

1. Study the “Brute Forcing HTML Form Authentication” section in chapter 5 of your Linux textbook.
2. Submit a 300-word description of the technique.