THE UNIVERSITY of NEW ORLEANS

CSCI 4621/5621 INTRO TO CYBER SECURITY

Lab Assignment 3: Webshell client

Due: **April 25, 11:59pm**

Goal

The purpose of this lab is to create a couple of simple scripting tools that automate access to a known vulnerable target.

Steps:

1-) Install a VM by using "web_for_pentester_i386.iso" from following link. The same iso file is also available on the assignment page.

"https://pentesterlab.com/exercises/web_for_pentester/iso"

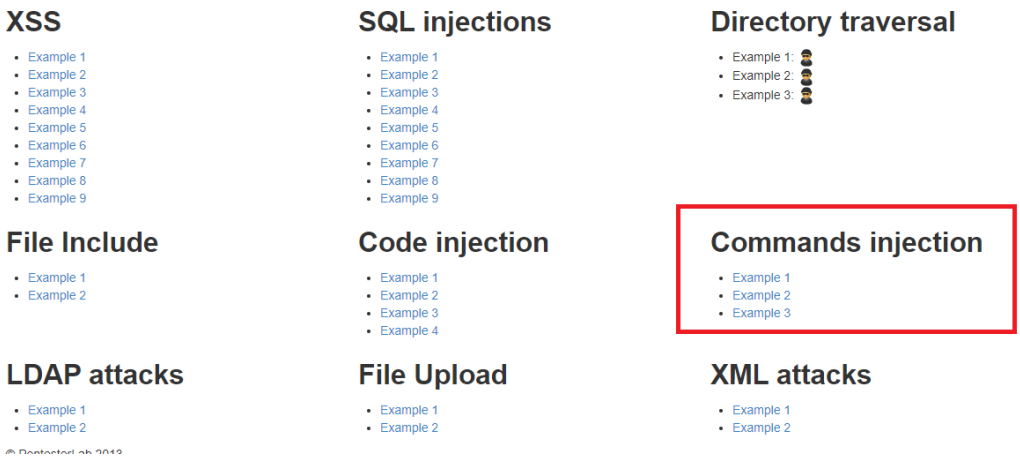
2-) Use the "Web for Pentesters 1 (PentesterLab.com).pdf" as your reference.

3-) Install a second VM (Ubuntu or Kali). If you already have a VM from previous assignments, you can use that machine.

4-) Note that both VMs need to be in the same network. Therefore, you need to use your own computer for this assignment. Do not use Cloud VM services.

Part 1: webshell client [50pt]

Specifically, you are targeting one of *commands injection* examples (presumably Example 1 as the easiest).



As demonstrated in class, we have full remote shell execution, but the interface is clunky and not suitable for scripting and automation.

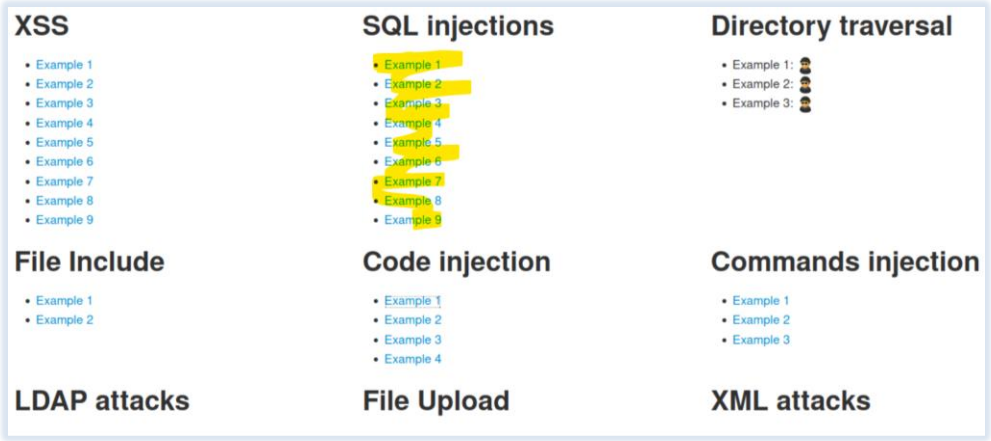
Task 1

- Create an interactive shell client named **lab3sh** that allows normal remote shell similar to what you get from bash.
- It should take one command parameter – the IP address of the **Web for Pentesters I** VM and should provide a REPL (Read-Eval-Print Loop)
- Example interaction:

bash>./lab3sh 10.1.2.3
lab3sh> whoami
www-data
lab3sh> pwd
/var/www/codeexec
lab3sh> cat /etc/passwd
…

Part 2: sqli client [50pt]

Specifically, you are targeting one of SQL injection examples (presumably Example 1 as the easiest).



As demonstrated in class, we have full SQL injection compromise, but we aim for something suitable for scripting and automation.

Task 2

Create an interactive shell client (REPL) named **lab3sqli** that takes the IP address of the target as its single parameter and supports the following commands:

- **dbs** → list databases
- **tables <database>** → list tables for given DB
- **columns <database> <table>** → list columns for given DB and table
- **dump <database> <table>** → dump table content

Deliverable

- The main deliverables of your work are your code/scripts and a (brief) report explaining your approach.
- Python is the recommended implementation language, although other mainstream languages are also acceptable
- This is a tool development exercise, so your audience for the report is technical, a fellow pentester, for example. Make sure you document example runs of your tools.

Evaluation

You may work on this assignment either individually, or in groups of two. In the latter case, make sure that you:

- clearly state the group membership in the front page of your report; and
- submit the (same) report via Canvas on behalf of each member.

You may consult all available online/offline resources, but you may not actively solicit help; e.g., you can read a discussion on *Stack Overflow*, but you may not post a question related to the assignment.

Submission

Place your entire submission in a single zip archive and submit via Canvas