Lab Assignment 5
Offline Password Cracking, Armitage, and WebGoat Experiment

Cliff C. Zou
University of Central Florida

Question 1: (**Offline Password Cracking**)

I have created two accounts in Kali Linux, 'final1' and 'final2', and the two password related files (only keeping the two accounts' lines), /etc/passwd and /etc/shadow can be downloaded from the assignment webpage.

Please download these two files to your Kali Linux VM, and use the John the Ripper offline password cracking tool to find out the passwords for these two accounts. Please use screenshot to show how you do it.

Question 2: (Armitage Exploitation)

Please run your Kali Linux VM and your metasploitable Linux VM at the same time. Make sure they can see each other. If you have run Armitage on your Kali Linux VM before, please open Armitage, remove all hosts in the Armitage target window, then restart your Armitage to do this assignment.

(1). What are the IP addresses of these two VMs?

(2). Run Armitage on your Kali Linux, then conduct nmap scan inside Armitage. Use screenshot image to show the Armitage interface where the target window section will only show the metasploitable Linux computer's icon with the correct OS information (after removing all other unrelated network devices).

(3). After completing the above scanning process, use 'Hail Mary' flooding attack to let Armitage conduct all possible attacks to the vulnerable Linux VM. When Hail Mary attack finishes, the VM should have been compromised (red light-bolted!). Use screenshot image to show the Armitage interface after the attack finishes. And how many successfully compromising sessions have been created?

Question 3: (SQL Injection Attack and Owasp-Zap)

(1). Download and install the WebGoat on Kali Linux. Use the screenshot image to show that you have run successfully of the WebGoat in your Kali Linux browser. The screenshot image should show the initial user login page of the WebGoat.

(2). Run Owasp-Zap and set it up as the web proxy for your Kali Linux browser. Make sure to change the proxy port to be 7000. Use the screenshot images to show how you set the browser with Owasp-zap as proxy on port 7000, and how you change the Owasp-zap default port to be 7000.

(3). Complete the WebGoat lesson "Lab SQL Injection: Stage 1: String SQL Injection". Show how you use the Owasp-zap to intercept user login request page and change the password field to successfully conduct the SQL injection attack.