Lab Assignment 4:
Online Password Cracking and Metasploit Attack

Cliff C. Zou
University of Central Florida

Question 1: (**Online Password Cracking**)
In class, I have demonstrated how to use Hydra to do online password guessing attack to obtain Win7 VM's user account password through the window's remote desktop service. In this question, you need to use Hydra to crack Metasploitable Linux VM user password via the ssh service.

(1). On your Kali Linux, copy the /usr/share/john/password.lst to the /root directory, then use a text editor to remove all the '#!comment:….' lines at the beginning of the file. Then insert this password 'msfadmin' right after the password 'abc123' (this 'abc123' is one of the first 10 passwords). Use screenshot to show the beginning content of this edited password.lst file by using command 'head'.
(2). Run both Kali Linux and Metasploitable Linux VM. On your Kali Linux VM, run Hydra to do password attack to the SSH service running on the Metasploitable Linux VM, against the default account of 'msfadmin'. Please use the edited password list file in the /root directory for this attack. Make sure that you configure Hydra to run 4 connections in parallel, and display what passwords have been tried.

Please show the screenshot image of this hydra attack, which should find the correct password 'msfadmin' within a dozens of tries.

Question 2: (**Metasploit attack to vulnerable Linux**)
In class, I have demonstrated how to use Metasploit on Kali Linux to compromise the Metasploitable Linux VM against the 'Unreal IRCd' vulnerability. Please repeat this remote compromising attack with the following requirements: (a). When compromising is successful, use the 'reverse' shell for the remote access; (b). For the reverse connection of the shell, let the shell connect back to the Kali Linux on local port of '4000'; (c). When the shell is successful generated, run the command 'uname -a' to confirm that you are running this command on the remote Metasploitable Linux machine.

Please provide screenshot images to show all your operation commands, and the result of the successful attack with the result of the 'uname -a' command.

Question 3: (**Metasploit attack to WinXP**)

Set up your Kali Linux VM and your vulnerable WinXP with IE6 VM ready (this is the vulnerable WinXP I provided in class, it is still downloadable from my webserver). Make sure they can see each other. Then on Kali Linux VM, run Metasploit to attack the vulnerable WinXP by using the MS10-018 'drive-by download' vulnerability with these two requirements: First, payload uses the reverse-tcp meterpreter remote shell; Second, the malicious webserver running on local Kali Linux should work on the normal HTTP port 80.

(1). Use screenshot images to show how you use metasploit to successfully compromise your WinXP VM.

(2). Under the newly created meterpreter shell, display the compromised WinXP IP configuration, and then display its system information by use the 'sysinfo' command.

Please use screenshot images to show your operation commands and the attack results.

Question 4: (**Metasploit attack to WinXP**)

This time, you are required to run Metasploit to attack the vulnerable WinXP on the MS10-046 'drive-by download' vulnerability. This attack has the following requirements: First, the attack payload should generate a remote desktop control of the WinXP; Second, you can use this remote desktop to remotely operate on the vulnerable WinXP (not just viewing); Third, this remote desktop control is using reverse-tcp mode.

(1). Use screenshot images to show how you use Metasploit to successfully compromise your WinXP VM.

(2). Show the screenshot of the remote desktop window created on the Kali Linux derived from this attack.