CSUS, College of Engineering and Computer Science
Department of Computer Science
CSC 154 – Computer System Attacks and Countermeasures

Lab 3 - Pentesting

Goal: To use Kali to perform a penetration testing towards Metasploitable.

Deliverable: A lab report, with an **electronic submission** to Canvas to me, is expected to include the screen shots when you go to the following milestones in the lab. A demo may be requested when necessary.

Instructions: Please refer to the following steps, and hand in the deliverable with required screenshots.

1. Downloading and installation of Metasploitable, which is an intentionally vulnerable Linux virtual machine that you can download from below website (http://sourceforge.net/projects/metasploitable/files/Metasploitable2/);

2. Downloading and installation of Kali, which is a Linux distribution designed for penetration (https://www.kali.org/);

3. The virtual machines can be hosted based on vmware or virtualbox. Configure the network in vmware/virtualbox setting to make them accessible to each other.

---

4. Let's start based on the lab environments set up during Lab 1;

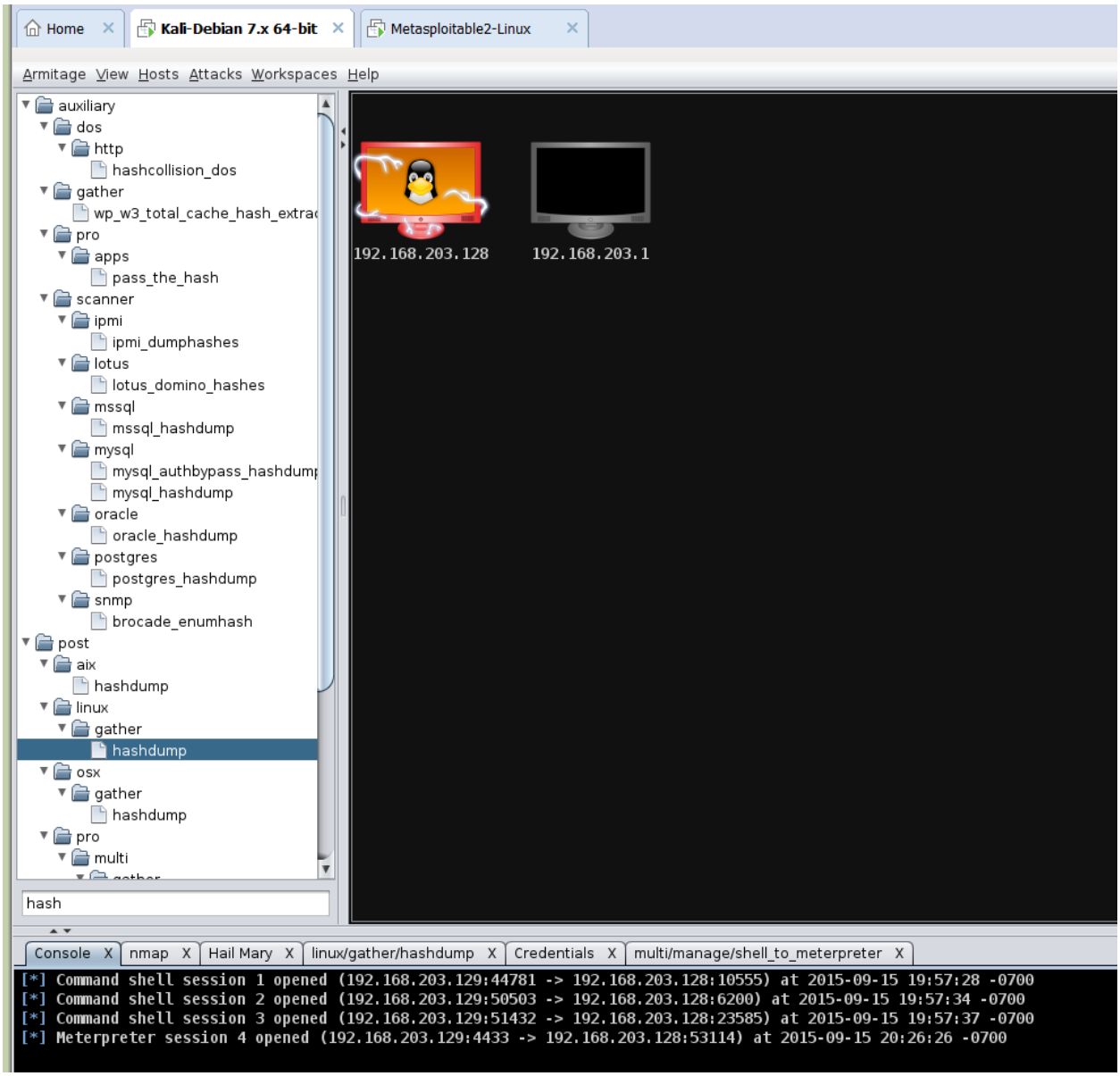
5. Open both Kali and Metasploitable, use ifconfig to know both IPs;

6. In Kali, open a terminal, run command: service postgresql start; and then run command: armitage;

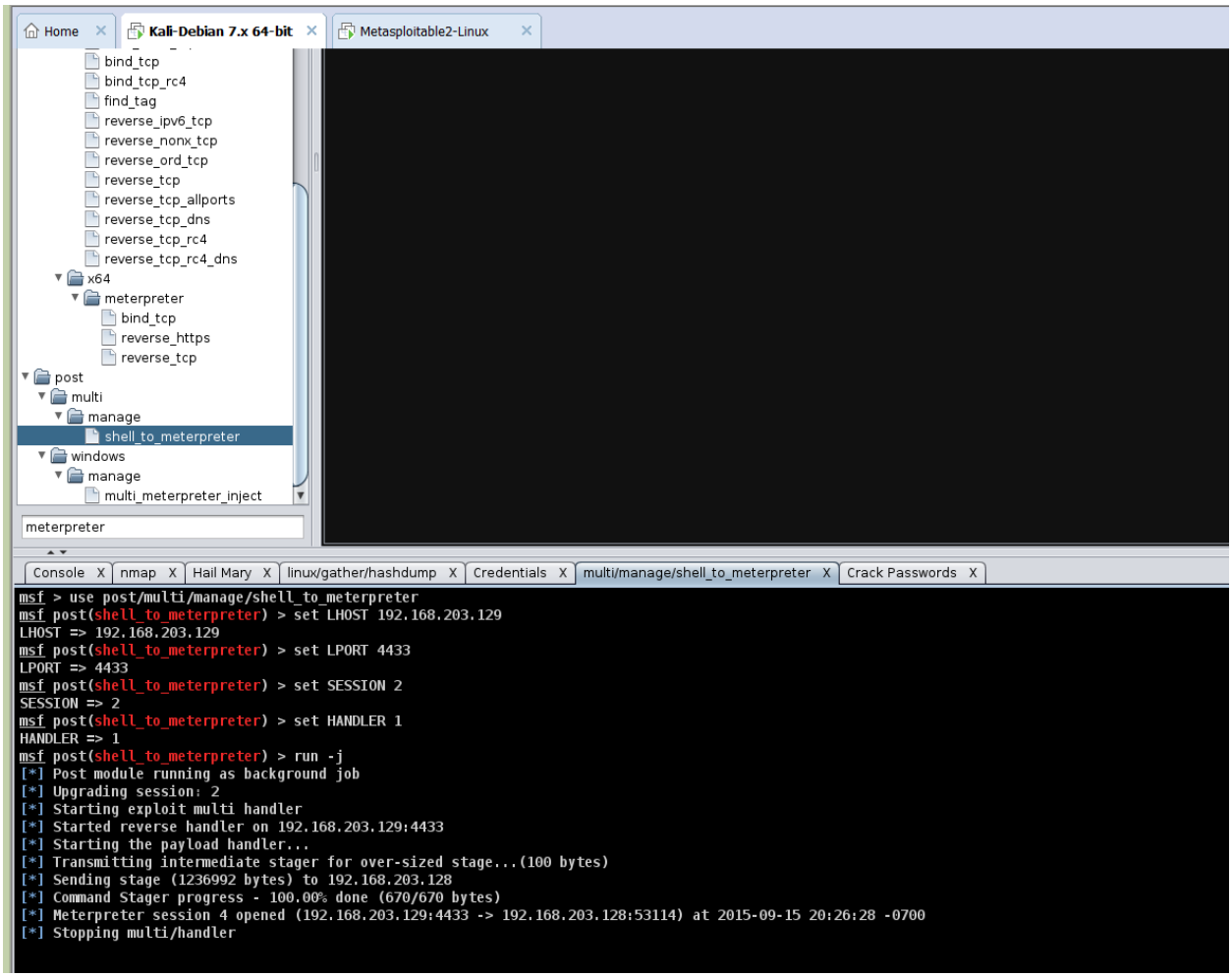
7. Go to the windows menu "hosts", go to "nmap scan", go to quick scan;

8. In the prompt windows, set the IP range where the IP of Metasploitable belongs to;

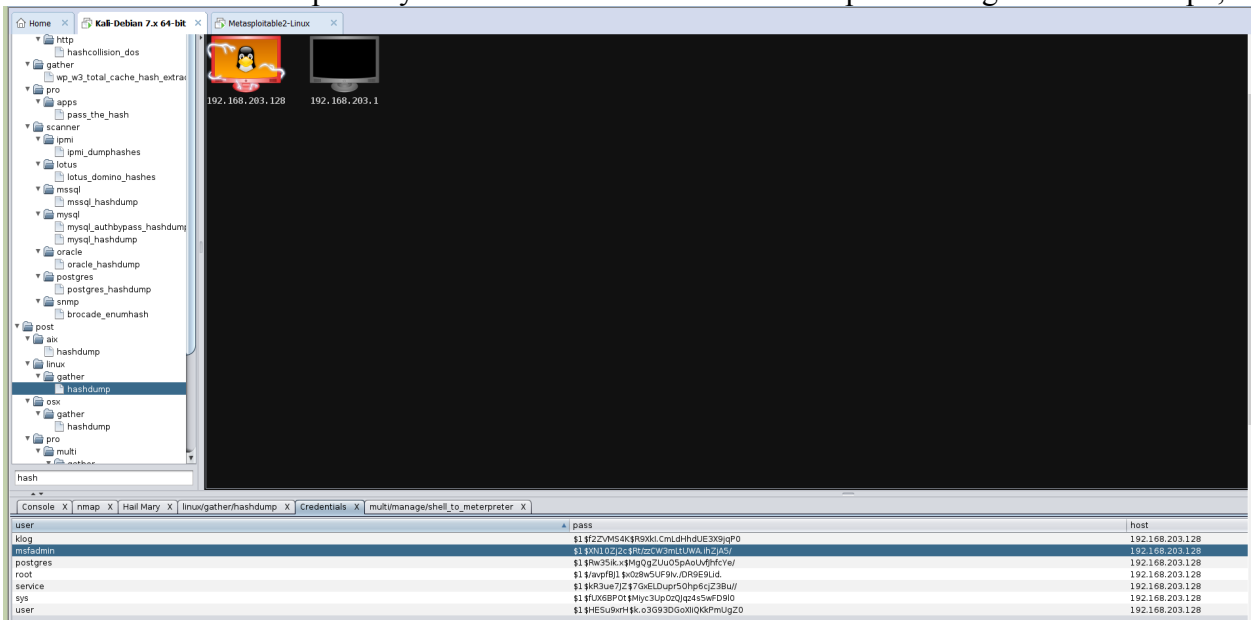
9. Go to "attacks", go to "Hail Mary". You are expected to see the following view, where the victim machine is highlighted with red color;



10. Now, please search “meterpreter” in the left column, and choose “post-multi-manage-shell_to_meterpreter”, and run it; you are expected to see the following picture;



11. Right Click the victim host icon, to go meterpreter, click “interact”, then the meterpreter session will be open to you. You can run commands like “post/linux/gather/hashdump”;



12. In the meterpreter session, play with some commands of meterpreter (you can find the command cheatsheet online); you are free to try any with no restriction, take screenshots whenever you have something good to share with the class

Requirement: The report will all be evaluated based on the following grading criteria.

Correctness	25%
Completeness	25%
Clarity	25%
Quality of English writing	25%

Appendix-Set-up:

1. The lab has been tested to work successfully for Kali versions through v1.1.0 (you can check your Kali version by command *lsb_release -a*), metasploitable 2, Dirbuster v1.0, based on VMware Workstation 11.0.0 build-2305329; If your lab has problems, please try to use Kali v1.1.0 instead of v2.
2. When opening the virtual machines, please choose "host-only: a private network shared with the host" in Virtual Machine Settings->Network Adaptor->Network Connection;
3. When you have network connection problem, VMware->Edit->Virtual Network Editor can help you restore defaults of VMnets;
4. On the operating system Metasploitable 2, mysql was configured to have no password for the root. However, tikiwiki requires mysql's password for root should be "root". (Using command *ls –al|grep setup* you can find *tiki-setup_base.php* where you can further get to know that *db/local.php* is the basic configuration for database prerequisite. Here, you will find the password that tikiwiki will give mysql is "root".)

   So, we need to either delete the password or change mysql to have "root" as the password. The command for the latter case is: *mysql –u root*; *set password = PASSWORD('root')*; or *update user set password=PASSWORD("root") where User='root'*; *flush privileges*;
5. When you want to connect to Internet, you can create another network adaptor in the VM settings and set it to NAT mode. You need to open the VMware with administrator privilege to get this done.