CIS6395: Homework 4

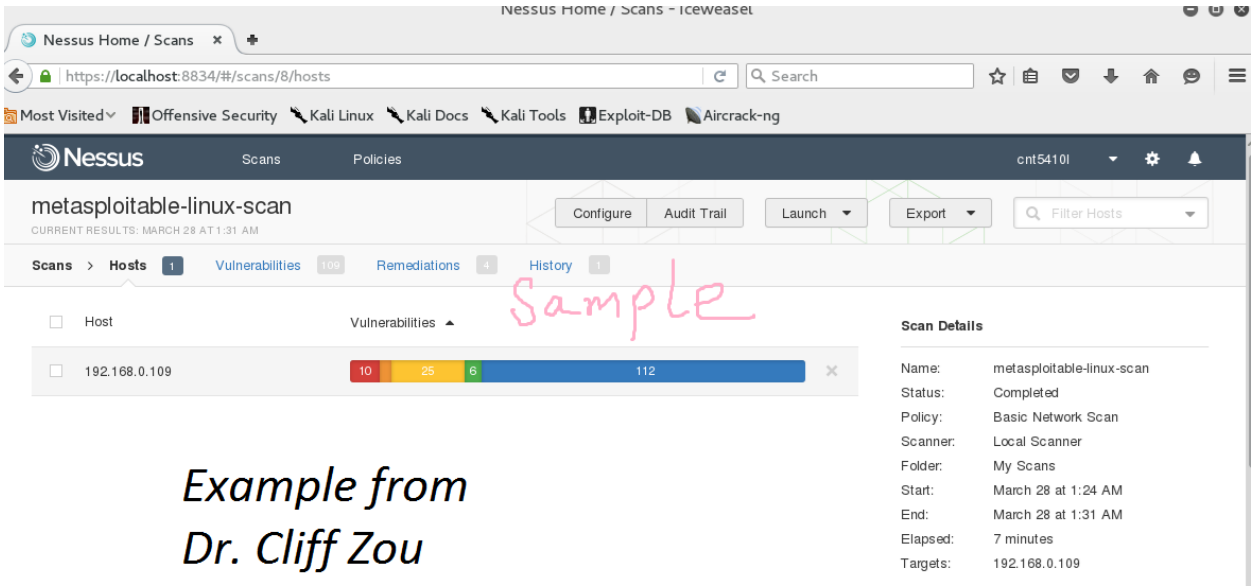
University of Central Florida
Cliff C. Zou
Assigned: Nov. 27th, 2016; Due: midnight Dec. 4th, 2016

Question 1: (**Nessus installation and testing, 25 points**)

Following my teaching in class and slides, please download and install Nessus (home-only free version) on your Kali Linux VM.

(1). On your Kali Linux VM, use browser to access and use the Nessus installed on the same VM. Please show the screenshot image of your browser showing the Nessus login interface.

(2). After you log in your Nessus, run network scan to scan your Metasploitable Linux VM. After the scan finished, show your scan result screenshot image, something like (it would be OK if you found less than 10 critical vulnerabilities):



Question 2: (**Online Password Cracking, 25 points**)

In class, I have demonstrated how to use Hydra to do online password guessing attack to obtain WinXP VM's user account password, and then run remote desktop to control the WinXP.

(1). Run your WinXP VM, change the default user 'IEUser' password to be 'computer'.
(2). On your Kali Linux VM, run Hydra to do password attack to the remote desktop service running on the WinXP VM, against the default WinXP account 'IEUser'. Please use the password list file: /usr/share/john/password.lst for this attack.

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

(3). With the password on hand, conduct remote desktop connection to your WinXP VM. Show the screenshot image of your command together with the WinXP logon interface.

Question 3: (Metasploit compromising WinXP, 25 points)

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. For payload, use the reverse-tcp meterpreter remote shell.

(1). What are the IP addresses of your Kali Linux and your vulnerable WinXP?

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

(3). Under the newly created meterpreter shell, display the compromised WinXP IP configuration, and then display the password hash of all accounts in your WinXP. Use screenshot images to show the results.

Question 4: (Armitage Exploitation, 25 points)

Please run your Kali Linux VM, your metasploitable Linux VM, and your vulnerable WinXP VMs together. Make sure they can see each other and can see your host OS. 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 three VMs and your host OS?

(2). Run Armitage on your Kali Linux, then conduct nmap scan in Armitage. Use screenshot image to show the Armitage interface where the target window section will only show these two computers' icons 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 these three target machines. When Hail Mary attack finishes, the two VMs should have been compromised (red light-bolted!). Use screenshot image to show the Armitage interface after the attack finishes.