Lab Assignment 3:
Reconnaissance and Scanning

Cliff C. Zou
University of Central Florida

Question 1: Please use Internet information gathering method we introduced in class to find out for the domain name “nba.com”:

(1). What is the domain’s registrar name?

(2). Provide the list of authoritative DNS name servers (provide their names would be fine, no need for IP addresses)?

(3). What is the domain’s admin name and, address and phone number?

Please explain how you find the above answers, and show the screenshot images.

Question 2: Use google hacking techniques introduced in class to do information gathering about the domain “ist.ucf.edu”:

(1). The list of word files (with file type of .doc) you can find in IST that contain keyword “phone”. Please show the Google search phrase you have used to get your answer.

(2). Find the PDF files in IST that contains “security” in the PDF title (note: not file name). List these PDF files’ title. Please show the Google search phrase you have used to get your answer.

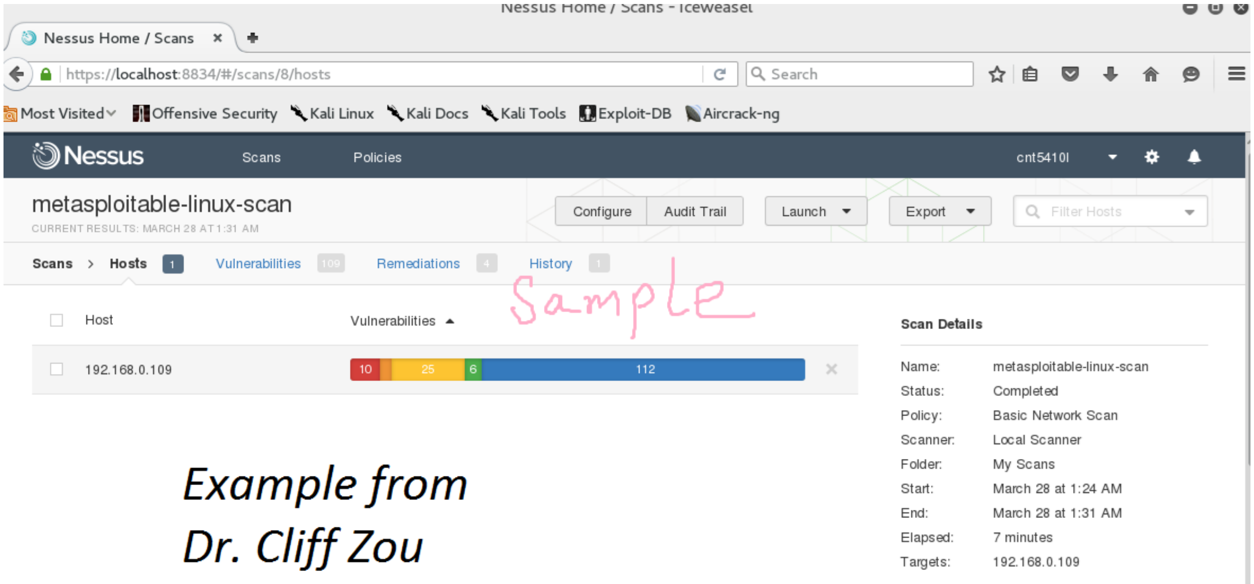
Please show the screenshot images of your Google search result webpages.

Question 3: (**Nessus installation and testing**)

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):



metasploitable-linux-scan

CURRENT RESULTS: MARCH 28 AT 1:31 AM

Host	Vulnerabilities
192.168.0.109	10 25 6 112

Sample

Scan Details

Name:	metasploitable-linux-scan
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	March 28 at 1:24 AM
End:	March 28 at 1:31 AM
Elapsed:	7 minutes
Targets:	192.168.0.109

Example from
Dr. Cliff Zou

Question 4: (Nmap Scanning):

Run your Kali Linux and your Metasploitable Linux VM in the same virtual LAN. The on your Kali Linux, run nmap to conduct the following scan:

(1). Conduct standard ***fast*** scan to scan your Metasploitable Linux VM. Use screenshot image to show your command and result.

(2). Conduct ***fast*** scan to discover ***standard service*** opened on the Metasploitable Linux VM. Use screenshot image to show your command and result.