Computer Security Fundamentals – Spring 2023

Kali Linux, Port Scanning, Footprinting and OSINT **Total: 10 points**

Q1. Kali Linux Installation (2 pts)

As you might know, the Kali Linux is derived from Debian Linux with lots of its own tools installed on it. Most of the tools are for penetration testing and some of them are for hacking.

In your house, you might be able to set the setting of the Network in the VirtualBox as "Bridged Adapter". However, in the school, it looks like you can only use "NAT" for your setting. Otherwise, it cannot connect to the internet

Show me your installed Kali Linux and try to get some screenshots. I only need to have 2 pictures.

1) **The one picture is the prompt for an user's login (1 pt)**
2) **Another one picture is about your desktop (1 pt)**

Q5. nmap (4 pts)

Our sand server is located in vh222004.truman.edu

If you still remember, I use the "nslookup" to find out the following: this guy is equipped with 2 Ethernet cards. Of course, 2 interfaces are assigned with "2 different IP Addresses" respectively.

Now, you can use the "nmap" command to scan the 2 IP Addresses. Tell me the following:

1) **In the 1st scanning of IP Address, what are the opened ports below 6000? (1 pt)**
   (You can just give me a screenshot)

2) **In the 2nd scanning of IP Address, what are the opened ports below 6000? (1 pt)**
   (You can just give me a screenshot)

3) **Tell me what is the operating system (OS) this guy is using? (1 pt)**

4) **Tell me what is the version of Apache server this guy is using? (0.5 pt)**

5) **Tell me what is the version of OpenSSH this guy is using? (0.5 pt)**

Q3. Spiderfoot (4 pts)

Use the spiderfoot to make some queries against a target

Let's see what you can get?

Note: If you find something, you don't need to let the related person know to get us into unnecessary troubles. Trust me, they get panic easily! The best way is to go the website of online database to see how they "define" the anomalies?

1) **Go to the New Scan → "By Module" and check the "only one" following module: "Leak-Lookup"**
   Of course, you need to "deselect" all of modules first.

   Give a name to the scan in this time. (Any name)
   Then, put this Truman staff's email into the query "target"
   jmcnabb@truman.edu

   Start the scan!

   Note:
   This is a VERY IMPORTANT tool to check your own old email accounts.
   See if your emails is leaked everywhere in the internet?

   Tell me what do you have (Give me a couple of screenshots) from the query against this guy's email account. (2 pts)

2) **Go to the New Scan → "By Module" and check the "only one" following module: "URLScan.io"**
   Of course, you need to "deselect" all of modules first.

   Give a name to the scan in this time. (Any name)
   Then, put this Truman website into the query target
   www.truman.edu

   Start the scan!

   After the scanning, you will find our Truman uses a VERY special web server.
   Tell me what is the "name" of the web server and the "version" (it could be more than one web server) of that by giving me a couple of screenshots (and point out the name, of course). (2 pts)

Note: For all the "scans" here, they are actually "queries" against DB, not the real scans by yourself.