**CSC 312 Cybersecurity LAB 01 Points: 20**

**ELIJAH CHONG TAY**

Please download the required software from the URL I have provided in this assignment, even though newer versions of some of the software is now available. This ensures uniformity among all students for my grading purposes. Create the folder **C:\Software** to place all downloaded software.

**PART A**

* **Set up VirtualBox**

Oracle VM VirtualBox is a hypervisor (virtualization software) for x86 computers from Oracle Corporation ([**www.virtualbox.org**](http://www.virtualbox.org/)**)**. VirtualBox may be installed on a number of **host** operating systems, including: Windows, OS X, and Linux. It supports the creation and management of **guest** virtual machines running versions and derivations of Windows and Linux.

* Access [**https://download.virtualbox.org/virtualbox/6.1.38/VirtualBox-6.1.38-153438-Win.exe**](https://download.virtualbox.org/virtualbox/6.1.38/VirtualBox-6.1.38-153438-Win.exe)and download the VirtualBox executable code for Windows hosts.
* You will download **VirtualBox-6.1.38-153438-Win.exe** for Windows hosts. Copy the file to the folder **C:\Software**.
* Now that we have downloaded an executable file, we want to be sure that it does not have any virus content and has not been tampered with. First, scan the file with any virus scanning software you have access to. If there is any virus content, immediately delete the file.
* To verify that the file has not been tampered with, check its SHA256 hash. Open a command window and type the following command:

**SHA256**

C:\Users\etays> certutil -hashfile C:\Software\VirtualBox-6.1.38-153438-Win.exe SHA256

SHA256 hash of C:\Software\VirtualBox-6.1.38-153438-Win.exe:

e987f1705d8 79 959320a4d968be53d98dd5389425ebc66292a1b1d5241153f7

CertUtil: -hashfile command completed successfully.

Ensure that it reads as below (where 8 hex digits have been deleted)

**e9 87 f1 70 5d 87 79** 95 **93 20 a4 d9 68 be 53 d9 8d d5 38 94 25 eb c6 62 92 a1 b1 d5** 24 11 **53 f7**

If not, discard the file and start all over.

Provide the missing digits

* Install VirtualBox. It should be straightforward with no complications. Accept default options. Did you install VirtualBox successfully?

Yes

* **Installing VirtualBox Extension Pack**
* Access [**https://download.virtualbox.org/virtualbox/6.1.38/Oracle\_VM\_VirtualBox\_Extension\_Pack-6.1.38.vbox-extpack**](https://download.virtualbox.org/virtualbox/6.1.38/Oracle_VM_VirtualBox_Extension_Pack-6.1.38.vbox-extpack) and download the Extension Pack under VirtualBox 6.1.38.
* Copy the downloaded file to **C:\Software** and determine its SHA256 hash.
* Ensure that it reads as below (where 8 hex digits have been deleted)

SHA256 hash of C:\Software\Oracle\_VM\_VirtualBox\_Extension\_Pack-6.1.38.vbox-extpack:

052f26cf8c619b1aa0cad94c05ece0c1ae326248b4746c95e1deb0729ae4417a

CertUtil: -hashfile command completed successfully.

**05 2f 26 cf 8c 61 9b 1a a0 ca d9 4c 05 ec e0 c1 ae 32 62** 48 b4 74 6c **95 e1 de b0 72 9a e4 41 7a**

* To install the extension pack, run VirtualBox as Administrator. **Choose File Preferences Extensions**. Click **Add New Package** button on the right and select the downloaded extension pack. Accept the license agreement and let the extension pack install.

**PART B**

* **Installing Kali Linux**

Kali Linux ([**www.kali.org**](http://www.kali.org/)) is a [Debian](https://en.wikipedia.org/wiki/Debian)-derived [Linux distribution](https://en.wikipedia.org/wiki/Linux_distribution) designed for [digital forensics](https://en.wikipedia.org/wiki/Digital_forensics) and [penetration testing](https://en.wikipedia.org/wiki/Penetration_test). It is preinstalled with over 300 penetration-testing programs, including Armitage (a graphical cyber-attack management tool), nmap (a port scanner), Wireshark (network traffic analyzer), John the Ripper (a password cracker), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP (both web application security scanners). Kali Linux can run natively when installed on a computer's hard disk, can be booted from a live CD or live USB, or it can run within a virtual machine. It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits.

While it is possible to install Kali from scratch, it is much simpler to import a VirtualBox appliance provided by Offensive Security ([**www.offensive-security.com**](http://www.offensive-security.com/)). That is what we will do.

* Access [**https://kali.download/virtual-images/kali-2022.3/kali-linux-2022.3-virtualbox-amd64.7z**](https://kali.download/virtual-images/kali-2022.3/kali-linux-2022.3-virtualbox-amd64.7z)and download the Kali Linux 2022.3 VirtualBox image.
* You will download a file named **kali-linux-2022.3-virtualbox-amd64.7z**. Copy the file to **C:\Software**
* Determine its **SHA1** hash (not SHA256). Ensure that it reads as below (where 8 hex digits have been deleted)

**b0 64 23 86 22 74 ec 18 6e 73 df 9e 58 43 6f 7f f4 -- -- 20**

Provide the missing digits: 2386

* Unzip the file. Then double click the file name kali-linux-2022.3-virtualbox-amd64.vbox to install Kali in the VirtualBox. The process should proceed smoothly and the newly created virtual machine should now appear on the left column.
* **Explore Kali**
* Select Kali Linux in the list of machines available on the left. A brief indication of the properties of the virtual machine should appear on the right. If necessary, you may also select Settings and determine more information. There is no need to modify any of the properties of the virtual machine. Just explore the settings and report.

When the virtual machine is run, the amount of base memory it will use is 2048 mb

The number of processors (cores) it can take advantage of is 2 but at a max of 12

The virtual machine will have a virtual disk of 2048mb but at a max of 16384mb capacity.

The network adapter is attached to NAT. What does NAT mean?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Network Address Translation

Login credentials needed to login on this installation of Kali are:

Username: kali Password: kali

* Start the Kali Linux. Wait for it to boot completely and show the login screen. Login.

Press the Applications icon (most top left icon). All the preloaded tools are organized under various categories. On the left there is a listing of the tools categories. List these 13 categories.

Information Gathering, Vulnerability Analysis, Web Application Analysis, Database Assessment, Password Attacks, Wireless Attacks, Reverse Engineering m Exploitation Tools, Sniffing & Spoofing, Post Exploitation, Forensics, Reporting Tools, Social Engineering Tools

* Check the connectivity to the outside world by pinging **courses2016.brockport.edu**. Press **control-C** to stop the output.

Where you able to ping? yes

What is the IP address of **courses2016.brockport.edu**? 137.21.7.65

* Open a terminal window. Type the command **ifconfig** and determine the IP address.

The IP address is: 127.0.0.1

Is this a private or public IP address? private

* Open Firefox, use the URL [**www.whatismyipaddress.com**](http://www.whatismyipaddress.com/) and determine your public IP address. Close Firefox.

Public IP address: 67.240.197.240

* Close Firefox. Close the terminal window by typing the command: **exit**
* Shut the machine down by pressing the power button the right top.

**PART C**

**Examine Data Breaches**

The Privacy Rights Clearinghouse (PRC) is a nonprofit organization whose goals are to raise consumers’ awareness of how technology aﬀects personal privacy and empower consumers to take action to control their own personal information. The PRC maintains a searchable database of security breaches that impact consumer’s privacy. In this lab you will gather information from the PRC website.

* Open a web browser and enter the URL <https://privacyrights.org/data-breaches>.
* First spend time reading about the PRC. Click About in the toolbar.
* Go back again to the home page and scroll down until you see the “More” button at the bottom of the page (big orange button). Click the More button then choose “Data Breach Chronology”.
* Download a compilation of the Chronology of Data Breaches.
* On the Data Breaches page scroll down and observe the diﬀerent breaches and businesses listed under “Chronology Legend”.

List the type of Breach:

CARD - Fraud Involving Debit and Credit Cards Not Via Hacking (skimming devices at point-of-service terminals, etc.)

 HACK - Hacked by an Outside Party or Infected by Malware

 INSD - Insider (employee, contractor or customer)

 PHYS - Physical (paper documents that are lost, discarded or stolen)

 PORT - Portable Device (lost, discarded or stolen laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape, etc.)

 STAT - Stationary Computer Loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility)

 DISC - Unintended Disclosure Not Involving Hacking, Intentional Breach or Physical Loss (sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax)

 UNKN - Unknown (not enough information about breach to know how exactly the information was exposed)

List the type of Business:

BSF - Businesses (Financial Services, Banking, Insurance Services)

BSO - Businesses (Manufacturing, Technology, Communications, Other)

BSR - Businesses (Retail/Merchant including Grocery Stores, Online Retailers, Restaurants)

EDU - Educational Institutions (Schools, Colleges, Universities)

GOV - Government & Military (State & Local Governments, Federal Agencies)

MED - Healthcare and Medical Providers (Hospitals, Medical Insurance Services)

NGO - Nonprofits (Charities and Religious Organizations)

UNKN – Unknown

Now open the database that you installed in step 3. Create a customized list of the data that will only list data breaches of educational institutions. Observe the breaches for educational institutions.

How many breaches that were made public pertain to educational institutions? 9

* Go to the home page <https://privacyrights.org/>, scroll down to the website footer then choose “Spam”. In Spam page open the second guide called “Reducing Spam”. List a brief description of actions could be taken to reduce the amount of spams that you receive.
* Don’t open
* Don’t click links
* Don’t reply
* Set filters and block
* Create a secondary email
* Look to opt-out
* Report spammers
* Go again to the website footer then choose “Identity Theft”. In Identity Theft page open the second guide called “Reducing Your Risk of Identity Theft”. List a brief description of actions could be taken to reduce the risk of the identity theft.
* Limit your cards
* Watch your cards
* Protect your credit
* Make better passwords
* Protect your SSN

**PART D**

**Scan Web Browser Plug-ins**

Web browser plug-ins and add-ons can be security risks. In this activity you will check the health status of your web browser and any plug-ins using the Qualys BrowserCheck.

* Use your web browser to go to [https://browsercheck.qualys.com](https://browsercheck.qualys.com/).
* Click Learn more about Qualys BrowserCheck and read through the features of this program.
* Return to the home screen.
* Click Scan without installing plugin and then click Scan Now.
* A screen showing any insecure versions of plug-ins or browser updates that are missing will be displayed. If necessary click Fix It to address any security issues.
* Now you should take a screenshot for step e. Save the captured screenshot print it out and attached to your assignment.
* Graphical user interface, text, application, email

  Description automatically generated