CSE 5473 — Network Security Autumn 2020

Lab #3

Understanding the Privacy with TOR and Bluetooth *Due Nov 20th, 11:59PM*

1 Key Objectives

- Reinforce your concept about data security and privacy.
- Get familiar with Tor and Tor based applications (i.e. DarkWeb).
- Learn how to use Tor to protect your privacy.
- Refresh your memory about Bluetooth workflow and privacy .
- Learn how to use tools to analyze Bluetooth traffic.

2 Task 1: Experiment Setup

2.1 Install the Testing Platform

1. Please install VMware:
   - If you are MacOS users, please download and install VMware Fusion. You can download a free trial version (at `http://www.vmware.com/go/try-fusion-en`). For more details, please refer to `https://kb.vmware.com/s/article/2014097`.
   - If you are either Windows or Linux users, please download and install VMWare Station at `https://my.vmware.com/en/web/vmware/downloads/details?downloadGroup=PLAYER-1600&productId=1039&rPId=51984`.
2. Please download the System Image at `https://drive.google.com/file/d/1MrouCQ5BxxQsj4Z0sH7TVryol6x3VHHi/view?usp=sharing`.

   Please note that the System Image provided in this lab is different from the one used in lab#2. This lab has all the required software installed and all the software can be found in "/home/cse5473". Therefore, if you download and import this System image into your VMware, you can **SKIP** the following software installation steps:

   - **Installing** Tor Browser: You can use the following command to install Tor Browser:
     - Download Tor Browser at `https://www.torproject.org/dist/torbrowser/10.0.2/tor-browser-linux64-10.0.2_en-US.tar.xz`.
     - Unzip "`tor-browser-linux64-10.0.2_en-US.tar.xz`".
   - **Install whois.** Whois is a tool for searching the specific information (e.g., current registrar, registrant information) of a specific domain. You can use the following command to install whois.

```
$ apt install whois
```

- **Install Tor service.** Tor service can anonymize all the traffic from your machine. You can use the following command to install Tor service.

```
$ sudo apt install tor
```

- **Install Crackle**: Crackle is a Bluetooth hacking tool which works against Bluetooth legacy (i.e., Bluetooth 4.0 and Bluetooth 4.1). It allows an attacker to brute force the TK (Temporary Key) and decrypt the encrypted Bluetooth packets.
  - Download Crackle at `http://lacklustre.net/projects/crackle/crackle-0.1.tgz`.
  - Unzip Crackle.

    ```
    tar -zxvf crackle-0.1.tgz
    ```

  - Install dependency using the following commands.

    ```
    $ sudo apt-get install libpcap0.8-dev
    ```

  - Go to the directory of Crackle and type:

    ```
    $ make
    $ make install
    ```

3. Unzip and import the downloaded System Image into VMware (Check the link to see how to import the system image: `https://docs.vmware.com/en/VMware-Workstation-Player-for-Linux/14.0/com.vmware.player.linux.using.doc/GUID-DDCBE9C0-0EC9-4D09-8042-18436DA62F7A.html`).

4. Login onto the system using the following credentials[1]:

```
Username: cse5473
Password: 123456
```

3 Task 2: Understanding Identity Privacy via Tor and Tor Browser (50 Points)

3.1 Using Tor Browser to visit DarkWeb (20 Points)

(a) Run `start-tor-browser.desktop`.

```
$ tar -zxvf tor-browser-linux64-10.0.2\_en-US.tar.xz
$ cd tor-browser_en-US
$ ./start-tor-browser.desktop
```

[1] Root user's password is 123456 as well

Ubuntu does not allow Root user to run Tor Browser, and you may want to log out Root user using the following command:

```
$ exit
```

(b) Find available drakwebs at `https://www.thedarkweblinks.com/darknet-market-list/`. Copy one of the addresses to the address bar of Tor Browser and press "ENTER" (See Figure 1).

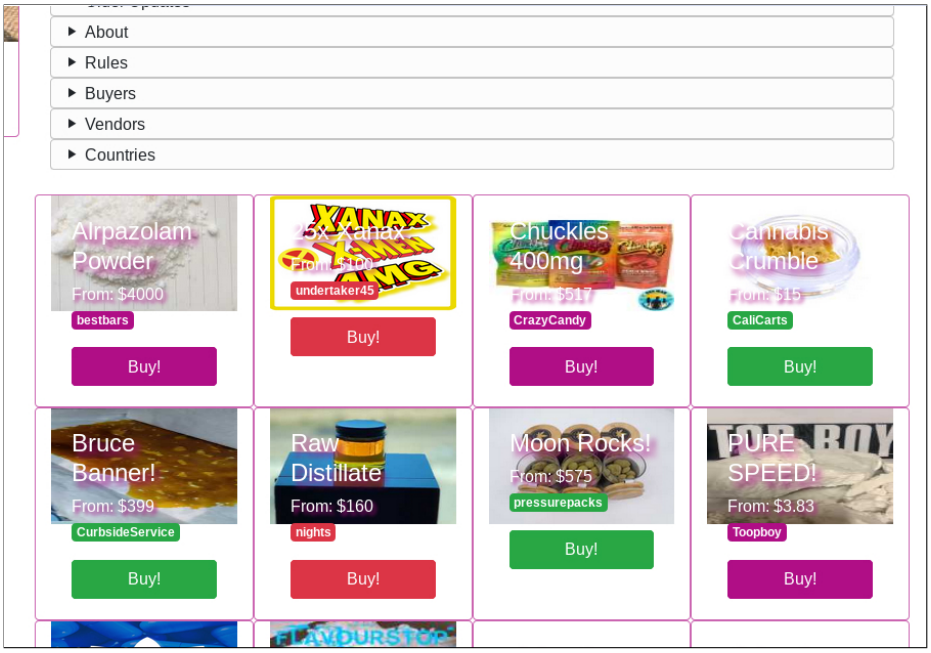

Figure 1: Dark Market

Caution: While browsing the dark webs, you should follow the following regulations:

- Some dark webs may require registration before accessing the contents. Please do not provide any personal information.
- Always use your alias to communicate with other people in dark webs.
- Please do not buy anything from dark webs.
- Please do not visit illegal content (e.g., child porn) on the dark webs.

Question 1. Put a screenshot into your report to show you have visited one of the dark webs successfully (5 points).

(c) Open your Firefox and visit `https://whatismyipaddress.com/` to check your IP address. Please remember the IP address, and we will use it later.

(d) Open your Tor Browser and visit `https://whatismyipaddress.com/` to check your IP address again.

Question 2. Are the IP addresses displayed in step 3 and step 4 the same? If not, explain why (5 points).

(e) Close your Firefox and relaunch it again. Go to `https://whatismyipaddress.com/` to check your IP address.

(f) Close your Tor Browser and relaunch it again. Go to `https://whatismyipaddress.com/` to check your IP address again.

Question 3. Are the IP addresses displayed in step 3 and step 5 the same? Are the IP addresses displayed in step 4 and step 6 the same? Please explain why (10 Points).

3.2 Understanding Tor via "whois" command (10 points)

(a) Check the information of `osu.edu` using whois:

```
$ whois osu.edu
```

Question 1. Put a screenshot into your report to show you have checked the information about `osu.edu` (5 points).

(b) Check the IP address of IP addresses displayed in Tor Browser (i.e., the IP addresses displayed in Section 3.1, Step 4 and Step 6) using whois.

Question 2. Put a screenshot into your report to show you have checked the IP addresses displayed in Tor Browser. Explain what you observed (5 points).

Please note that the IP addresses displayed can be either an IPV4 address or an IPV6 address, and whois can handle both.

3.3 Understanding Tor via Tor services (30 points)

(a) You can start Tor services using the following commands:

```
$ sudo service tor start
```

(b) Check the status of your Tor services:

```
$ sudo service tor status
```

Question 1. Put a screenshot into your report to show Tor service has been launched successfully (10 points).

(c) You can also check the running status of Tor service by visiting the following URL in Firefox: `http://127.0.0.1:9050`.

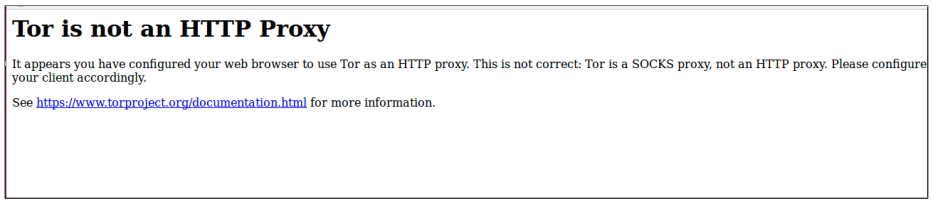

Figure 2: Check running status of the Tor service by using Firefox

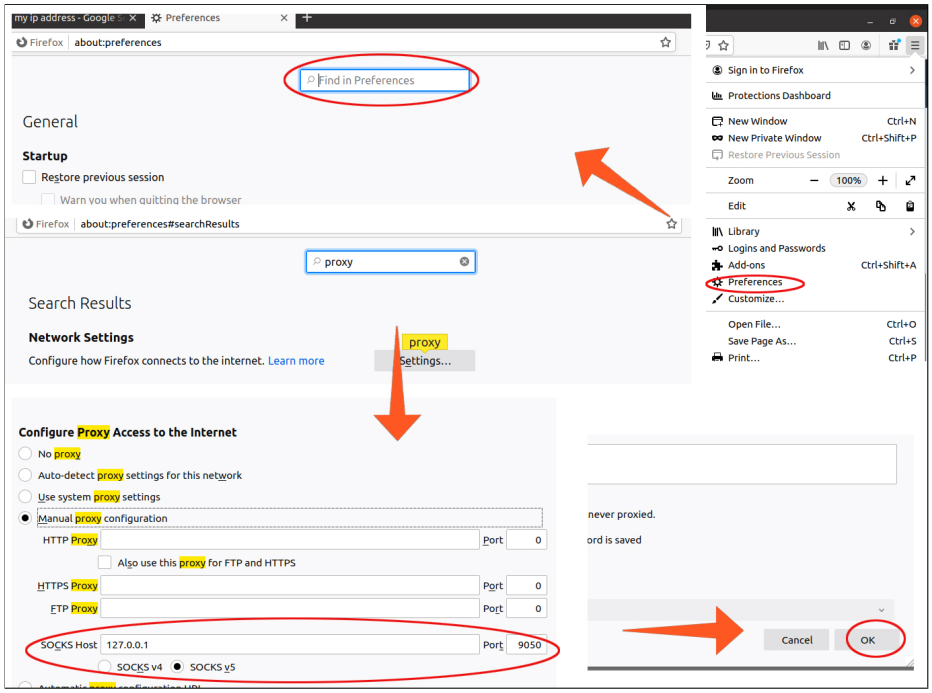

Figure 3: Enabling Proxy

(d) Configure your Firefox as follows. By doing that, we will use Tor services to tunnel the traffic (See Figure 3).

(e) Use your Firefox to visit `https://whatismyipaddress.com/` to check your IP address.

Question 2. Question 2. Put a screenshot into your report to show the IP address displayed in your Firefox. Explain what you observed (10 points)..

(f) Stop the Tor services using following command and disable Poxy (See Figure 4)

```
$ sudo service tor stop
```

(g) Use your Firefox to visit `https://whatismyipaddress.com/` to check your IP address.

Question 3. Are the IP addresses displayed in step 5 and step 7 the same? If not, explain why (10 points).

4 Understanding the Security and Privacy in Bluetooth (50 Points)

4.1 Install nRF Connect

- Please open your App Store (or Google Play for Android users) and search a mobile app named nRF Connect (See Figure 5).

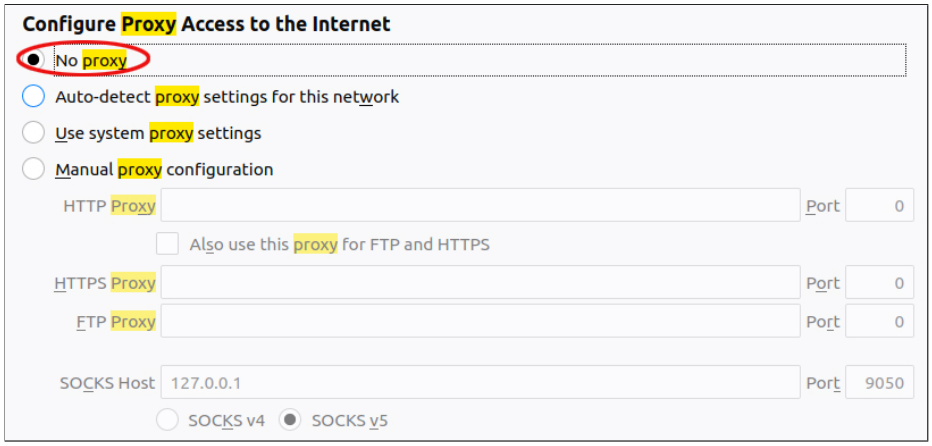

Figure 4: Disabling Proxy

- Install the app onto your iPhone or Android Phone. nRF Connect is a tool that enables Bluetooth Low energy traffic analysis.

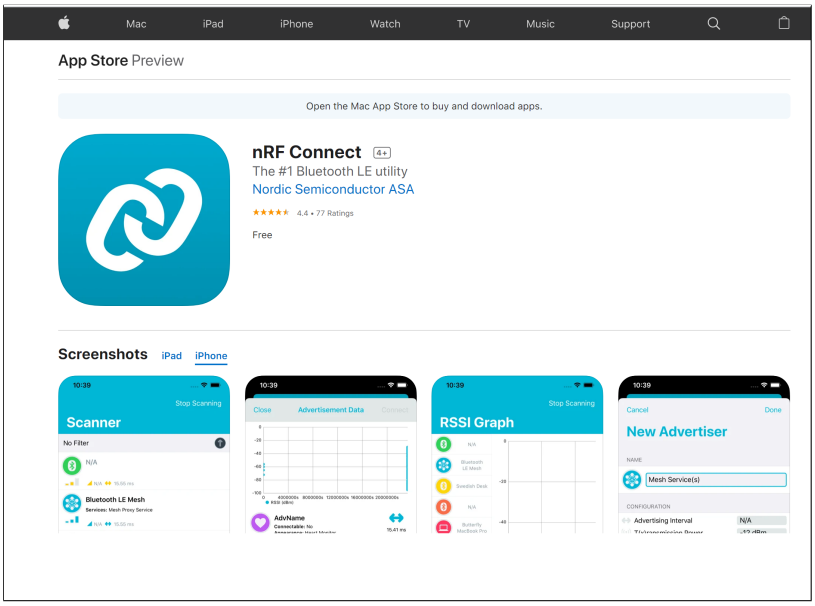

Figure 5: nRF Connect

4.2 Using mobile sniffer to observe the nearby Bluetooth Low Energy (BLE) devices (10 Points)

1. Open nRF Connect. nRF Connect will list the nearby BLE devices.
2. Check the manufacture data and MAC addresses of nearby BLE devices. The manufacture data will reveal the manufacturers of the BLE devices. Please note that iOS

does not support viewing the MAC addresses of other BLE devices.

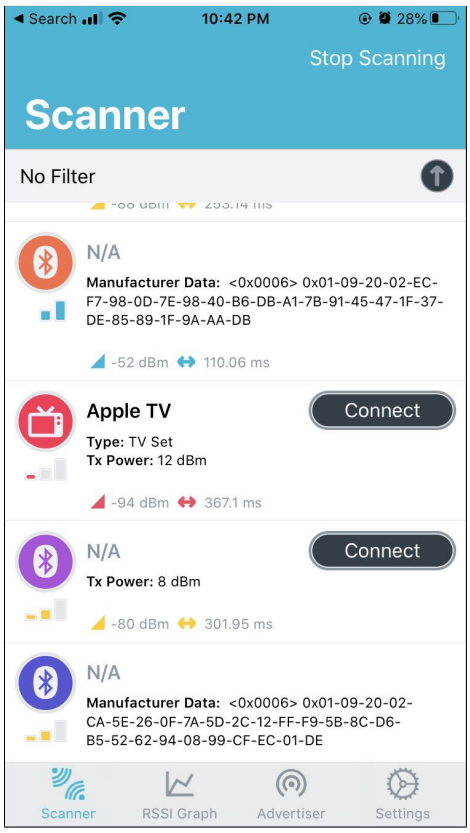

Figure 6: Nearby Bluetooth devices discovered by nRF Connect

Warnings: Do not attempt to connect other BLE devices, since it may be the violation of ethics.

Question 1. Put a screenshot into your report to show the BLE devices you have observed (10 points).

4.3 Analyzing the captured packets (30 Points)

1. Please log in your analysis platform using the provided username and password.
2. Run Wireshark.

```
$ wireshark
```

3. Configure your Wireshark to view Bluetooth packets.
   - Edit ⟶ Preferences ⟶ Protocol ⟶ DLT_USER (See Figure 7)
   - Configure the encapsulation Table. Particularly, "DLT" should set to "147" and the payload protocol should set to "btle".

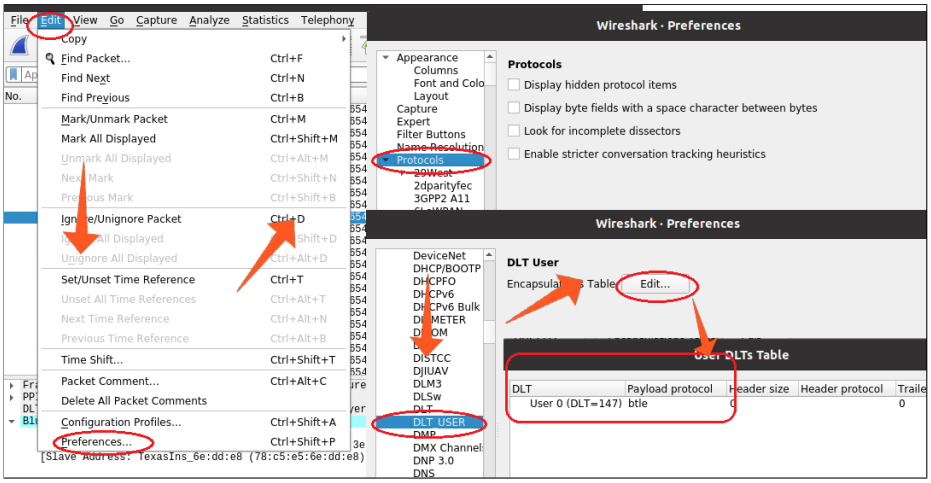

Figure 7: Configure Wireshark

4. Download the "blepcap.pcap" file at `https://drive.google.com/file/d/18iQ2MfIQYmQs8WOcRztuHce1W6YQSubp/view?usp=sharing`. Use wireshark to view the content.

5. Identify the types of the Bluetooth packets. In the example, there are 5 types of Bluetooth packets, including advertising packets (i.e., ADV_IND), scan request packets (i.e., SCAN_REQ), scan response (i.e., SCAN_RSP), connection request (i.e., CONNECT_REQ) packets, and data exchanging packets.

   Question 1. Check the format of advertising packets (i.e., ADV_IND) and answer the following question (10 Points):

   - What is the MAC address of the broadcasting device (3 points)?
   - What is the manufacture data of the broadcasting device (3 points)?
   - What is the UUID of the broadcasting devices (4 points)?

   Question 2. Check the format of scan request packets (i.e., SCAN_REQ) and answer the following question (10 Points):

   - What is the MAC address of the initiating device in SCAN_REQ (5 points)?
   - What is the MAC address of the device that the initiating device attempts to scan in SCAN_REQ (5 points)?

   Question 3. What are the security requirements of the broadcasting device (10 Points)?

   Tip: Security requirements of a device can be observed in pairing response packets, which is a special type of data exchanging packet (See Figure 8).

4.4 Install Crackle and Decrypt encrypted Bluetooth packets (10 Points)

1. Go to the directory of Crackle and type:

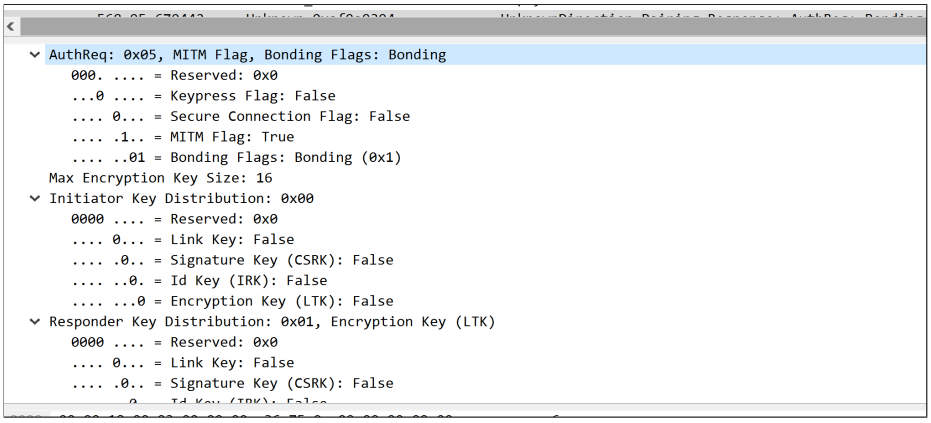

Figure 8: Checking security requirements of a device

```
$ make
$ make install
```

2. Download and unzip the testing samples at `http://lacklustre.net/bluetooth/crackle-sample.tgz`.

3. Identify Just Works Pairing:

```
$ crackle -i ltk_exchange.pcap
```

Question 1. Put a screenshot into your report to show you have identified Just Works Pairing (5 points).

4. View encrypted Bluetooth packets in file `encrypted_known_ltk.pcap` using Wireshark. It can be observed that once connected, the data exchanging packets are unreadable (See Figure 9).

5. Decrypt the Bluetooth packets using a given long term key (LTK):

```
$ crackle -i encrypted_known_ltk.pcap -o decrypt.pcap -l 7
    f62c053f104a5bbe68b1d896a2ed49c
```

6. View the decrypted Bluetooth packets in file `decrypt.pcap` using Wireshark. We can see the GATT read request now.

Question 1. Put screenshots into your report to show you have decrypt the Bluetooth packets successfully (5 points).

5 Submit Your Lab Report

Please write a report describing how you solve each of the problem above, and submit at CARMEN.

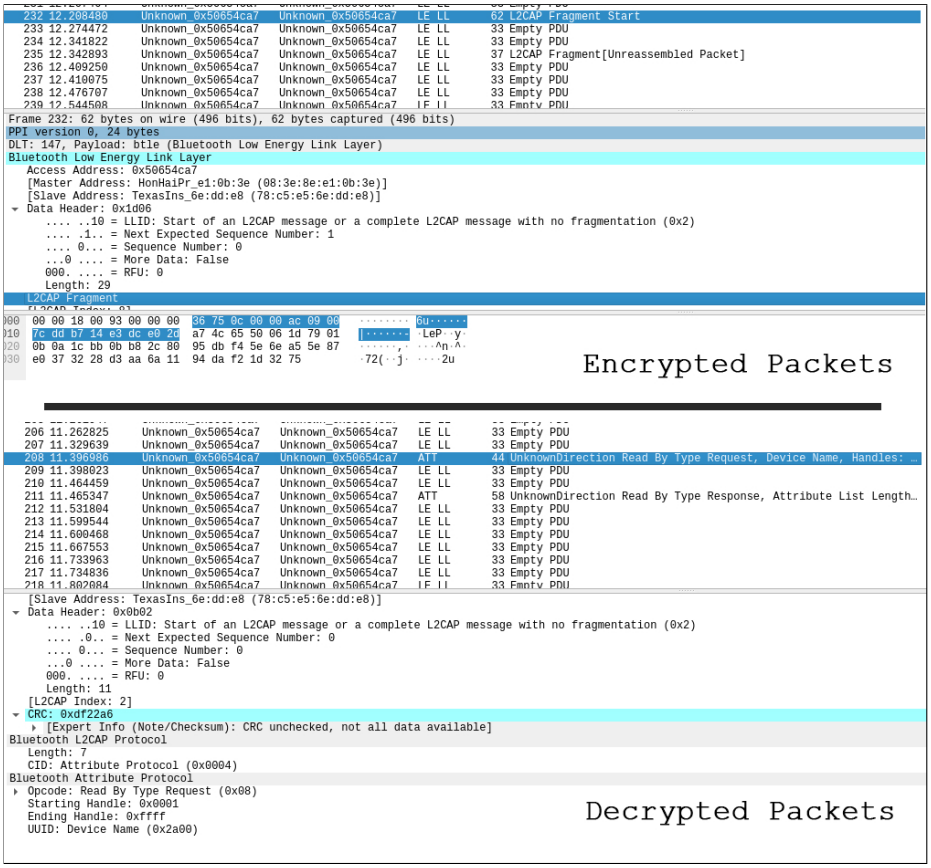

Figure 9: Encrypted packets v.s. decrypted packets

6 Code of Conduct

These labs are intended for educational purposes only, to provide a safe and legal means to gain an understanding of security by understanding threats and vulnerabilities. They are not intended for (and are not to be used for) any purposes other than for education.

Some of these labs are based on existing exploits, and students are to exploit their own virtual machines ONLY. Do not try them outside your personal devices. Use of anything learned in, during, or resulting from this class that is in any manner illegal, unauthorized, or unethical is forbidden. There are serious consequences for illegal computer hacking. Any student who violates the rules is subject to legal action, will take sole responsibility of his/her actions, and cannot hold any claim on the responsibility of the faculty, staff, or the university. Students who violate these conditions of the labs will get a failing grade in the class and may be subject to legal action. Do not incorporate or implement viruses, worms, spyware and/or Trojan horses in ANY of these labs. Only the tools and resources specified in the given lab may be used. Any student who exploits fellow student's accounts or gains the solutions to the labs by means other than specified is engaging in academic misconduct. Academic misconduct will be treated seriously.