Lab 5: Wi-Fi Attacks with Pineapples

Created: Fall 2022, Updated: Spring 2024

Monday sections: submit by 04/14 (no need for access codes)

Wednesday sections: submit by 04/16

README/NOTICE: This lab does not require approval codes. Instead, a full lab report will be submitted to HuskyCT as done previously. Questions ask for screen shots and video recordings. Please attach all questions, screen shots, and video recordings (uploaded to Google Drive, shared as a link) to a single PDF or word document.
Ensure that TAs have access to the videos or substantial points will be deduced per question. Enable "anyone with the link" access to video recordings if shared on Google Drive. When using lab laptops, you can transfer recordings to the VM and then download them at home to create your report. Do not use your phones to take screenshots and recordings, these are often of unacceptable quality. This lab requires working with a physical device during the lab period. We advise you to start working on the lab before your section time so you can make best use of both 2-hour class periods.

Wi-Fi is the common technology for wireless local-area communication, used by most laptops, phones, and other wireless computing devices. The protocols are defined in a series of IEEE standards numbered 802.11, with a letter identifying the specific variant, e.g., IEEE 802.11n. Users identify a specific Wi-Fi network by its `name', e.g., UConn-Secure; these `names' are referred to as **SSID**s, which stands for Service Set IDentifiers.

In this lab, we will learn a bit about some of the risks associated with Wi-Fi, mainly, the risk of `rogue access point' attack, using a special `hacking tool' called Pineapple, produced by Hak5. The **Pineapple** is a tool for Wi-Fi penetration testing, that can be used to launch multiple attacks and detect different Wi-Fi vulnerabilities; we will use it for the rogue access point. We believe all students will use the *Mark VII Pineapple*. We also have an older model, *Pineapple Tetra*, which is also okay for our needs, but we don't think we'll need to use these.

Throughout this lab, you will find the Pineapple Mark VII documentation page very helpful (scroll down, it has many sections). There's also plenty of other online sources you could use: YouTube videos, Q&A sites and more. But we believe this site should suffice. Just notice that documentation isn't always for the version you use.

At the end of this lab, you will rebox the Pineapple in its original packaging. Do not throw or take the packaging (or the Pineapple 😊).

Question 1 (10 points):

Before starting with this task check if your pineapple needs to be configured. They may advise you to skip to Step (3). Your first task is to configure your Pineapple Mark VII device which will be the main workhorse for this lab. This task consists of two or three steps: **(1) connecting the Pineapple, (2) factory**

reset and recovery, and then **(3) Pineapple configuration.** Step (2) should hopefully not be required, as the Pineapples should usually be already installed when you receive them.

Text instructions are provided below; you can also use a video tutorial that Mason (a prior TA) has kindly prepared for you: https://www.youtube.com/watch?v=eJJUxfhIa14. If you watch this or another video in the lab, please use earphones to avoid disturbing other students.

Step (1): connecting the Pineapple. Note: instructions assume you use a Windows 11 laptop; adjustments may be required for another operating system. Feel free to use a lab laptop, ask your TA when they are distributing equipment.

1. Unbox the device.
2. Unplug the Wi-Fi Pineapple completely from all power sources (if connected to any).
3. Connect the three antennas to the Wi-Fi Pineapple. This must be done before powering on the pineapple (or it may be damaged!).
4. Hold the reset button on the device.
5. **With the reset button held**, connect a USB-to-USB-C cable between your laptop's USB port, and the USB-C port on the Wi-Fi Pineapple. (It may help to disconnect the laptop from the Ethernet)
6. Continue holding the reset button until the LED blinks red three times, then release the button and the LED will (should) show solid red.
7. From your computer, configure the USB Ethernet interface (ASIX) associated with the Wi-Fi Pineapple to have a static IP address of 172.16.42.42 with the netmask 255.255.255.0, as follows.
    a. Go to Windows settings --> Network and Internet --> Ethernet --> change adapter options.
    b. You will see three ethernet interfaces. One of these should be ethernet-over-usb. The other two are related to the VBox and physical RJ-45 Intel Ethernet cards.
    c. Right Click on the ethernet-over-USB interface and select properties.
    d. Select "Internet Protocol Version 4 (TCP/IP)" from the list and hit properties.
    e. Select the option to configure the manual IP address and enter the IP address 172.16.42.42 with the subnet mask 255.255.255.0. The number here can be an arbitrary number between 2-255, we just picked 42. This would instruct your computer to use IP address 172.16.42.42 for the interface, i.e., when sending or receiving IP packets over this interface. The mask (255.255.255.0) means that if the computer sends a packet to any IP address of the form 172.16.42.x, where x is an integer between 0 and 255, then it should send this packet to the network connected to the ethernet-over-USB interface. Notice our VMs are on a different network. You may need to also give IP for DNS resolver, you can use 8.8.8.8.

Step (2), perform only if needed: factory reset and recovery. You will need this step only if your pineapple got into a bad configuration for some reason. Consult with the TA if you think this happens; the TA may provide another solution instead of reset (e.g., a different pineapple). Factory reset and recovery should take no more than 10-15 minutes max, if it takes longer, consult the TA.

The instructions for factory reset and recovery are available from the official (Hak5) website; we give below instructions tailored to our needs, esp. when installing from within the lab. If you watch the video in the lab, please use earphones to avoid disturbing other students.

The Wi-Fi Pineapple features a firmware recovery web interface which allows you to restore the device to factory state. This recovery interface is only accessible via the USB Ethernet interface and cannot be accessed via Wi-Fi.

1. Download the recovery firmware and the latest firmware (currently version 2.1.3). If you are **using the lab's network** (and laptop), download a zip containing both files from http://submit.edu/downloads. If you use a non-lab laptop (over VPN), you will need to download the latest firmware (currently version 2.1.3) and the recovery firmware from Hak5. But best use the lab laptops.
2. Navigate to the recovery tab, upload the recovery firmware file (image) from the first step and flash the firmware. The image is the file "**pineapple-mk7-upgrade.bin**." that you downloaded from the VM.
3. **Do not power off or unplug the Pineapple Mark VII until the recovery process is completed.** A LED blinks until the process completes, which will take between **5–10** minutes.
4. When finished, the Pineapple will reboot, and you may access in Chrome the initial setup page at http://172.16.42.1:1471. Notice the port (1471).
5. You now should proceed with setting up your pineapple, specifically, installing the updated firmware (currently version 2.1.3). Chose the option of setup using (your existing) USB-C Ethernet connection, by quickly pressing the reset button, and then choose the file you've downloaded and it'll install.

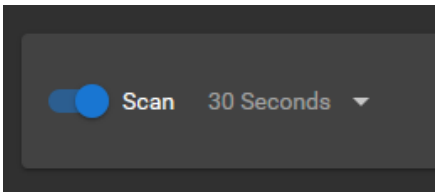
Step (3), Pineapple configuration. Now you can proceed to setup your device. The setup page is shown below.

1. From your computer, use Chrome to browse to http://172.16.42.1. The IP address 172.16.42.1 is of the form 172.16.42.x (with x=1), hence, as explained above, you computer is now configured to communicate to this addresss using the ethernet-over-USB interface, which is connected to the Pineapple. The Pineapple will be waiting for traffic on this IP (and expect to communicate with the laptop at IP 172.16.42.42).
2. Set a root password of **cyberlab**
3. Choose **secure-<section_number>-<group_number>** as your management SSID, which you can use to manage the pineapple. Use password **cyberlab**.
4. Under Open AP Setup type: **open-<section_number>-<group_number>** as the Open Access Point (AP) SSID. Uncheck the Hide Open Access Point Box.
5. Under "Client Filters Setting" click Deny Mode and under SSID filters setting click Deny Mode.
6. Accept the EULA and Software License.
7. The web interface provides a terminal for command line, or you can SSH using Mobaxterm.
8. The server may display HTTP Error; this is normal. Go to your wireless networks, you should see the two networks you created there.
9. Join the management wireless network you created, secure-<section_number>-<group_number>, and then log into the webpage still on the address 172.16.42.1:1471. This is the administration console for the Pineapple, and you should see the Dashboard; the Dashboard is also accessible from the right-hand side menu.
10. Click on the Settings button located on the bottom left corner of the web interface, then navigate to the "Networking" tab. Under the section "Wireless Client Mode", note the **interface name** then click on "scan". Select "cse3140" as the network with password "ciscoCSE3140".

11. **Note: If you need to restart your pineapple** (remove all configuration) you can do this by holding the setup button on the back of the device for five seconds. This will remove all your settings.

Submit in HuskyCT: Screen shots of the Wi-Fi administration console and dashboard, and explanation, in your own words, of the different fields and their values. Include the interface name in your report as noted in step 10 above, it is typically 'wlan2'. Use the documentation to understand, but do not copy verbatim.

Question 2 (10 points): Go to the Recon tab on the side menu. It contains two tabs (in the top line), Scanning and Handshakes. In the `Scanning' tab, enable scanning by clicking the switch to the on position:



Connect (from a PC) to the ***unprotected network*** you created (**open-altschuler-<section_number>-<group_number>)**.

Submit in HuskyCT: Screenshots of the Scanning and Handshakes tabs (within Recon). Explain, in your own words, the different fields and their values.

Question 3 (15 points): On your phone, disconnect from Wi-Fi and start a personal hotspot. This can typically be found within the settings application on your device. If you can change the name of your hotspot, change it to either your name or CSE3140 followed by your section and team. (On Android: you can change the name in Settings under Wi-Fi Hotspot. On iPhone: you can change your device name under Settings->General->About. The name of your device is your hotspot name). Scan again and remain on the Recon tab. You may have to change "30 seconds" to "continuous" for continuous scanning.

1. Can you find this access point?
2. Can you see the users connected to this or any access point?

Try connecting to your phone's personal hotspot (from a laptop or another phone). Click on the network and a client (if available) to see details and options; if you can find, click further to see `tagged parameters' and 'security information'. Notice the `deauthenticate' button; we'll return to it soon.

Return now to the Handshake screen, and see if any handshakes were captured.

Notice: you can download captured handshakes for analysis; one format available is PCAP which is supported by the popular WireShark analysis software (and others). But since you may not have learned networking yet, we will not ask you to do this.

Submit in HuskyCT: Answers to the above questions and screen shots of the Scanning tab addressing all the above aspects. Explain, in your own words, the different fields and values. Report any handshakes found. No need to explain the "tagged parameters".

Question 4 (15 points): Connect your laptop to the unprotected network you created. SSH to root@172.16.42.1. Recall the root password should be set to **cyberlab**. Run the following command to view unprotected http traffic. Note: the **interface-name** is the name of the interface found in question 1, when the wireless client mode was setup. On most pineapples, this should default to 'wlan2'.

tcpdump -i **interface-name** -vv port 80

While this is running, connect via a browser to http://172.16.48.80 (or the backup at 172.16.48.90).

Repeat, using the lab's open network, CSE3140 (Pwd: ciscoCSE3140).

Submit in HuskyCT: Screen shots showing the results. Do you see any traffic? List any IPs you see sending http traffic. What could these correspond to?

Question 5 (10 points): Let's look now at encrypted wireless networks. Switch your laptop over to the secure wireless network you created. Restart your SSH session and rerun: tcpdump -i **interface-name** -vv port 80, where the **interface-name** is the same as question 4. Access http://172.16.48.80 from a web browser.

1. Can you see the traffic?
2. Does being on a protected network help? Why?

Submit in HuskyCT: Answers to the above questions and the results of the tcpdump.

Note: several wireless security protocols are vulnerable; you can learn about this in CSE 3400.

Question 6 (10 points): Connect (if not connected already) to your management (secure) wireless network. Then, click on the Recon tab to the left; make sure `Scan' is on. Click on the drop down and select 30 seconds. Then start a scan. This is the Pineapple internal wireless management package. Start with the scan. The results page will show you every wireless signal that is detectable from pineapple.

Answer the following:

1. What wireless networks are visible? Each row is a separate network.
2. Can you identify an access point that announces more than one network? How do you know?
3. In the security column, what are the different values listed? (e.g. WPA2, Open, etc)

Submit in HuskyCT: Answers to the above questions and screenshots showing visible networks.

Question 7 (10 points): The Pineapple can impersonate specific or all Wi-Fi networks. Click on the Wi-Fi symbol on the left sidebar, which is for the PineAP suite. On your phone, start your personal Wi-Fi access point using either your name or CSE3140 and your section and team numbers (e.g., CSE3140-Sec02-Team12), and configure your Pineapple to impersonate (only) this network by the following:

1) Under the PineAP tab, choose "Evil WPA".
2) Configure the Evil WPA settings to the same as your personal hotspot (with the same SSID, encryption type and password).
3) Be sure to enable "enabled" and "capture handshakes", then hit "save".
4) **Do not** enable "Impersonate all networks."

Disconnect your laptop (or other device) from Wi-Fi, and then try to reconnect to your personal access point on your phone. Check if the laptop/device joined your (fake) wireless network. You may have to repeat this process multiple times until they do (since you compete with the `real' network). Try to adjust the settings on your pineapple to increase the probability that they join your impersonation wireless network.

5) Explain the steps you took and the impact(s) you observed. If the device joins successfully, you should notice a notification. Report your findings.

After successful impersonation, switch your laptop over to the secure wireless network you created. Restart your SSH session and rerun: tcpdump -i **interface-name** -vv port 80.

6) Do you see any traffic? Report your findings.

Submit in HuskyCT: Screen shots showing the results, a video of your successful impersonation attempts and answers to the questions above.

Question 8 (10 points): Read about deauthenticating clients. Experiment with deauthenticating your device from your phone access point. If deauthentication is successful, try to reconnect and see if impersonation worked. This attack is called the **evil twin attack**. It allows the attacker to become a Man-in-the-Middle to the traffic, i.e., to eavesdrop, inspect, modify, inject, and block traffic.

1) Explain the results of your deauthentication experiments. What did you observe?

Submit in HuskyCT: Answers to the above questions, screen shots of the attack, and a screen recording showing the process successfully working.

Question 9 (10 points): In this question we will use the Pineapple to perform a DNS hijack attack. DNS, the Domain Name System, maps domain names (e.g., bank.com) to IP addresses.

1. Create DNS entries on your Pineapple that redirect requests to the domains (websites) *bank.com* and *test.com* to the static IP address of your VM, where you will place the fake HuskyBanking website you prepared in Lab 4. Check here for helpful information.
2. Test from the laptop connected to the Pineapple's open (insecure) network, that when you connect to both **bank.com** and **test.com, you** are directed to your created (fake) webpage. Provide screen shots and photos showing your pineapple configuration, and the redirection to your fake webpage.
3. Note: a real attack usually combines such DNS hijack attack with the evil twin attack of the previous question. We do not ask you to do it, since we want the attack to be against the lab's `bank.com' site (and not against real websites), and in the evil-twin we `hijacked' your phone's network.

Submit in HuskyCT: An explanation, screen shots and a screen recording showing the process.

Once you finish this lab, rebox the Pineapple carefully in original packaging and return to the TA.