Lab10: Wi-Fi Phishing 2

Pre-Requisite Knowledge and Skills

1. Understand basic knowledge of Computer network.
2. Be able to configure and use Linux and its applications.
3. Be able to configure and run Wireless Router or Access point
4. Understand basic knowledge of PHP.
5. Understand basic knowledge of DNS.

Learning Objective:

1. Understand characteristics and vulnerabilities of Wi-Fi network.
2. Understand DNS in data communication.
3. Understand and discuss DNS attack in data communication.
4. Explain countermeasures of Phishing attack in data communication.

Recommended Running Environment and Software:

1. Raspberry Pi with accessories

Instructional Material:

1. One Raspberry Pi 3B+
2. Internet connection
3. One PC, Mobile device, Laptop, or Raspberry Pi with Wi-Fi capability
4. Instructions of this activity

Video Demonstration:

1. to be developed

Lab Assessment:

1. Exercises
2. Quiz

Note before starting the lab

This lab is designed for advanced student, who has a basic knowledge of Computer Network and Data Communication. Depending on the knowledge level of student, Instructor should adjust the amount of lab work. For novice students, it is recommended to use pre-built Image for this lab and allocate more time on discussion.

Lab Instructions

This lab requires one (1) Raspberry Pi, running Raspbian or Linux OS with one (1) Wi-Fi adapter and Ethernet port, Internet access, and one (1) PC, Laptop, Mobile device, or Raspberry Pi with Wi-Fi capability.

Getting start with Raspberry Pi

Raspberry Pi requires Monitor, SD card, SD card reader, USB keyboard and mouse. Raspberry Pi is diskless computer and OS should be installed in SD card. You can use any size of SD card that can contain and run Linux OS.

Download Raspbian OS IMG first from the link below.
https://www.raspberrypi.org/downloads/raspbian/

Now, SD card should be formatted and copy the IMG to SD card using SD card formatter. Simple insert the SD card to the reader and plug the reader into the PC. Then, open formatter application and format SD card as shown in Figure 1. Click the "Format" button and then, select "yes" to execute format command.

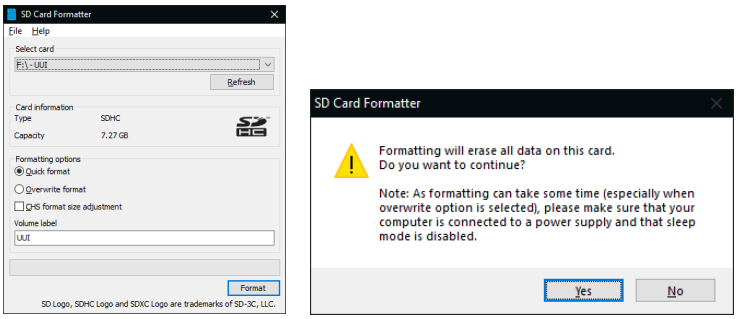


Figure 1. SD Card Formatter

Now, we need to copy OS IMG to SD card using application called "balenaEtcher". Figure 2 shows the UI of application. First, select the IMG file, generally its extension is .iso, .zip, or .img. Select the IMG file and choose the SD card. Then, click "Flash" to upload the OS into SD card.

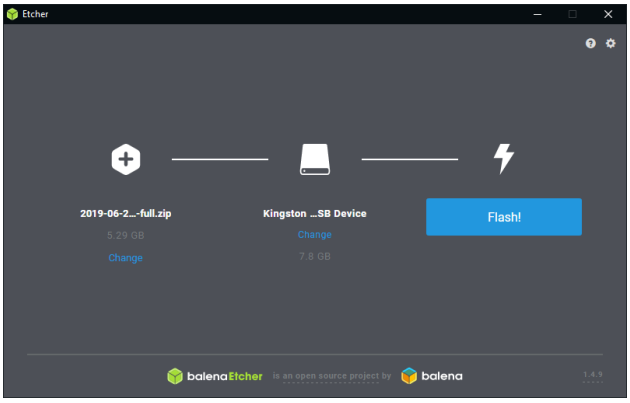


Figure 2. Copying IMG file to SD card

Insert SD card to the Raspberry Pi and it is ready to start. In order to run Raspberry Pi, one monitor and USB keyboard and mouse for each Raspberry Pi is recommended. However, you can switch and use them for multiple Raspberry Pi if you need.

Once Raspbian is running at the first time, it will ask to set the password for the user. Default login user should be set as “pi”. But you can create new user. Remember the user login ID and password. We need them for the rest of activities. Once log in the system, you will need to set up the network connection. Raspbian is based on Debian Linux OS and setting up network is similar to the Linux system. If you are familiar with Linux system, now set up the network. If not, please watch and follow the Demo video. If Wireless router is used, correct through Wi-Fi or Ethernet cable. If Wireless router is correctly configured, IP address will be automatically assigned and read to connect Internet. Raspbian may ask for the update if you are connected to Internet. If you want, you can update, but it is not necessary. If you choose to update, wait until it finishes the update and restart the system.

Now, Raspberry Pi should be ready to configure for this lab.

Discussion 1: Open Discussions before starting the lab

At this moment, it is a good time to check if student understand background information and attack scenario. Depending on student knowledge level, Instructor may adjust the level of discuss.

- **What is Wi-Fi? Where do you find them?**
  Wi-Fi is a wireless networking technology that allows computing devices (e.g., laptop, smartphone, printer, and etc.) to access the Internet. In general, Internet access is allowed through wireless router or access point. People may have their own Wi-Fi at home and business. Most of business place such as Starbucks, Panera, Target, and etc. provides free Wi-Fi service. Student may already know and use Wi-Fi.

- **What is the structure of Wi-Fi network?**
  In Wi-Fi network, there is a central device that connects multiple devices. Wireless access point (AP) is a central node and all mobile devices should connect to AP for the communication. This means that all packet should go through this AP or Wireless router. This network topology is called Star topology.

- **Do you think Free Wi-Fi is secure?**
  Due to Broadcasting nature of wireless communication, sniffing attack is possible. Therefore, Password protected Wi-Fi which uses encryption is preferred to prevent the sniffing attack in general. However, we cannot say it is secure because of structure of Wi-Fi. Secure application could be one of the solutions but not still not secure enough. We will explore it in this lab.

After the discussion, students understand about Wi-Fi and should be ready to move on the rest of this lab.

Wi-Fi Phishing attack Scenario

Free Wi-Fi is available everywhere in these days and people are enjoying free Wi-Fi for their online activities such as web surfing, online shopping, and etc. without hesitation. Wi-Fi Phishing attack takes advantage of general behavior of people about free Wi-Fi usage to steal credential information. The architecture of Wi-Fi Phishing attack is illustrated in Figure 3.

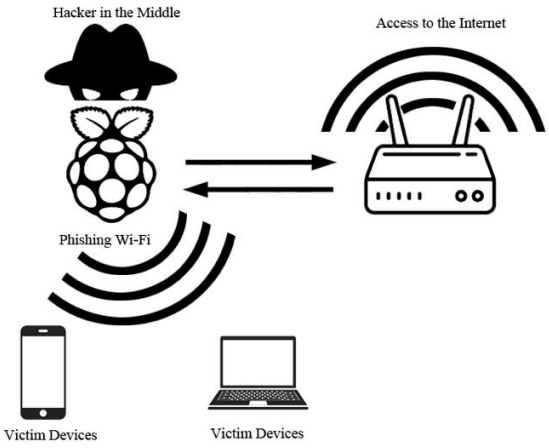


Figure 3. Architecture of Wi-Fi Phishing attack

This attack is a Man-in-the-middle type attack. The basic idea of Wi-Fi Phishing is placing the Phishing device (i.e., Raspberry Pi) between Public Wi-Fi and users and provide an Internet access service just like Free Public Wi-Fi. As shown in Figure 3, Phishing device (Raspberry Pi) is normally connecting to Public Wi-Fi and also advertise itself as a Public Free Wi-Fi to attract users. When user select Phishing device to access the Free Wi-Fi, user becomes a victim. This lab will introduce how easily user credential can be stolen.

This lab utilizes Domain Name System (DNS) to steal user credential information. Let's have a discussion about DNS first before we proceed.

Discussion 2: What is DNS and how does it work?

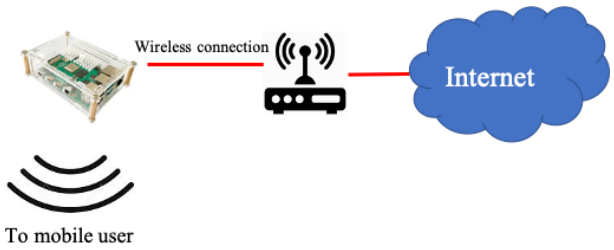
- Domain Name System is kind of address book of the Internet. The address in Internet is IP address consisting of 32 binary or 4 decimal number (e.g., 192.168.0.1). However, human remembers better with the name than number. People remember name such as www.google.com not its IP address such as 216.58.192.196. In addition, IP address could be changed at any time. Therefore, there should be a way to translate name address to IP address. DNS server helps to translation. When user type www.google.com in web-browser, it asks DNS server to obtain IP address of www.google.com. Then web browser contacts Google web server using obtained IP address. Your ISP has their own DNS server.

Lab Setup and Configurations

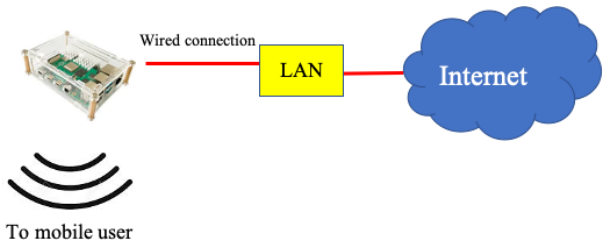
General basic required installations and setups for Wireless Access point is available in Basic Configuration document. Please refer it if you want let student do these jobs. Otherwise, use pre-built image. The required in detail configurations for this lab is in "Lab10-Configuration Instruction". Use this instruction for advance students to build their own system.

Practically, we need two wireless adapters for Raspberry Pi, one to provide the Wi-Fi service and the other to access Free Wi-Fi for Internet access. If you do not have two Wi-Fi adapter or Wi-Fi

is not available, you can use Ethernet connection (i.e., Ethernet cable) to connect Internet instead of Public Wi-Fi for the convenience as shown Figure 4.



(a) Lab Setup with Wi-Fi



(b) Lab Setup without Wi-Fi

Figure 4. Two possible Wi-Fi Phishing Lab Setups

There are three major parts of configuration in the Raspberry Pi besides basic setups and configurations. One is Apache2 and Bind for DNS, fake webpage with proper action, and local DNS server.

Lab Setup

Step1: Setup Attacker's device (Raspberry Pi)
Follow the basic setup instruction or use pre-built image to configure Raspberry Pi first. The next step is to place the attacker's device between user and Free Wi-Fi. If two Wi-Fi adaptors and Wi-Fi network are available, use one adaptor to connect Wi-Fi network. As mentioned above, you can use Ethernet cable to connect the Internet instead for the convenience. Once connect to the Internet in either way, make sure your device has an IP address and connection is active. You can check your Internet connection by accessing any websites or ping know website such as google.com. If not, you should check your Internet connection. Make sure you have an Internet access.

Step 2: Setup Free Wi-Fi for Phishing
Wi-Fi adaptor will be using to deploy Free Wi-Fi network for users to login. Follow the basic setup to deploy Wi-Fi access point service with required services including DHCP, IP routing, and etc. or use pre-built image. Make sure your wireless adaptor has IP address of 192.168.4.1 255.255.255.0. If you want to use other IP address, you should modify IP address correspondingly in every configuration. In order to check your Wi-Fi access point, use any wireless capable device to connect this Wi-Fi.

Discussion 3: Now it is good time to ask students how we can steal user credential information using Wi-Fi access point and DNS. They do not need to use technical term here. Let them have enough time to discuss freely with their own idea to make it possible. Following is an idea of this lab and use it to help students in their discussion.

- Remember the traffic flow in Wi-Fi network. All traffic has to go through Wi-Fi AP and Wi-Fi AP will forward the packets for users. Therefore, we can modify the AP to forward the packet to somewhere we want. However, it should follow the Internet protocols.
- DNS is one of Internet service, which translates name address to IP address for user to access the web server. So, if we can tweak the DNS server, we can redirect user to some other web server instead of actual web server.
- This lab uses this mechanism in Phishing attack.

Note: From Step 3 to Step 5, you can find the corresponding steps in Lab10-Configuration Instruction. Use them to configure if you want to create your own. If you use pre-built image, you do not need any configuration. In each Step, discuss implemented techniques to make this attack possible.

Step 3: Installing Apache and Bind

In order to run web service and DNS, we need to install couple of packages, Apache and Bind. Apache is a cross-platform software, which establishes the connection between a server and the web-browser. So, we need to install and run Apache in order to run our own web server for faked webpage. Bind is an implementation of the Domain Name System (DNS) of the Internet, which performs both DNS server and resolver in the network. Therefore, we need to install both to implement web service with DNS.

Step 4: Building fake webpage

There are several well-known web servers such as Google, Facebook, LinkedIn, and etc. and lots of people access them every day. The main idea of this attack is to use this. Running one faked webpage in the local machine and redirect traffic to this local server when user tries to access this website. In our example, we use LinkedIn. First, download the LinkedIn “index.html” file from their website and modify it for our purpose. The main modification here is to add a script to save user input into a log file. User input here are username and password. For more detail process, refer Lab10-Configuraiton Instruction.

Step 5: DNS server configuration

Next, we need to configure the DNS server to redirect specific address to local server. Once user access the Phishing Wi-Fi network, DNS server will let user go to any website except for target website. Only when user access target website (LinkedIn for this lab), it will be redirected to local web server (faked webpage). Then, faked webpage will ask for sign-in and our script will run to save username and password to log file. Therefore, user would not even know user is Phished and credential information is revealed. All configuration processes are in Lab10-Configuraiton Instruction.

Step 6: Access the Phishing Wi-Fi

User PC or other type of device with Wi-Fi capability to connect Phishing Wi-Fi. Then, open web-browser and surf the web such as google, yahoo. And etc. Now, try to access www.linkedin.com at the web-browser. You should see Sign-In page as shown in Figure5. Then, sign in. **DO NOT USE** your real user ID and Password!

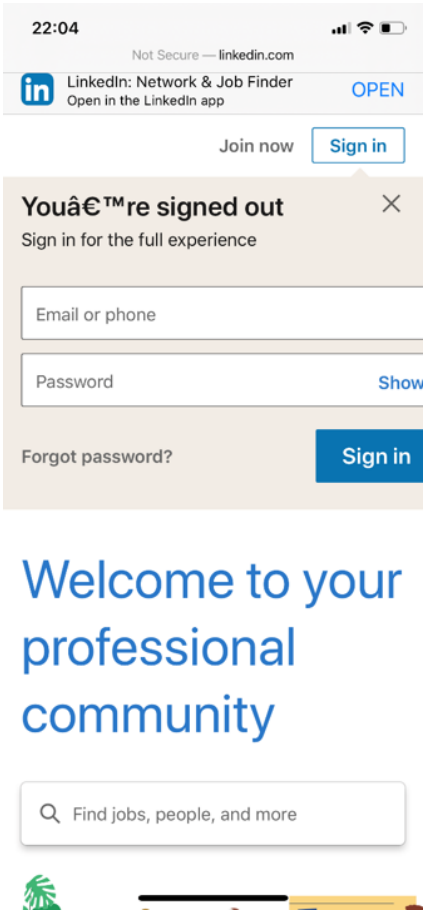


Figure 5. Example of LinkedIn faked webpage

Step 7: Collecting user credentials

In order to obtain collected user credential information, use either terminal or file-browser application at Raspberry Pi. The location of file is depending on how you configure in "get.php" file. As a default in pre-built image, it should be in "/home/pi/Desktop/". The file name is "password.txt". Use either application to see the password file. The output should look like as in Figure 6.

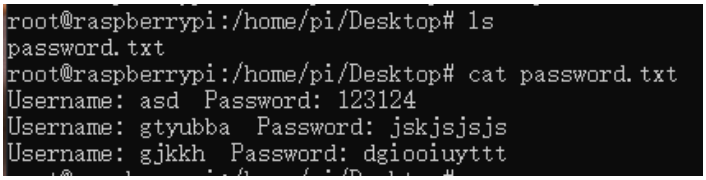


Figure 6. Text file storing victim's credential information

As you see, user credential information is revealed in log file.

Discussion 4: Discuss about the countermeasure of this attack. How we can avoid this attack?

- Let students have enough time to discuss how to avoid this type of attack.
- Technically, this type of attack is not easy to detect and avoid. Even with password protected Wi-Fi cannot prevent this type of attack because it utilizes DNS.
- There are couple of ways.
- First way is to check with network owner (e.g., Starbuck, Panera, Target, etc.) if it is their Wi-Fi network or not.
- Second is to check the translated IP address.

Step 8: Countermeasure

In order to avoid this type of attack, one of the ways is to check the translated IP address. We will use ping and "whois" website to check if translated IP address is genuine. We will use www.google.com as an example.

Open CMD in Windows or Terminal in Linux or Mac.
Then, type "ping www.google.com". You will see corresponding IP address as shown in Figure 7.

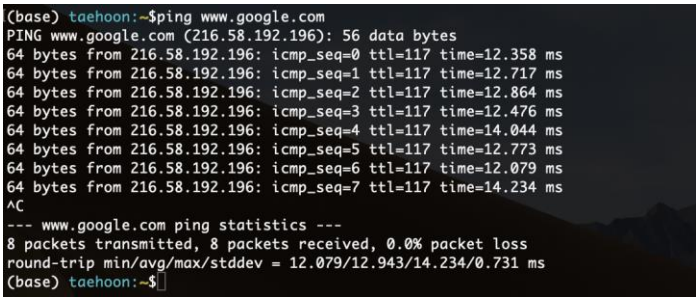


Figure 7. Output of ping results.

Now go to https://whois.domaintools.com/ and enter IP address from ping result. It is 216.58.192.196 in this example. Then, you will see something like in Figure 8, which indicates it is IP address of Google.

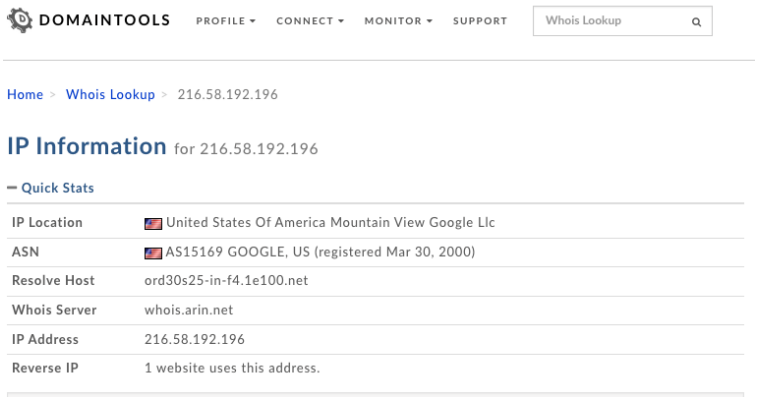


Figure 8. IP address information at "whois.domaintools.com".

Discussion 5: Discuss other types of Phishing attack. Ask student what other Phishing attacks in cyberworld and let them discuss freely.