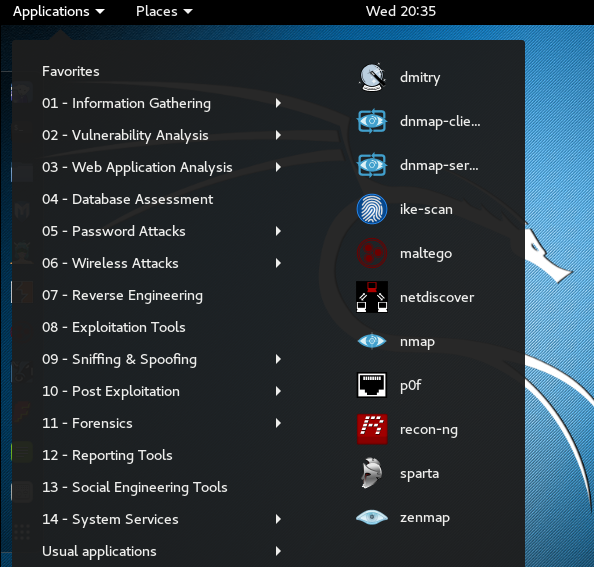
|  |
| --- |
| Lab 3: Packet Analysis II  * The due date and time is 4:00 Thur, September 21 (Sec 01) / 7:00 Thur, September 21 (Sec 76). * This is an individual assignment, and is worth 20 points. * You should provide the answers using the accompanying outcome file. Change the file name following the naming convention suggested below. * The naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Lab 1\_ImG.docx). If you do not follow the convention, I will deduct 1. * Do not copy any of the sample screenshots provided as illustrations. * You should not scan any live servers using Nmap and hping3. For violation, you may be expelled from the school (not a joke!). |

## Prep

* Study Nmap using the following sites.
  + http://nmap.org/
  + http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
* In Kali, Nmap can be found via the navigation path of Applications > 01- Information Gathering > nmap. Or, launch a Terminal and type “nmap” on the command shell.



## Task 1. Figuring out the IP addresses

* You have to know the IP addresses of your host and the Kali before you conduct the next tasks.
* Task

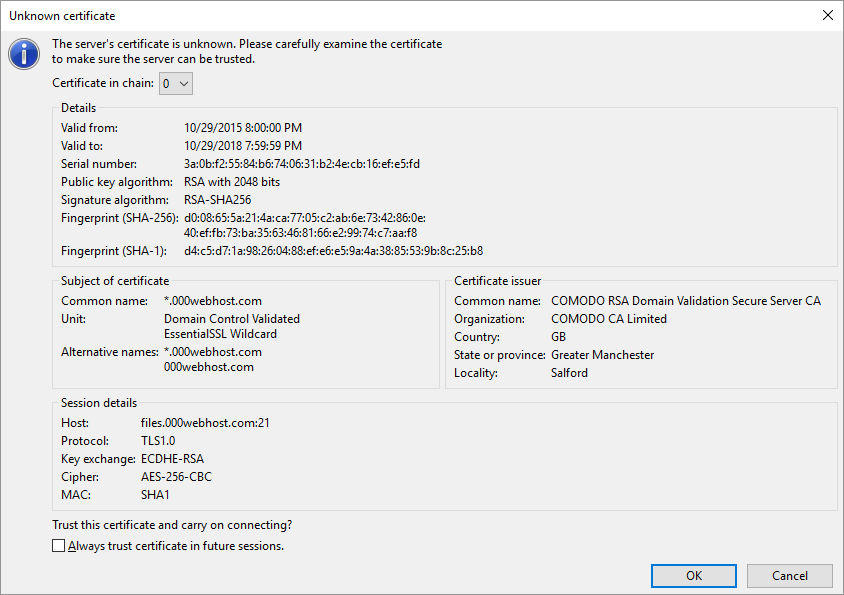
1. Report the IP address of your host and the subnet mask (use ipconfig /all). If you use wireless, the IP address of “Wireless LAN adapter Wi-Fi” is the active physical interface. Report with a screenshot.
2. Report the IP address of your Kali (use ifconfig). Report with a screenshot.

## Task 2. Analyzing FTP Signatures

* Upload the text file (LittlePrince.txt) to the designated site and capture the packets for this activity with Wireshark.
* First, you should install the ftp client FileZilla on your host. The Mac version is also available.
* Persona-SQL has FileZilla and Wireshark installation. However, I recommend you to do this task at home. The school network generates too many irrelevant packets.
* The ftp server and account information:
* Host files.000webhost.com
* Username liquid-seamanship
* Password louisville9
* Folder to upload files public\_html/CIS480
* Steps:

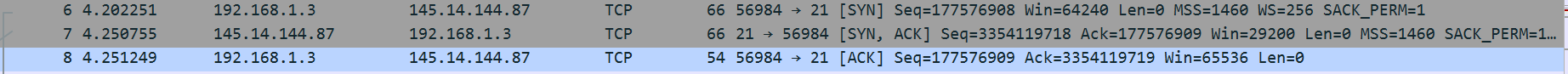
1. Close any browser, email, etc on your host that can generate internet traffic.
2. Change the name of the textfile to “LittlePrince-[your-lastname].txt.”
3. Launch FileZilla.
4. Turn on Wireshark on the host by following Capture > Options > Input > Select Interface > Start.
5. Connect to the ftp server.
6. Upload the textfile to the designated directory.
7. After the uploading is successful, stop Wireshark.
8. Save the captured traffic as “\*.pcapng.”

* Note
* If you see the following screen on ftp login, click on OK. The site is using a certificate for encryption.



* Task

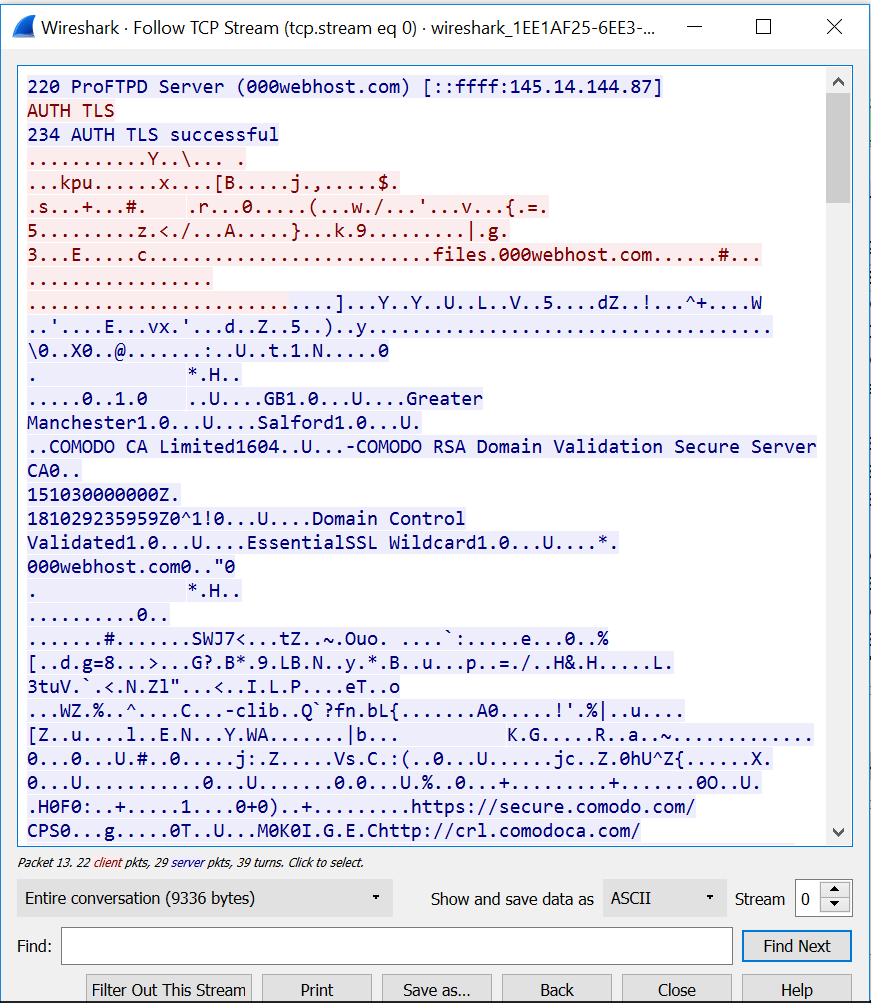
1. Identify the three TCP packets used for the initial 3-way handshaking. Take a screenshot of the TCP packets.



* **Hint**: These packets are placed right before ftp packets.

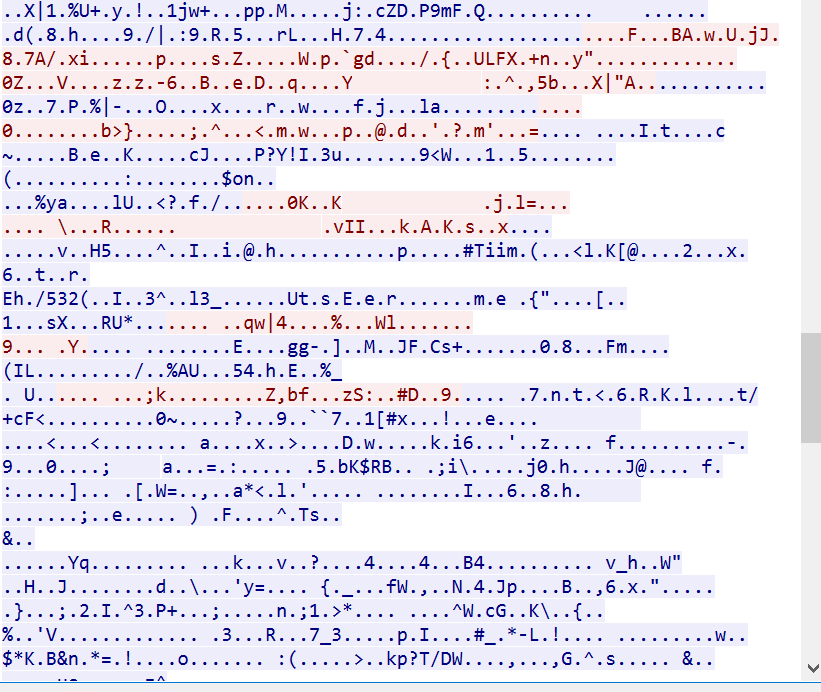
1. Identify the FTP packets that show the Username and the Password. In fact, the Username and the Password are encrypted and we cannot figure it out. However, we can guess which packets have that information. Follow the TCP stream and take a screenshot of the TCP stream.

* **Hint**: Use the display filter “ftp.” And right-click on the packet of your interest and Follow > TCP Stream to understand the data flow. Use the IP address of the ftp server to recognize the relevant TCP stream. Use the display filter “tcp.stream eq xx” (replace xx with the integer) as necessary.



1. Identify the FTP-DATA packets used for the textfile uploading. Follow the TCP stream and take a screenshot of the TCP stream. The textfile is uploaded across many FTP-DATA packets. So, any part of the data is okay.

* **Hint**: You need to check out TCP packets after FTP packets.



* Note:

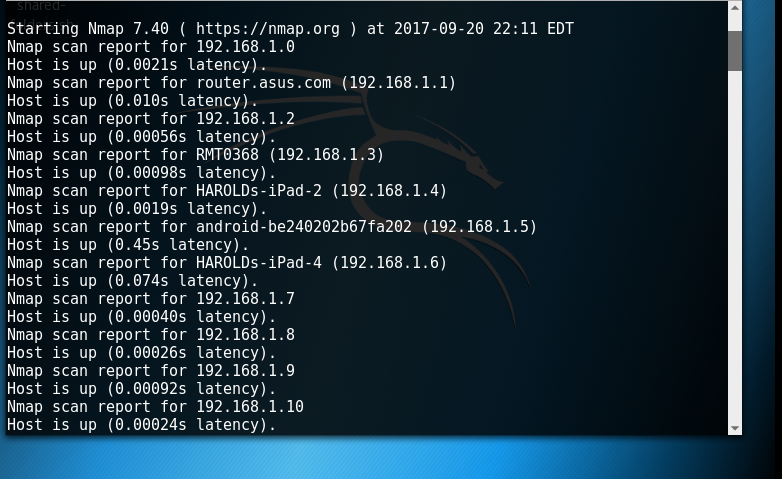
1. If you don’t capture the traffic on Wireshark, it is possible that you have not selected the right interface.

## Task 3. Ping Sweeping

* Perform a ping sweeping attack with Nmap by sending a series of ICMP echo request packets to a range of IP addresses on a network.
* Pick a random private network address on your host and scan the network using the Kali.
* For ping sweeping, you have to provide the “network address”/“CIDR notation of the subnet mask.” (e.g., 192.168.10.0/24). Use **-sP** flag for ping sweeping. It takes a while and so be patient. 
* In general, this is the command we use for Ping Sweeping.
  + $ nmap -sP x.x.x.0/24 , where x.x.x.0 is the IP address of the network.
  + (Example) $ nmap -sP 192.168.10.0/24 , where x.x.x.0 is the IP address of the network.
* Task

1. Report your result in a screenshot like below.

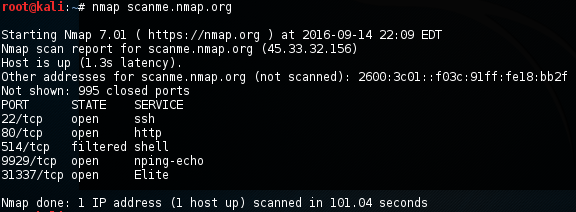
My Screenshot



## Task 4. Port Scanning

* Port scanning is an attempt to connect to a computer’s ports to see whether any ports are active and listening.
* Scan the target (scanme.nmp.org) from your Kali and capture the packets with Wireshark on Kali.
* Steps:

1. Start Wireshark on your Kali after selecting the proper interface. To launch Wireshark, type “wireshark” on the command shell.
2. Run the following command and wait until you get the following result. Then, stop Wireshark by pressing the red button.



* Task

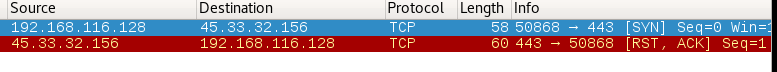
Answer the following questions. Provide a screenshot for each question to support your answer. For the answers, use the display filter “tcp.stream eq xx” (replace xx with the integer) as necessary.

1. Which type of TCP packet (e.g., SYN, SYN/ACK, or ACK) was sent from your Kali to the victim?

As you can see in the screenshot below question 2 (from tcp stream 0) my Kali box sent a SYN request

1. Which type of TCP packet (e.g., SYN, SYN/ACK, or ACK) was received from the victim to the Kali in response?

As you can see from the screenshot, my Kali box received an RST,ACK packet from the victim.



## Task 5. SYN Flooding Attack

* Perform a SYN flooding attack using **hping3** against your host from your Kali. The detailed info of Hping3 can be found here: http://linux.die.net/man/8/hping3.
* **Steps**

1. Start Wireshark on the Kali.
2. Create a command using the following template (you should type the command on the command shell. No copying and pasting!):
   1. **Hping3 -S target\_ip\_addr -a spoofed\_ip\_addr --flood**

-S --syn set SYN flag

-a --spoof spoofed source address (use a private IP address: 192.168.x.x)

-p --destport destination port (default 0)

-i --interval wait (uX for X microseconds, for example -i u1000)

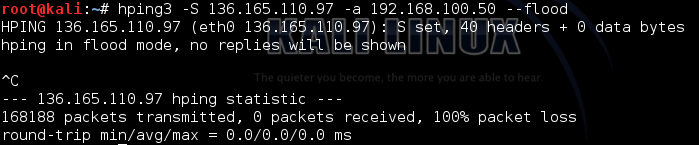
--fast alias for -i u10000 (10 packets for second)

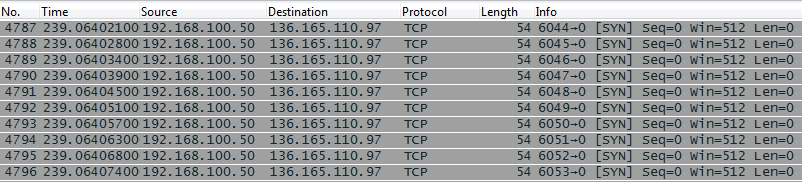
--faster alias for -i u1000 (100 packets for second)

--flood send packets as fast as possible. Don't show replies. (usage: -i flood, or --flood)

**target\_ip\_addr**: provide the IP address of your host

**spoofed\_ip\_addr**: provide a random private IP address

* In the example below, 136.165.110.97 is the victim’s IP address and 192.168.100.50 is the spoofed IP address (a random IP address). 
* The following is the packets captured with Wireshark. You should stop the Kali by pressing CNTL+C to prevent the crash of the host.



* Task

1. Launch a SYN flooding attack using the IP address of your host as the victim and a random private IP address as the spoofed address. Report your Wireshark result in a screenshot.

