The Department of Electrical and Computer Engineering

The University of Alabama in Huntsville

CPE 435 Lab-10

Introduction to Wireshark and Packet Analysis

### **Introduction to Wireshark**

Wireshark is a packet analyser tool. Apart from being a packet analyser, it is also a network sniffer tool. So it provides the option of capturing packets flowing in and out of a network as well as analyzing and troubleshooting with a nice GUI. It allows live capture of packets which means you can capture and save information about the networks packets from a live network in real time.

To run live capture, a user needs sufficient privileges. However, you can analyze the packet-data based on trace files without super user privileges.

### How to run Wireshark on Linux

Open a terminal (type **Ctrl+Alt+t**). Once you are inside the terminal, type **wireshark** and hit enter. You should see a screen similar to the following figure.

File	Edit	View	Search	Terminal	Help
00qq	30@eb	216-0	8:~> w	ireshark	

It should open the GUI as shown in the following figure.

1	te Witeshark Hetsenrik Rosiyear. (Witeshark 3.30.54 (Sitt Bay Selensen From an	ireut) - 1
File full View En Capture Analyze Etablishs Telephony Tesls Internal	is Help	
004 d 0 x 0 0 + + + + + + + + + + + + + + + +		
File: + Eprimer.	care which are	
WIRESHARK The World's Most Popular Network	Protocol Analyzer avri)	
Capture	Files	Online
Mis Interface: can be exectifier capturing in this system with the current configuration. Eculate's an incertain/situation	Cyper spreadury coplanel the	Website
denied	Care ration	User's Guide     Technologia India India India India
losermol ra -G ninohalk , your, esername, / as root.)	Sample Captures	- Security
Ine Capture Help Inform for details.	A real and a second of the spectrum of the second	State with Piresheet as catarily as possible
Refresh Interfaces		
OCC North Phy Boltradian		
Capture Help		
- Hearte Casture	_	
The second secon		
Network Media		
Question internation for capitaling an internal (2018) -		
Ready to load or capture RicPadaria		Profile: Default

We will download trace files that are available online and then analyze them to extract some information.

In your report, please make sure that you include screenshots of all the steps as you perform them as a proof of your work even if the assignment does not mention explicitly.

### How to run Wireshark on Windows or Mac

You may go to the following <u>link</u> to download wireshark for Windows or Mac machines.

# Subtask 1 (Introduction)

- 1. Go to <u>SampleCaptures The Wireshark Wiki</u>. This website contains a list of sample trace files that are output of network capturing. Let us find a simple unencrypted trace file, load it in wireshark and analyze it.
- 2. Go to <u>number 20</u>, which should give you telnet packets as the following figure shows.

#### Telnet

telnet-cooked.pcap (libpcap) A telnet session in "cooked" (per-line) mode.

telnet-raw.pcap (libpcap) A telnet session in "raw" (per-character) mode.

3.

Download the first pcap file **<u>telnet-cooked.pcap</u>** 

- 4. On the wireshark window, select **File->Open** to open a dialog box that lets you choose the pcap file. Navigate and open the pcap file that you downloaded earlier.
- 5. Once you select **Open**, you will see a window something like the following figure.

1910	1.000	1000000	271120 BB 21	room step eee	
3		182.348.8.2	342.368.8.3	TOP 74 De-image-Im > Inford 10001 Deguñ Mino20120 Levoñ Milo1000 DACK FERMIG TiveLo10022818 Tierrol Milo1	
		132.358.8.1	310.308.8.2	PDF IN tailant > Se-image-im [SYM, WOR] Sep-8 Ack-0 Min-11178 Lan-8 MSH-3448 MS-1, MSV81-3447311 TheoretAllIS608	
1		182.348.8.2	302.388.8.3	10 <sup>4</sup> 66 Decimage the a finite (400) Single dated bioxidize Level Threfold/SIDDE Threfold/STD	
		182.108.8.1	210.008.0.1	RUBET RITEILET BILD	
		132.368.8.1	202.308.8.2	TOJART AN Talbat Bata	
		182.108.8.1	210.008.0.1	10 <sup>4</sup> BH 38-lange-ls > Telest IROX Deg-28 Alk-4 Min-31128 Len-4 Thul-IRII980 Theor-DWR3172	
7		112.348.8.2	392.304.8.3	TOJAET AN Telest Bats	
		182.388.8.1	310.381.8.3	10 BE brief, a la lange in 1800 head datait Manifilm Lend ThathingHIT2 Theory(1000000	
1		132.358.8.1	392.399.8.2	10.467 R1 Twinet Bets	
18		182.348.8.2	202.308.0.3	TELET 138 Trivet Esta	
12		132.108.8.1	392.399.8.2	NP M tylinet > 20-image-im [MCM] Seq-28 Ark-89 Min-17212 Lan-0 TSual-D007272 Theor-18232000	
12		110.168.8.1	202.368.8.3	TRANET BATTelevet Bate	
12		182.108.8.1	310.308.8.3	TAURT 75 Twittet Bats	
<ul> <li>BY300</li> </ul>	BC 85 Bytes	an wire item bits), t	W bytes captured itse	k1150	
+ Ether	mat II, See:	Western8, 97-ab 97 100	hilds off (\$7) at (\$7), Date	Lite-Ref. Strikfisher (Mitediner Stelef) fal	
A DESCRIPTION	NAME AND ADDRESS OF	manufact & manufacture of	AND IN A DESCRIPTION OF AN ADDRESS OF ADDRESS	LIT: THE TAR & T LITET TAR & T	

Internet Protocol mersion 4, Soci 201.100.00.1 (100.300.0.1), Buti 201.000.0.2 (100.300.0.1)
 Transmission Central Protocol, Soc Port: Solvet (20), But Part: Sm.Smage.in (2000, Sept.4, Ack: 3), Lett 0

#### Assignments

- 1. How many packets are captured in the .pcap file that you loaded?
- 2. List all the communicating parties in the .pcap file. Can you also identify the ports being used by each of them?
- 3. What protocols are used for communication by the communicating parties ?
- 4. What is the total duration of the communication? (You may want to see the first and last frame)
- 5. What is the frame length and number of the longest frame transferred? Who is the source and destination of that packet?

# Subtask 2 (Real Hacking and Stuff)

Now that you have sniffed someone in a network and got the data that is being transferred. You also know who is involved in communication. Now we want to see if we can get something of real value for us. Maybe someone has transferred his/her username and password over the network that we sniffed.

### Assignments

- 6. Select frame number 8. Who is the sender and receiver of this frame?
- 7. On the window that appears below the listing of all the frames (as shown below), expand Internet Protocol Version 4. What is the Time To Live for frame 8? What does this mean?

	33 2.575448	192.168.0.1	292.188.0.2	TELMET	89 Televi Dois
	35 2.576676	192,168,8,1	192.160.0.2	TCP	65 23 → 2550 [ADK] Seg=343 Ack=207 Hin=17373 Len=0 TSval=2467377 TSecr=18235003
	36 2.577672	192,168.0.1	393.160.0.2	TELNET	75 Yelset Data
	27 3.589239	192.108.0.3	382.18E-0.1	TEP	00 1910 + 28 [ACK] 5eq-307 Ack-152 Min-81120 Len-0 Toval-1028889 Theor-2407877
	38 3.581505	192.168.0.2	392.188.0.1	TELNET	72 Telmet Data
	39 3.582813	192.168.0.1	192.185.0.2	TOP	65 25 = 1550 [ADK] Seq=152 Ack=215 Wite=17376 Len=0 TSval=2467379 TSecr=18253994
	40 3.847152	192.058.0.1	392.160.0.2	TELNET	60 Telmet Bats
	41 3.859258	192.168.0.3	393.160.0.1	TOP	66 1558 + 23 [ACK] Seq=213 Ack=154 Min=32128 Len=0 T5Val=18234022 TSec7=2467388
	42 3.868413	192.168.0.1	192.188.0.2	TELNET	so Talast Data
	45 3.868575	192.168.0.3	192.168.0.1	TELMET	ep Telmet Dets
	44 3.001308	192,108,8,1	102.100.0.2	TELET	to 23 + 1000 [MUN] SERVICE MERCINE MERCINE SYMEROME (SWEROME SECURICHEED
1.0	and the Add burton of	on wine /Still birts)	66 betes centured (5)	at hitsh	
	and the state of the state of	the second se	an obtain realize an fai		

Ethernet II, broi mecternijefianist (00.00.00.01.01.00.07), boti Lite-Caujababfifa (00.00.02.05.05/fa) Driemet Protocol Version 4, broi 192.166.0.3, Osti 192.166.0.2 Dramamization Control Protocol, Bro Porti 23, Ost Porti 1930, Sepi 4, Acki 30, Leni 0

8. Select frame 8 again. Right click on it, and select Follow > TCP Stream. What information can you see? What is the username and password that is transferred? 9. Repeat the same procedure in **telnet-raw.pcap**. Find the login information used to

- verify credentials. (Select frame 8 again)
- 10. What do you think is wrong with these two files that you analyzed? How can you not allow anyone to know your password that you send for authentication?
- 11. Load the file uftp v3 transfer.pcapng. The protocol used is UFTP. What is UFTP? Can you identify two parties that are involved in file transfer? (Use your intelligent guessing) 12. Write differences between TCP and UDP.

### Subtask 3 (Decrypting The Encrypted)

Let us now work on encrypted protocol.

- 13. What is the difference between https:// and http://? What is the encryption standard used by them, if any?
- 14. Download the file **mysql complete pcap**. Is it encrypted? Please justify.
- 15. Download the file **mysgl-ssl-larger.pcapng**. Is it encrypted? Please justify.
- 16. Download the zipped file **snakeoil2 070531.tgz**. Extract the content in your local folder. Load the .pcap file in wireshark. Is it encrypted?
- 17. Perform the decryption of the .pcap file as demonstrated in class by the instructor.
  - 1. What frame number requests the image apache pb.png?
  - 2. Does the server provide the image? What is the status code that implies the response has a payload?
  - 3. Attach the image apache\_pb.png to your report.
- 18. What is the response that the server provided when requested for openlogo-25.jpg? Can you see the html code sent as a response? If yes, copy and paste it in a .html file and load it in your favorite browser. Attach the screenshot of how the response looks like in the web browser.

# Subtask 4 (Vulnerability Analysis)

The following assignment is to be done at the **students own machine**. You do not have permission and user rights to do this on campus machines. Please make sure that you do not reveal any important information to your reports when you attach screenshots. (Please blur out any sensitive information)

- 19. The first thing that you will do is capture packets. You can use wireshark or tcpdump to capture packets. While you can capture packets from wireshark, I suggest you use tcpdump so that you can be familiar with a new tool. Following are the procedures that you will follow:
  - 1. Find the interface that is connected to the internet. Do **ifconfig** in the terminal and

select the one which is connected to the internet. Wireshark should show you the interface in its GUI.

Start packet capture in tcpdump using tcpdump -i <interface> -s 65535 -w
 <filename>. Or select the bluefin below File menu in wireshark after you select the interface if you wish to use wireshark.

3. Please visit the website <a href="http://www.openoffice.org/">http://www.openoffice.org/</a>. What is wrong with this website?

4. After it is completely loaded, stop the capture. You may want to navigate around the website before stopping the capture. You can select the button in Wireshark GUI or kill the tcpdump process if you are using tcpdump.

5. Load the file in wireshark. If you are using wireshark, it is already loaded.

6. Try to find at least two images that are sent by the server to your machine and attach them to your report.

7. What are the vulnerabilities of the website that you can see right away?

8. Repeat similar operation for <u>https://www.uah.edu/</u>. Attach two images sent from the server to your machine if you can. If you cannot view any images, comment on why this might be.

### Deliverables

### Lab Report

The following material in each section is expected:

- 1. Cover page with your name, lab number, course name, and dates
- 2. Observations and Answers
  - a. Please include answers to any questions from the lab document, as well as any necessary supporting documentation in the order they appear. This includes screenshots from wireshark to support your answers.

The report should be submitted as a single pdf document with the source code for your program within it.

### **Recorded Demonstration**

The following material in each section is expected:

- 1. Introduce yourself and give the name of the lab
- 2. Walk through subtask 3 in its entirety (questions 13 to 18). You must show that your initial pcap file is encrypted and that you can successfully decrypt it by adding the RSA key correctly.

The demonstration may be in person or recorded and submitted as an mp4 file alongside the report.