Universidad de Costa Rica

Facultad de Ingeniería

Escuela de Ciencias de la Computación e Informática

Redes de comunicación de datos

Tarea 6 Wireshark

2025

Autor

David González Villanueva C13388

I) Exercise One: Good old telnet

File: telnet.pcap

Work: reconstruct the telnet session

Questions

1. Who logged into 192.168.0.1?

- Username: **”fake”** (29 y 31)
- Password: **“user”** (36 y 38)

2. After logging what the user does?

- El usuario hizo ping a la página de yahoo (75)
- Pidió el contenido de la lista de directorios (79, 81 y 83)
- Hizo log out (87)

TIP: telnet traffic is not secure

II) Exercise two: massive TCP SYN

File: massivesyn1.pcap and massivesyn2.pcap

Work: Find files differences

Questions

1. massive syn1.pcap is a **“ataque DoS”** attempt

1. massive syn2.pcap is a **“ataque DoS distribuido”** attempt

TIP: pay attention to source IP 3 Wireshark Exercises

III) Exercise three: compare traffic

Files: student1.pcap and student2.pcap

Scenario: You are an IT admin in UCR, you had reported that student1 (a new student) cannot browse or mail with its laptop. After some research, student2, sitting next to student1, can browse with any problems.

Work: compare these two capture files and state why student1's machine is not online

Solution

1. student 1 must **“debe estar en la misma subred que el gateway”**

TIP: pay attention to first ARP package

IV) Exercise four: chatty employees

File: chat.pcap

Work: compare these two capture files and state why student1's machine is not online

Question

1. What kind of protocol is used?

- TCP
- MSNMS

2. Who are the chatters?

- tesla_brian@hotmail.com (Brian)
- tesla_thomas@hotmail.com (Thomas)

3. What do they say about you (sysadmin)?

- Thomas → Brian: “Not much, did you hear about the new IT guy they hired?”
- Brian → Thomas: “ohh yea, i hear he is a real jerk”
- Thomas → Brian: “I've heard the same”
- Thomas → Brian: “maybe we should try hacking into a server to mess with him?”
- Brian → Thomas: “sounds good to me”

TIP: your chat can be monitored by network admin