Nathalie Alfaro Quesada, B90221.

Exercise One: Good old telnet

File: telnet.pcap

Work: reconstruct the telnet session

Questions
1. Who logged into 192.168.0.1?
    Username: fake Password: user

2. After logged what the user do?
    El usuario hace ping a yahoo.com

TIP: telnet traffic is not secure

Exercise two: massive TCP SYN

File: massivesyn1.pcap and massivesyn2.pcap

Work: Find files differences

Questions

1. massivesyn1.pcap is a SYN Vertical attempt
2. massivesyn2.pcap is a SYN Horizontal attempt

TIP: pay attention to source IP

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. student1 must debería revisar que la IP solicitada esté en línea, el ARP no envía la dirección MAC conectada a la IP dada.

TIP: pay attention to first ARP package

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 y MSNMS.
2. Who are the chatters?
   Brian y Thomas.

3. What do they say about you (sysadmin)?
   Lo que se observa en el contenido de los mensajes es que uno pregunta qué pasa, otro dice una grosería y que van a intentar hackear el servidor.

TIP: your chat can be monitored by network admin