I) Exercise One: Good old telnet

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

2. After logged what the user do?
Realizó una comprobación de conexión con yahoo.com y solicitó un listado de archivos en el directorio home para luego cerrar la sesión. podemos saber esto debido a que el tráfico de Telnet no es seguro.

II) Exercise two: massive TCP SYN

Questions
1. massivesyn1.pcap is a Port Scanning attempt
2. massivesyn2.pcap is a SYN Flood attempt

III) Exercise three: compare traffic

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:

El estudiante no está enviando un ARP request para obtener el MAC del router, por lo que no se puede conectar a este mismo, no puede enviar ni recibir tráfico fuera de su red local, el debe de configurar correctamente su gateway y verificar la resolución ARP.

IV) Exercise four: chatty employees

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

Question
1. What kind of protocol is used?
En este caso están utilizando un protocolo llamado MSN Messenger, para chatear
2. Who are the chatters?
Son dos Brian y thomas y básicamente se están poniendo al día y hablando del nuevo sujeto de IT.

3. What do they say about you (sysadmin)
Al parecer han escuchado que soy un tonto y quieren hacer un hackeo para molestarme.