

Exercise One: Good old telnet

Who logged into 192.168.0.1?

login: fake

password: user

After logging in, what did the user do?

\$/sbin/ping www.yahoo.com

Exercise two: massive TCP SYN

massivesyn1.pcap is a port scan attempt

massivesyn2.pcap is a SYN flood attempt

Exercise three: compare traffic

student1 must fix its IP configuration to ARP to 192.168.0.10 instead of 192.168.0.11

Exercise four: chatty employees

1. What kind of protocol is used?

MSNMS

2. Who are the chatters?

Brian and Thomas

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

That I'm a jerk. They also plan on hacking a server to annoy me.