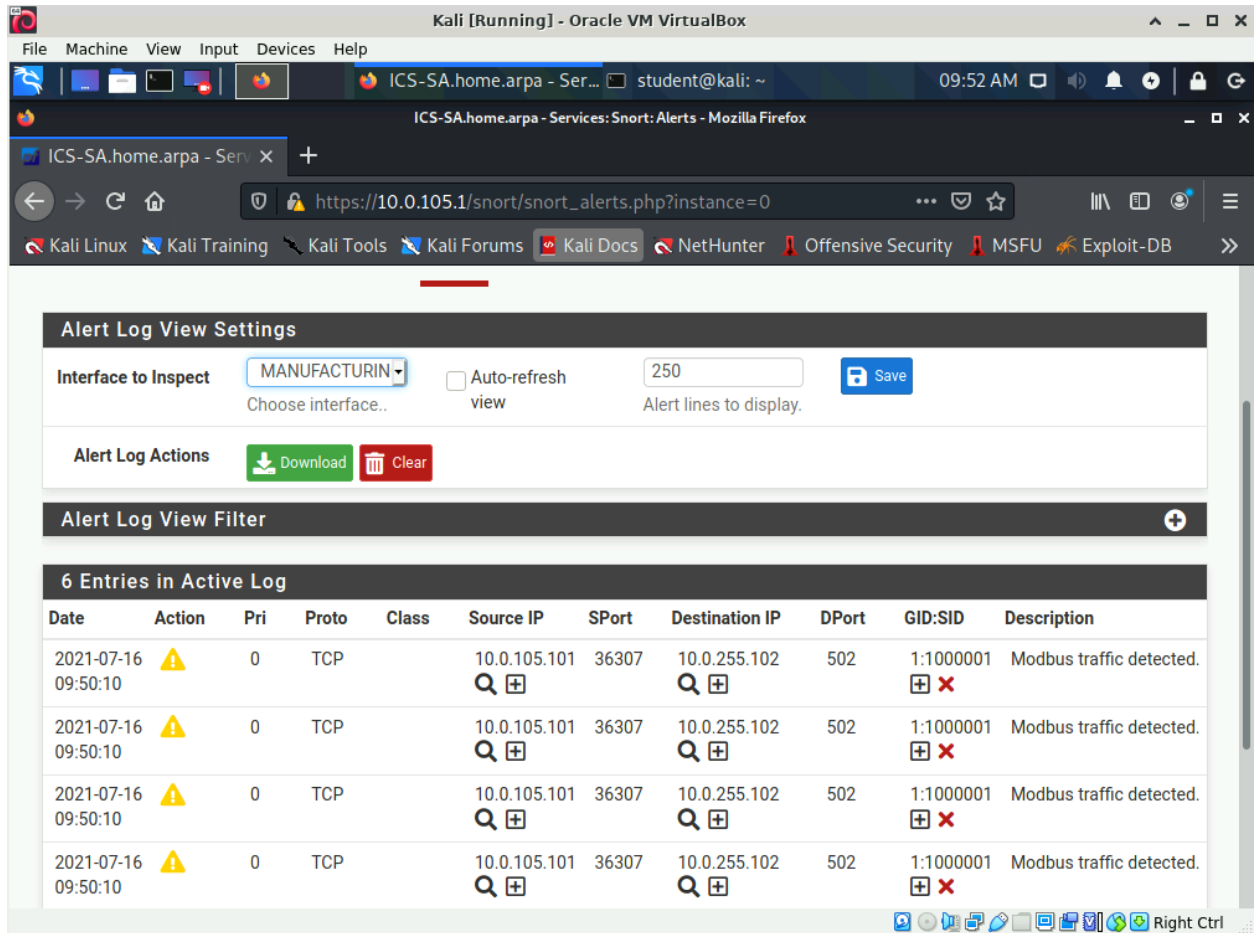


# IDS/IPS Lab Form

Name:

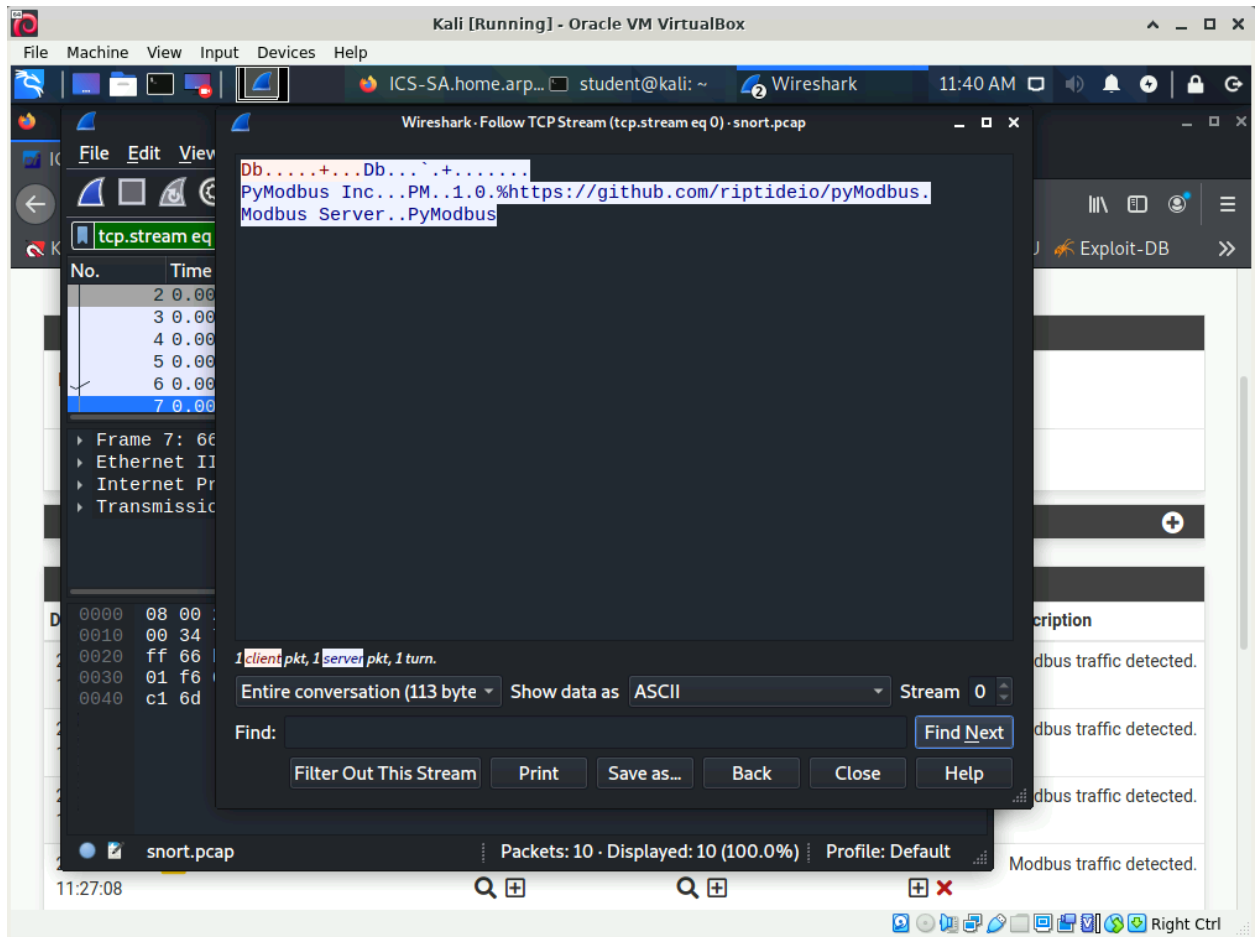
Date:

1. Paste the screen shot taken in Part 3 – “Enable and test an Intrusion Detection System (IDS)” into this question:



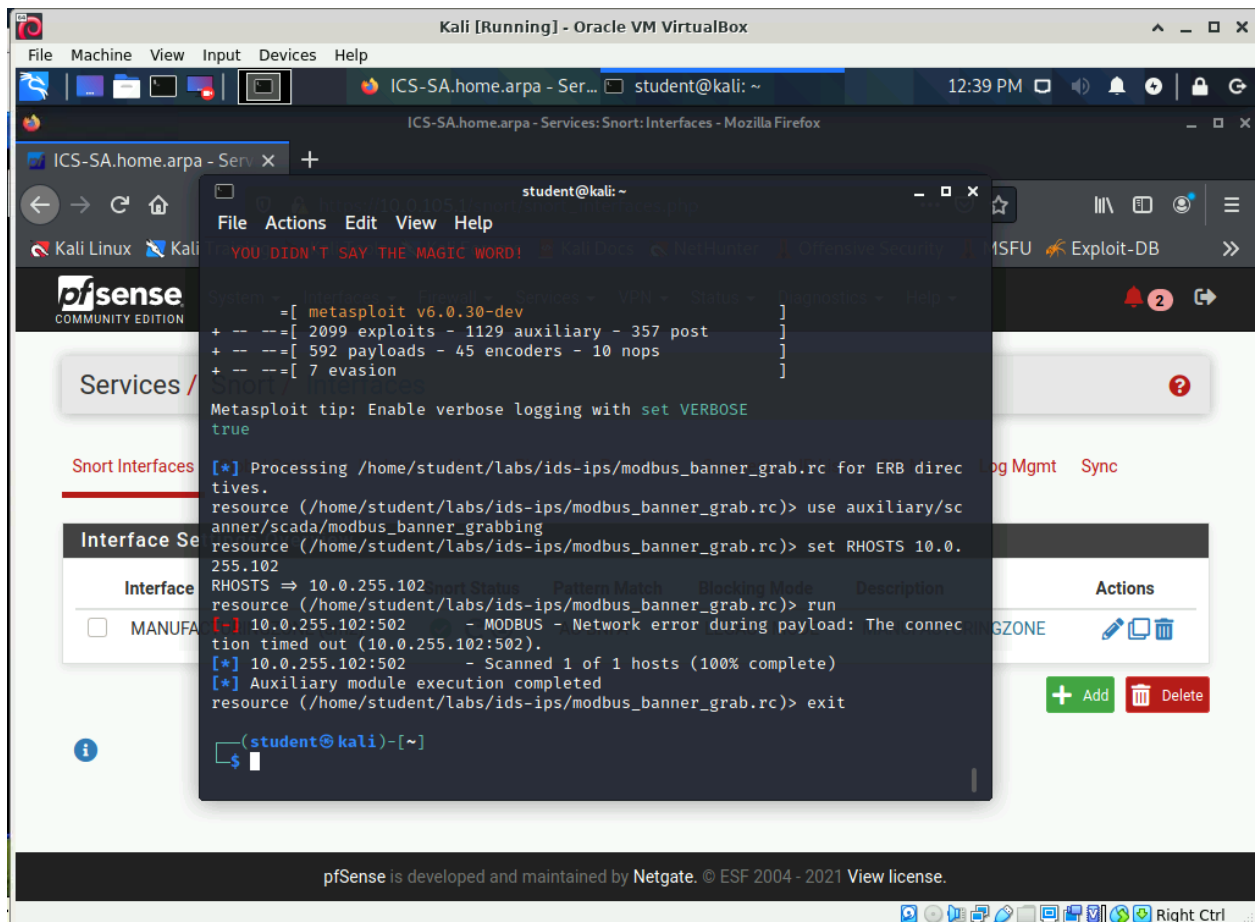
The screen show submitted by the student should show a different time and/or some other difference from this and the reference example.

2. Paste the screen shot taken in Part 4 – “Configure IDS Packet Capture” into this question:



The screen show submitted by the student should show a different time and/or some other difference from this and the reference example.

3. Paste the screen shot taken in Part 5 – “Enable and test an Intrusion Prevention System (IPS) “ into this question:



The screen show submitted by the student should show a different time and/or some other difference from this and the reference example.

- After completing Part 5 – “Enable and test an Intrusion Prevention System (IPS)” why is the Kali system unable to administrator the pfsense?

When the pfsense system detected Modbus traffic going from the Kali system to the PLC it blocked the Kali system’s IP address. Because the Kali system’s IP address has been blocked it is unable to access either the Web site or the PLC. The Kali system is being completely prevented from accessing the pfsense machine or any of the systems located behind the pfsense machine.

- If the Kali system was in the Manufacturing Zone network and was a critical component in your ICS, would you want to configure Snort to act as an IDS or an IPS? Explain your answer.

If the Kali system was connected to the Manufacturing Zone network and was a critical part of the ICS, the Snort system should be configured as an IDS. If the Snort system is configured as an IDS and a false positive occurs this will generate an alert. The ICS will continue functioning normally.



If the Snort system is configured as an IPS and a false positive occurs the Kali system's IP address will be blocked. This will prevent the Kali system from communicating with the rest of the ICS which could cause costly damage or even safety issues.