

# Zoning Lab Form

Name: |

Date: |

1. Paste the screen shot taken in the “Capture and view data transmitted in the Cell-Area zone” part of the lab into this question:

|

|

2. What does the value in Register 0 probably represent?

|

|

3. What does the value in Register 1 probably represent?

|

|

4. Paste the screen shot taken in the “Capture and view data transmitted in the Manufacturing zone” part of the lab into this question:

|

|

5. Why was the network ping traffic between the Kali-Modus system and the PLC captured but the data between the PLC and other ICS systems was not?

|

|

6. If using proper zoning techniques is more secure why might companies not configure their systems using this technique?

|

|



7. If you were to capture data on the Cell-Area zone and you consistently observed the following data what might you conclude regarding the functionality of the cooling system?

The image shows a Wireshark capture of Modbus data on the interface 'cell-area-zone'. The capture is filtered for 'cell-area-zone'. The packet list shows several Modbus queries and responses. The selected packet is a Modbus query (Frame 1571) for 'Read Holding Registers (3)' with a request frame of 1568. The packet details show the following structure:

- Frame 1571: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface cell-area-zone, id 0
- Ethernet II, Src: VMware\_01:91:89 (00:0c:29:01:91:89), Dst: VMware\_cd:19:3f (00:0c:29:cd:19:3f)
- Internet Protocol Version 4, Src: 10.0.255.102, Dst: 10.0.255.100
- Transmission Control Protocol, Src Port: 502, Dst Port: 1114, Seq: 36, Ack: 49, Len: 15
- Modbus/TCP
- Modbus
  - .000 0011 = Function Code: Read Holding Registers (3)
  - [Request Frame: 1568]
  - [Time from request: 0.000905231 seconds]
  - Byte Count: 6
  - Register 0 (UINT16): 0
  - Register 1 (UINT16): 60
  - Register 2 (UINT16): 10

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 0c 29 cd 19 3f 00 0c 29 01 91 89 08 00 45 00  ..)??..)....E.
0010 00 37 16 4b 40 00 40 06 11 ab 0a 00 ff 66 0a 00  7.K@.@. ....f.
0020 ff 64 01 f6 04 5a 56 01 b9 bc e2 f3 ca da 50 18  d..ZV. ....P.
0030 fa 48 40 50 00 00 52 70 00 00 00 09 00 03 06 00  H@P..Rp .....
```

The status bar at the bottom indicates: wireshark\_cell-ar...102\_iRmCDa.pcapn: Packets: 2684 · Displayed: 2684 (100.0%) · Dropped: 0 (0.0%) · Profile: Default