**LESSON 3 – NETWORK SECURITY**

**ACTIVITY 3.2.2 – BASELINE NETWORK TRAFFIC**

**ATTENTION -** *Remember, you will lose any work you do in the lab once the lab session expires. You will need your security baseline files in another activity, so it’s very important that you download copies of each baseline file to your school’s local machine.*

**ATTENTION -** *Save your baseline files to your school’s local machine.*

**VOCABULARY**

|  |  |
| --- | --- |
| abstraction |  |
| security baseline |  |
| sudo |  |

COMMANDS (record the command and options)

|  |  |
| --- | --- |
| sudo tcpdump |  |

Recreate the network topology diagram for the water treatment facility shown in Figure 1. Leave plenty of room between the hosts so you can document network traffic later.

|  |
| --- |
|  |

Below your topology diagram, summarize the operational requirements for each host. For example, on TargetWindows01, administrators remotely log into this machine using Remote Desktop.

|  |
| --- |
|  |

Find SSH, FTP, TCP, DNS, HTTP, and Ethernet in the OSI Model below and document in which layer they occur, recording both the number and the name of the OSI and TCP/IP layers.

|  |
| --- |
|  |

What is the purpose of the PumpMonitor?

|  |
| --- |
|  |

What is the purpose of the PumpPLC?

|  |
| --- |
|  |

Add to your network topology by diagramming what happened on the network: You used FTP to transfer a log file from PumpPLC to PumpMonitor. Recall you filtered out SSH data on port 22 so you will not have packet data related to your login session on TargetWindow01.

|  |
| --- |
|  |

Add to your network topology by diagramming what happened on the network, namely a file transfer from PumpMonitor to Web01.

|  |
| --- |
|  |

Add to your network topology by diagramming what occurred on the network, browsing Web01 via HTTP. Recall that you blocked port 22 for SSH traffic to and from TargetWindows01 but you did not block port 80 for HTTP traffic.

|  |
| --- |
|  |

**CONCLUSION**

Describe the purpose of “baselining” a network. Provide an example of an operation requirement from this activity.

|  |
| --- |
|  |