Network segmentation after host-based configuration requirements for project two are achieved by creating firewall IPV4 rules that allow only the admin network to connect and communicate with the FTP server. This leaves all other operating systems in the packet tracer without a rule to communicate with the FTP server. All these devices don’t need a deny statement to block communications with the FTP server if there is no rule for the connection the system will not try to connect to the other systems. The deny statement is for blocking unwanted or suspicious connections that are not needed or could compromise the system. The allow which is the one used in this case was put into place for the IP address 192.168.1.0 gateway for the admin network and with a wildcard mask of 0.0.0.255 which means the first three octets must match but the last octet does not, if it is valid. According to (Illumio, 2023) an advantage of these host-based firewall rules is the ability to enforce segmentation down to process level, more granular than just specific ports.

The FTP server is using least privilege because the users jsmith and bjones can only read and list. This means that the users cannot write, delete, or rename anything in the FTP server as they will only need these to do their jobs. On the flip side the FTP server is most likely under maintenance by the administrator which is why he is the only one to have all permissions to the FTP server.

An approach for network isolation in a network might be for a honeypot. As the honeypot needs to be isolated for protection against attackers so that when infiltrated the organization does not need to worry about them accessing the network architecture while the employees are trying to learn what tools and techniques are being used by their adversaries. This is an important step before deploying a honeypot because not doing so leaves your network defenseless because a honeypot is supposed to look like an easy target with bad defense that is what draws the attention of the hackers.

**References**

Illumio. (2023). *Network Segmentation*. Illumio. <https://www.illumio.com/cybersecurity-101/network-segmentation#:~:text=Host-based%20segmentation%20uses%20workload%20telemetry%20to%20create%20a>