Assignment 12 RTOS

Dan Blanchette

March 2023

1 Instructions

Research each port and answer the following question:
Why has U of I blocked these TCP ports on our VandalRTOS network?

2 Port Descriptions and Importance

2.1 TCP 25

This port is responsible for relaying email traffic on the internet. This port can be used for this purpose, or another port number within a certain range can be specified. In some circumstances, port 25 must be used on an STMP server. U of I may want to specify a custom port for this and limit access to port 25 to ensure no one can directly access or disrupt email services.

2.2 UDP 161-162

These ports are responsible for sending and receiving commands for network devices. The University would probably not want someone to have access to sending instructions to any connected device on the network. Conversely, someone with access could intercept instructions as they are being passed and learn how to create and manipulate device behavior that they could flood the network with.

2.3 UDP 42

This port allows for remote access to the network. This port operates at the network, transport, and session layers. This port is usually blocked to prevent access through this vulnerability. It allows remote communication from one computer to an application running on another person's computer on the network.

2.4 TCP 172

This port allows two hosts to establish a connection with one another. This port should be blocked because it can establish a private communication channel between two entities. The implications of this can be innocent or malicious, depending on the intent of use for the port.

2.5 TCP/UDP 1433-1434

These ports are used for SQL server traffic. It would be wise to block these ports because someone could flood these channels with packets to be updated to databases. Likely this can be used to commit a DDOS attack on a database, affecting other systems that need to query those systems for standard operations.

2.6 TCP Protocol 53

This protocol is blocked due to it being deprecated. Protocol 53, also known as the SwIPe security protocol, was largely used in the '90s and lacked source authentication, data integrity, and confidentiality. It makes sense why this functionality would be blocked and no longer utilized due to the sophisticated nature of modern computers.

2.7 TCP Protocol 55

This protocol, also known as MOBILE, is responsible for telecommunications and internet mobility access. The risk of this type of protocol being exploited can result in network disruptions to mobile services such as smartphones with internet servers that are being accessed by these devices.

2.8 TCP Protocol 77

This protocol provides real-time reliable data transfer. Know as SUN ND, if someone was able to modify the functionality of this protocol, it could affect the nature of the real-time data delivery it is known for.

2.9 TCP/UDP 135-139

These are RPC (Remote Procedure Call) ports. If they are not blocked, denial of service attacks through these port addresses is possible from malicious users. It makes sense that the University would want to monitor and protect these ports as much as possible to prevent loss of access to critical systems on the network.

2.10 TCP 445

This port was exploited in 2017 by the WannaCry ransomware attack. This port vulnerability caused a lot of damage to businesses, banks, and other public entities. Now that it is known, it would make sense for the University to prevent falling victim to a ransomware attack. As we have noticed, most hackers who conduct these types of attacks make it very difficult to regain control of their systems due to the attacker locking out the victim until they meet their demands.