Lab H

Brandon Trinkle

Arizona State University

Course Number: IFT 202

Professor Gary Grindle

Feb 17, 2024

**Part 1**

The three controls I implemented where enabling a guest network, enabaling WPA2 encryption, and enabling firewall protection. Within enabling the firewall protection I also turned on ignoring packet ping to WAN port and forbidding pings to LAN port.

The first control enabled was establishing a guest network. According to the FTC (Federal Trade Commission Consumer Advice, 2022) there are two benefits to setting up a guest network. First, using a guest network protects you from sharing your home network’s Wi-Fi password. This means you share a guest network password for your guest, and they use a separate network from your home network. Secondly, this protects your network from your guests who may potentially be carrying malware on their device (unknowingly). This would protect your home devices from being corrupted from sharing a network with a guest who may have an infected device.

The second control I implemented was enabling WPA2 encryption. There are three different types of encryptions: WPA, WPA2, WPA3. The go in order by effectiveness; WPA is an older encryption, thus it has less security features. WPA3 is the best, and newest, encryption and offers the most benefits and security. Our setup did not have WPA3 as an option, so we chose WPA2. According to the FTC, “Encryption scrambles the information sent through your network. That makes it harder for other people to see what you’re doing or get your personal information.” (Federal Trade Commission Consumer Advice, 2022)

The last security feature I implemented was setting up the network firewall. A firewall will protect your router from adversaries attempting to access your network. Additionally, I also added features like ignoring pings from WAN port and blocking pings from LAN port. What adversaries try and do when looking for potential targets is ping devices to search for networks. Enabling this blocking feature will block pings to the network. When they receive a packet loss they will assume there is no network available.

Part 2

Guest Network

A screenshot of a computer

Description automatically generated

WPA2 Encryption

A screenshot of a computer

Description automatically generated

Firewall settings

A screenshot of a computer

Description automatically generated

# References

Federal Trade Commission Consumer Advice. (2022, December). *How To Secure Your Home Wi-Fi Network*. Retrieved from Federal Trade Commission Consumer Advice: https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network