**Name:** Coral S. Schmidt Montilla **ID:** 148830

**Objective:**

Upon completion of this activity, you will be able to identify firewall limitations in protecting assets and implement best practices in firewall configuration.

**Student Instructions:**

Create at least three different rules for firewall application. More details about the web app at <https://groups.inf.ed.ac.uk/tulips/projects/1617/mjartan.pdf>. Please complete the assignment. This activity has a value of 15 points.

Rule 1: Block All Incoming Traffic by Default

This rule sets the firewall to deny all incoming connections unless we specifically allow them. It’s a good starting point because it limits exposure by default.

Command: iptables -P INPUT DROP

Rule 2: Allow Web Traffic (HTTP and HTTPS)

Since the app needs to be accessible on the web, we need to open up ports 80 and 443 for HTTP and HTTPS. These are the standard ports for web traffic.

Commands: iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

Rule 3: Block a Suspicious IP Address

If we know there’s an IP that’s trying to mess with the system or cause problems, we can block it directly. This rule blocks traffic from one specific IP.

Command: iptables -A INPUT -s 203.0.113.10 -j DROP