Khaleed Martin

nscc | w0474751

OSYS3030 – Additional Hardening Configs for my Server

October 12, 2023

Blow are additional rules that I added for my server presented in question format:

1. Add additional rules for any services you identified when you ran the last command in Part A.

**One additional rule I introduced to harden the server was to limit who can send DNS queries to my server. I restricted the DNS queries to my own subnet. I used the command:**

A black screen with white text

Description automatically generated

1. Create ufw rule(s) to ensure that you can only access from the host(s) that you use to manage your server.

**The IPs used are phony IP addresses, however they demonstrate allowing only a specific IP address on my server through port 22 (now updated to 2222). After I allowed my Ips, I then denied other IPs with the command “sudo ufw default deny incoming”. This allows only my IPs and now blocks all other ones connecting via ssh.**

A black screen with white text

Description automatically generated

1. You’re planning to use Rsync in the future to simplify administration. Create a rule to allow rsync to work with one other host on your network.

A black background with white text

Description automatically generated

1. You recently read about a vulnerability that may allow your server to be used and an open relay for outgoing mail. To mitigate this you’ve decided to explicitly deny any outgoing SMTP traffic.

Since the perpetrators are trying to use my server to relay outgoing mail, I would go ahead and block the port that is used for relaying (port 25). This would block all outgoing SMTP traffic.

A black screen with white text

Description automatically generated