**Question 2: Unsecured Web Server**

Suppose you find a server running HTTP on port 80, despite compliance guidelines requiring encryption in motion. What do you do? ​​

I have found a server running HTTP on port 80, though my organization’s compliance guidelines require encryption.

For Project 1, we did allow servers to run HTTP on port 80. This was ok as this was a virtual setup that I had control over, and I was the only one using it.

If this was a real deployment, I would have port 80 closed, and open it only when required, such as if I am using an application that requires me to get or renew a certification. Outside of those examples such as that, I would configure the primary web server to redirect all web traffic to port 443, so that it gets encrypted. I would do this by editing the etc/config files to add something along this line:

server {

# redirect all HTTP to HTTPS

listen 80;

server\_name example.com www.example.com;

return 301 https://example.com$request\_uri;

Running HTTP on port 80 is potentially a problem as port 80 does not encrypt data, it sends data through as plain text. There is nothing inherently wrong with any port, as they are basically just doors that are left either open or closed. However, encrypting data makes it much safer from bad actors who might be trying to uncover sensitive information, such as login and password info.

This solution should not be a problem for clients we work with who use port 80 as their default, as we are simply redirecting our traffic to a safer port. This would largely be a “set it and forget it” approach, but occasionally would need to open port 80, as mentioned above, to allow for certifications and re-certifications.