Domain: Network Security

Question 1: Faulty Firewall
"Suppose you have a firewall that's supposed to block SSH connections, but instead lets them through. How would you debug it?"

Current Firewall configuration is allowing SSH connections through. This is a security risk and must be fixed by closing port 22.
The command nmap was used to scan for open ports in the target machine Capstone 192.168.1.105, port 22/tcp ssh and 80/tcp http were open.

For project II, several virtual machines were nested in Hyper-V Azure. Kali 192.168.1.90, the attack machine, Capstone 192.168.1.105, the target machine, and an ELK server 192.168.1.100, a network monitoring machine that holds Kibana dashboards.

Penetration testing on the target machine showed useful information about folder structure, names and content. The dirb command - a content scanner - was used. Upon investigating further, there is a section of the site, called /secret_folder/ with no public access under /company_folders/. Successful directional traversal vulnerability was found after typing the following path: *192.168.1.105/company_folders/secret_folder/* prompt us to enter Ashton's credentials.

The name "Ashton" was found as part of the "Meet our team" section of the company's site. Ashton is a young employee who is managing the /company_folder/secret_folder. Two other names were found as well, with useful information about who controls what. For example, "Hanna" is the VP of IT and "Ryan" is the CEO. A brute force attack using Hydra provided the password for Ashton, thus success access to get into the /secret_folder/.

From Kali we could ssh into Ashton's computer as well. This is a very vulnerable port that would need to be immediately closed to provide more security. Part of a much needed system hardening is to use a good firewalld, a dynamically managed firewall, and set up rules to block/allow incoming traffic. Regular port scans need to happen to detect/correct any open ports. An alarm must be set up to detect the number of requested ports per source IP. The alarm will trigger an email and log file to be sent if the threshold is reached.