Question 1: Faulty Firewall

A firewall turns away any data that does not meet its policy, as determined by the firewall administrator. The most common cause of firewall failure is misconfiguration usually due to user error.

The machines that shared the network in Project 3 where:

- Capstone machine. ip address 192.168.1.105
- Elk machine. ip address 192.168.1.100
- Kali Linux machine. ip address 192.168.1.90
- Target 1 machine. ip address 192.168.1.110

The VM's that where servers are:

- Capstone and Elk Machine are servers.
- Protocols used where: http, ssh, netbios-ssn, and rpcbind

The VM's that where clients where:

- Target1 machine which communicated with the ELK server
- Kali Linux machine which communicated with the capstone machine and target1 machine.

The network policies in place where:

In Project 3 we were able to establish an SSH connection on one of the VM's that we used. This was due to the fact that port 22 was open and the user used a very weak password.

To help with this issue there would be a few things I would double check to increase the security. I would check the sshd_config file and configure SSH to listen to on a different port than the standard 22/tcp. I would also make sure that key-based authentication is being used.

To test out that the actions above are effective I would run a configuration test or an internal Pentest. This will help in determining if the changes were effective and what other changes might be needed.

The specific configuration I would check on a faulty VM would be the ssh_config file. I would check to make sure that SSH key-based authentication is being used. To test that my fix is effective I would redo the steps that we did in project 3 to try and ssh into the target1 machine.

My solution does not guarantee that the network will be immune to any unauthorized access. There is alway the possibility of a careless user placing their key in an insecure location, copying them to multiple computers, and not protecting them with a strong password. However I

would implement Failed Login Attempts monitoring in Kibana. I would set it up to alert to lock an account when more than 10 failed login attempts in a row are detected.