**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?

Today, cybersecurity is becoming more prevalent and needed given today’s surge of electronic and cloud services. So, maintaining proper security controls on any system, server, etc. is key to ensuring safety, integrity, and confidentiality as we meander throughout the web. Within this cluster of online technologies, we have tools to ensure our devices protection. A well-known security tool is a firewall. Firewalls use rules to block or allow certain protocols to run on a machine, such as SSH (secure shell). Suppose we want to block SSH connections on a device. This would not allow anyone to access to your device through SSH, and limits potential access for a malicious actor. Personally, I have configured something similar in my Cybersecurity Bootcamp from UC Davis. In our first project we created virtual machines on a virtual network put behind a NSG or network security group. This NSG acts as a firewall in the Azure cloud. When we created our first VMs we worked with the principle of least privilege, meaning we blocked all incoming traffic from any source to our virtual network. Then we allowed our “Jumpbox” VM SSH access only from one whitelisted IP, which was my personal public IP. This allowed me access into the jumpbox and limited all other traffic. We did the same with other VMs we created in this virtual network however, we limited the SSH connections into these VMs to the Jumpbox VM. Meaning, only I could SSH into the Jumpbox, and only the Jumpbox could SSH into the other virtual machines. If any other attempt were made without following these rules, the user would be prompted an error or “host unreachable” message. If, for some reason, you could SSH into the other VMs without going through the Jumpbox, or anyone could SSH into the jumpbox, then I would have to make sure my rules are clear and correct. I would double check what Ips are allowed SSH connections, what traffic is blocked, and what traffic is allowed (also any other pre-existing rules). This could easily be seen in the inbound rules of the network security group. If all rules have the correct parameters, then I would make sure the virtual network and virtual machines are connected to this NSG. If the network is not connected to the NSG, then there is no firewall intact, allowing any connections into our network. After checking the inbound rules thoroughly and making sure the security group is assigned, the VMs on this network should be immune to all unauthorized access. To further the security of the systems I would also link my Kibana Elasticsearch (ELK Stack) to my VM and capture any failed SSH attempts. (Kibana is a great open source tool that you can use to monitor the virtual machines you create)