**Jaquan Stevenson**

**Elk Stack Project**

**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? If I had a firewall that was supposed to block SSH connections, but somehow allowed them through I’d first check my virtual network rules. By examining the network rules, I will be able to see if external traffic is allowed through SSH. I can then configure these rules to either deny traffic through SSH connections completely or designate which sources are allowed to send traffic on the network through SSH.

Make sure each section of your response answers the questions laid out below. ​

1. Restate the Problem
2. Provide a Concrete Example Scenario
   * In Project 1, did you allow SSH traffic to all of the VMs on your network? In project one we did allow SSH traffic to all our VM’s.
   * Which VMs did accept SSH connections? For this project we allowed SSH connections on our Elk-Project-JumpboxVM, Elk-Project-Web1. Elk-Project-Web2, and ElkServerVM’s.
   * What happens if you try to connect to a VM that does not accept SSH connections? Why? Within this project if you try to connect to a VM that does not accept SSH connections, you will be denied access. This error may be due to a default-ssh rule is missing or has been misconfigured.
3. Explain the Solution Requirements
   * If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is? If one VM did not accept SSH connections, I would assume the source of the error pertained to a networking rule that was configured incorrectly (potentially a source or destination, an SSH service, or an allow/deny action).
   * Which general configurations would you double-check? I would generally double-check the source and destination access, the SSH service and protocol, configuration priorities, as well as allow/deny actions.
   * What actions would you take to test that your new configurations are effective? After reconfiguring my network rules, I would attempt to SSH into another machine, if successful, I know that I have reconfigured my rules properly and troubleshot all prior issues.
4. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem? Within the Azure UI we would navigate to the VM we’d like to inspect, from the overview page of the VM we navigate into “networking” section which then shows us all our VM rules. We then open our SSH rule to inspect the configuration, making any necessary changes.
   * Which specific configurations and controls would you check? I would specifically check configurations for Port 22 (SSH) within my VM’s.
   * What would you look for, specifically?
   * How would you attempt to connect to your VMs to test that your fix is effective? To check that our fix is effective we’ll open a virtual machine and initially SSH into an ansible jumpbox we previously created using its public IP address, *ssh* [*azureuser@20.187.96.19*](mailto:azureuser@20.187.96.19). From our ansible jumpbox we would then SSH into our Elk-Project-JumpboxVM (*ssh* [*azureuser@20.211.120.55*](mailto:azureuser@20.211.120.55)*)*, also utilizing the VM’s public IP address. From our Elk-Project-JumpboxVM, we are then able to use any of the private IP addresses from our created VM’s to SSH directly into the machines.
5. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access? In short, this solution does guarantee immunity to all unauthorized access. The only real threats to the network would have to be performed internally.
   * What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​

**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? ​​If we happen to find a server running HTTP on port 80, despite compliance guidelines requiring encryption motion, we will close the HTTP on port 80 and open a HTTP on port 443 instead. We would do this because HTTP on port 443, supports encrypted connections, while HTTP on port 80 does not.

1. Restate the Problem
2. Provide a Concrete Example Scenario
   * In Project 1, did you have servers running HTTP on port 80? If so, why was it permissible to do so? In project 1, I did have servers running HTTP on port 80. It was permissible to do because there were other safety nets in place (SSH configurations) that were already authorization only access points
   * In a real deployment, which specific machine would you configure differently? How, and why? In a real deployment I would configure
3. Explain the Solution Requirements
   * Why is running HTTP on port 80 a potential problem? Running HTTP on port 80 is a potential problem because the port provides an unencrypted connection between the web browser and the web servers, which leaves sensitive user data exposed to potential cybercriminals and lead to severe data misuse.
   * How would you reconfigure a server to serve HTTP traffic safely? The best practice to reconfigure a server to serve HTTP traffic safely would be to block all traffic by default and explicitly enable only specific traffic to known services.
   * How does this solution fix the problem? This solution fixes the problem because it provides control over server traffic and reduces the possibility of a breach because of service misconfiguration.
4. Explain the Solution Details
   * Which tools and technologies would you use to implement this solution in Project 1? To implement this solution in Project 1, I would use the network configurations/rules in my Azure UI to mitigate potential risk factors.
   * How, specifically, would you use these tools to harden your deployment? Configurations in my Azure UI would be the primary tool used to implement security changes.
5. Identify Advantages and Disadvantages of the Solution
   * Will your solution break clients that used to communicate with the server over port 80? My solution may initially break clients that used to communicate with the server over port 80, however, they would simply need to update (restart) their devices in order to implement changes.
   * Do you have to do any work to keep this solution running longterm? Or can you simply "set it and forget it?” Simply put, yes there will be work to keep this solution running long term. Servers will need be updated daily or weekly, to ensure securities are properly functioning. One cannot simply “set and forget” the server changes.