**Question 1: Setting Alerts in a New Monitoring System**

How do you determine which alerts to set in a new monitoring system?

Note: In Project 1, you did not set up any alerts. However, you still have enough experience to answer this question.

1. Restate the Problem

This project is a configuration of an ELK stack server in order to set up a cloud monitoring system

1. Provide a Concrete Example Scenario
   * Describe the network you built for Project 1. Identify the VMs on the network and what they do. This network includes of 4 VMs. Jump box and 3 webservers.
   * Which VMs should be publicly accessible? Jump Box
   * Which VMs should not be publicly accessible? Web server
2. Explain the Solution Requirements
   * Consider the VMs that should not be publicly accessible from the internet. Which alert(s) should these VMs fire and when? Alarm for any traffic from outside of the network to theses VMs
3. Explain the Solution Details
   * Which tool in Project 1 would you use to set such an alert? Firewall
   * What would the alert rule be? Alarm for any failed SSH attempt or ping request
4. Identify Advantages and Disadvantages
   * Are there any malicious circumstances that the alert(s) discussed above do not address?