**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
2. Provide a Concrete Example Scenario
   * Describe the network you built for Project 1. Identify the VMs on the network and what they do.
   * Which VMs should be publicly accessible?
   * Which VMs should not be publicly accessible?
3. 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?
   * Why should these VMs be associated with these alerts?
4. Explain the Solution Details
   * Which tool in Project 1 would you use to set such an alert?
   * What would the alert rule be? For example, would the alert fire upon a failed SSH attempt or a ping request?
5. Identify Advantages and Disadvantages
   * Are there any malicious circumstances that the alert(s) discussed above do not address?

**Setting Alerts in a New Monitoring System**

**Problem**

Creating and maintaining a new monitoring system can be a daunting and cumbersome task. Many considerations must be taken into account, including what alerts to set on each monitored machine and why.

**Example Scenario**

In this project, I configured two identical "web servers" to host DVWA containers, which were not publicly accessible. There are things alerts do not address. For a publicly accessible jumpbox VM, I would set an alert to notify me in the event of a failed SSH login. The below tables describe the subnets, machines on each, and the machine's purpose:

**RedTeam (**10.0.0.0/16**)**

| **Machine Name** | **IP Address** | **Purpose** |
| --- | --- | --- |
| JumpBox-Provisioner | 10.0.0.4 | Runs ansible, configures and provisions other machines. |
| Web-1 | 10.0.0.5 | Runs DVWA Application via docker container. |
| Web-2 | 10.0.0.6 | Runs DVWA Application via docker container. |

**ELK-Virtual-Network (10.3.0.0/16)**

| **Machine Name** | **IP Address** | **Purpose** |
| --- | --- | --- |
| Elk | 10.3.0.5 | Runs ELK stack via docker container. |

All of the above machines, only the JumpBox-Provisioner VM is publicly accessible via SSH, and only from one IP address (my home network IP: 68.206.66.79). All other machines are not publicly accessible via SSH. I configured an ELK Stack VM for monitoring and log collection. The web interface, Kibana, is publicly accessible from my home IP. The VMs that are not publicly accessible should have alerts about any traffic coming from outside to the VM.

**Solution Requirements**

Since the majority of the virtual machines are not be publicly accessible, alerts should be configured when SSH access is attempted to these machines. The Web-VMs should only be accessible on HTTP via the load-balancer; additional alerts should fire when HTTP access is attempted on these machines. Moreover, Alert should be configured on each of the machines to warn of ping attempts.

**Solution Details**

In Project 1, I would have used the Kibana web interface to configure these alerts. In addition to the alerts mentioned above, I would like to guarantee **no unauthorized SSH access** occurs on the Jump Box, so I would set an alert to warn of failed SSH attempts, or any SSH attempt from an unauthorized IP address.

Overall, the following alerts should be configured on the virtual machines:

* Jump Box Provisioner
  + Failed SSH attempts
  + Ping attempts
  + Any SSH attempt from unauthorized IP addresses (i.e. Except my home network)
* NewWeb1, newWeb2
  + Failed SSH attempts
  + Ping attempts
  + Any SSH attempt from outside the virtual network
  + Any HTTP attempt from unauthorized IP addresses (i.e. Except my home network)
* Elk
  + Failed SSH Attempts
  + Ping attempts
  + Any SSH attempt from outside the virtual network
  + Any Kibana web interface access from unauthorized IP addresses

**Advantages and Disadvantages**

While the above alerts should cover the vast majority of malicious circumstances, unforeseen events can take place that compromise any given machine on the network and can lead to unauthorized access of the network. Even when all packages are updated with security patches, malicious actors can still gain access to networks.

If a malicious actor were to gain physical access to one of the Azure data centers, our network could be compromise and we may not know. Although the likelihood of this taking place is minimal, we should be caution about this.