Interview Question

Domain: Cloud Security

Question 1: Cloud Access Control

How would you control access to a cloud network?

Cloud network Access control is very important for cloud network security. Critical assets can be compromised if access control is not properly configured. For example, in the ELK Project I deployed a cloud-based network that needed to have access controls in place. There were 5 VM’s deployed: Jump-Box, ELK-server, and 3 VM’s hosting the DVWA website. Jump-Box was my VM provisioner and is also used as a gateway to my other VMs. It is important that access to any of the other machines go through this VM to decrease my attack surface to my network. This makes it easier to control what traffic enters the network and who can have access to the servers lessening the likely hood of a compromise. A Security Group (RedTeamNSG) was created to serve as a firewall only to allow my local machine to access the Jump-Box-Provisioner through a secure SSH connection via port 22. When setting up this type of connection the way that I decided to setup a secure connection was using an SSH key instead of a Username and Password. This was to lessen the possibility of a brute-force attack intended to gain access to the Jump-Box. The RedTeamNSG also allowed SSH connections to go out of the Jump-Box to two different virtual networks (RedTeamNet) and (RedTeamNet2). These networks were peered together to be able to communicate between each other and allow a secure connection from the Jump-Box to the Web VMs (RedTeamNet) and from the Jump-Box to the ELK-server (RedTeamNet2) via SSH port 22 in order to be able to configure or redeploy them if necessary. Only allowing access from Jump-Box to ELK should lock out the possibility of another machine accessing the ELK if somehow the network was compromised. The same setup was configured on the other 3 DVWA VM’s. There was also a rule established to allow any communication back and forth between Virtual Networks allowing DVWA’s to share system, file, and pcap logs via TCP:9200 with the ELK-server for monitoring. A more secure ruleset is to be very specific about source and destination IP/Ports to be allowed. Front end Security rules differ from ELK and DVWA’s since DVWA servers are going to be accessed publicly through HTTP port 80 whereas the ELK server will only be accessible to system administrators to monitor webserver activity via TCP:5601. At this point no local firewalls have been implemented on the VM’s, only external.

This setup allows for scalability. If demand grew to the point another VM is needed to be added to the webserver pool this can easily be done by adding its internal IP address to the /etc/ansible/hosts file under [webservers] and executing the playbook to configure the new machine to host the DVWA.

The advantages of this type of setup are high availability as a load balancer was installed in front of the DVWA’s ensuring there is no single point of failure and quick deployment if the Jump-Box or ELK-server were to fail. A disadvantage is that you are not in physical control of the infrastructure or if for whatever reason the Microsoft Azure experienced an outage. Most SLA’s guarantee a level of availability, but there have been scenarios where other providers were not able to uphold this agreement due to an outage causing monetary loss and/or damage to reputation.