Todd Peralta

Cyber Security

Interview Question: Cloud Security

Question: How would you control access to a cloud network?

Access controls on a cloud network if mis-configured can be a devastating blow to a company's data. For example, when Capital One had a data breach it was because of unconfigured access control settings. During my studies with the Berkeley Extension Program for Cyber Security Professionals we covered control access and network security groups in a cloud network environment that we built from scratch. We went in depth to make it as identical as we could to a real life scenario. For example, when an organization is breached they would limit access to only their engineers and implement remote access to authorized employees as I did in Project 1 of my bootcamp.

During my project with Azure architecture we created 4 sets of virtual machines and deployed subnets in our Azure cloud networks. With these subnets we had to create rules and conditions to be able to access the vms, jump box provisioner and ansible containers using network security groups. We used these NSGs on our virtual networks to be able to SSH from our home IPs to be able to access our virtual machines and deploy ansible containers. We had to configure and make sure no outside traffic would be able to get into our network through open ports or misconfigured rules.

When creating and deploying our networks we connected our virtual networks to our ansible containers we had to set rules such as secure shell protocol to destination Port 80 and 22 to make sure all IP configurations were set into place to be able to access and deploy the containers and secure incoming traffic. Not only did we just secure our virtual machines but, we deployed an ELK- Stack network to be able to log and supervise incoming traffic and data. The Elk stack is commonly used in network production, you can initially expand the network with additional machines to create more log information. ELK is an acronym for elasticsearch, logstash and kibana. Access controls also worked as firewalls to be able to set secure connections. We created SSH keys from our ansible containers to be able to securely access our vms and jump box through port 22

Rules included in our NSG, load balancer and jump box were set in place to be able to access ports through priority rulesets. Meaning each priority was set so the network security groups could order what was important. My initial security group rules were allowing SSH, allowing the load balancer to maintain traffic on my network and allowing internet access into my network. These rules allowed VMs within the network to only speak to each other and the jumpbox. With the use of SSH keys I can modify configurations on a VM. This promises that brute-force attacks will never grant access.

The advantages of my project worked well because it only gave access to authorized users. The disadvantages to my project are that it is difficult to scale when new users are added that need access to the network and we have to create more safeguards to protect the network. A solution to these problems would be creating a VPN gateway to the private network. This would help scalability by allowing me to monitor users and security around the network. An appropriate time to use a VPN on Azure VMs would be when remote users need access from personal computers. This would enhance security to make sure no organizational assets are comprimised.