Interview Question

Taney Aaron Paul

Domain: Cloud Security

Question 1: Cloud Access Control

How would you control access to a cloud network?

Project one was an exercise in deploying a cloud network as opposed to an on-premises network. There were several benefits to the cloud network over the on-premises network. One major benefit of the cloud network it that it would much less cost prohibitive. Another benefit of the cloud network over an on-premises network would be no need for maintenance or costly hardware upgrades. There was a bit of learning curve in regards to the setup for the virtual network. For example was the need to setup specific access controls to the virtual network. The reason for the need to configure access controls was to have strict security control over the virtual network and machines. The main access control enacted was to allow exclusive SSH access (protocol 22) into the virtual network from my own personal computer. This was done specifically by way of whitelisting my own public IP address of 98.156.172.161 and denying every other IP address. There was also an inbound rule enacted that enabled restriced access via port 80 to prevent unauthorized entry to my web servers. This was setup by once again exclusively allowing my own personal IP address of 98.156.72.161. This allowed my jumpbox ssh access via port 22 to install the Ansible-playbook across multiple VM’s including the Elk server. This was necessary to for reasons of security and ease of deployment of the containers across the virtual network. These details relate back to the original question because they are the steps needed to maintain a high level of availability for the Web servers and also a enhanced level of security for the Elk server. This setup would allow me to access the Jump box and no direct access to the Elk server would ever be needed which would ultimately result in a much more secure Elk server. The info presented also relates as it is what would be useful in making deployment of the playbook to other virtual machine within the virtual network. Each access control achieved the measures of confidentiality, accessibility and integrity which are paramount to the concept of cybersecurity as a whole. In particular was the integrity of the load balancer which a much needed component of availibility. The main inbound rule set for each network security group or firewall was the restriction of every IP address except our own. Access to the jump box works by way of logging in via SSH from a whitelisted IP address. Access to the web servers one and two also works by way of SSH. This solution is scalable in that the ansible playbook can be copied to a number of virtual machines and also the virtual machines themselves can be easily duplicated as needed. At present the jump box is the best solution as it provides secure access and allows the creation of operational parameters that you could duplicate and upload to every server within the virtual network. Two of the main disadvantages that kept us from using a VPN are that they increase latency and are also cost prohibitive. The increase in latency is inversely proportional to the availability of the of access of the web servers. If one were to desribe what a benefit of the VPN would've been to acknowledge that it could have allowed data-tunneling via encryption from any and all servers within the virtual network to external workstations. The appropriate use of a VPN would not have been in this case as cost is an issue and their security benefits can be defeated with the correct know how.