Amanda Patterson

6/4/2021

Project 13 Interview Questions

Domain: Network Security/Question One: Faulty Firewall

Network security is designed to protect your network and data. Sometimes things go wrong with the Network security which requires action. If I have a firewall that is supposed to block SSH connections, but instead lets them through I would debug it by viewing and amending the network security inbound/outbound rules. During Project 13 Part One I allowed SSH traffic to all the VMs on my network. All the VMs did ultimately accept SSH connections. There were times that if I tried to connect to a VM, it gave me an error (time out/ could not connect). Whenever my VM does not accept SSH connections I had to double check the inbound/ outbound rules. I set my SSH rules to (Source = Any, Source port range = \*, Destination =Any, Service = SSH, Destination port range = 22, Protocol = TCP, Action = Allow, Priority =300, Name = SSH ALLOW, Description =Allow SHH). If I wanted to block an SSH connection I would take the same steps to amend the inbound/ outbound rules. Selecting Deny will allow me to Deny what I needed denied and selecting Allow will Allow me to allow what I needed allowed.

Once the inbound/ outbound rules are double checked in the Network Security Groups via “Settings”, I would attempt to see if the firewall would block my SSH connection. The Secure Shell (SSH) command is network communication protocol that enables two computers to communicate. I used the command SSH username@host\_ip\_address while in my terminal to test the communication. Communication can be successful or unsuccessful depending on the rules which allow/ denies specific traffic. The advantage of double checking the SHH command and rules will let you know what ports opened/ closed and what rules are set to allow and deny. Once you know you can adjust depending on your goal. Based on the rules I have set up my solution guarantee that the Project 1 network is now "immune" to all unauthorized access. Sites like Kibana / Windows Log can help me monitor to ensure that I identify any suspicious authentication attempts.