Network Security

Faulty Firewall

Hi, my name is Darryl Owens. I want to thank you for the interview opportunity. I want to discuss the faulty firewall situation we had to mitigate with you to get started. But before we dive deep into the firewall, I tried to give you a definition of what a firewall is and how it helps us in so many ways. A firewall is a part of a computer system or network designed to block unauthorized access while permitting outward communication. So a firewall is like your Captain America shield that will protect you from all harm. Sorry there, I got carried away. I'm a big Marvel fan but getting back to business.!

The first question was about allowing ssh traffic to all VMs on the network, and the answer is NO. The reason for not allowing so much traffic was because we only had the jump-box-provisioner and the elk VM and the ones appointed the duty to open the gates to the ports for the sake of the project. The reason is that you don't want to have all of your VMS vulnerable by being open to ports it's the holiday's Cybercriminals with the gift of hacking or controlling your systems with whatever techniques they have in mind. Hence, we have to be mindful strong and protect our VMs. I was able to find out because I wanted to check my work, aka "think like a hacker," to try to connect a VM that does not accept SSH connections, and great news, it didn't work. We received an error message on the command line that was a small victory for a junior soc analyst. We take all wins in this cyberwar.

If one of our VMS were to accept ssh connections, the game plan would focus on the VM getting ssh connections and consider looking in azure security groups at the rules or going into the container and checking the ansible configuration or the host's file. I will retest the new configurations by connecting ssh to the fixed VMS to see if our troubleshooting was successful. The specific panes I would investigate would be the RedTeamSG, or you would know it as the Security Group, and I will move to the Inbound Security Rules as shown in this screenshot.

The solution does guarantee that the network is immune to all unauthorized access. Still, if this machine were in the wild, I would add more security precautions. Having security logs to determine suspicious traffic makes my rules more specific of what I want for the network. Before logging into the container, we have passwords connected to make it harder for any cybercriminal to infiltrate.