Activity File SARAH DUCKETT

Interview Questions

Network Security

In response to a possible faulty firewall that is allowing SSH into the network when it should not this will need to be researched to determine source of breach. In completing project 1 we did not allow SSH into all of our virtual machines. SSH was only allowed in our Jump Box Provisioner machine. This function was not allowed on the Web1 ,Web2 or the Elkstack. To SSH into these machines you would need to be in the container which reside on the Jump Box If you tried to access the IP address of any of these from outside the container you would get a permission denied public key error or a server time out error.

If the virtual machine was allowing SSH to occur I would assume that it and was related to my public key and would start there. I would also check my port permissions and check the security rules in place for this machine. Once any issues that were discovered and corrected I would attempt to SSH into the machine via bash from my local computer to see if I could access.in t

The Azure panes that I would review to investigate this would be the inbound security rules found under Network Security tab and I would also check in this network security group to make sure that port 22 is not accessible as this should only be left open for testing purposes.

Per review of internet there are several ways to review the SSH activity on a server to monitor. This includes using netstat or the WHO command.

In the project we allowed port 80 to be used in our Elk Server load balancer because it was not a real world server deployment.

If I found that HTTP was running on port 80 I would redirect the traffic from port 80 to port 443. Port 80 is not a secure port. I would not close port 80 so that it could still receive but have it run through 443 which is a secure port. I would update this by updating inbound rules on the virtual machine. I would not recommend setting this and forgetting it. I would not recommend that action for any IT SECURITY related task. I would monitor the traffic on port 4 43 for overloading and possible intrusions after this was implemented.