Project Day 3 Interview

Domain :Network Security

Faulty Firewall

If we have a firewall that is supposed to block SSH connections, but instead is allowing them in We would have to debug it. Some ways of debugging the firewall would be by checking again to see if the rules for the firewall have any errors or maybe have allowed traffic instead of deny. For example in Project 1 we allowed traffic to all the vms on the network, but only from a specific source IP which was our own, and then we set inbound rules to deny all inbound traffic setting this to a high priority but not higher than the rule that allows inbound traffic from our personal ip address. We would have to check if there are any other rules that have a higher priority than the rule to deny traffic on the firewall. Our Elk vm did accept ssh connections , as well as our jumpbox. If we try to connect to a VM that doesn't allow SSH it wont allow us to connect, because it's not configured to do so, the firewall configuration is set to deny SSH connections so it'll block the traffic. If one of my project VM's would accept ssh connection when not supposed to I would think either something is wrong with the rules in firewall or maybe I am allowing ssh from that vm. After checking the rules of the firewall, and changing any errors, I would try to ssh again from the vm that was able to SSH in the linux terminal to see if I'm still able to do so. Check the inbound rules pane and look at the rules. It won't guarantee that it is immune to unauthorized access but that is why we need to implement defense in depth to cover more areas that can bring vulnerabilities.I would use kibana, filebeat to check log files, and metricbeat.