**Interview Activity**

**Aaron Plekan**

**Domain: Network Security**

**Faulty Firewall**

It is always important to be able to have a firewall block SSH connections because you do not want unwanted users to be getting into your systems shell. Debugging is typically the method to take to make sure no one except yourself can get into the shell.

In project 1 we allowed the Jump-box VM to be SSH from your local internet source. For our project, we set it up so you can only connect to my jump-box from my IP address. The Web VMs that were created can be SSH into while you are in the jump box but not from your source internet. If I were to try to SSH into one of the Web VMs, it would time out on me and constantly try to connect but won’t.

If one of my VMs was able to get SSHed in then i would immediately know that I need to restrict access to port 22. You always want to check to see if that is open to the world or just restricted to just you. SSH typically runs on port 22, so you can whitelist everything and just keep it with your own IP address. I was able to set it up so that you only have access to the Web VMs from your jump-box. There are a few more rules in place to help prevent others under the NSG.

When I am going into my Azure UI, I would be going under the network security group. When you are under there, you can change your rules for each VM.  I added port 22 and included my IP address to be the only SSH into the jump-box. Then I added a rule that once you are in the jump-box then you can SSH into the other VMs if needed.  Once you have that in place, you want to see if you can then access the VMs after restricting the traffic. If it times out, then you have successfully stopped others from getting in. I tested this by trying to SSH into the Web VMs from my IP address instead of being the Jump-Box. I was unsuccessful on getting in, which means it actually did work.

When looking at everything that I’ve done, I can determine that it should hopefully be fool proof. The toughest thing would be if my IP address changed, then it would be significantly harder to get back in. At that moment, I would have to go to my Azure UI and change some of the rules so I can get access again. If we created a VPN for the network, we would be able to monitor users more effectively. This also would allow us to work remotely if needed.

**Domain: Cloud Security**

**Cloud Access Control**

Controlling access to cloud networks is a very important topic for corporations. I say this because only a select few people within the company should have access, so you need to maintain an orderly fashion on who can get in. It is our job to make sure that the right people are gaining access.

In our project, we actually did set up multiple VMs within the cloud network. When we were setting it up we did have to configure access controls for the VMs. I set it up so only I can gain access to them for the time being. I set up some rules under NSG to make sure that I am truly the only to gain access to the VMs. When looking at a company, you can see that setting up specific rules are always a good route to take. Some of the most important ones to configure was port 20 because this will actually restrict access to everything i didn’t list. I also had to add a load balancer to help maintain the traffic.

When I was setting everything up. I had to set up a NSG first and foremost. This blocked all IP addresses except for mine to gain access to it. I set it up so I can only get access to the Virtual Jump-Box. I used an SSH key as well so brute force was not an option for others to gain access. I denied all inbound as well under the rulesets.

The most prominent rule that was set was for port 22. Again I set it up so only my IP can gain access to it. I set it up so you can SSH from jump-box into the virtual network. You won't be able to gain access to the Web servers if you aren't in the jump-box. I used port 80 so the web servers can send and receive data/messages.

For the project itself, this way was extremely useful because there weren’t many people that needed to gain access to the servers. If more and more people needed to gain access then I would have to constantly change the NSG. One way to improve all of this is using a VPN. The reason why we didn’t use it was because I was the only one trying to gain access to it. The advantages of using VPN would be once more people have access, then we can help monitor it a lot more. Why we would use one would be when people also have to work remotely. That way they can work from wherever they are at the time.

**Domain: Logging and Monitoring**

**Challenges of Collecting Large Amounts of Log Data**

Dealing with large amounts of log data can always be very challenging to look at. One of the toughest things is that log management truly can’t distinguish between good and bad activity. It doesn’t separate the two so you will have to manually go through and figure out what can be considered bad.

When we were doing project 1, we were using log data when we went into Kibana. We were investigating all different types of data and from multiple countries as well. I was able to see the different types of files that were being downloaded and what for exactly. When i was scrolling the most populated times of the day, i was just getting a lot of activity for social media websites. I was looking for something suspicious within the logs but I was mostly seeing people posting and downloading stuff from facebook/twitter.

The information I was needing was all in Kibana. Kibana was all from our elk servers that we set up within our virtual network.  Kibana helped navigate the different charts and look for specific activities that were occurring at the time. Typically what an analyst needs to monitor logs would be the different types of functions and methods presented to them. Pattern recognition and normalization is always important to have because they can help compare incoming messages with a pattern book. For our project, we were using Kibana and going into the data management section. Within there were graphs that help show the data that was incoming. We were able to single down to specific times and from which countries as well.

When looking at all the different logs/graphs, it is safe to say most were pretty convenient for filtering data coming through. The one i found easiest to use was the average bytes vs unique visitors graph. That one truly showed what time of day and which countries were bringing in the most traffic. From there you could click on the specific times and then look through the sources and IP addresses that were coming through.

Some of the data that I didn’t use was the chart that shows the source and destinations. I feel like this could have helped a little bit more on what exactly those people were trying to accomplish but it didn't affect what I was wanting to do for the project. I feel like it would have not totally changed my outcome and conclusions to what I was doing. It was curious to see where a lot of the traffic was getting diverted to but it did not serve any purpose for me.