Domain: Network Security

Question 1: Faulty Firewall

Suppose you have a firewall that's supposed to block SSH connections, but instead lets them through. How would you debug it?

Make sure each section of your response answers the questions laid out below.

1. Restate the Problem

Due to the privileged access to mission critical systems attenable through SSH connections, it is imperative for organization's to properly manage remote access to their network. Organizations can achieve greater efficiency and security with SSH remote connections. However, if this service is not carefully managed, it can drastically increase the attack surface and introduce new threats to the organization.

2. Provide a Concrete Example Scenario
    - In Project 1, did you allow SSH traffic to all of the VMs on your network?

In my cybersecurity bootcamp, I managed SSH connections to an Azure virtual network that I created. While setting up the cloud environment, I was careful to only allow SSH connections to the systems that required remote access from my local workstation as allowing SSH traffic to all the VMs would have unnecessarily exposed critical systems to the untrusted internet.

    - Which VMs did accept SSH connections?

I established an SSH connection through one VM that I used to configure other created VMS in the cloud environment. Specifically, I allowed for a SSH connection to a jump box provisioner that I used to configure two web VMs, each running an instance of DVWA, and an ELK server to create a security monitoring solution for the virtual network.

    - What happens if you try to connect to a VM that does not accept SSH connections? Why?

In the virtual environment that I created, if I attempted to SSH into one of my web servers, I would have received a permission denied error. This would be by design because the network security group that I created did not specify an inbound security rule allowing SSH connections to the web servers.

3. Explain the Solution Requirements
    - If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is?

It is vital for organizations to have an efficient management system when configuring SSH to network assets from a remote network. Allowing SSH access to a system that should have this

service restricted will unnecessarily open up the attack surface and increase the risk exposure to any organization. This is why the firewall configuration must be checked to see if an improper rule has been created allowing the undesired access.

- Which general configurations would you double-check?

Luckily when I created my virtual network, I did not face a situation where an SSH connection was established when it was not supposed to be. However, if I were ever presented with this exact situation in the virtual network that I created, I would check my network security group to make sure there is no inbound security rule allowing SSH on any network servers that should not allow remote connections.

- What actions would you take to test that your new configurations are effective?

To make sure the new configurations took place as desired, I would attempt to log in remotely to the network servers to see if a connection was established or blocked as intended.

4. Explain the Solution Details
    - Which specific panes in the Azure UI would you look at to investigate the problem?

In my cloud environment project, I was tasked with ensuring proper security configurations were in place to thwart attacks and ensure the security posture of the cloud environment was upheld. I did this by managing inbound security rules within the network security groups created in the Azure portal.

- Which specific configurations and controls would you check?

Within the network security group, I would look for inbound security rules relating to SSH traffic.

- What would you look for, specifically?

In my cloud project, I had to set up inbound security rules to establish SSH connections to my jump box provisioner and from my jump box provisioner to each of my VMs. To ensure that SSH connections were disabled, I would examine the security rules to verify there are no rules that allow SSH connections from any outside source IP addresses destined for the virtual network. Even though, SSH is inherently run with TCP protocol, I would block all protocols using this service to further mitigate any change of the network being accessed through an SSH remote connection. In addition, I would make sure an inbound security rule was created to deny all SSH traffic coming into the network as required.

- How would you attempt to connect to your VMs to test that your fix is effective?

After the network security group has been configured properly and it has been determined that the rules match the desired outcome, the next step to ensure the network denies all SSH

connections is by testing out the connections from an external workstation to each of the VMs in the network. To accomplish this, I would upon up a command line interface and attempt to SSH into each VM. For example, I would run the command: ssh RedAdmin@40.112.62.73 , where RedAdmin is the username and 40.112.62.73 is the IP address of the jump box provisioner to test the connection. I would duplicate this command to attempt to establish an SSH connection to all devices on the network and ensure permission is denied to each one.

5. Identify Advantages/Disadvantages of the Solution
    - Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?

One of the things I have learned throughout my bootcamp program is that a network can never be fully “immune” to security attacks or from unauthorized access. The goal is never to make sure your network is 100% free from attacks as this is virtually impossible to attain. Rather, the goal should be to build on security mechanisms and apply the concept of defense in depth mentality to ensure various security measures are in place in the event an attacker is able to circumvent any of the measure in place on the network. The defense in depth concept was something I had in mind when creating my network. I first accomplished this by creating inbound security rules to prevent unauthorized access. In addition, I made sure SSH connections could not be established via passwords, which are inherently weak and can be brute forced. Instead, I relied upon generated SSH key pairs to authenticate my local workstation to the VMs I created in the cloud. The rules I created in the NSG and use of SSH keys did not make my network immune from unauthorized access. However, they substantially enhanced the security posture of my network and mitigated any risks of unauthorized access.

The inbound security rules created were one way to prevent unauthorized access to the network. To further bolster the security posture of the network, I also

    - What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?

The functionality of the virtual network that I created was a big accomplishment for me. Being able to create a full working cloud environment is something I never thought I would be able to do. Not only was I able to build a fully working cloud environment and provision Ansible containers to deploy web servers, but I was also able to fully create a full network monitoring solution with the ELK server that I created. Installing filebeat and metricbeat on my web VMS and using Kibana to visual the responses really helped me gain insight on what to focus on when reviewing aggregated log files. One of the things that I looked for was suspicious authentication attempts. The log data taken from each VM, which had an instance of filebeat installed, allowed me to use Kibana to review not only successful SSH logins, but also invalid login attempts as well.

Question 2: Unsecured Web Server

Suppose you find a server running HTTP on port 80, despite compliance guidelines requiring encryption in motion. What do you do?

1. Restate the Problem

Organizations often are tasked with sending and receiving sensitive data. When this data is in transit, it becomes susceptible to various security attacks such as a man in the middle or eavesdropping attack that could compromise the confidentiality of that data. This is why it is imperative for organizations to ensure any data in motion is adequately encrypted with a strong cipher and ensure all data is transmitted via HTTPS protocol through port 443.

2. Provide a Concrete Example Scenario
    - In Project 1, did you have servers running HTTP on port `80`? If so, why was it permissible to do so?

In Project 1 of my cybersecurity bootcamp, I created a cloud environment that used servers running on HTTP port 80. Although this should never be applied in a real-world setting, the use of HTTP in the network I created was permissible in this instance because no sensitive data was being transmitted.

    - In a real deployment, which specific machine would you configure differently? How, and why?

In the real-world, especially in the health and financial sector, HTTP protocol should never be used to transmit data. This is because organizations deal with sensitive data and must adequately protect the confidentiality of the sensitive data they work with. All servers handling data should be forced to encrypt the data they transmit by forcing HTTPS traffic through port 443.

3. Explain the Solution Requirements
    - Why is running HTTP on port `80` a potential problem?

Any data transmitted through port 80 using HTTP protocol is not using any encryption mechanisms to conceal the data. This means that data is transmitted in plain text and has the potential to lose its confidentiality if an unauthorized user access this data.

    - How would you reconfigure a server to serve HTTP traffic safely?

To ensure data in transit is adequately protected and maintains its confidentiality, I would reconfigure my servers to utilize the HTTP Strict Transport security mechanism to interact with only HTTPS connections.

    - How does this solution fix the problem?

The use of HTTP Strict Transport will force users who attempt to reach a website through HTTP to upgrade to an HTTPS connection. This will ensure that the data being transmitted to the web server will be encrypted and mitigate against the risk of a man in the middle attack.

4. Explain the Solution Details

- Which tools and technologies would you use to implement this solution in Project 1?

Although HTTP Strict Transport Security (HSTS) is not an option, there are methods that can be applied to ensure all traffic sent to the cloud environment created in project 1 is encrypted and adequately protected. To achieve this desired result, I would rely on specific inbound security rules in the network security group configured to the network.

- How, specifically, would you use these tools to harden your deployment?

The goal is to ensure that data in transit is encrypted and maintains its confidentiality. To accomplish this goal, we can deny all traffic using HTTP protocol through port 80. At the same time, we can set up inbound traffic transmitted to the network to be received using the HTTPS protocol via port 443.

5. Identify Advantages and Disadvantages of the Solution
    - Will your solution break clients that used to communicate with the server over port `80`?

In the long run it will be advantageous for clients to utilize this method of encrypting information transmitted over the internet to maintain the confidentiality of their data. Their data will be better protected and they will have peace of mind when typing in their credit card information and hitting the submit button. However, the use of this technology will present some limitations to certain users. Even though there is widespread support for the use of HSTS among the major browsers such as MS Edge, Firefox, and Google Chrome, users whose browsers do not support this technology will be unable to connect to a website through HTTPS and may be unable to access the desired content.

- Do you have to do any work to keep this solution running longterm? Or can you simply "set it and forget it?"

As with any security mechanisms put in place within a network, the enabled firewall configurations will need to be adequately monitored and maintained to ensure they are not altered and still capable of producing the desired results.