**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 Firewall is supposed to block/allow traffic to local network based on the ACL
2. Provide a Concrete Example Scenario
   * In Project 1, did you allow SSH traffic to all of the VMs on your network? SSH was only allowed to a Jump-Box from specific sources
   * Which VMs did accept SSH connections? From outside Jump-Box and VMs will only except connections from Jump-Boxes
   * What happens if you try to connect to a VM that does not accept SSH connections? The access will be denied/blocked Why? Access is controlled by network security group and by default all outside access is blocked
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? Network security group is misconfigured
   * Which general configurations would you double-check? Network security group, make sure thee is an explicit rule that blocks all traffic unless allowed
   * What actions would you take to test that your new configurations are effective?
   * Try to access from the source that is not listed in the “allowed/permitted” sources and ports: SSH/HTTP/HTTPS, etc
4. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem? Network Security Group
   * Which specific configurations and controls would you check? Inbound Security Rules
   * What would you look for, specifically? The source, ports and destination
   * How would you attempt to connect to your VMs to test that your fix is effective?
   * Try to SSH to VMs ( make sure it is blocked ), only HTTP is allowed
5. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access? There is always a probability of hacking/vulnerability, but it is easy to mitigate/restore the services because of the availability set and container replacement
   * What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​ ELK sever

**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

Since HTTP port 80 is considered not be a secured port due to clear text transmission, there are some way to minimize the impact

1. 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? 3 web servers were accessible over port 80 mostly due to the idea of high availability, if any goes down another are still running, plus it is easy the replace any compromised one thanks to ansible(Jump-Box)
   * In a real deployment, which specific machine would you configure differently? In real world it would be HTTPS access only
   * How, and why? One of the options could be port forwarding were HTTPS requests will be forwarded to HTTP on the inside network
2. Explain the Solution Requirements
   * Why is running HTTP on port 80 a potential problem? Data is transferred in clear text
   * How would you reconfigure a server to serve HTTP traffic safely? Only accept HTTPS
   * How does this solution fix the problem? It minimizes potential data integrity while in transmition mode
3. Explain the Solution Details
   * Which tools and technologies would you use to implement this solution in Project 1? Microsoft Azure along with Network Security groups to manage/control network to the resources.
   * How, specifically, would you use these tools to harden your deployment? Allow access only from trusted resources and specific ports and block all other traffic.
4. Identify Advantages and Disadvantages of the Solution
   * Will your solution break clients that used to communicate with the server over port 80? Yes, as HTTP traffic will be blocked, and they will need to use HTTPS
   * Do you have to do any work to keep this solution running longterm? Or can you simply "set it and forget it?” Servers should be monitored updated and patched. Scheduled backups should be also performed.

**Domain: Cloud Security**

**Question 1: Cloud Access Control**

How would you control access to a cloud network?

1. Restate the Problem

Cloud network became an essential part of nowadays world to run the business and with its easiness to implement and use the notion of SECURING it is no less important and should not be neglected as securing of on-premises network.

1. Provide a Concrete Example Scenario
   * In Project 1, did you deploy an on-premises or cloud network? Cloud network
   * Did you have to configure access controls to this network? Yes, allow only needed ports and trusted connections
   * What kinds of access controls did you configure, and why were they necessary? Only allow SSH connection to a Jump-Box, with asymmetric ssh key and specific source Ips, this why communication is more secure.
   * How do these details relate to the interview question? Good understanding of network infrastructure and flow on top with process involved makes a good presentation of the knowledge of the subject.
2. Explain the Solution Requirements
   * In Project 1, what kinds of access controls did you have to implement? Consider:
     + NSGs around the VNet? Around the VMs? NGSs around Vnet
     + Local firewalls (ufw, etc.) on each VM? Firewalls: ufw, firewalld
     + Protocol allow/deny lists? Inbound security rules, where port 80 and port 22 where allowed through with lower priority number and interVnet traffic, but deny everything else rule with higher priority number.
   * What did each access control achieve, and why was this restriction necessary for the project? SSH access to Jump-Box from specific IP sources protected the rest of the network form unnecessary exposure to the Internet and therefor reduces the chances of potential attack on the network infostructure
3. Explain the Solution Details
   * Which rules do you set for each NSG in the network? Allow SSH connection to a Jump-Box from specific IPs and port 80(HTTP) to the WEB servers set as a availability group behind a load balancer also from specific IPs for the purpose of the project.
   * How does access to the jump box work? SSH using public IP address – 13.82.70.210
   * How does access from the jump box to the web servers work? SSH from Jump-Box using local IPs: 10.0.0.10, 10.0.0.11, 10.0.0.13
4. Identify Advantages/Disadvantages of the Solution
   * Does your solution scale? Yes, it is scalable
   * Is there a better solution than a jump box? I do not want to say better, there is always room to make thing better, but I like the idea of the Jump-Box, because this resource can be turned off while not in use and therefor it makes access to network resources even more difficult, as private part of SSH key is located on it.
   * What are the disadvantages of implementing a VPN that kept you from doing it this time? Extra cost to implement and maybe slower connection.
   * What are the advantages of a VPN? It secures communication between the peers, without exposing local resources to public network.
   * When is it appropriate to use a VPN? VPN is a good implementation for employees “on the go”, while using public WiFi like hotels, coffee shops, etc.

**Question 2: Corporate VPN**

What are the advantages and disadvantages of using a corporate VPN, and under what circumstances is using one appropriate?

1. Restate the Problem ---- By design VPN is considered to be a preferred way of accessing company/corporate network/resource for employees by means of security, but it is not always a case, because a connected VPN device now has access to inside network bypassing some front end security implementations.
2. Provide a Concrete Example Scenario
   * In Project 1, which VMs did you have on the network? Jump-Box, Web1, Web2, Web3 and Elk-Server.
   * Which tools did you use to control access to and from the network? SSH along with SSH keys.
   * If you didn't use a VPN, what did you use? Network Security Group rules, controlling inbound access.
   * What disadvantage(s) did your non-VPN solution have? It exposes Jump-Box
   * What advantage(s) did your non-VPN solution have? Simplicity of implementation and reasonable security access/control, plus Jump-Box can be turned off while not in use.
3. Explain the Solution Requirements
   * Would a VPN meet the access control requirements you had for Project 1? Sure it would.
   * How would a VPN protect the network just as well, or better, than your current solution? It would protect it a bit better, as Jump-Box would not be exposed to the outside world
4. Explain the Solution Details
   * Which Azure tools would you use to implement a VPN to your Project 1 network? Virtual Network Gateway and Azure VPN client
   * How would you onboard users to the new VPN system? Azure VPN client needs to be installed and configured
5. Identify Advantages and Disadvantages of the Solution
   * In Project 1, would a VPN have been an appropriate access control solution?
   * Under what circumstances is a VPN a good solution? It is a good solution for IT team to connect to corporate resources/tools and remote employees
   * When, if ever, is a VPN "overkill"? Even though VPN considered to be a good practice, but it can decrease network performance and may potentially increase a work to network/security team due to user errors/misuses. Again it all depends on the scale of the company and how valuable resources are that need to protected.

**Question 3: Containers**

When is it appropriate to use containers in cloud deployments, and what are the security benefits of doing so?

1. Restate the Problem

Containers became an essential part of a cloud world today, because to bring on demand scalability and availability without exposing or compromising the rest of the services on the network besides its own and therefor minimizing the risk vulnerability and impact to the rest of the network/resources if a container was compromised.

1. Provide a Concrete Example Scenario
   * In Project 1, when did you use containers? Setup Ansible on a Jump-Box, DVWA web container on the web servers, ELK-server.
   * What did you use containers for? To bring up necessary services/tools: DWVA, Kibana, etc.
2. Explain the Solution Requirements
   * Why was this an appropriate use for containers? Containers require minimum resources and can be easily replaced.
   * What security benefits did you expect from using containers? Containers only expose themselves without compromising the host system
3. Explain the Solution Details
   * In Project 1, how did you configure VMs to be able to run containers? Docker environment was used/installed.
   * How did you select and install the correct container?

sudo docker run IMAGE\_NAME

* + How did you verify that it was running correctly? sudo docker container list -a

1. Identify Advantages/Disadvantages of the Solution
   * How would you have achieved the same thing without containers? setup/configure a virtual machine
   * What are the advantages to doing it without containers? one of the advantages could be a more disk space, more configuration options and tools.
   * What are the disadvantages? I think the biggest one is waste of unused resources and longer down time.

**Question 4: Cloud Infrastructure as Code**

What are the security benefits of defining cloud infrastructure as code?

1. Restate the Problem With development of cloud computing the management and configuration of the resources became more robust and at the same time simple to manage, where the file with configuration code can bring up or restore and modify a necessary resource in a matter of minutes
2. Provide a Concrete Example Scenario
   * In Project 1, when did you use infrastructure as code (IaC)? ELK server
   * What tool did you use? Ansible automation and orchestration tool
   * What did you use it to do? Code files with proper “commands” called playbooks, that are executed by Ansible.
3. Explain the Solution Requirements
   * Were there any alternatives to IaC? Yes, another option was to shh into the host machine and download and configure necessary packages/programs
   * What benefits does IaC have over alternative approaches? The biggest advantage is that resource can be brought up quick and almost eliminates any user errors in configuration.
4. Explain the Solution Details
   * In Project 1, which specific configurations did your IaC set up? Ansible playbook file that sets up the resource and a configuration file that is copied over to make sure that resource is configured properly to meet the environment needs.
   * How did you run and test these configurations? With a command: ansible-playbook elk.yml, where at the end of the installation/setup process results are shown.
5. Identify Advantages/Disadvantages of the Solution
   * Are there any disadvantages to using IaC over the "traditional" approach? May be configuration of dependencies

**Domain: Logging and Monitoring**

**Question 1: Setting Alerts in a New Monitoring System**

How do you determine which alerts to set in a new monitoring system?

Note: In Project 1, you did not set up any alerts. However, you still have enough experience to answer this question.

1. Restate the Problem Since monitoring system allows to view almost any angle of the processes and system health, it makes more sense to monitor only the ones that are being used and are crucial for availability and integrity of the setup.
2. Provide a Concrete Example Scenario
   * Describe the network you built for Project 1. Identify the VMs on the network and what they do. Network consists of 3 WEB servers, a Jump-Box, used to setup and configure the rest of the VMs, and Elk-Server collects/monitors data/logs from 3 WEB servers.
   * Which VMs should be publicly accessible? 3 WEB servers
   * Which VMs should not be publicly accessible? Jump-Box and Elk-Server
3. Explain the Solution Requirements
   * Consider the VMs that should not be publicly accessible from the internet. Which alert(s) should these VMs fire and when? Any SSH/Telnet/HTTP(s) attempt from outside IPs or subnet( that is not allowed )
   * Why should these VMs be associated with these alerts? It is a sign malicious activity
4. Explain the Solution Details
   * Which tool in Project 1 would you use to set such an alert? Filebeat
   * What would the alert rule be? For example, would the alert fire upon a failed SSH attempt or a ping request? It could fire upon failed SSH or ‘untrusted’ network, etc
5. Identify Advantages and Disadvantages
   * Are there any malicious circumstances that the alert(s) discussed above do not address? It does not address ‘legitimate’ activity in case the credentials were compromised

**Question 2: Challenges of Collecting Large Amounts of Log Data**

What are the challenges of collecting huge amounts of log data? How do security analysts deal with them?

1. Restate the Problem Since the log data can hold billions of lines of text that most of the time hold ‘unnecessary’ information, security analysts will have to customize the output, by applying filters to the logs files, so only crucial data is displayed.
2. Provide a Concrete Example Scenario
   * In Project 1, when did you deal with log data? Investigating trojan file download
   * What kind(s) of data did you investigate? Log data for HTTP traffic
   * How much data were you dealing with?
   * What were you looking for?
3. Explain the Solution Requirements
   * What information did you need to find what you were looking for?
   * What does an analyst need to analyze large amounts of log data to find this information? Log files associated with the event
   * In Project 1, what tools did you use to analyze log data? Kibana
4. Explain the Solution Details
   * How did you use these tools to find the log data? E.g., which charts, graphs, etc. were useful for parsing the logs?
5. Identify Advantages and Disadvantages of the Solution
   * What kinds of data did you not inspect during Project 1?
   * Would having access to this additional data have changed your process or conclusions? If so, how?

**Question 3: Escalating Security Events**How do you determine if a security event or alert is important enough for escalation?

1. Restate the Problem Security evets or alerts are set to triggered on certain activity that should draw attention of security analyst
2. Provide a Concrete Example Scenario
   * What kinds of events and alerts did you encounter in Project 1? File transfer, virus, C2 activity
   * Which of these events was most interesting or suspicious? Inside back door attack
   * Why was the event suspicious? What led you to investigate it? Event message notification with identified potential threat
3. Explain the Solution Requirements
   * What do you need to figure out in order to determine if this event is worth escalating? Research prior history events, to see of there are multiple events with similar signature
4. Explain the Solution Details
   * How did you use Kibana to find this information? Kibana IP Lookup > SrcIP. Then navigate in a dashboard where various detailed data is presented.
5. Identify Advantages and Disadvantages of the Solution
   * How confident are you in your conclusion?
   * What additional data would be useful to determine if your conclusions are correct? Outside research

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.