### **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
2. Provide a Concrete Example Scenario  
   * In Project 3, which machines were on the network?

* Kali VM 192.168.1.90 / OS - Linux
* Target1 VM 192.168.1.110 / OS - Linux
* Capstone VM 192.168.1.105 / OS -Linux
* ELK Stack VM 192.168.1.100 / OS - Linux  
  + Which VMs were servers? Which protocol(s) did they serve?
* Target 1 is the Web Server. It’s objective is to store, process and deliver web pages to the users. This intercommunication is done using Hypertext Transfer Protocol (HTTP). On port 80
* When anyone requests for a website by adding the URL or web address on a web browser’s (like Chrome or Firefox) address bar, the browser sends a request to the Internet for viewing the corresponding web page for that address.
* A Domain Name Server (DNS) converts this URL to an IP Address (For example 192.168.1.110), which in turn points to a Web Server.
* In this exercise it is also an SSH server. This allows remote [login](https://en.wikipedia.org/wiki/Login) and [command-line](https://en.wikipedia.org/wiki/Command-line_interface) execution. SSH applications are based on a [client–server](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) architecture, connecting an [SSH client](https://en.wikipedia.org/wiki/SSH_client) instance with an [SSH server](https://en.wikipedia.org/wiki/SSH_server).On port 22.
  + Which VMs were clients? Which servers did they communicate with?  
    - The client VM was the Kali Linux and communicates with Target 1 being the Web server.
  + What network access policies were in place?
* SSH. This allows remote [login](https://en.wikipedia.org/wiki/Login) and [command-line](https://en.wikipedia.org/wiki/Command-line_interface) execution. SSH applications are based on a [client–server](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) architecture, connecting an [SSH client](https://en.wikipedia.org/wiki/SSH_client) instance with an [SSH server](https://en.wikipedia.org/wiki/SSH_server).

SSH aims to make remote connections to computers much more secure. SSH does this by encrypting, or scrambling, the connection between your computer and the remote computer.

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

A potential source of vulnerability would be if anyone from anywhere is able to connect to the SSH server.

* + Which general configurations would you double-check?  
    - I would check the iptables.

iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on the system, iptables looks for a rule in its list to match it. If it doesn’t find one, it resorts to the default action.

iptables almost always comes pre-installed on any Linux distribution. To update/install it, just retrieve the iptables package:

sudo apt-get install iptables

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

Try to SSH from 192.168.1.105 to Target 1 (192.168.1.110).

Explain the Solution Details

* + Which specific configurations within the faulty VM would you inspect to investigate the problem?

The iptables.

* + Which specific settings would you check?

For example, to allow traffic from 192.168.1.105/24 network and otherwise drop the traffic (to port 22).

iptables -A INPUT -p tcp --dport 22 --source 192.168.1.105/24 -j ACCEPT iptables -A INPUT -p tcp --dport 22 -j DROP

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

Try to SSH from 192.168.1.105 to Target 1 (192.168.1.110).

1. Identify Advantages and Disadvantages of the Solution  
   * Does your solution guarantee that the Project 3 network is now "immune" to all unauthorised access?

Yes, because other attempts to SSH into Target 1 except coming from 192.168.1.105 will be dropped automatically by the firewall as configured in the iptables.

* + What monitoring controls might you add to ensure that you identify any suspicious authentication attempts and/or failures?

In the ELK stack you configure a monitor that alerts the security team about the number of attempts to login to Target 1.

Also in the ELK stack you can set monitors on where connections are coming from using geolocation.

#### **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

The problem is the unsecure HTTP protocol.

1. Provide a Concrete Example Scenario  
   * In Project 3, did you have servers running HTTP on port 80? If so, why was it permissible to do so?  
     The server is running HTTP on port 80 because it is a Web Server.
   * In a "real" deployment, which specific machine would you configure differently? How and why?

The Web Server. Specifically to protect the web servers and the data they process.

**Remove unnecessary services**Default operating systems and configurations lack comprehensive security.  
The more services running on the server operating system, the more ports are left open – meaning more doors into the network that a malicious hacker could exploit. This can also boost the server performance.

**Create separate environments for development, testing, and production**Web applications that are in their early development stages will often have security vulnerabilities and can be exploited using freely available online tools.  
Keeping development and testing to servers isolated from the public internet, and not connecting them to important data and databases will ensure that the Web Server is safe from attackers.

**Set permissions and privileges**Setting minimum privileges for users to access web app files and back end databases can be instrumental in preventing loss or manipulation of data.

**Keep patches up to date**Failure to keep software up to date with the latest patches can allow cybercriminals to reverse-engineer pathways into the network.

**Segregate and monitor server logs**Store the server logs in a separate location in the system and monitor and check them frequently. Unusual log file entries reveal information about attempted and successful attacks and should be investigated as and when they arise.

**Install a firewall**Software-based firewalls are easy to set up and manage and will protect the web server from unauthorised communication and intrusions.

**Automate backups**Making regular server backups ensures that if the security defences are compromised, recovery and restoration of data will be done quickly. Automation can improve efficiency.

1. Explain the Solution Requirements  
   * Why is running HTTP on port 80 a problem?

* Port 80 provides an unencrypted connection between the web browser and the web server which then leaves the sensitive data exposed to a potential attacker.  
  + How would you reconfigure a server to serve HTTP traffic safely?
* The server either needs to offer only access to HTTPS by switching HTTP off or make sure that the client will access the HTTPS part by using HSTS\* or by redirecting every HTTP request from the client to HTTPS.

\***HTTP Strict Transport Security** (**HSTS**) is a policy mechanism that helps to protect websites against [man-in-the-middle attacks](https://en.wikipedia.org/wiki/Man-in-the-middle_attack) such as [protocol downgrade attacks](https://en.wikipedia.org/wiki/Protocol_downgrade_attack)[[1]](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security#cite_note-mdn-security-1) and [cookie hijacking](https://en.wikipedia.org/wiki/Session_hijacking). It allows [web servers](https://en.wikipedia.org/wiki/Web_server) to declare that [web browsers](https://en.wikipedia.org/wiki/HTTP_cookie) (or other complying [user agents](https://en.wikipedia.org/wiki/User_agent)) should automatically interact with it using only [HTTPS](https://en.wikipedia.org/wiki/HTTPS) connections, which provide [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS/SSL), unlike the insecure [HTTP](https://en.wikipedia.org/wiki/HTTP) used alone.

* + How does this solution fix the problem?

It will ensure that the interaction is encrypted.

1. Explain the Solution Details  
   * Which tools and technologies would you use to implement this solution in Project 3?

I would shift it to HTTPS.

HTTPS is the protocol where encrypted HTTP data is transferred over a secure connection. By using secure connections such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), the privacy and integrity of data are maintained and authentication of websites is also validated.

* + How would you specifically use these tools to harden your deployment?

1. Purchase an SSL certificate,
2. Install the SSL certificate on the website’s hosting account,
3. Make sure that any website links are changed from http to https so they are not broken after the https switch, and
4. Set up 301 redirects from HTTP to HTTPS so that search engines are notified that the site’s addresses have changed and is automatically redirected to the https address after the switch.

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

When a 301 redirect from HTTP to HTTPS is set up, so anyone who has bookmarked a page on your site is automatically redirected to the https address after you flip the switch.

* + Do you have to do any work to keep this solution running long-term? Or can you simply "set it and forget it?"
* It can be set and forgotten.