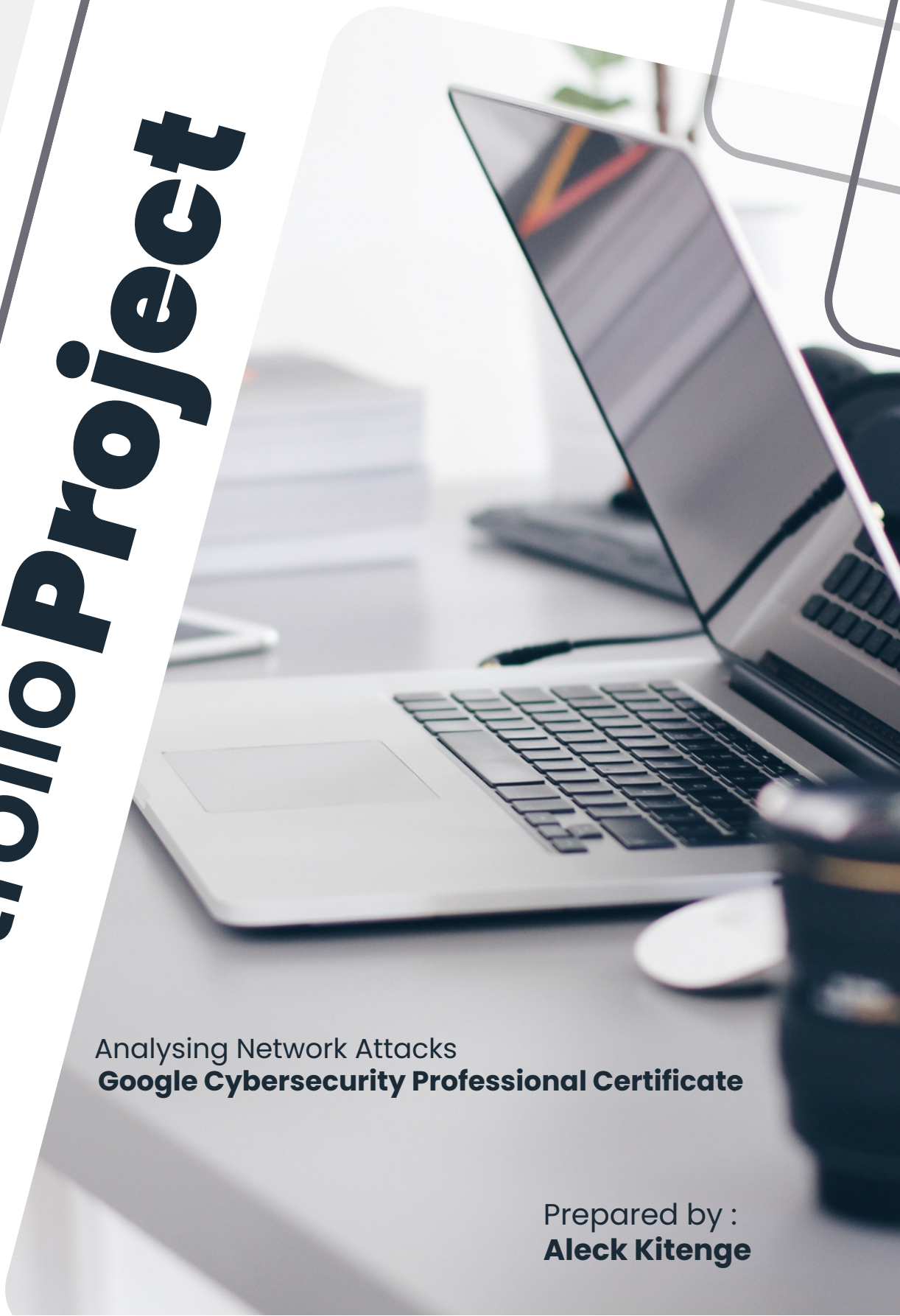
Portfolio Project



Analysing Network Attacks

Google Cybersecurity Professional Certificate

Prepared by :
Aleck Kitenge

1 Activity Overview

In this activity, you will consider a scenario involving a customer of the company that you work for who experiences a security issue when accessing the company's website. You will identify the likely cause of the service interruption. Then, you will explain how the attack occurred and the negative impact it had on the website.

Review the following scenario. Then complete the step-by-step instructions.
You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.
One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.

You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.

You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

2 Activity Questions

Section 1: Identify the type of attack that may have caused this network interruption

One potential explanation for the website's connection timeout error message is:

The logs show that:

This event could be:

Section 2: Explain how the attack is causing the website to malfunction

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:

1.

2.

3.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

Explain what the logs indicate and how that affects the server:

3

Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

A DoS attack could be causing the website's connection timeout error message. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This type of DoS attack is called SYN flooding.

Section 2: Explain how the attack is causing the website malfunction

When you visit a website, your browser and the web server communicate with each other using the TCP protocol. This communication process is called a handshake. It consists of three steps:

1. Your browser sends a SYN packet to the web server, requesting a connection.
2. The web server replies with a SYN-ACK packet to accept the connection request and reserve resources for you.
3. Your browser sends a final ACK packet to acknowledge the permission to connect.

In a SYN flood attack, a malicious actor sends a large number of SYN packets to the web server all at once. As the logs indicate, this overwhelms the server's resources and prevents it from establishing new connections with legitimate visitors. As a result, you may receive a connection timeout error message.