# Cybersecurity Incident Report

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.

| **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:   * An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is generated by a gateway server that was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser. * An [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. RST stands for reset, acknowledge. The visitor will receive a timeout error message in their browser and the connection attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN request.   This event could be: DoS attack . more accurately SYN flood attack. | |
|
|  | |

| **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: 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  Explain what the logs indicate and how that affects the server: The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web server, you can assume this is a direct DoS SYN flood attack. |

* What do you currently understand about network attacks?

—The network attack of Dos has occurred in this scenario.

* Which type of attack would likely result in the symptoms described in the scenario?

—DoS SYN flood attack

* What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)?

—In case of Dos attack only a network or a server get targeted while in DDoS attack multiple devices or servers in different location are targeted with unwanted traffic.

* Why is the website taking a long time to load and reporting a connection timeout error?

—As SYN requests were coming in rapid pace.

* Describe the attack. What are the main symptoms or characteristics of this specific type of attack?

—The DoS SYN attack has occurred.

The symptoms are - the ip address keep flooding with syn packets

* Explain how it affected the organization’s network. How does this specific network attack affect the website and how it functions?

—The organization has to face the service attack as a result the providing service to the customer will be the issue here.

* Describe the potential consequences of this attack and how it negatively affects the organization.
* *Optional:* Suggest potential ways to secure the network so this attack can be prevented in the future.