

Section 4: Explain how the attack is causing the website to malfunction.

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

-Specifically, this attack causes slow web browsing because most of the system is busy validating and analyzing incoming connections. When multiple requests are generated simultaneously, the server tends to generate more effort and prioritize requests.

In detail, these include:

- Slowness
- Malfunction
- Long waiting times to navigate the website

Explain how it affected the organization's network. How does this specific attack affect the network, the website, and its operation?:

-This attack blocked new users from accessing the website because they didn't receive the necessary login information, potentially resulting in lost sales and a damaged reputation.

Describe the potential consequences of this attack and how it negatively impacts the organization:

-This attack, taking this website as an example, which consists of tourist travel sales, its main objective is to sell the product they offer, without having the site operational its functionality drops by 95% which has a critical impact, in addition to users who have already purchased the trip and cannot access the site to verify their ticket or are in the process of their trip and cannot see the steps to follow.

Optional: Suggest possible ways to secure the network to prevent this attack in the future:

-Based on what I've learned from the course so far, in my opinion, one way to avoid massive DDoS attacks would be to configure a more specific firewall, an NGFW, to set a limit on requests from the same IP address to the site so that the server is not exceeded or saturates. This would only work for this specific case.

Christian Danglades