Report Network SYN Attack

Tags:

#Cybersecurity/Lab

Date & Time: 2025-06-24 12:21

Section 1 identify the type of a attack that may have caused this network interruption

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

The normal process should be like this:
- The handshake process takes a few millisecond to complete.
- When the connection between the endpoints is establish, the server will send the `sales.html` web page, and then the browser will rendering it.
- In the process we use HTTP method, like `GET`, and HTTP status code, like `200 OK`.

But instead this machine host `203.0.113.0`, port `5792`, is making a lot of request to the server, and the the server responded using TCP, `[RET, ACK]`, to the port `443`, and then the time is start to increase after each request from the `203.0.113.0`, so this is assign to `SYN Flood attack`, which is a type of `DoS`.

The logs shows that:

There's a lot of request are send, and after each request the time is increase, and that is unnormal, because the packet(Data), are send to unknown IP address.

The event could be:

It's assign for denial of service attack(DoS), and the attacker may turn it to DDoS 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. Normal handshake:
`198.51.100.23` host send `[SYN]` request to the server `192.0.2.1`
Unnormal handshake:
`203.0.113.0` host send `[SYN]` request to the server `192.0.2.1`, but the server will never response.

2. Normal handshake:
The server will response with `[SYN, ACK]` packet
- Unnormal handshake:
The server not able to send the response, because the attacker floods it with `[SYN]` request

3. Normal handshake:
The host will send `[ACK]` packet to establish the connection.
- Unnormal handshake:
The server not able to send the response, because the attacker floods it with `[SYN]` request

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

The SYN packets, is operate at the Transport layer, when the three way handshake are not complete, the time response from the server will increase, which will lead to `timeout error message` from the server side, using status code like 500-599. At the end the server will never make a full connection with the machines, which will lead to `Service interruption` .

Explain what the logs indicates and how that affects the server

In the network traffic that I captured, the number of request is increase, but the time also as wall, and after that, the connection is not complete establish between the endpoints, and that's assign for SYN floods which is type of DoS attack.

Notes:

We need to use strong VPN's server, to prevent stilling IP address, to prevent the attack.
Also we need to configure our firewalls to block this machine `203.0.113.0`, and also create new internal network, or simple solution, we should change our IP's to this server `192.0.2.1`.

Reference:

0857-15-4-25 SYN Flood attack