Cybersecurity Incident Report

Scenario

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 a DoS attack. This can be deduced as the logs show that the web server stops responding after receiving a large number of SYN packet requests, all sent from a single IP address. This event could be the result of a DoS attack known as SYN flooding.

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. This handshake consist of:

1. The [SYN] packet: Stands for "synchronize". Initial request from a client to connect to a web server.
2. The [SYN, ACK] packet: Stands for "synchronize acknowledge". Web's server response to the SYN packet request, agreeing to the connection.
3. The [ACK] packet: Stand for "acknowledge". Final step to establish a successful connection. Client's machine acknowledging the permission to connect.

A malicious actor can overload the server with SYN packet requests for the first part of the handshake. This causes the server to be unable to respond to other requests, as the number of SYN requests far exceeds the server's resources to handle them. As a result, the traffic is slowed down.

The web server is overloaded by SYN packets and is incapable of responding to other requests. Due to this, two types of errors occur: time-out error messages (the server takes too long to respond) and an [RST, ACK] packet (the visitor doesn't receive the SYN, ACK packet).

Section 3: Logs examples

Color as text	No.	Time (in seconds & milliseconds)	Source	Destination	Protocol	Info
red	52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	54	3.49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...

Start of the attack by the IP address 203.0.113.0. The handshake is initially correct.

Color as text	No.	Time (in seconds & milliseconds)	Source	Destination	Protocol	Info
red	57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win-5792 Len=120...
red	59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
green	60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red	61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
green	62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
green	63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win-5792 Len=120...
red	64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
green	65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win-5792 Len=120...
red	68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win-5792 Len=120...

Start of the abnormal behavior. The attacker keeps sending more SYN requests, but the server is still able to respond normally to visitor traffic.

Color as text	No.	Time (in seconds & milliseconds)	Source	Destination	Protocol	Info
yellow	73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win-5792 Len=120...
yellow	77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)

In the next rows, the server begins to struggle. These are examples of failed communications between legitimate visitors and the web server, showing the two types of error messages.

Color as text	No.	Time (in seconds & milliseconds)	Source	Destination	Protocol	Info
red	214	51.176992	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	214	51.500005	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	214	51.823018	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Finally, the rest of the log shows that the web server stops responding to legitimate traffic. From log item number 125 on, the server stops responding. The only communication is the SYN packets of the attacker. As there is only one IP address, it can be assumed that it is a DoS Syn flood attack.