# Activity: Analyze network attacks

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The described scenario shows that it was a Denial of service (DOS) attack from a single source IP address. It was identified that the attacker is flooding the server with TCP/IP SYN packets to cause the server to crash and not able respond to the legitimate traffic. The network logs from wireshark shows the IP address, time of attack, port numbers trying to access, and other information regarding the attack. The website's connection timeout error message was sent by the network gateway, gateway sends this type of messages if the server was not able to respond in intime to the client’s request.So the request has to be send again or the request for accessing the website is denied.  By the observed scenario, the attacker successfully launched the TCP/IP SYN Flood DOS attack and made the server to not respond for the legitimate clients and will make the server to crash down. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Here’s the explanation that how the attack took place:  When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The three steps of the handshake are:  1. The [SYN] packet is the initial client request, trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”  2. The [SYN, ACK] packet is the web server’s response to the client’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.”  3. The [ACK] packet is the client’s message acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”  By following the above three-way-handshake method, the connection is established between the client and server. But the intruders/attacker can take advantage of this handshake process, They try to send only SYN packets to the sever and not sending their acknowledge message in the third step, so the server has already acknowledged the attackers request by reserving system resources for the final step and will be waiting to get the acknowledge from the client.  In this way the attacker sends large number of SYN packet requests in very short time, resulting the server overwhelmed with traffic.  We have identified the cause by examining network logs using wireshark (Network traffic analyzer/packet sniffer), helped us to identify why the issue is raised and by whom.  Action to be performed immediately: Block the attacker’s IP address using firewall filteration or setting up firewall rules, and also should block the spoofed IP addresses which look like legitimate IP addresses. |

# Activity Exemplar: Analyze network attacks

|  |
| --- |
| **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. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of DoS attack called SYN flooding. |

|  |
| --- |
| **Section 2: Explain how the attack is causing the website malfunction** |
| When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps:   1. A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect.   In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.  The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message. |