# Activity Exemplar: Analyze network attacks

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| We discovered a significant issue affecting our website. The problem is a type of attack called a SYN flood attack. This occurs when an attacker overwhelms our server with connection requests, making it difficult for real users to access our site.  Analysis Details:  Identifying the Attack:  We noticed an unusual number of connection requests from an unfamiliar source (203.0.113.0).  The attack is characterized by an excessive rate of connection requests.  Impact on Organization:  Our website is struggling to handle the high number of connection requests.  Legitimate users are experiencing timeouts and can't access our site.  Consequences of the Attack:  The website shows errors (504 Gateway Time-out) due to the server struggling to respond.  Legitimate connections are being dropped, causing users to receive errors.  Type of Attack:  This is a direct attack on our service, known as a SYN flood attack.  SYN flood attacks overload the server by exploiting its connection setup process. |

|  |
| --- |
| **Section 2: Explain how the attack is causing the website malfunction** |
| Time Incident Occurred: Afternoon, triggering an automated alert.  How IT Became Aware:  The monitoring system sent an alert about the web server issue.  Actions Taken by IT:  The server was temporarily taken offline for recovery.  The firewall was set up to block the attacker's IP address (203.0.113.0).  Key Findings of IT Investigation:  Many connection requests from IP address 203.0.113.0.  Unusual connection request rate causing server overload.  Legitimate interactions highlighted in green, failed ones in yellow.  Likely Cause of Incident:  An attack called SYN flood overwhelmed our server by flooding it with connection requests.  Next Steps:  Keep an eye on network traffic for signs of more attacks.  Strengthen security measures to detect and stop SYN flood attacks.  Investigate any vulnerabilities that might have been exploited.  Suspected Root Cause:  Lack of effective measures to handle a large number of incoming connection requests, allowing the attacker to overwhelm our server.  Recommendations for Prevention:  Implement tools to identify and block malicious traffic.  Adjust network settings to limit the number of incoming connection requests from one source.  Consider using advanced protection against these types of attacks. |