Example of a

Cybersecurity Incident Report

This report **example** is for a different security event than the scenario presented in the activity. This example should only be used to familiarize yourself with the expected report format.

| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** | |
| --- | --- |
| The network protocol analyzer in this case tcpdump log, indicates that port 53 is unreachable when attempting to access. The log shows an abnormal number of TCP SYN requests originating from anonymous IP (203.0.113.2). This event could be indicated as a SYN flood DoS (Denial of Service) attack to the company’s web server. The objective of this attack is to flood the target server with SYN packets/requests, and then rendering it to make the server unable to make connection requests. | |
|

| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| --- |
| In the log data show us that the yummyrecipeforme.com was unreachable and the one that took damage was the server (203.0.113.2) with DNS protocol traffic (Port 53) start from 1:24 PM, it will sent error message “udp port 53 unreachable”. In general of a normal web server interaction there are 3 steps to establish hans-shake between client and server. This hand-shake are:   1. The client sends a SYN or synchronize request to the server. 2. The server will respond with a SYN/ACK packet to acknowledge the receipt of the device's request and establish the connection. 3. Once the server receives the final ACK packet from the device, a TCP connection is established   Indication of SYN flood attack accident to the web server:   1. Malicious actors can take advantage of the protocol by flooding a server with SYN packet requests for the first part of the handshake and if the number of SYN requests is larger than the number of available ports on the server, then the server will be overwhelmed and become unable to function. 2. As observed in the tcpdump log, server (203.0.113.2) was being sent continuous SYN requests to flood the server. This behavior causes the server to become unreachable due to the SYN requests being larger than the number of available ports on the server, then the server will be overwhelmed and become unable to function.   The consequences of this attacks:   * The website will likely experience slow loading time, and ultimately leading to connection timeout for legitimate users. * Common users cannot access the request to the website due to the server being overloaded. * The company may face a significant revenue loss due to the attack that causes the customer can’t access the website. * The company’s reputation will be damaged, as users will give negative comments about * the website performance. |