Cybersecurity Incident Report

|  |
| --- |
| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** |
| The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the website: https://www.yummyrecipesforme.com/ . Port 53 is primarily used for DNS Resolution. When we want to connect to the internet, we type the URL into the web browser, that URL is then translated into an IP address by the DNS and the result is then returned to our browser in the form of a successful connection to the webpage. We further see that this is a UDP connection type, this indicates the type of protocol the connection adheres to. In this case, UDP is supposed to be time-sensitive and highly responsive and is highly utilized for large file transfers and DNS resolution. Further to this there is a ICMP confirmation indicating the issue with the IP address of the website and not the main users. This may indicate a network outage by way of a server being down. |
|

|  |
| --- |
| **Part 2: Explain your analysis of the data and provide one solution to implement** |
| The incident occurred today at 13:23 and when reported we ran network diagnostic tools including a packet sniffer and log analyzer. In total 3 requests were sent from my PC to the website URL and accompanying IP address of that website. at roughly 2 minutes apart. All 3 came back with the same error message on the logs that would have been present with our users. At this point, to avoid a full system outage and to confirm business continuity I would recommend a reset on port 53. This should allow us to address the issue without taking the whole server offline. Additionally, it would be beneficial for the IT team to check the Firewall Settings to rule out a Misconfiguration. It is also Important to note that the DNS server may be down due to a Denial-of-Service Attack on the network. |