# **Cybersecurity Incident Report:**

# **Network Traffic Analysis**

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that: UDP port 53 is unreachable to users trying to reach yummyrecipiesforme.com  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server  The port noted in the error message is used for: the port 53 is a port for DNS service and the word unreachable indicates the UDP message requesting the domain did not go through to the DNS server because no service was listening on the receiving DNS port.  The most likely issue is: the most likely issue could be that the DNS server at 203.0.113.2 is either down due to an attack by a malicious actor. |
|  |

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: the incident occurred at 12:24:32.192571 which translate to 1:24pm and 31.192571 seconds  Explain how the IT team became aware of the incident: the IT team could have been aware of the incident due to user complaints or monitoring alerts from network protocol analyser tools, tcpdump that confirms that the DNS request was unreachable for port 53.  Explain the actions taken by the IT department to investigate the incident:  The IT departments inspect network traffic and network data to determine the cause of the network related issues during the cybersecurity incident. Some key findings from the investigation would be to find out what affected UDP port 53 at IP address 203.0.113.2 and why it was unreachable. The IT department would also need to check firewall rules or security policy that may have prevented DNS servers from receiving the DNS request.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident:  It may have been possible that the incident was caused by the DNS server being misconfigured causing it to fail to listen on UDP port 53 for incoming DNS requests or that the DNS server was experiencing an outage due to an DDOS attack preventing it from responding to DNS requests however without further information it is difficult to pinpoint the exact cause. |