# 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:  Several clients were unable to access the client company website “yummyrecipesforme.com”, and shows an error “destination port unreachable”  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  “udp port 53 unreachable length 254”  “udp port 53 unreachable length 320”  “udp port 53 unreachable length 150”  The port noted in the error message is used for:  The 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 most likely issue is:  There could be a lot of traffic already going to udp port 53, hence the request from legitimate users is not reaching that port. This could be an indication of a DoS attack. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred:  1:24pm, 32.192571 seconds  Explain how the IT team became aware of the incident:  Several customers of the client reported that they were not able to access the client company website “yummyrecipesforme.com” and saw the error “destination port unreachable” after waiting for the page to reload.  Explain the actions taken by the IT department to investigate the incident:  Currently we are inspecting network data and traffic to determine what is causing network related issues. In the meantime, this event is being handled by security engineers and other analysts have reported the issue to the direct supervisor.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   1. The destination IP address is 192.51.100.15 2. The query identification number is 35084+ and the ‘+’ sign after it indicates that there are flags associated with the udp message 3. The “A?” indicates a flag associated with the DNS request for an A record maps to the domain of the IP address   Note a likely cause of the incident:   1. This may be a security incident and can be categorized under the DoS attack 2. But this could also be an overload due to the suddenly increasing number of people trying to access the website at the same time, due to whose traffic, port 53 seems unreachable |