Cybersecurity Incident Report

# Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The network traffic logs from the tcpdump analysis reveal that DNS requests sent via the UDP protocol to port 53 of the DNS server (IP: 203.0.113.2) result in ICMP error messages. These error messages specifically state: "udp port 53 unreachable."  
  
This indicates that the DNS server is not listening on port 53, which is the standard port used for DNS queries. As a result, the client machine is unable to resolve the domain name www.yummyrecipesforme.com into an IP address, leading to the browser displaying a “destination port unreachable” error when trying to load the website.  
  
Key details from the log:  
- Protocols involved: UDP for DNS request, ICMP for error response.  
- DNS requests sent to: 203.0.113.2:53  
- ICMP response from: 203.0.113.2 to 192.51.100.15  
- Error: "udp port 53 unreachable"  
- The same error is repeated multiple times, indicating persistent failure.

# Part 2: Explain your analysis of the data and provide at least one cause of the incident

Time incident occurred:  
Around 13:24:32, as per the timestamp in the logs.  
  
How the IT team became aware:  
Multiple customers reported that they were unable to access the company’s website. The browser displayed a message saying “destination port unreachable”.  
  
Actions taken:  
The IT department attempted to reproduce the issue and launched a tcpdump analysis to capture network traffic during a page load attempt. DNS queries were analyzed and error responses were observed.  
  
Key findings:  
- DNS server (203.0.113.2) is unresponsive on UDP port 53.  
- ICMP errors indicate the port is unreachable.  
- The DNS query for www.yummyrecipesforme.com is not being resolved, preventing HTTPS traffic from being initiated.  
  
Likely cause of the incident:  
The DNS service on the server 203.0.113.2 is either down or misconfigured. Port 53 may be blocked by a firewall or the DNS daemon might not be running. Consequently, domain resolution fails, and access to the website is not possible.