Cybersecurity Incident Report

Network Traffic Analysis

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

The tcpdump log shows that the computer sent DNS queries using the UDP protocol to the DNS server at 203.0.113.2 on port 53. However, instead of receiving a valid DNS response, the server replied with ICMP error messages stating "udp port 53 unreachable." This indicates that the DNS server was not reachable on port 53 at the time of the request.  
  
The primary protocols involved in the log are:  
- UDP: Used to send DNS queries.  
- ICMP: Used to report back errors when the DNS server failed to process the UDP requests.  
  
Repeated ICMP responses indicate a systemic failure to reach the DNS service on its expected port. This prevented successful DNS resolution for the domain www.yummyrecipesforme.com, blocking access to the website.

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

The issue was first reported at approximately 1:24 PM, as confirmed by timestamps in the tcpdump log.  
  
Users reported being unable to access www.yummyrecipesforme.com and instead received a "destination port unreachable" error. This symptom appeared consistently, suggesting a DNS resolution failure.  
  
The current status is that DNS queries to the server are not reaching a responsive service on port 53, causing ICMP errors to be generated.  
  
So far, it has been discovered that:  
- DNS queries were made using UDP.  
- The DNS server at 203.0.113.2 replied with ICMP errors.  
- Port 53 was noted as unreachable, halting the DNS resolution process.  
  
Next troubleshooting steps:  
- Verify the DNS server is online.  
- Ensure port 53 is open and the DNS service is active.  
- Check firewall or ACL settings that might block UDP port 53.  
- Implement secondary DNS redundancy for critical systems.  
  
The suspected root cause is that the DNS server was either offline or its port 53 was blocked/misconfigured, leading to a failure in resolving the domain name and consequently, access failure for the website.