Cybersecurity Incident Report:
Network Traffic Analysis

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

The DNS and ICMP traffic log indicates that there is an issue with the DNS query and response process for the domain "yummyrecipesforme.com.".

This may indicate a problem, such as:

- The DNS server is not reachable or is offline.
- The DNS server may be experiencing high traffic or congestion.
- The DNS server may not have a record for the requested domain ("yummyrecipesforme.com.").
- There could be network connectivity issues between the DNS client (192.51.100.15) and the DNS server (203.0.113.2).

The negative possibility is:

- Are caused by DoS attacks.
    - DNS Amplification Attack.
    - DNS Flooding Attack
    - ICMP Flood Attack

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred earlier when the human resources (HR) team reported that they could not reach the background check web portal.

The network security team responded and began running tests with the network protocol analyzer tool tcpdump.

It is important to ensure that the server is not being compromised by threats, Therefore threats must be investigated first.

If the issue persists, you may need to investigate whether the domain name is correctly entered and must be there are no network connectivity issues between the client and the server, including investigate the DNS server's logs and configuration to identify the root cause of the error.

Recommended Actions:

To resolve the issue, the following steps can be taken:

- Solutions for DoS:
    a. Traffic Filtering: Implementing traffic filtering at the network perimeter should be the first priority. Use firewalls, routers, and intrusion prevention systems (IPS) to block known malicious traffic and protect critical assets from direct attack.
    b. Rate Limiting and Connection Limiting: Set up rate-limiting and connection-limiting rules for certain types of traffic to prevent abuse of resources and limit the impact of potential DoS attacks.
    c. Cloud-based Protection: Consider utilizing cloud-based DDoS protection services. Cloud providers can handle large-scale DDoS attacks before they reach the organization's network, providing an additional layer of defense.
    d. Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS solutions that can detect and block DoS attack attempts in real-time. Early detection helps in initiating appropriate response measures promptly.
    e. Load Balancing: Implement load balancing to distribute incoming traffic across multiple servers or resources. This helps evenly distribute the load and improves the ability to handle traffic spikes.

- Check the DNS server's status: Ensure that the DNS server at IP address 203.0.113.2 is operational and capable of responding to DNS queries.
- Verify DNS configuration: Confirm that the DNS server is configured to handle DNS requests for the domain "yummyrecipesforme.com" and has the necessary DNS records for the domain.
- Test network connectivity: Investigate and resolve any network connectivity issues between the DNS client (192.51.100.15) and the DNS server (203.0.113.2).
- Review firewall settings: Check if any firewalls or security measures are blocking DNS traffic to port 53 on the DNS server.
- Examine DNS server logs: Review the DNS server's logs to identify any errors or issues related to the domain "yummyrecipesforme.com."