DNS Incident Analysis Report

Context

This report is based on a mock scenario provided by the Google Cybersecurity course on Coursera. The goal of this exercise was to analyze network traffic logs, identify the root cause of a connectivity issue, and suggest possible mitigation steps. The scenario simulated an issue where users were unable to access a specific website due to DNS resolution failures.

Problem Summary

Users and the IT team attempted to access the website **www.yummyrecipesforme.com**, but received a "destination port unreachable" message. Network protocol analyzer logs indicated that outgoing DNS queries were being sent over UDP port 53, but no responses were received. Instead, an ICMP error message **"udp port 53 unreachable"** was logged.

Port 53 is essential for DNS resolution, as it is responsible for converting domain names into IP addresses. If DNS queries fail, users cannot resolve domain names, leading to connectivity issues. The issue could be due to a misconfigured or downed DNS server, or a firewall blocking DNS traffic on port 53.

Additionally, the logs included flags such as **+** and **A?**, which provide more details on how the DNS request was processed. The **+** flag tells the destination device that even if it doesn't have an immediate answer, it should still try to give a response. The **A?** flag indicates that the request is asking for an **IPv4 address resolution** of the domain name. Since these flags appear in the logs but no response was received, it further confirms that the DNS query never made it to a valid DNS resolver.

Incident Analysis

The issue was reported around **1:20 p.m.**, when users began experiencing difficulties accessing the website. The IT security team investigated the issue using the **tcpdump** network protocol analyzer. The logs confirmed that the DNS request was sent, but the destination port (53) was never reached. As a result, the only response received was an **ICMP error message** indicating that port 53 was unreachable. This suggests a failure in data transmission.

In summary, the DNS query never reached a valid DNS listener. Further investigation is required, but the most likely causes are:

- A firewall blocking outgoing or incoming traffic on port 53.
- A failure or misconfiguration on the DNS service provider's end.

Mitigation Steps

To further diagnose and potentially resolve the issue, the following actions should be taken:

1. **Check firewall settings** to confirm whether port 53 is being blocked.
2. **Test with an alternative DNS provider** (e.g., Google DNS: 8.8.8.8) to determine if the issue is specific to the current DNS service.
3. **Contact the DNS service provider** to verify if their servers are operational and request assistance in resolving any misconfiguration.
4. **Restart or reconfigure the DNS server** (if managed internally) to ensure it is properly handling queries.

Conclusion

This scenario provided a valuable opportunity to analyze network logs, diagnose a DNS-related issue, and develop a structured response plan. Understanding how to investigate and mitigate such incidents is essential for cybersecurity professionals, particularly those working in **Security Operations Centers (SOC)** or **network security roles**. If this were a real-world event, the next steps would involve continuous monitoring and validation of implemented fixes to ensure stable network connectivity.