**Google CyberSecurity Professional Certificate Course**

Cybersecurity Incident report : Network Traffic Analysis

**\*This report is an example which was given in the activity on event based scenario**

Part 1 – Summary of the problem found in the DNS and ICMP Log

* The UDP Protocol reveals that when the initial outgoing request comes from my computer to the DNS server requesting the IP address of the website, that request is sent in a UDP packet
* When the data packet is sent on the network issues occur and the ICMP protocol comes into action and return an error of port 53, which states the UDP packet was undelivered to the port 53 of the DNS server.
* The port noted in the error message is used for analyzing more details about the DNS server
* Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval

Part 2 – Cause of the Incident

* The time incident occured is around 1:24pm 32.197 seconds
* Customer’s notified the organization that they are receiving a error message “destination port unreachable” when they try to visit website “yummyrecepiesforme.com”, now the cybersecurity team will analyze the issue for the client organization they are working so the customers can access the website properly.
* The cybersecurity team did packet sniffing analyzing using tcpdump and in the resulting log file we found out that port 53 is unreachable, now the next step is to check wether the DNS server is down or port 53 is blocked by firewall.
* The DNS server is down for likely reasons like a Denail of service attack or other misconfigurations.