Cybersecurity Incident Report
By: Shihab Islam

Upon investigation of the Yummy Recipe company, the  Logs report that the DNS server is currently down and is unable to properly receive data packets using the UDP protocol. Upon analysis, doing a TCPdump by sending ICMP packets to the port  only reports back “UDP port 53 is unreachable”. Which is unusual since port 53 is normally able to receive all traffic regards to DNS servers. The Log states that the attack occurred today at 1:23 pm. Our IT team recognized there was an issue when we were hacking our own servers at the time to test its defenses. After realizing such a huge weakness we the defense team are reporting to our supervisors and then the security engineers to get the vulnerability patched. After showing them our logs by using a SIEM tool to packet sniff the error messages, we troubleshooted the Dns server to check its functionality. If the server is not damaged then we go on to check the firewall and edit it to not block port 53. One possible reason why so much traffic exists is that an internal threat purposely DOS attacked the network. Which caused the  DNS server to shut down and crash.