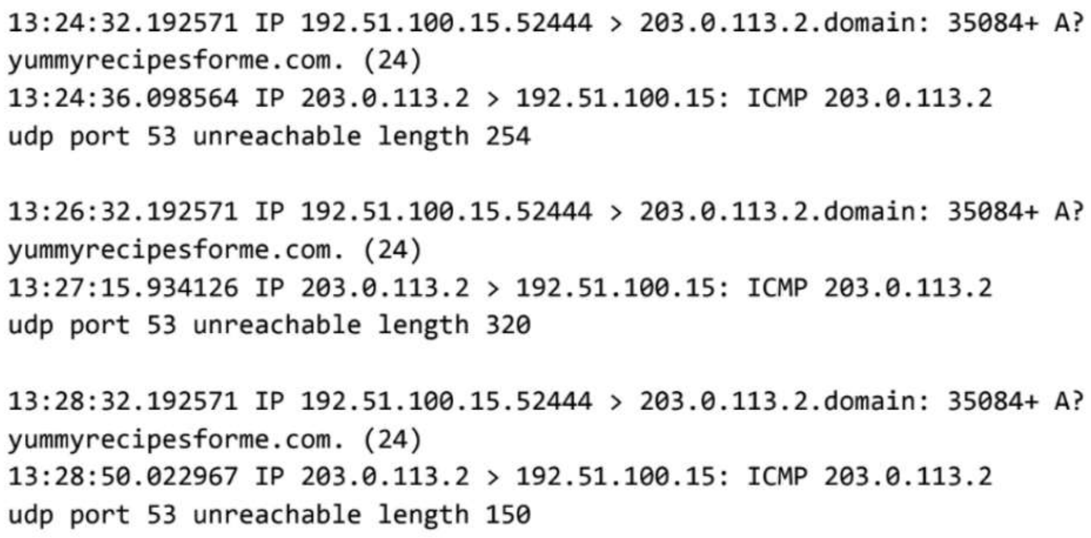
Cybersecurity Incident Report: Network Traffic Analysis

This report of mine covers an example scenario that details the problem experienced by a company's employees and the steps taken by the cyber security team employees, of which I am a member (Burak Kılıç). Below, the reports regarding the problem and the subsequent situation are divided into two sections.



```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Part 1: Provide a summary of the problem found in the tcpdump log

The problem first started when company employees received the error "UDP port 53 unreachable" when connecting to their company website www.example.com. The issue was first reported at 10:54 a.m. today. Port 53 is normally used to connect to the DNS server using the UDP protocol. In the record taken from the above script, the UDP message sent from the internet browser to the DNS appears in the first two lines. Just below that, in the third and fourth lines, is the ICMP error response sent from the DNS server to the internet browser. Since Port 53 is related to the DNS server, we can know that the problem here is related to the DNS server.

In the script, the number used to identify error codes is 35084 and this number is also marked with “A?” command. Both of these prove to be related to the DNS protocol.

Part 2: Analyzing the data and providing potential causes to the incident

In the script, date and time information can be seen on the first line. In the numbers that appear as 13:24:32.192571, 13:24 indicates the time and 32.192571 indicates the second. The problem was reported when some employees noticed the error "Destination host unreachable" while trying to access the www.example.com website. We, as the security analysts, have already reported the problem and reported it to our managers, and then the security engineers started to deal with the problem.

While investigating the problem, using "tcpdump" to find out why the packets were not arriving, it was discovered that DNS port 53 was unreachable in the log. In this case, we rolled up our sleeves to find out whether the DNS server was down or the firewall was blocking the traffic. There are cases where blocking a port on the firewall is used to prevent an attack from that port. Such an obstruction may also be possible. At the same time, the DNS server may have crashed due to a DOS (Denial of Service) attack.

Prepared by: Burak KILIÇ