INCIDENT REPORT | 001 | ACCESS ERROR

DETAILS

DNS Server IP: 203.0.11.2
Port affected: UDP 53
Response from the server: ICMP timed out/unreachable

Logs
- An incident occurred at 1:24PM (32 sec.).
- A second incident occurred at 1:26PM (32 sec.) and 1:27PM (15 sec.).
- A third incident occurred at 1:28PM (32 sec.)/(50 sec.).

Some users tried to connect to yummyrecipesforme.com (203.0.11.2) and reported it to an analyst. I confirmed that error and began troubleshooting the issue.

A team member used tcpdump in order to begin investigating the route of a request to the domain, 203.0.11.2.

A team member observed the error in real-time, noting a connection issue on the DNS server's side.

```
o-taylor-bryant@taylor-terminal:~$ dig yummyrecipesforme.com
;; communications error to 203.0.113.2#53: timed out
;; communications error to 203.0.113.2#53: timed out
;; communications error to 203.0.113.2#53: timed out

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> yummyrecipesforme.com
;; global options: +cmd
;; no servers could be reached
```

A request from my machine (192.51.100.15) was sent to the DNS server (203.0.113.2) on port 53 to access the site yummyrecipesforme.com.

This is based on the results of the network analysis, which presented that the ICMP echo replied and returned the error message:

```
"udp port 53 unreachable"
```

This error message is used for reporting that a domain is not able to connect via the DNS.

POTENTIAL PROBLEMS

The DNS server, 203.0.113.2, is having a connection error and needs to be reestablished with the DNS service provider.