Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that:

All outbound DNS (Domain Name System) queries were successfully sent from 192.51.100.15 to 203.0.113.2 on UDP (User Datagram Protocol) port 53.

Zero DNS replies were received; instead, each query triggered an ICMP (Internet Control Message Protocol) error.

The browser was therefore unable to resolve the IP address for www.yummyrecipesforme.com, preventing HTTPS (Hypertext Transfer Protocol Secure) communication from beginning.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:

ICMP Type 3 Code 3 – “Destination Unreachable / Port Unreachable.”

Each ICMP packet included the original DNS query, confirming that DNS was the traffic being rejected.

Packet lengths (254, 320, and 150 bytes) varied, but all contained the original request’s headers and part of the payload.

The port noted in the error message is used for:

Port 53/UDP – port for DNS queries and responses.

The most likely issue is:

DNS service outage or filtering on server 203.0.113.2 (e.g., daemon crash, misconfigured firewall or ACL).

Since DNS resolution fails, users receive a “destination port unreachable” error after the browser fails to reach the web server via HTTPS.

Part 2: Analysis of the data

Time incident occurred:

The first failed DNS query was captured at 13:24:32 on 22-Apr-2025, aligning with the time users reported th

Explain how the IT team became aware of the incident:

Multiple users contacted support after experiencing the “destination port unreachable” error.
The cybersecurity team attempted to access the website and confirmed the issue internally.

Explain the actions taken by the IT department to investigate the incident:

- Launched tcpdump with a filter for udp port 53 or icmp.
- Re-attempted to access the website to generate fresh traffic.
- Analyzed packet timestamps, source/destination addresses, and ICMP codes.
- Verified that no HTTPS connection was attempted—indicating the issue occurred during DNS resolution.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS se

- All DNS queries used Transaction ID 35084+ and source port 52444.
- All replies were ICMP Type 3 Code 3 (Port Unreachable).
- The target DNS server was 203.0.113.2, which responded with rejections.
- The failure occurred at the DNS resolution step—before the HTTPS request was initiated.

Note a likely cause of the incident:

The DNS service on 203.0.113.2 was either down, firewalled, or misconfigured.

Possible causes include a crashed DNS daemon, a firewall rule change, or a misconfigured intrusion prevent

Suggestions:

- Verify the DNS server is reachable (e.g., via ping or ssh).
- Check the status of the DNS service and restart if needed.
- Review recent firewall or security rule changes.
- Update clients to use a fallback DNS resolver until the issue is resolved.
- Implement monitoring and logging to detect future service disruptions.

Apendix A: Packets breakdown

1. DNS Query (UDP Packet)

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

Timestamp: 13:24:32.192571
Protocol: IP
Source IP: 192.51.100.15
Source Port: 52444
Destination IP: 203.0.113.2
Destination Port: .domain = UDP port 53 (DNS)
Transaction ID: 35084+ — Query ID 35084, with recursion desired (indicated by +)
Query Type: A? — Requesting A record (IPv4 address)
Domain Name: yummyrecipesforme.com
Size of DNS query: (24) bytes

2. ICMP Error Response (Port Unreachable)

13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

Timestamp: 13:24:36.098564
Protocol: IP
Source IP: 203.0.113.2
Destination IP: 192.51.100.15
Message Type: ICMP
ICMP Type/Code: Destination Unreachable – Port Unreachable
Error Detail: Indicates port 53 (DNS) on 203.0.113.2 is unreachable
Encapsulated Info: Includes a portion of the original DNS query that caused the error
Packet Length: 254 bytes (includes ICMP header + encapsulated data)

3. DNS Query (Repeated)

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

Timestamp: 13:26:32.192571
Protocol: IP
Source IP: 192.51.100.15
Source Port: 52444 (same source port used again)
Destination IP: 203.0.113.2
Destination Port: .domain = UDP port 53 (DNS)
Transaction ID: 35084+ — Reusing the same query ID
Query Type: A? — IPv4 address request
Domain Name: yummyrecipesforme.com
Size of DNS query: (24) bytes

4. ICMP Error Response (Repeated)

13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

Timestamp: 13:27:15.934126
Protocol: IP
Source IP: 203.0.113.2
Destination IP: 192.51.100.15
Message Type: ICMP
ICMP Type/Code: Destination Unreachable – Port Unreachable
Error Detail: DNS server still unreachable on port 53
Encapsulated Info: Original DNS query again included
Packet Length: 320 bytes

5. DNS Query (Another Retry)

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

Timestamp: 13:28:32.192571
Protocol: IP
Source IP: 192.51.100.15
Source Port: 52444 (again reused)
Destination IP: 203.0.113.2
Destination Port: .domain = UDP port 53
Transaction ID: 35084+ — Same ID and query structure
Query Type: A?
Domain Name: yummyrecipesforme.com
Size of DNS query: (24) bytes

6. ICMP Error Response (Final)

13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150

Timestamp: 13:28:50.022967
Protocol: IP
Source IP: 203.0.113.2
Destination IP: 192.51.100.15
Message Type: ICMP
ICMP Type/Code: Destination Unreachable – Port Unreachable
Error Detail: Server still not answering on port 53
Encapsulated Info: Contains portion of original request
Packet Length: 150 bytes

Repeated Attempts
Same pattern occurs at:
13:26:32 / 13:27:15
13:28:32 / 13:28:50

This indicates that the client (192.51.100.15) keeps retrying DNS resolution for yummyrecipesforme.com, but the DNS server (203.0.113.2) is either:

Down
Blocked
Not running a DNS service on port 53