Cybersecurity Incident Report: Network Traffic Analysis

Scenario

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”
log from tcpdump packet data

In the tcpdump log, you find the following information:

1. The first two lines of the log file show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.
2. The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server.
3. In front of each request and response, you find timestamps that indicate when the incident happened. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds.
4. After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this information is displayed as: 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address, which in this example is your computer’s IP address. The IP address to the right of the greater than (>) symbol is the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computers IP address 192.51.100.15.
5. After the source and destination IP addresses, there can be a number of additional details like the protocol, port number of the source, and flags. In the first line of the error log, the query identification

number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message.

6. The error message, "udp port 53 unreachable" is mentioned in the last line. Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.
7. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.

Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.

As an analyst, you can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents. Later in this course, you will demonstrate how to manage and resolve incidents. For now, you only need to analyze the situation.

This event, in the meantime, is being handled by security engineers after you and other analysts have reported the issue to your direct supervisor.

Cybersecurity Incident Report

Incident Summary

After analyzing the tcpdump log, it was observed that a DNS request was made using the UDP protocol from the client system (192.51.100.15) to the DNS server (203.0.113.2) on port 53. The domain being queried was yummyrecipesforme.com. The protocols involved were:

- UDP – for sending the DNS request
- ICMP – for returning error messages from the DNS server

The logs show that the DNS request was not successfully delivered, and the ICMP response returned the message: "udp port 53 unreachable". This pattern repeated multiple times, confirming that the DNS server was not accepting traffic on its DNS port (53). This error suggests that the DNS service is either down, misconfigured, or blocked by a firewall.
Technical Analysis

- Time of First Occurrence: 13:24:32.192571
- Protocols Observed: UDP, ICMP
- Services Involved: DNS

- Client IP: 192.51.100.15
- DNS Server IP: 203.0.113.2
- Port Affected: 53 (UDP)
- Error Message: "udp port 53 unreachable"

Issue Explanation and Status

The issue was first detected when DNS resolution failed for the website yummyrecipesforme.com. The user reported inability to access the site, and tcpdump logs showed the repeated ICMP errors responding to the failed DNS queries. The ICMP messages indicate that the DNS server could not receive or process requests on port 53.
Information Discovered So Far:

- No DNS responses received from the server.
- All queries resulted in ICMP “unreachable” errors.
- The server never acknowledged the incoming UDP DNS requests.

Current Status of the Issue

The DNS resolution is still failing, and the server is not responding on port 53. The issue has been reported to the security engineering team for further analysis and server-side investigation.
Next Steps for Troubleshooting

- Check if the DNS service is running on the server.
- Verify if port 53 is open and not blocked by a firewall.
- Confirm the server is online and reachable from the client network.
- Restart DNS service if necessary.
- Monitor logs for any signs of deliberate blocking or misconfiguration.

Suspected Root Cause

The root cause is likely a service outage or firewall block on the DNS server, preventing it from receiving and responding to DNS requests on port 53.