

Activity Overview

In this activity, you will analyze DNS and ICMP traffic in transit using data from a network protocol analyzer tool. You will identify which network protocol was utilized in assessment of the cybersecurity incident.

In the internet layer of the TCP/IP model, the IP formats data packets into IP datagrams. The information provided in the datagram of an IP packet can provide security analysts with insight into suspicious data packets in transit.

Knowing how to identify potentially malicious traffic on a network can help cybersecurity analysts assess security risks on a network and reinforce network security.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

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.”

```
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
```

In the tcpdump log, you find the following information:

- 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.
- 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.
- 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.
- 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.
- For the ICMP error response, the source address is 203.0.113.2 and the destination is your computer's IP address 192.51.100.15.
- Additional details include protocol information, port numbers, and flags. The query identification number appears as 35084. The plus sign (+) indicates flags associated with the UDP message. The "A?" flag represents a DNS request for an A record.
- The third line displays the protocol of the response message as ICMP, followed by an ICMP error message.

- The error message “udp port 53 unreachable” indicates that the DNS service on port 53 was not reachable.
- The remaining lines show that ICMP packets were sent multiple times, but the same error was received.

Now that you have captured data packets using a network analyzer tool, your task is to identify which network protocol and service were impacted by this incident and prepare a follow-up report.

As an analyst, you inspect network traffic to determine the cause of network-related issues during cybersecurity incidents. This event is currently being handled by security engineers after being reported to your supervisor.