Security Incident Report

Network Traffic Analysis

Wendy Alayon
08/06/2024 **@syszern**

Table of Contents

Security incident report

Scenario

A cybersecurity analyst working at a company specializing in providing IT services for clients received reports from several customers of a client company who were unable to access the website www.yummyrecipesforme.com. The customers encountered the error message “destination port unreachable” after waiting for the page to load.

The cybersecurity analyst was tasked with analyzing the situation and determining which network protocol was affected during the incident. To start, the analyst attempted to visit the website and also received the error message “destination port unreachable.”

To troubleshoot the issue, the analyst loaded the network analyzer tool, tcpdump, and attempted to load the webpage again. The process began with the browser sending a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name, as part of the DNS protocol. The browser then used this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage.

The network analyzer showed that when UDP packets were sent to the DNS server, ICMP packets containing the error message “udp port 53 unreachable” were received.

```
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:

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 data packets have been captured using a network analyzer tool, it is the security analyst's job to identify which network protocol and service were impacted by this incident. Subsequently, the analyst will need to write a follow-up report.

In the meantime, security engineers are handling the event after the issue was reported to the direct supervisor by the analyst and other team members.

Summary of Issues Identified in DNS and ICMP Traffic Logs

The process began with the use of the UDP protocol to contact the DNS server, initiating a request to map the website's domain name (yummyrecipesforme.com) to its IP address. The ICMP protocol was also involved, as evidenced by its presence in the log events, transmitting error messages regarding the communication with the DNS server. The network protocol analyzer tool, tcpdump, captured UDP packets originating from the source computer directed towards the IP address and port of the DNS server. The presence of a plus sign after the query identification number indicates flags associated with the UDP message, while the "A?" symbol signifies a DNS query for an IPv4 address (A record). Additionally, tcpdump recorded ICMP error responses from the DNS server back to the source computer, containing the error message "udp port 53 is unreachable." Port 53 serves as the default port for DNS queries and responses. An ICMP error message referencing port 53 suggests a disruption in DNS communication. Combined with flags associated with DNS protocol operations, it indicates likely DNS server unresponsiveness, causing difficulties in domain name retrieval.

Analysis of Data, Identification of Incident Causes, and Recommended Solution

The incident occurred today at 1:24 p.m., as documented by the network protocol analyzer tool, which timestamped the first log event. Following numerous reports from customers of the client company, detailing their inability to access the website www.yummyrecipesforme.com and encountering the error message "destination port unreachable," the cybersecurity team, entrusted with providing IT services to the client organization, initiated an investigation to restore website accessibility. A cybersecurity analyst within the team began scrutinizing network traffic and data using a network protocol analyzer tool called tcpdump, while also attempting to load the webpage.

Examination of the resulting logs revealed that UDP port 53, commonly utilized for DNS traffic, was unreachable. The subsequent course of action involves determining whether this unreachability stems from the DNS server being offline or if traffic to port 53 is being obstructed by the firewall. Potential causes for the DNS server's unavailability include a successful Denial of Service attack (DoS) or a configuration error.