Cybersecurity Incident Report: Analyze Network Layer Communication

Scenario

You are a cybersecurity analyst working at a company that specializes in providing IT consultant services. Several customers contacted your company to report that they were not able to access the 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 visit the website and you also receive the error "destination port unreachable." Next, you load your network analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer. The analyzer shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an 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 DNS and ICMP log, you find the following information:

1. In the first two lines of the log file, you see 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. Next you find timestamps that indicate when the event happened. In the log, this is the first sequence of numbers displayed. For example: 13:24:32.192571. This displays the time 1:24 p.m., 32.192571 seconds.
3. The source and destination IP address is next. In the error log, this information is displayed as: 192.51.100.15.52444 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address. In this example, the source 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.

4. The second and third lines of the log show the response to your initial ICMP request packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the ICMP packet was undeliverable to the port of the DNS server.

5. Next are the protocol and port number, which displays which protocol was used to handle communications and which port it was delivered to. In the error log, this appears as: udp port 53 unreachable. This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The word "unreachable" in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message "udp port 53 unreachable."

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.

Provide a Summary of the Problem Found in the DNS and ICMP Traffic Log

- DNS server is down as a result of port 53 being unreachable. The ICMP request packet indicates that the packet has not been delivered to the port of DNS server successfully.
- As we know, Port 53 is commonly used for DNS. That being said, the most likely issue is the DNS is not responding and it can be caused by DDOS attack against the DNS server.
- The UDP protocol reveals that: DNS is not responding.
  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: at port 53 , UDP port 53 unreachable.
- The port noted in the error message is used for: DNS Server
  The most likely issue is: DNS server is not responding.

Explain Your Analysis of the Data and Provide at Least One Cause of the Incident

- Time incident occurred: 1.23pm.
- Explain how the IT team became aware of the incident: The customer reported to the company that they were unable to gain access to the company's website. It was then reported that the message on the web page is "port unreachable".
- Explain the actions taken by the IT department to investigate the incident: Security engineers had a look on the webpage and received an error "port being unreachable". The team used TCPdump (network analyzer) to see the network traffic surrounding the website.

- Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Go to website then load the webpage while monitoring the networks via TCPdump. It received lots of traffic. Sent UDP packets and received ICMP response to return to the host that indicates port 53 unreachable.
- Note a likely cause of the incident: Determine whether port 53 is working or not. IF it's fine, then check firewall.
  -Firewall: The ability to block network traffic on specific ports. Port blocking can be used to stop or prevent an attack.
  -DOS: There could be flood of information being sent to the network device to make it crash or unable to function. The hacker could disable dns server using DOS attack. Or someone within the organization might have disabled port 53 on firewalls.