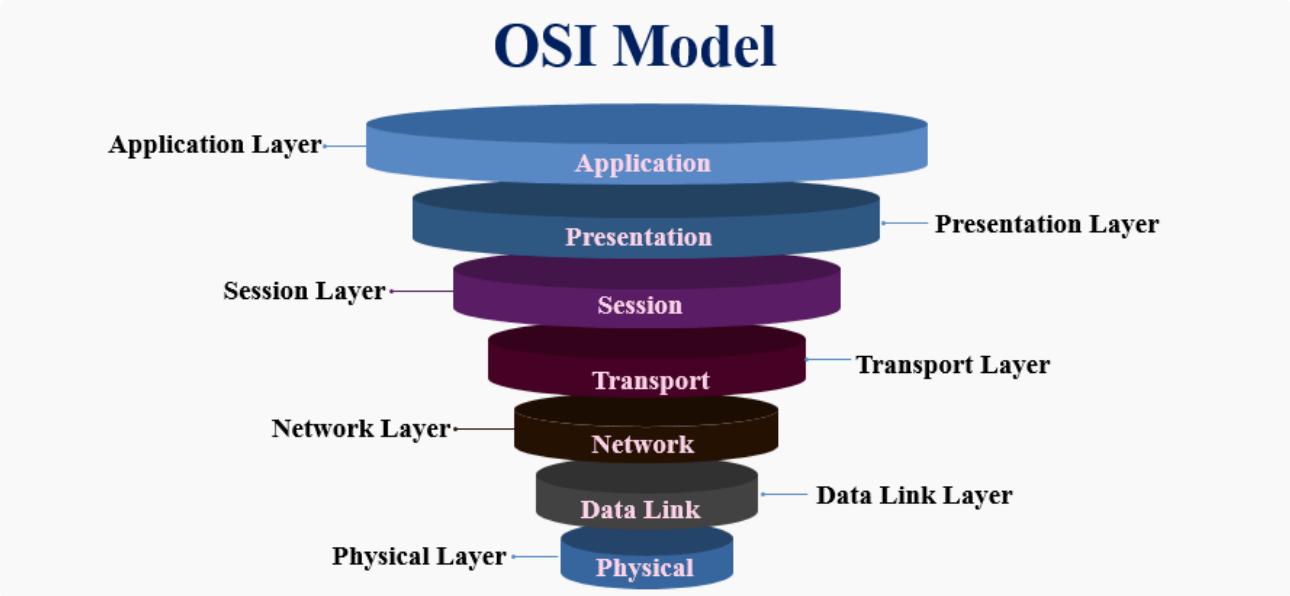
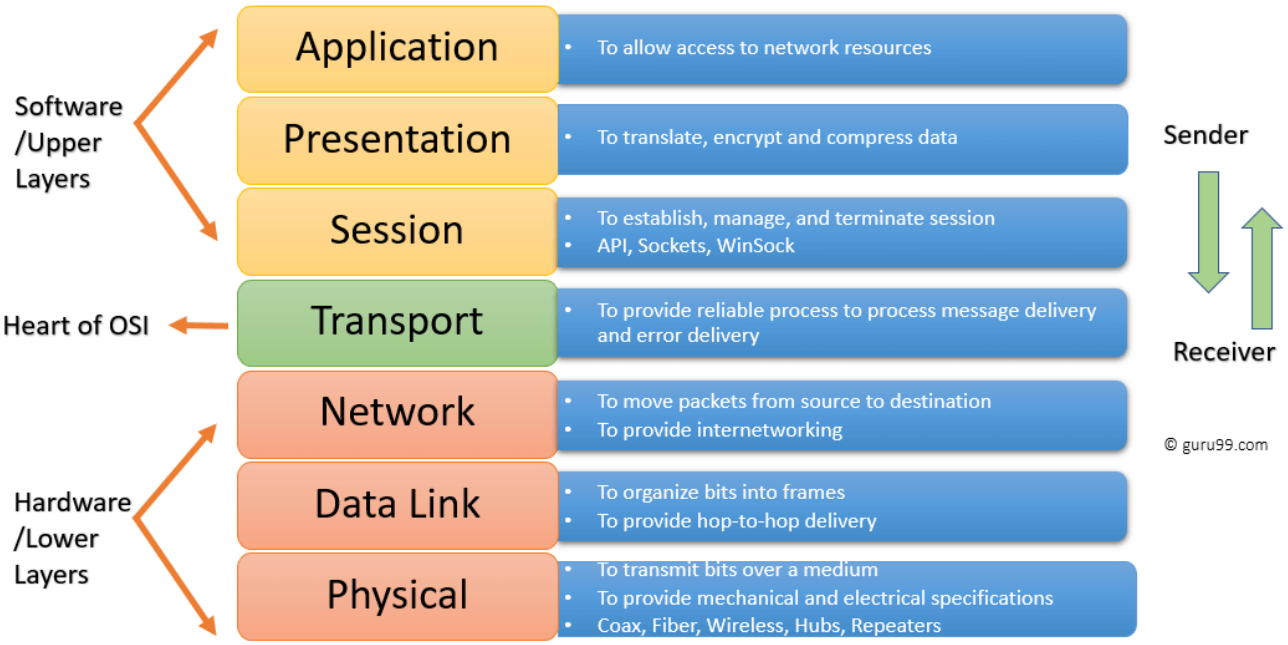
Tags:

#Lab/Cybersecurity

Prompt For This Lab GCS





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:

> **Tip**
>
> Review the scenario below. Then complete the step-by-step instructions.

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.

My Job:

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.

The Solution:

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;

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:

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. ==

> ⚠ Attention
>
> Then, you will need to write a follow-up report.

Step 3: Provide a summary of the problem found in the tcpdump log

After analyzing the data presented to you from the tcpdump log, identify trends in the data. Assess which protocol is producing the error message from the DNS server for the yummyrecipesforme.com website. *Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS.*

In your analysis:

- Include a brief summary of the tcpdump log analysis and identify which protocols were used for the network traffic.
- Provide a few details about what was indicated in the log.
- Interpret the issues found in the log.

Part 1

The tcpdump log, is for solving the clients issues, and it's important to know, that if this issue still running, then the site of the company will loess clients. The protocols used in the network traffic are:

- DNS
- ICMP
- HTTPS
- UPD

When I try to rich the website, the browser will send a request to the DNS server using UDP protocols, and the expected result is a response from the DNS server with the correct Host address for the Doman address that the clients try to rich, but instead the output from the tcpdump analyzer, is a ICMP error, and port 53 is a port for DNS service, and that's mean the problem is in the DNS server, or in firewall configuration. It's possible that this is an indication of a malicious attack on the web server.

Part 2

The incident occur at 1:24PM, and main issue, is that when a client try to establish a connection with the DNS server via UDP packet, the response is a ICMP error, and that's way the clients can't rich the company website. So the main issue found DNS issue, or firewall misconfiguration. If the DNS server is down, then this assign to DDoS attack, and if the port number is blocked then this is might an internal threat.
