Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

A Denial of Service (DoS) attack targets a network or server, overwhelming it with excessive traffic to disrupt normal operations. The goal is to make the network crash or become unresponsive to legitimate users, potentially costing the organization both time and money. A Distributed Denial of Service (DDoS) attack is a more advanced version, utilizing multiple devices or servers from various locations to flood the target with even more traffic, increasing the chances of success.

One common example of a DoS attack is where an attacker crafts a special packet that causes a router to take extra time to process it, leading to a system overload without a massive increase in traffic.

Network Level DoS Attacks

1. SYN Flood Attack:  
   This attack exploits the TCP handshake process. A device sends a flood of SYN requests to a server, and if the server is overwhelmed by these requests (more than its available ports), it can’t complete the connection, causing it to crash.
2. ICMP Flood Attack:  
   In this attack, the attacker repeatedly sends ICMP packets to a server, forcing it to respond. This consumes all bandwidth for incoming and outgoing traffic, leading to a server crash.
3. Ping of Death:  
   This attack involves sending an oversized ICMP packet (larger than the 64KB limit) to a vulnerable system, causing it to crash. It’s akin to overloading a system with an enormous, unmanageable request.

In summary, these attacks overload network devices either through large volumes of requests or by manipulating specific protocols, causing disruption and rendering the system unusable.

# Read tcpdump logs

A **network protocol analyzer**, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers  include:

* SolarWinds NetFlow Traffic Analyzer
* ManageEngine OpManager
* Azure Network Watcher
* Wireshark
* tcpdump

This reading will focus exclusively on tcpdump, though you can apply what you learn here to many of the other network protocol analyzers you'll use as a cybersecurity analyst to defend against any network intrusions. In an upcoming activity, you’ll review a tcpdump data traffic log and identify a DoS attack to practice these skills.

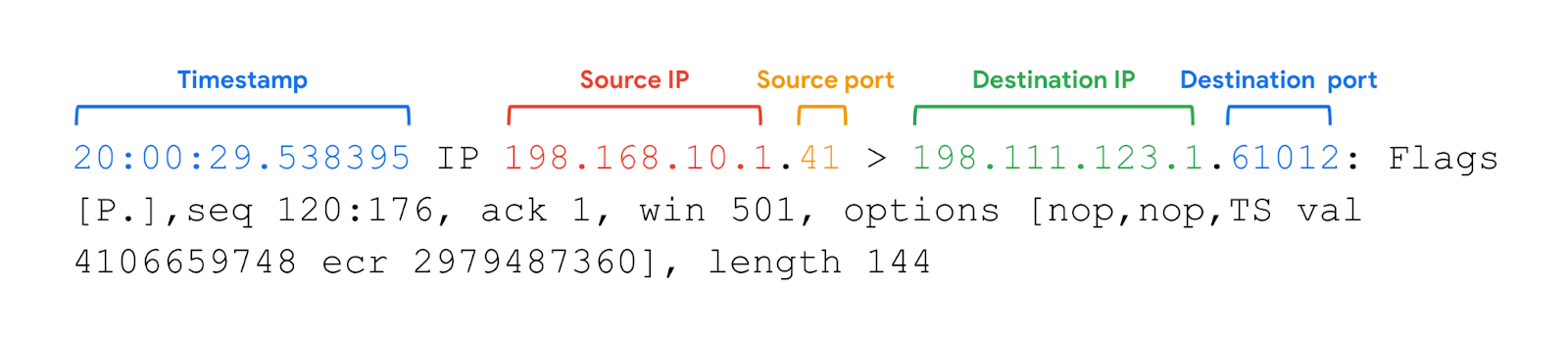
## tcpdump

**tcpdump** is a command-line network protocol analyzer. It is popular, lightweight–meaning it uses little memory and has a low CPU usage–and uses the open-source libpcap library. tcpdump is text based, meaning all commands in tcpdump are executed in the terminal. It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions.

tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans. It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications.

## Interpreting output

tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed. The output of a packet capture contains many pieces of important information about the network traffic.



Some information you receive from a packet capture includes:

* **Timestamp**: The output begins with the timestamp, formatted as hours, minutes, seconds, and fractions of a second.
* **Source IP**: The packet’s origin is provided by its source IP address.
* **Source port**: This port number is where the packet originated.
* **Destination IP**: The destination IP address is where the packet is being transmitted to.
* **Destination port**: This port number is where the packet is being transmitted to.

**Note:** By default, tcpdump will attempt to resolve host addresses to hostnames. It'll also replace port numbers with commonly associated services that use these ports.

## Common uses

tcpdump and other network protocol analyzers are commonly used to capture and view network communications and to collect statistics about the network, such as troubleshooting network performance issues. They can also be used to:

* Establish a baseline for network traffic patterns and network utilization metrics.
* Detect and identify malicious traffic
* Create customized alerts to send the right notifications when network issues or security threats arise.
* Locate unauthorized instant messaging (IM), traffic, or wireless access points.

However, attackers can also use network protocol analyzers maliciously to gain information about a specific network. For example, attackers can capture data packets that contain sensitive information, such as account usernames and passwords. As a cybersecurity analyst, It’s important to understand the purpose and uses of network protocol analyzers.

## Key takeaways

Network protocol analyzers, like tcpdump, are common tools that can be used to monitor network traffic patterns and investigate suspicious activity. tcpdump is a command-line network protocol analyzer that is compatible with Linux/Unix and macOS®. When you run a tcpdump command, the tool will output packet routing information, like the timestamp, source IP address and port number, and the destination IP address and port number. Unfortunately, attackers can also use network protocol analyzers to capture data packets that contain sensitive information, such as account usernames and passwords.

# Real-life DDoS attack

Previously, you were introduced to Denial of Service (DoS) attacks. You also learned that volumetric distributed DoS (DDoS) attacks overwhelm a network by sending unwanted data packets in such large quantities that the servers become unable to service normal users. This can be detrimental to an organization. When systems fail, organizations cannot meet their customers' needs. They often lose money, and in some cases, incur other losses. An organization’s reputation may also suffer if news of a successful DDoS attack reaches consumers, who then question the security of the organization.

In this reading you’ll learn about a 2016 DDoS attack against DNS servers that caused major outages at multiple organizations that have millions of daily users.

## A DDoS targeting a widely used DNS server

In previous videos, you learned about the function of a DNS server. As a review, DNS servers translate website domain names into the IP address of the system that contains the information for the website. For instance, if a user were to type in a website URL, a DNS server would translate that into a numeric IP address that directs network traffic to the location of the website’s server.

On the day of the DDoS attack we are studying, many large companies were using a DNS service provider. The service provider was hosting the DNS system for these companies. This meant that when internet users typed in the URL of the website they wanted to access, their devices would be directed to the right place. On October 21, 2016, the service provider was the victim of a DDoS attack.

## Leading up to the attack

Before the attack on the service provider, a group of university students created a botnet with the intention to attack various gaming servers and networks. A **botnet** is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder." Each computer in the botnet can be remotely controlled to send a data packet to a target system. In a botnet attack, cyber criminals instruct all the bots on the botnet to send data packets to the target system at the same time, resulting in a DDoS attack.

The group of university students posted the code for the botnet online so that it would be accessible to thousands of internet users and authorities wouldn’t be able to trace the botnet back to the students. In doing so, they made it possible for other malicious actors to learn the code to the botnet and control it remotely. This included the cyber criminals who attacked the DNS service provider.

## The day of attack

At 7:00 a.m. on the day of the attack, the botnet sent tens of millions of DNS requests to the service provider. This overwhelmed the system and the DNS service shut down. This meant that all of the websites that used the service provider could not be reached. When users tried to access various websites that used the service provider, they were not directed to the website they typed in their browser. Outages for each web service occurred all over North America and Europe.

The service provider’s systems were restored after only two hours of downtime. Although the cyber criminals sent subsequent waves of botnet attacks, the DNS company was prepared and able to mitigate the impact.

## Key takeaways

As demonstrated in the above example, DDoS attacks can be very damaging to an organization. As a security analyst, it’s important to acknowledge the seriousness of such an attack so that you’re aware of opportunities to protect the network from them. If your network has important operations distributed across hosts that can be dynamically scaled, then operations can continue if the baseline host infrastructure goes offline. DDoS attacks are damaging, but there are concrete actions that security analysts can take to help protect their organizations. Keep going through this course and you will learn about common mitigation strategies to protect against DDoS attacks.