NETWORK FORENSIC TOOL

Report For Web Traffic Analysis

Summary

DoS/DDoS Attack

A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

How to identify a DDoS attack

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such as a legitimate spike in traffic — can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

• Suspicious amounts of traffic originating from a single IP address or IP range

• A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version

• An unexplained surge in requests to a single page or endpoint

• Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g., a spike every 10 minutes)

There are other, more specific signs of a DDoS attack that can vary depending on the type of attack.

Types of DoS Attacks and DDoS Attacks

Teardrop attack

A teardrop attack is a DoS attack that sends countless Internet Protocol (IP) data fragments to a network. When the network tries to recompile the fragments into their original packets, it is unable to.

For example, the attacker may take very large data packets and break them down into multiple fragments for the targeted system to reassemble. However, the attacker changes how the packet is disassembled to confuse the targeted system, which is then unable to reassemble the fragments into the original packets.

Flooding attack

A flooding attack is a DoS attack that sends multiple connection requests to a server but then does not respond to complete the handshake.

For example, the attacker may send various requests to connect as a client, but when the server tries to communicate back to verify the connection, the attacker refuses to respond. After repeating the process countless times, the server becomes so inundated with pending requests that real clients cannot connect, and the server becomes 'busy' or even crashes.

Protocol attack

A protocol attack is a type of DDoS attack that exploits weaknesses in Layers 3 and 4 of the OSI model. For example, the attacker may exploit the TCP connection sequence, sending requests but either not answering as expected or responding with another request using a spoofed source IP address. Unanswered requests use up the resources of the network until it becomes unavailable.

Application-based attack

An application-based attack is a type of DDoS attack that targets Layer 7 of the OSI model. An example is a Slowloris attack, in which the attacker sends partial Hypertext Transfer Protocol (HTTP) requests but does not complete them. HTTP headers are periodically sent for each request, resulting in the network resources becoming tied up.

The attacker continues the onslaught until no new connections can be made by the server. This type of attack is very difficult to detect because rather than sending corrupted packets, it sends partial ones, and it uses little to no bandwidth.

Introduction

Network Forensic Tool for DDoS Detection

This is a report on network forensics focusing on web-based traffic, specifically targeting the detection of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. The analysis presented in this report is conducted using a specialized network forensic tool designed to capture, import, and analyze network packets to identify malicious activities aimed at disrupting services.

The network forensic tool enables investigators to capture network packets in real-time, marking the status of the captured file as "captured". Additionally, it allows for the importation of pre-existing packet capture (PCAP) files, with the status being marked as "imported". Each captured or imported file is saved with a specific hash value to ensure data integrity and authenticity.

Upon obtaining the PCAP file, whether captured or imported, the tool performs a thorough analysis of the network traffic within the file. The analysis aims to identify patterns and anomalies that are characteristic of DoS and DDoS attacks. This includes examining various metrics such as packet counts, IP addresses, protocol usage, and traffic behavior over time.

After analyzing the traffic, the tool provides a detailed output indicating whether a DoS or DDoS attack pattern was observed. If an attack pattern is detected, the tool identifies the specific type of attack, such as SYN flood, UDP flood, or application-layer attacks like Slowloris. The findings are compiled into a comprehensive report, detailing the nature of the detected attack, the methodologies used for detection, and relevant statistics and insights.

Analysis Result

Case Details:

Case Name: DDOS
Organization Name: UDOM
Investigator Name: Neema
Date: 2024-07-09

PCAP Files:

Pcap File	Date	Status
outputs/UDOM-DDOS-1.pcap	2024-07-09	imported
outputs/UDOM-DDOS-2.pcap	2024-07-09	imported
outputs/UDOM-DDOS-3.pcap	2024-07-09	imported
outputs/UDOM-DDOS-4.pcap	2024-07-09	imported

PCAP Analysis Report:

PCAP File: UDOM-DDOS-1.pcap
Total Packets: 576014
TCP Count: 576014
UDP Count: 0
HTTP Count: 8
SYN Count: 576014
SYN-ACK Count: 0
ACK Count: 0
SYN without ACK Count: 576014
SYN-ACK Ratio: 0.0
SYN-ACK Ratio Result: ■[91mPossible SYN flood attack.■[0m
Proportionality Ratio Result: Packets within proportional rate
File Hash: a3e3bd84d1b1ee8349b9a847dd9b3620
Analysis Date: 2024-07-09 13:53:15

IP	Count
99.99.99.98.20475	1
99.99.99.22.36691	1
99.99.99.166.46932	1
99.99.95.17.11201	1
99.99.94.141.4908	1

PCAP File: UDOM-DDOS-2.pcap
Total Packets: 12000
TCP Count: 3
UDP Count: 11830
HTTP Count: 0
SYN Count: 0
SYN-ACK Count: 0
ACK Count: 3
SYN without ACK Count: 0
SYN-ACK Ratio: 0.0
SYN-ACK Ratio Result: SYN-ACK ratio within threshold.
Proportionality Ratio Result: ■[91mPossible UDP flood attack.■[0m
File Hash: efffc444dedfb7c5d4e958a49385bc28
Analysis Date: 2024-07-09 13:56:15

IP	Count
8.8.8.8.53	6430
8.8.4.4.53	847
212.8.51.69	500
212.8.51.71	370
212.8.51.72	276

PCAP File: UDOM-DDOS-3.pcap
Total Packets: 37841
TCP Count: 37841
UDP Count: 0
HTTP Count: 1
SYN Count: 37841
SYN-ACK Count: 0
ACK Count: 0
SYN without ACK Count: 37841
SYN-ACK Ratio: 0.0
SYN-ACK Ratio Result: ■[91mPossible SYN flood attack.■[0m
Proportionality Ratio Result: Packets within proportional rate
File Hash: 80edd1c312211cc70243159ab41dac71
Analysis Date: 2024-07-09 13:56:28

IP	Count
98.24.74.165.16963	2
97.85.198.105.18625	2
96.99.168.95.8934	2
96.92.220.63.53804	2
95.40.221.139.50476	2

PCAP File: UDOM-DDOS-4.pcap
Total Packets: 19774
TCP Count: 0
UDP Count: 19774
HTTP Count: 0
SYN Count: 0
SYN-ACK Count: 0
ACK Count: 0
SYN without ACK Count: 0
SYN-ACK Ratio: 0.0
SYN-ACK Ratio Result: SYN-ACK ratio within threshold.
Proportionality Ratio Result: ■[91mPossible UDP flood attack.■[0m
File Hash: 3695b99655c4f29ad00f4ce50ad44f76
Analysis Date: 2024-07-09 13:56:44

IP	Count
86.97.35.193.12760	5441
88.85.109.124.52458	1774
118.69.234.70.47028	1722
42.231.62.105.3621	1253
123.13.153.136.31334	1015