

LEARN ABOUT  
THE LAYERED  
DEFENSE  
AGAINST DDOS  
THAT HAS WORKED  
FOR MORE THAN 2500  
ORGANIZATIONS.

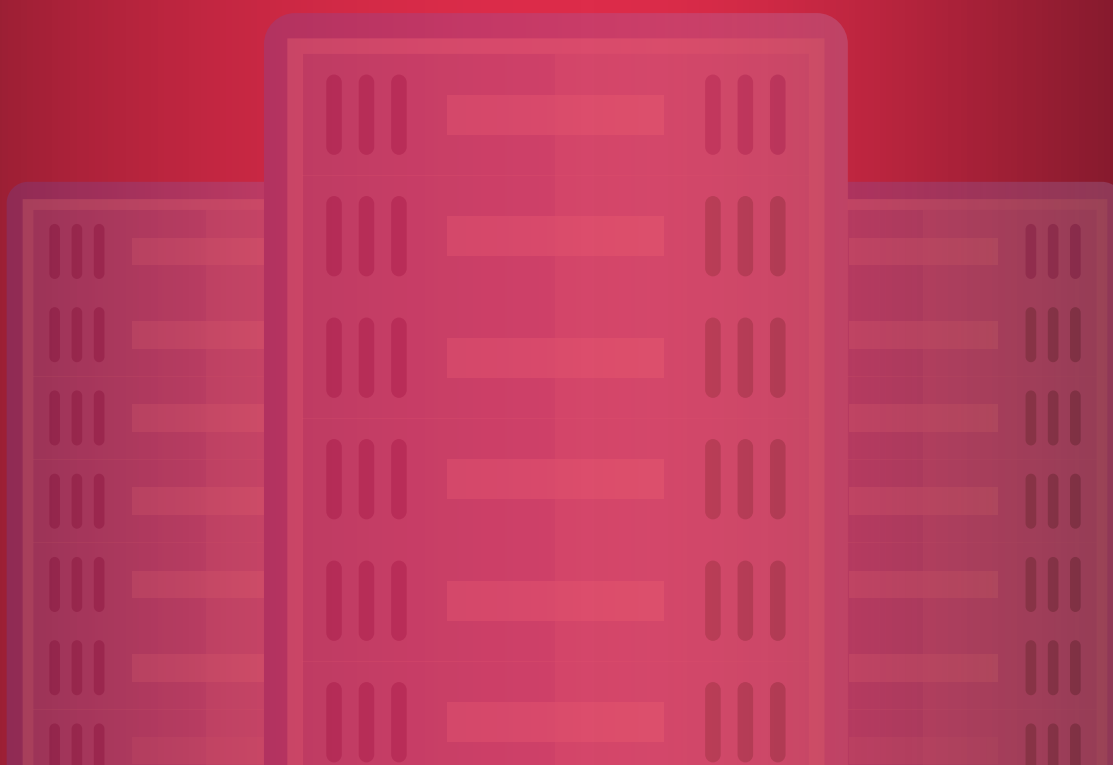
# Exploring the Methodology of **DDoS** **Attacks**



# Preface

A distributed denial of service (DDoS) is a cyberattack where a malicious entity overwhelms a victim's server with spoof requests that render the server incapable of processing legitimate requests. DDoS attacks have evolved exponentially due to the difficulty in differentiating spoof requests from legitimate ones. DDoS attacks are dangerous because they can act as a decoy to distract cybersecurity teams from focusing on more critical threats, such as data exfiltration. Imagine a company that is witnessing a business interruption due to a denial of service (DoS) attack. While security teams are focused on getting their systems unclogged, there could be a malicious insider attempting to access sensitive information.

This paper aims to technically explore the three DDoS attack styles (volumetric-based attacks, application-based attacks, and protocol-based attacks). It also explains how ManageEngine Log360 can provide effective defenses against DDoS attacks by allowing you to identify them, and take preemptive measures to secure your network.



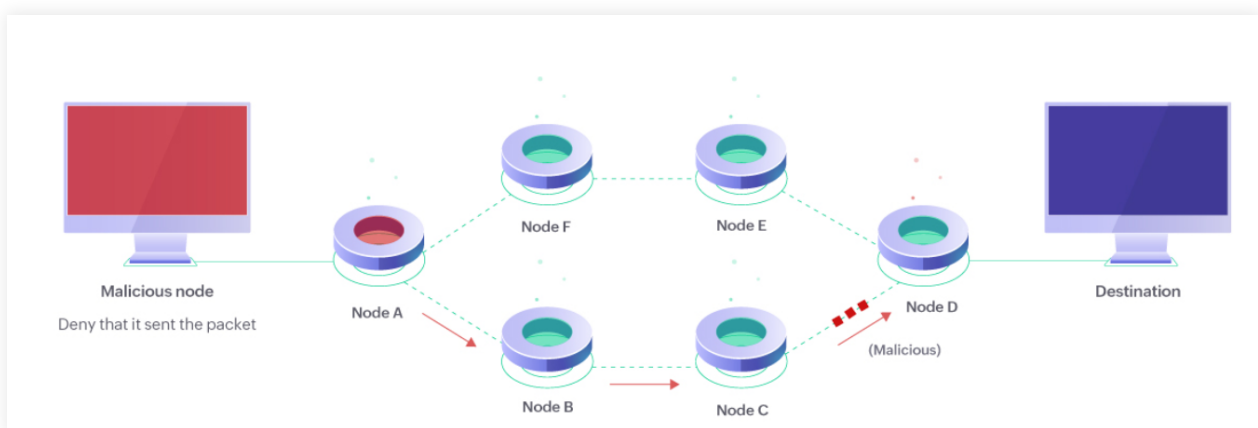
# Introduction

This section will walk you through the main DDoS attack styles.

**Volumetric-based attack:** This occurs when perpetrators target a victim's systems by attacking with a botnet, a network of rogue, interconnected devices that focus on a common task, such as sending multiple fake requests that disable servers. The attacker's goal is to overload the victim's server, or cause a CPU starvation process that continuously denies the required resources to process legitimate server requests. Botnets can be used to trick users into downloading or running malware, or exploiting browser vulnerabilities from harmless-looking links or websites so hackers can invade a network. This ploy is intended to entice users to download a snippet of code that connects to the hacker's device, and executes malware that launches a volume-based DDoS attack.

**Application-based attack:** These types of attacks target the application layer of the Open Systems Interconnection (OSI) model. For example, the victim's web servers might be targeted with numerous HTTP GET requests, and large files from the victim server might be retrieved in overwhelming numbers. Attackers can also run a massive number of queries through the victim's server, application, or database to bring the service down. An application-based DDoS attack is launched through a repudiation attack,\* or by the spread of infectious malware or viruses across all nodes in the network.

*\*Repudiation attack: This refers to a node's denial that it ever sent a data packet to the destination node. For instance, an infected node, A, sends a data packet to a destination, D. When D receives the packet, it notices that the packet contents have been tampered with. D relays an error message back to A. But A denies that it ever sent the packet.*



Repudiation attack

**Protocol-based attack:** These attacks leverage vulnerabilities in the third and fourth layers of the OSI model. Effective communication between a client and server relies on a three-way handshake to establish the authenticity of the parties involved. The attacker launches an attack by initiating multiple requests to connect to the server, overwhelming the server with fraudulent connection requests. Attackers also leverage vulnerabilities in communication protocols to hijack sessions. A hacker does this by impersonating a node in the session.

	<b>Volumetric</b>	<b>Application</b>	<b>Protocol</b>
<b>What is it?</b>	An attack that uses amplification techniques to overload the bandwidth of the victim's server.	This attack exploits vulnerabilities in layer seven of the protocol stack.	An attack that leverages vulnerabilities in Transmission Control Protocol (TCP) three-way handshakes, and affects the third and fourth layers of the protocol stack.
<b>Effect on target</b>	The overload of traffic prevents a user from accessing resources in the victim's server.	The attack dominates all of the processes and transactions of the victim's servers.	The attack binges on the processing capacity of the victim's server, preventing it from processing genuine requests.
<b>Types of attack</b>	Ping floods, DNS amplification attacks	HTTP flood attack, Slowloris attack	SYN flood attack, IP fragmentation attack

DDoS attacks often result in frustrated IT departments and organizations becoming angry over the disruption in services, halts to productivity, and damage to their reputation. All the above factors can result in a huge loss of revenue for an organization.

# Gain an Understanding of Application Layer DDoS Attacks

This section deals with two types of application-based DDoS attacks: HTTP flood attacks, and Slowloris attacks.

## HTTP Flood Attack

Before we approach the technicalities of an HTTP flood attack, let's take a look at how HTTP requests work.

An HTTP request adheres to a request and response protocol when a client requests information from a server, and receives a response from the server.

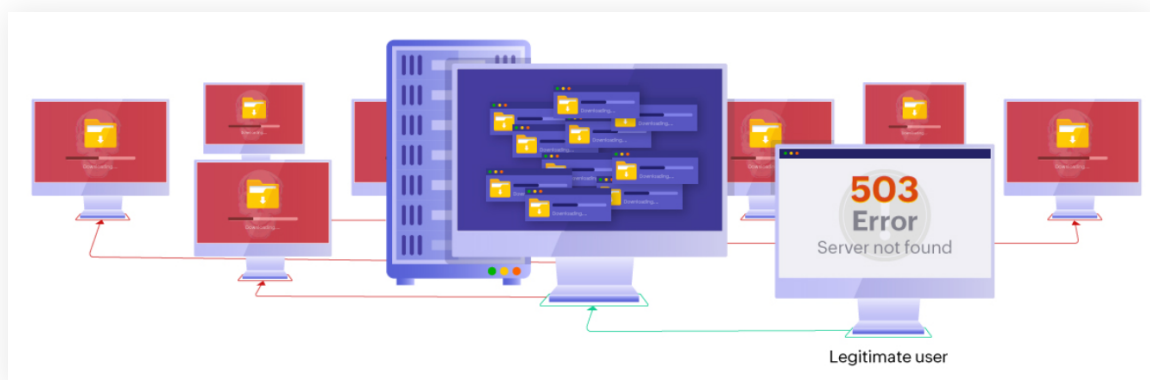
The two most popular HTTP methods are the GET, and the POST methods.

**GET Method:** A query string is added to the URL to request access from the server for a particular resource.

**POST Method:** Used to send information to a server to create or update a resource.

## HTTP GET Flood Attack

In a GET flood attack, a threat actor requests the download of a large file, like a script or an image, from the victim's server. This request is sent via a GET string. Similar requests for the same large file from the same server are made as part of a coordinated attack involving several other computers. This leads to the victim's server being overloaded with fraudulent requests and unable to service legitimate requests.



Attacker using GET request to download large files from victim's server

## HTTP POST Flood Attack

In an HTTP POST flood attack, a hacker attempts to exploit forms on a website. Since a POST method is used to send data from the client to the server, a threat actor can create random parameters in the HTTP request form to send large amounts of data to the server. This overwhelms the server, and does not allow it to process the data sent by legitimate clients, leading to a denial of service.



A hacker sends large amounts of spoof data to victim server.

## Slowloris Attack

Slowloris is a denial-of-service attack program which allows a hacker to overwhelm a targeted server by opening and maintaining many simultaneous HTTP connections between the hacker and the victim.

An HTTP request sent between the client and the server contains information about the resource the client wants, along with details such as who is making the request, or where the request is coming from.

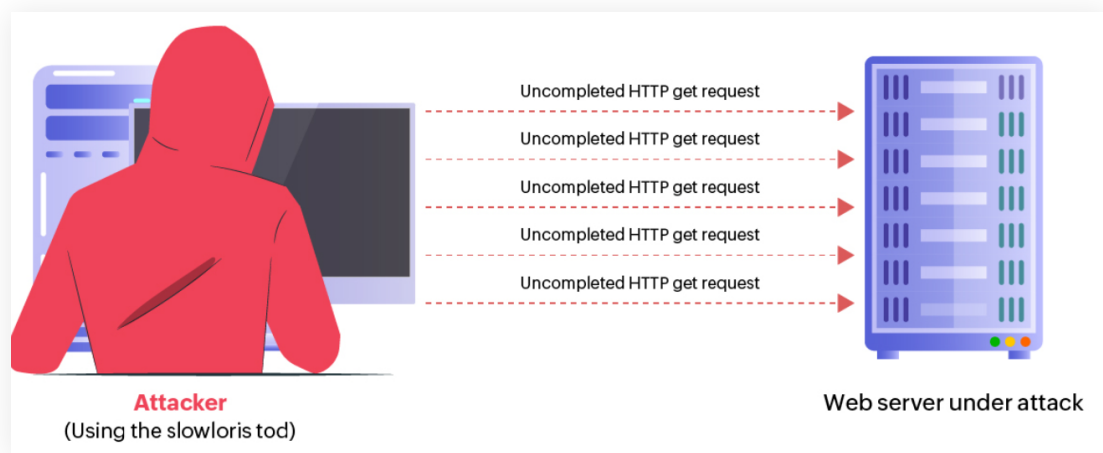
The end of an HTTP request is signaled by a carriage return (CR) character which is followed by a line feed (LF) character.

CR and LF are control characters used to mark a line break in a text file.

- *CR = Carriage Return ( $\backslash r$ ,  $0x0D$  in hexadecimal,  $13$  in decimal)—moves the cursor to the beginning of the line without advancing to the next line.*
- *LF = Line Feed ( $\backslash n$ ,  $0x0A$  in hexadecimal,  $10$  in decimal)—moves the cursor down to the next line without returning to the beginning of the line.*

*A CR immediately followed by a LF (CRLF,  $\backslash r\backslash n$ , or  $0x0D0A$ ) moves the cursor down to the next line and then to the beginning of the line.*

In a Slowloris attack, a hacker manipulates the request from the client to never include a carriage return character in the request. This signifies to the server that there is still data that is being sent by the client via a request. A Slowloris attack is also programmed to circumvent session timeouts by the server by sending a small byte of data just before the session can be terminated. This leads the server to misread this scenario as the client transmitting data at a painfully slow speed, so the request is kept open with small bytes of data being transmitted at strategic intervals. This kind of open-ended request is multiplied on numerous computers, resulting in a large number of open requests that exhaust the server. Again, as with all DDoS attacks, this prevents a server from processing legitimate requests.



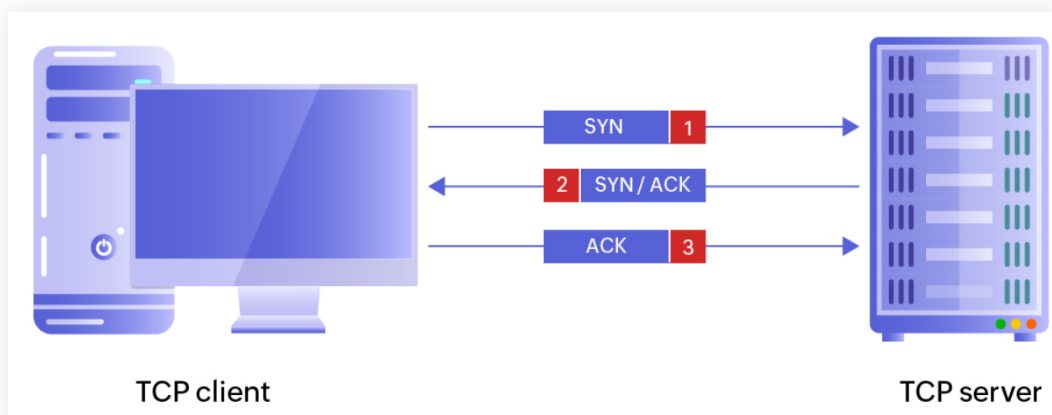
Hacker sends numerous open requests to victim's server causing it to crash

# A View Into DDoS Attacks on Protocol Layer

## SYN Flood Attack

SYN flood attacks are a common DDoS attack that target the protocol layer during client-server communication. Client server communication relies on a three-way handshake to ensure a proper connection. SYN flood attacks leverage this three-way handshake to create numerous incomplete connections that overload the server.

## TCP Three-way Handshake



TCP three-way handshake

To establish a connection with the server, the client sends a SYN request containing a Synchronize Sequence Number. To acknowledge that it has successfully received the SYN message, the server sends back an ACK message. After this ACK message has been received from the server, the client responds with another acknowledgement to confirm that the connection is now established and secure.

## How SYN Floods Leverage TCP Three-way Handshakes

In a SYN flood attack, the client initiating contact is manipulated into doing two things: sending several SYN requests, and refusing to respond to the server's SYN-ACK message.



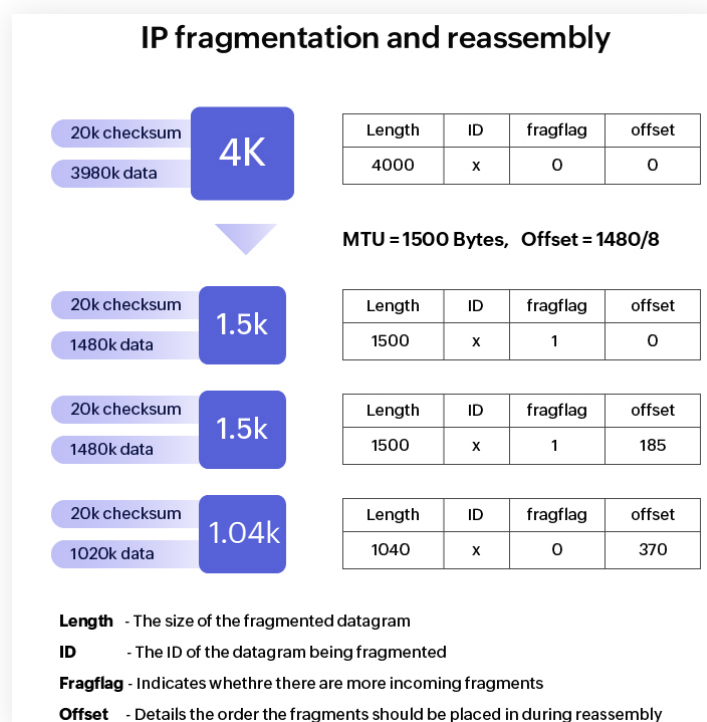
These two deviant activities lead to the creation of an overwhelming number of open connection requests that trick the server into waiting for the client to communicate. Client server connections are logged in a TCP connection table. This table gets filled up quickly with fraudulent client communication requests blocking other legitimate requests. This achieves a denial of service and interruption in business.

With advanced masking techniques like IP spoofing,\* it becomes more challenging to identify compromised devices that initiate phony connections.

*\*IP spoofing: Hackers use tools to alter the source address present in the packet header to dupe the recipient system into believing the packet is from a legitimate source. In a DoS attack, hackers use spoofed IP addresses to overload computer servers with packets of data, causing them to crash.*

## IP Fragmentation Attack

DDoS attacks can also exploit fragmentation mechanisms when data is transmitted over a network. Fragmentation of data is vital since different networks have various limits for datagram sizes. The diagram below describes how a datagram is fragmented.



Fragmentation of a datagram can be prevented by appending a "don't fragment" flag before transmission. If a datagram is above the acceptable limit of a network, an error message is declared.

DDoS attacks can exploit the fragmentation of datagrams to overload a network.

## IP Fragmentation Attack

These kind of DDoS attacks target the reassembling of the datagrams that depend on TCP/IP reassembling mechanisms. When these mechanisms are targeted, data fragments overlap each other. This puts a strain on the server that is trying to process incoming data, and makes it impossible for legitimate requests to be processed. This attack was prevalent on old Windows operating systems like Windows 95 and Windows NT. While patches on subsequent operating systems reduced the likelihood of an attack, the possibilities surfaced again in the Windows Vista and the Windows 7 operating systems.

## UDP Fragmentation

In this kind of an attack, the target network is bombarded with spoof User Datagram Protocol (UDP) requests that are clearly over the network specified size limit of the datagram. Since this large datagram is fragmented and transmitted over the network, the server's resources are utilized to reassemble it. However, since this data is fraudulent, it cannot be reassembled properly, leading to the server being overwhelmed with processing incorrect data. This leads to a denial-of-service to legitimate requests.

# A Cross-section of Volumetric style DDoS Attacks

## Ping Floods

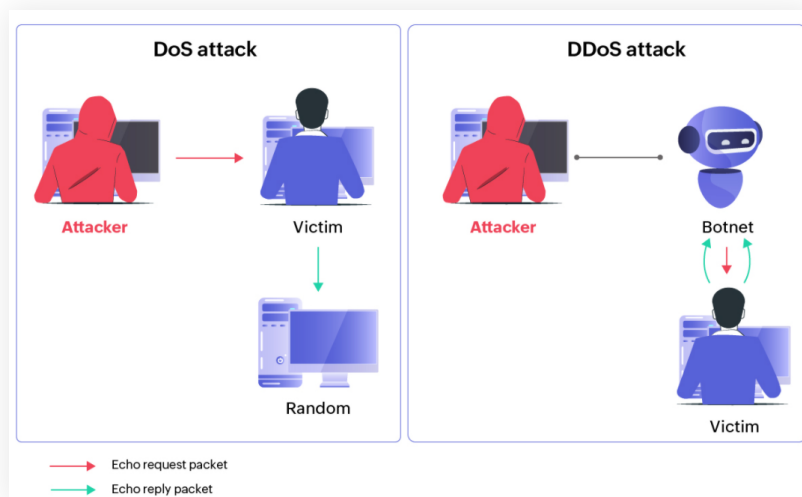
A ping flood attack is a kind of volumetric DDoS attack that relies on the Internet Control Message Protocol (ICMP) to cause a denial of service.

ICMP is a network layer protocol that is used to diagnose communication errors that occur when a client and server attempt to communicate. ICMP protocol allows routers to generate error messages that are sent to the source IP address to indicate that a data packet was not delivered to the destination successfully.

Another way an ICMP protocol proves useful is for pinging the routing path between the devices that want to communicate. A ping is a pulse that is sent from one device to another to calculate latency between the devices. When pinging, the time taken to send a data packet to a destination device and to receive an echo back is calculated.

## How Ping Floods Exploit the ICMP Protocol

In a ping flood, the attacker sends a stream of pings to a victim's machine requesting an echo to be sent back from the victim's machine. The victim's machine sends back an echo reply in response to this request. Ping requests and their responses require bandwidth and so an overload of these pings will binge on the victim's bandwidth slowing down the network on the victim side. This slows down the legitimate traffic in the network.



Attackers overloading ping requests and responses to the victim's server causing it to slow down.

A ping flood relies on knowing the IP address of the victim. A victim's IP address could be resolved in multiple ways. The attacker might have physical access to a computer to get its IP Address. This is called a targeted local disclosed ping flood, and it targets a single system on a local network.

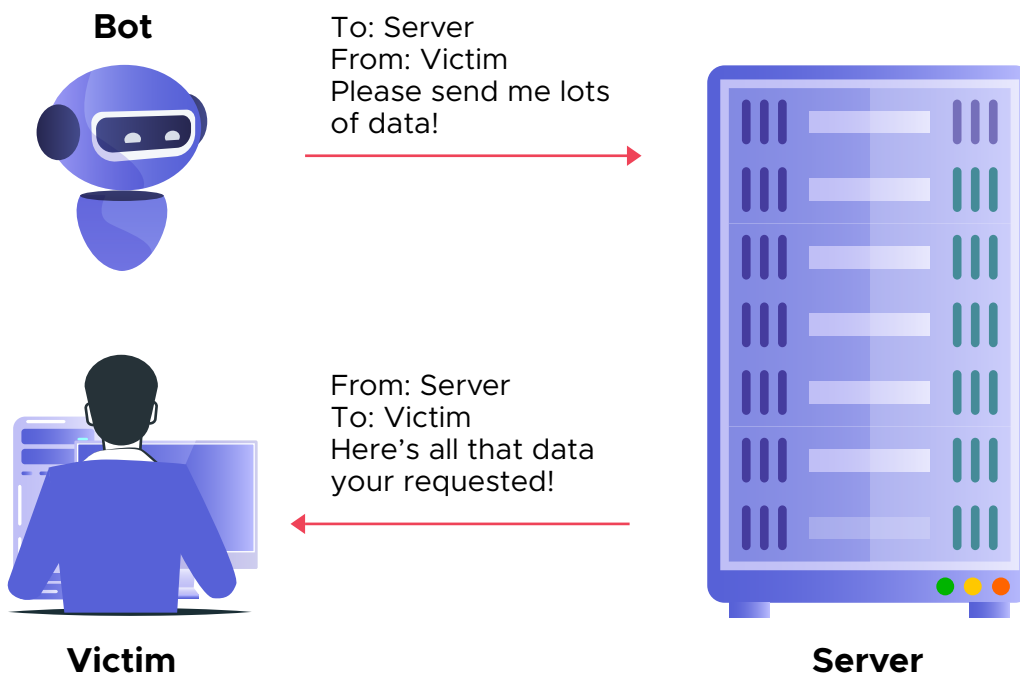
Ping floods can also target routers within a network. This also relies on the hacker knowing the IP address of a router in order to flood the particular router with pings. This is called a router disclosed ping flood attack. Additionally, hackers have also resorted to external programs to resolve IP addresses of the victim's systems, or blindly target source IP addresses with ping floods.

## DNS Amplification Attack

In a DNS amplification attack, a threat actor exploits DNS resolution and IP spoofing techniques to overload a target server with oversized UDP packets. These large-sized payloads are sent in huge volumes to a victim server, crippling it.

An attacker begins by sending out a DNS resolution request for a website to a DNS resolver citing a spoofed source address. This is actually the IP address of the victim's server that is forged by the attacker. The DNS resolver resolves this request and sends the response to the spoofed address, which is the victim's server. Since communication needs to be fast, UDP is a preferred protocol for DNS requests. The drawback to this is that the UDP doesn't check if the source address is correct or not. So unwanted DNS resolutions are directed towards an unsuspecting target that never requested it in the first place.

An enterprise's network is not going to be crippled by a few unwanted DNS resolution responses, so the hacker amplifies the DNS response. This amplification is accomplished by requesting more information from the resolver other than just the IP address of a website. An attacker could also append a request for information on an entire domain. Since information will be transmitted in the response, the response is amplified. An amplified response will result in fragmentation of datagrams over the network. The target's server will attempt to reconstruct these datagrams, which will consume a lot of resources unnecessarily resulting in a denial of service for legitimate requests.

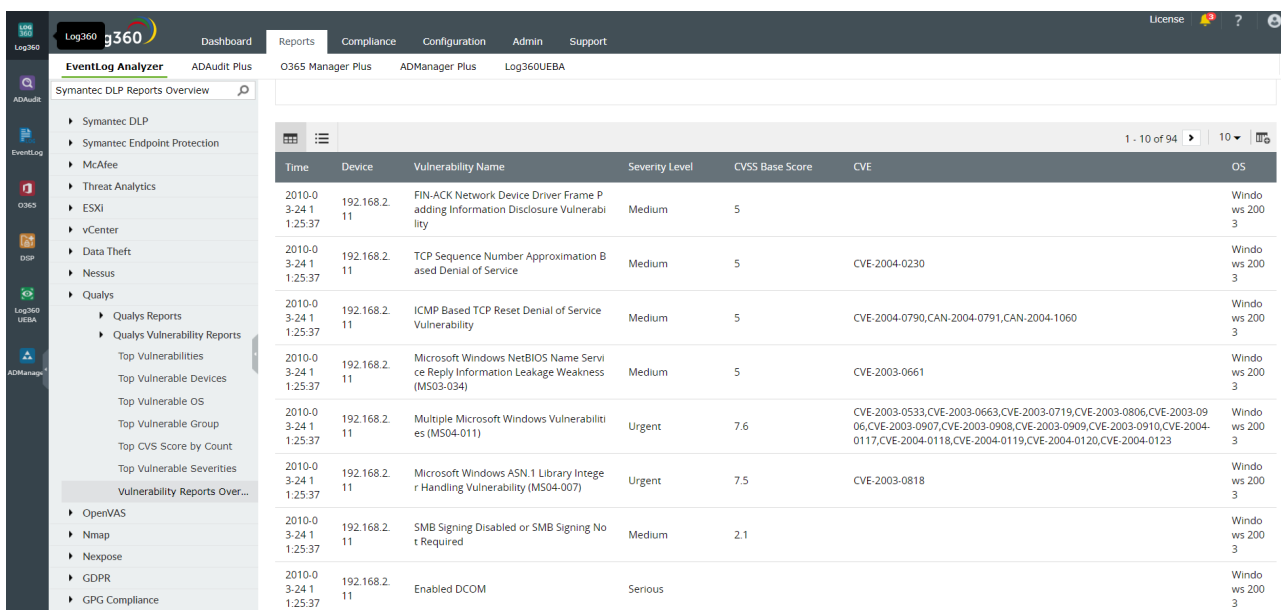


# How Log360 Can Protect You From DDoS Attacks

DDoS attacks over the years have evolved into more powerful mutations that are capable of bringing down even large organizations equipped with advanced security solutions.

Log360 is a cost effective SIEM solution that:

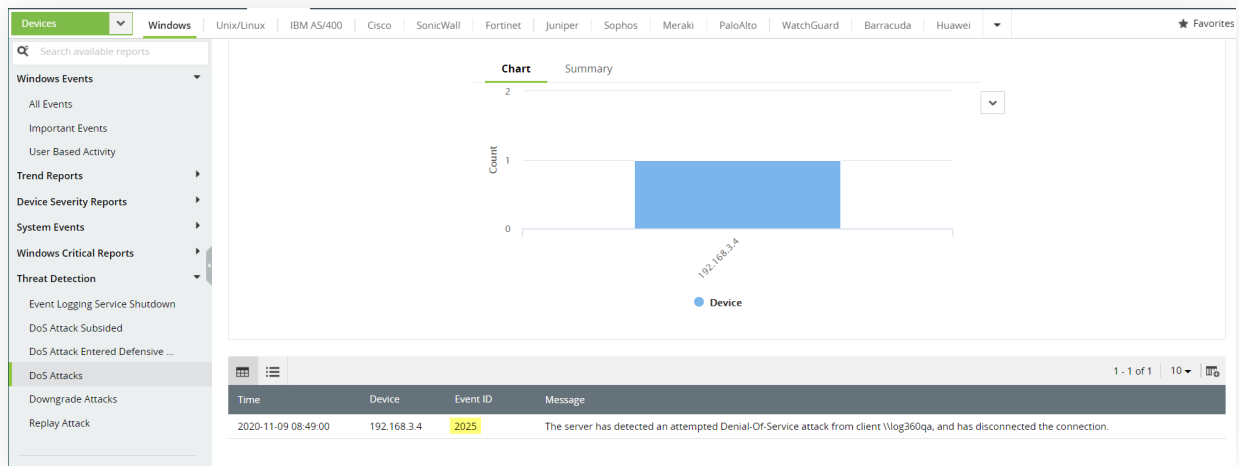
- Audits log data from network security devices, like intrusion detection systems and firewalls.
- Provides real-time alerts about DoS and DDoS attacks.
- Detects repeat connection requests from a specific IP address.
- Identifies potential attacks on important internal servers and files with instant alerts when access attempts exceed an established threshold.



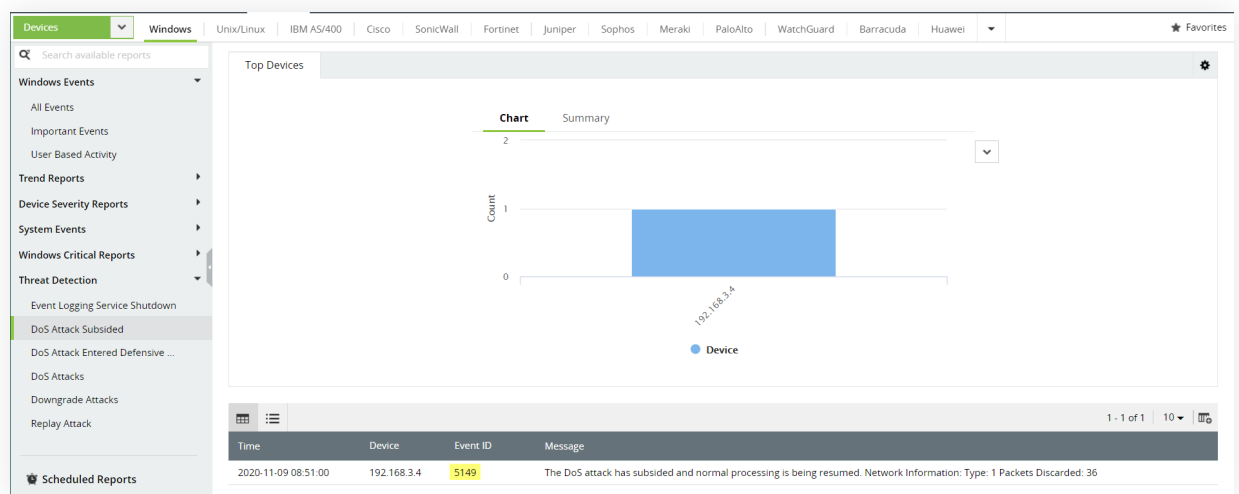
The screenshot shows the Log360 interface with a vulnerability report table. The table has columns for Time, Device, Vulnerability Name, Severity Level, CVSS Base Score, CVE, and OS. The report lists several vulnerabilities on a Windows 2003 server (192.168.2.11) detected on 2010-03-24 at 1:25:37.

Time	Device	Vulnerability Name	Severity Level	CVSS Base Score	CVE	OS
2010-03-24 1:25:37	192.168.2.11	FIN-ACK Network Device Driver Framing Information Disclosure Vulnerability	Medium	5		Windows 2003
2010-03-24 1:25:37	192.168.2.11	TCP Sequence Number Approximation Based Denial of Service	Medium	5	CVE-2004-0230	Windows 2003
2010-03-24 1:25:37	192.168.2.11	ICMP Based TCP Reset Denial of Service Vulnerability	Medium	5	CVE-2004-0790,CAN-2004-0791,CAN-2004-1060	Windows 2003
2010-03-24 1:25:37	192.168.2.11	Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness (MS03-034)	Medium	5	CVE-2003-0661	Windows 2003
2010-03-24 1:25:37	192.168.2.11	Multiple Microsoft Windows Vulnerabilities (MS04-011)	Urgent	7.6	CVE-2003-0533,CVE-2003-0663,CVE-2003-0719,CVE-2003-0806,CVE-2003-0906,CVE-2003-0907,CVE-2003-0908,CVE-2003-0909,CVE-2003-0910,CVE-2004-0117,CVE-2004-0118,CVE-2004-0119,CVE-2004-0120,CVE-2004-0123	Windows 2003
2010-03-24 1:25:37	192.168.2.11	Microsoft Windows ASN.1 Library Integer Handling Vulnerability (MS04-007)	Urgent	7.5	CVE-2003-0818	Windows 2003
2010-03-24 1:25:37	192.168.2.11	SMB Signing Disabled or SMB Signing Not Required	Medium	2.1		Windows 2003
2010-03-24 1:25:37	192.168.2.11	Enabled DCOM	Serious			Windows 2003

Vulnerability report in Log360.



DoS Attacks report in Log360. This report details attempts of DoS attacks against your network.



DoS Attack subsided report in Log360. This report shows instances of DoS attacks that have tapered off so that normal processing of requests can be resumed.



DoS Attack entered defensive mode report in Log360. This report records instances of DoS attacks where preventive measures have been activated to mitigate the attack.

Log360 also has advanced modules to manage your Active Directory space and mitigate threats to it.

# Get started with Log360.

Ready to get started with Log360?

Download

If you're still unsure, take your time and explore Log360 through a personalized demo.

Schedule a personalized demo

ManageEngine  
**Log360**

ManageEngine Log360, a comprehensive SIEM solution helps enterprises to thwart attacks, monitor security events, and comply with regulatory mandates. The solution comes bundled with a log management component that provides better visibility into network activity, incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents, ML-driven user and entity behavior analytics add-on that baselines normal user behaviors and spots anomalous user activities, threat intelligence platform that brings in dynamic threat feeds for security monitoring and aids enterprises to stay on top of attacks.

For more information about Log360, visit [manageengine.com/log-management](https://manageengine.com/log-management).

\$ Get Quote

↓ Download