What is the Internet Control Message Protocol (ICMP)?

The Internet Control Message Protocol is used to diagnose network issues over the Internet.

Learning Center

- What is a DDoS Attack?
- What is a DDoS Botnet?
- Common DDoS Attacks
- Flood Attacks
- DDoS Attack Tools
- Glossary

Learning Objectives

After reading this article you will be able to:

- Define the ICMP
- Describe how ping and traceroute work
- Understand how the ICMP protocol can be used in DDoS attacks

RELATED CONTENT

TCP/IP

UDP

Memcached DDoS Attack

What is a DDoS Botnet?

Copy article link

What is the Internet Control Message Protocol (ICMP)?

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.

What is ICMP used for?

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP. The traceroute utility is used to display the routing path between two Internet devices. The routing path is the actual physical path of connected routers that a request must pass through before it reaches its destination. The journey between one router and another is known as a 'hop,' and a traceroute also reports the time required for each hop along the way. This can be useful for determining sources of network delay.

The ping utility is a simplified version of traceroute. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender's device. Although ping does not provide data about routing or hops, it is still a very useful metric for gauging the latency between two devices. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.

Unfortunately network attacks can exploit this process, creating means of disruption such as the ICMP flood attack and the ping of death attack.

How does ICMP work?

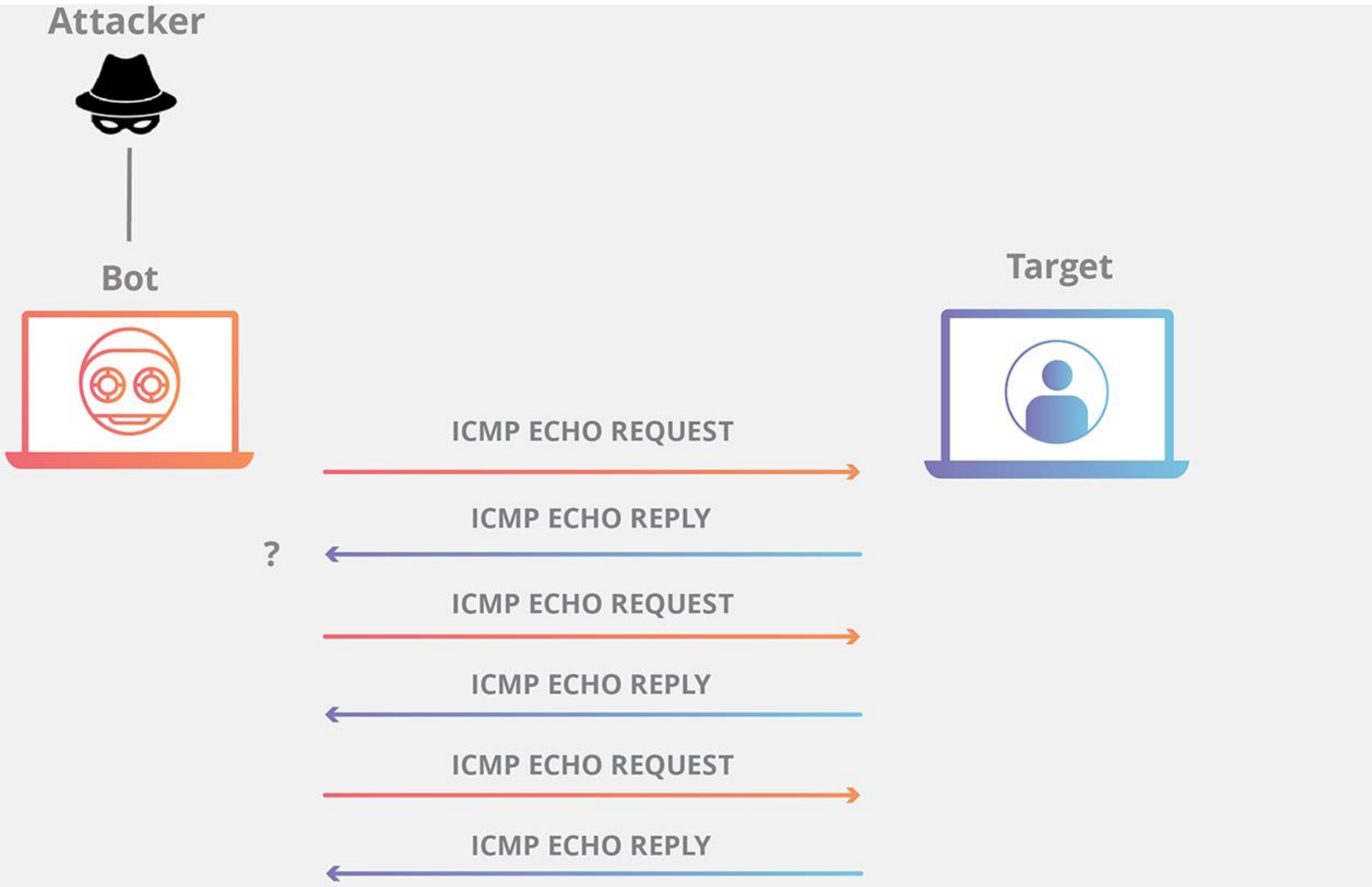
Unlike the Internet Protocol (IP), ICMP is not associated with a transport layer protocol such as TCP or UDP. This makes ICMP a connectionless protocol: one device does not need to open a connection with another device before sending an ICMP message. Normal IP traffic is sent using TCP, which means any two devices that exchange data will first carry out a TCP handshake to ensure both devices are ready to receive data. ICMP does not open a connection in this way. The ICMP protocol also does not allow for targeting a specific port on a device.

How is ICMP used in DDoS attacks?

ICMP flood attack

A ping flood or ICMP flood is when the attacker attempts to overwhelm a targeted device with ICMP echo-request packets. The target has to process and respond to each packet, consuming its computing resources until legitimate users cannot receive service.

ICMP flood attack:


Attacker
Bot
Target
ICMP ECHO REQUEST
ICMP ECHO REPLY
?
ICMP ECHO REQUEST
ICMP ECHO REPLY
ICMP ECHO REQUEST
ICMP ECHO REPLY

Ping of death attack

A ping of death attack is when the attacker sends a ping larger than the maximum allowable size for a packet to a targeted machine, causing the machine to freeze or crash. The packet gets fragmented on the way to its target, but when the target reassembles the packet into its original maximum-exceeding size, the size of the packet causes a buffer overflow.

The ping of death attack is largely historical at this point. However, older networking equipment could still be susceptible to it.

Smurf attack

In a Smurf attack, the attacker sends an ICMP packet with a spoofed source IP address. Networking equipment replies to the packet, sending the replies to the spoofed IP and flooding the victim with unwanted ICMP packets. Like the 'ping of death,' today the Smurf attack is only possible with legacy equipment.

ICMP is not the only network layer protocol used in layer 3 DDoS attacks. Attackers have also used GRE packets in the past, for instance.

Typically, network layer DDoS attacks target networking equipment and infrastructure, as opposed to application layer DDoS attacks, which target web properties. Cloudflare Magic Transit is one way to defend against network layer DDoS attacks.