FORGE

The Arkansas Cyber Defense Center

DDoS Attack

A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. A successful DoS attack consumes all available network or system resources, usually resulting in a slowdown or server crash. Whenever multiple sources are coordinating in the DoS attack, it becomes known as a DDoS attack.

Types of standard DDOS attacks:

Syn Flood: This method is most common and it occurs when an attacker sends a succession of TCP Synchronize (SYN) requests to the target in an attempt to consume enough resources to make the server unavailable for legitimate users.

UDP Flood: Similar to a SYN Flood in that an attacker uses a botnet to send a significant amount of traffic to the target server. The difference is that this attack is much faster, and rather than attempting to exhaust server resources, it seeks to consume all of the available bandwidth on the server's network link, thereby denying access to legitimate users.

SMBLoris: An application-level DDoS attack that occurs when a cyber threat actor opens multiple SMB connections to a device, maliciously consuming memory with minimal attack cost. SMB is a remote access protocol used for providing shared access to files, printers, and various communications between devices over port 445.

ICMP Flood: Occurs when an attacker uses a botnet to send a large number of ICMP packets to a target server in an attempt to consume all available bandwidth and deny legitimate users access.

HTTP Get Flood: Occurs when an attacker, or attackers, generate a significant number of continuous HTTP GET requests for a target website in an attempt to consume enough resources to make the server unavailable for legitimate users.

Why be aware of this attack?

Cybercriminals take advantage of normal behavior that occurs between network devices and servers, often targeting the networking devices that establish a connection to the internet.

What do threat actors want?

The main purpose behind a DDoS attack is the malicious consumption of resources.

How can a DDoS attack be prevented?

1. Enable firewall logging of accepted and denied traffic to determine where the DDoS may be originating.
2. Define strict "TCP keepalive" and "maximum connection" on all perimeter devices, such as firewalls and proxy servers.
3. Consider port and packet size filtering by the upstream network service provider.
4. Establish and regularly validate baseline traffic patterns (volume and type).

POWERED BY
SBA
U.S. Small Business Administration

Information provided by Forge Institute or any of its employees, contractors, or advisors does not constitute expert or technical advice for any particular matter. Due to the complex nature of cyber, individuals or companies should seek advice from their insurer, attorney or managed service provider. Nothing contained herein should be construed as consultative advice. Forge Institute bears no liability arising in connection with the information it provides. Use of Forge Institute information constitutes agreement to the legal Terms & Conditions & Privacy Policy located at www.forge.institute/terms. The Forge Institute ACDC is funded, in part, through a Cooperative Agreement with the U.S. Small Business Administration. All opinions, and/or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the SBA.

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599