

Forum:[Hack Forums](#)

Thread: [DDos attack methods explained](#)

muroseu - July 15, 2016, 4:30 am

There are 2 main types of ddos; layer 4 and layer 7. Layer 4 is your basic type of UDP or SYN attack and it works by exploiting the TCP connection. Layer 4 attacks are useful against unprotected web servers and home connections, basically anything that isn't using some form of ddos protection such as Cloudflare or Hyperfilter. Layer 4 attack power can range from 10mbps to 200gbps depending on the method used, the power of the server, and how fresh the amplification list is. Layer 4 attacks are somewhat easy to detect, but that does not mean they can't take down a ddos protected server.

Layer 7 or application layer attack is much harder to differentiate from legitimate traffic which is why it can pass right through services like Cloudflare and Incapsula. A layer 7 attack such as a HTTP GET basically connects to the server and requests a large amount of files and causes the server to crash from lack of resources. Layer 7 attacks can easily take down protected servers if they are setup correctly.

Layer 4 attack methods

UDP/UDP-Lag

- This is a pretty basic attack and is on all stressers. It sends a large number of UDP packets to the victim until it is overloaded. UDP-Lag attacks in bursts as to not hit the target offline completely.

SUDP

- This attack is the same as UDP but spoofs the requests to make it harder to mitigate.

SYN/SSYN/ESSYN

- These attacks are group because they all generally do the same thing. These attacks abuse the 3 way hand shake of the TCP protocol until the victim is overloaded.

DNS/NTP/CHARGEN/SNMP

- These attacks are an amplified UDP attack that abuses vulnerable servers by sending a spoofed request with the targets ip as the sender. The servers then send the target the information overloading the system. These attacks can range from 10gbps - 300gbps depending on many factors.

Layer 7 attack methods

XMLRPC

- This attack uses vulnerable Wordpress sites to send a massive attack.

HTTP GET/HTTP POST/HTTP HEAD

- These attacks complete the TCP 3 way handshake and then start requesting large files until the servers resources are maxed out.

SLOWLORIS

- This attack works mainly against Apache web servers by keeping a massive amount of connections open for so long that the server can no longer handle anymore legitimate traffic.

source: <https://www.hackbulletin.com>

VeloCityMods - *July 15, 2016, 4:32 am*

Awesome thread and great explanation thanks!

Not him - *July 15, 2016, 7:57 am*

I expected this thread to be some dumb shit since that's how it usually is when anyone on this forum tries explaining DoS and DoS methods but this was actually pretty nice. Good job.

hvault - *July 16, 2016, 1:34 am*

good and nice explanation, good job bro.