

Forum:[Hack Forums](#)

Thread: [\[Help\] Question about Web servers and tcp flooding](#)

XPRMX - November 1, 2018, 12:55 pm

Hello, I am asking a simple question to learn more about how tcp ddos works. Lets say I have an Xmas, essyn or some type of tcp script that sends rst/fin/ack/syn/psh etc. I send a flood to a web server running apache/nginx and ports 80/443 are open. Would the tcp flood be able to bring the website down (if it did would it be because the tcp packets went to the network therefore it downed website) or does the tcp flood attack the network/transport and the website remains unaffected? Thank you sorry but this has always bugged me not knowing.

edit: Is it also possible lets say Xmas can't bring the site down but an rst flood could?

CyberStrike - November 1, 2018, 1:16 pm

DDOS isn't something we discuss but one will not be able to keep it up infinitely nor is it an effective tactic in the long term. Well let's imagine a toilet, representing the connection from there we will represent the ddos attack as your head. For a good visual representation the following image should help:

Beyond that it's pretty much like sticking your head in a toilet flushing and when it overflows you claim victory and breaking the toilet.

XPRMX - November 1, 2018, 1:16 pm

(Nov 1, 2018 01:16 PM) SilentWatch Wrote: [\[CITE\]](#) DDOS isn't something we discuss but one will not be able to keep it up infinitely nor is it an effective tactic in the long term. Well let's imagine a toilet, representing the connection from there we will represent the ddos attack as your head. For a good visual representation the following image should help:

Beyond that it's pretty much like sticking your head in a toilet flushing and when it overflows you claim victory and breaking the toilet.

Great response but i just wanted some knowledge :(

sh4moon - November 1, 2018, 1:20 pm

(Nov 1, 2018 12:55 PM) XPRMX Wrote: [\[CITE\]](#) Hello, I am asking a simple question to learn more about how tcp ddos works. Lets say I have an Xmas, essyn or some type of tcp script that sends rst/fin/ack/syn/psh etc. I send a flood to a web server running apache/nginx and ports 80/443 are open. Would the tcp flood be able to bring the website down (if it did would it be because the tcp packets went to the network therefore it downed website) or does the tcp flood attack the network/transport and the website remains unaffected? Thank you sorry but this has always bugged me not knowing.

edit: Is it also possible lets say Xmas can't bring the site down but an rst flood could?
web servers can handle a lot of traffic. they're kind of designed for it lol. but they're still limited. a ddos sends so many packets that the server can't handle any other connections. since it can't handle the connections it just rejects them. the reason it drops the connection and can only handle

so many connections is the computer only has so many resources. the ddos uses all or most of those resources. sometimes causing a system crash.

SysAdmin - November 1, 2018, 1:41 pm

(Nov 1, 2018 01:20 PM)sh4moon Wrote: [\[CITE\]](#) web servers can handle a lot of traffic. they're kind of designed for it lol. but they're still limited. a ddos sends so many packets that the server can't handle any other connections. since it can't handle the connections it just rejects them. the reason it drops the connection and can only handle so many connections is the computer only has so many resources. the ddos uses all or most of those resources. sometimes causing a system crash.

Think of it as throwing pens at someone.

You throw one pen or two and they'll be able to catch it normally. Throw 50 pens at him at once and he'll miss most of them. Keep throwing pens at him while he's busy picking some up and he'll give up.

Replace pens with packets and there you have your explanation.

sh4moon - November 1, 2018, 1:45 pm

(Nov 1, 2018 01:41 PM)SysAdmin Wrote: [\[CITE\]](#) Think of it as throwing pens at someone.

You throw one pen or two and they'll be able to catch it normally. Throw 50 pens at him at once and he'll miss most of them. Keep throwing pens at him while he's busy picking some up and he'll give up.

Replace pens with packets and there you have your explanation.

except if you throw enough pens long enough the person will have a heart attack lol. same with the server, which crashes. that's a really good analogy. definitely using that one in the future.

CyberStrike - November 1, 2018, 1:47 pm

(Nov 1, 2018 01:16 PM)XPRMX Wrote: [\[CITE\]](#) Great response but i just wanted some knowledge :(Knowledge is cool ip reputation, white/blacklists, DPI (Deep packet inspection), and rate limiting are all there to work against you. Not to mention that often now attacks are rerouted and dropped to prevent such things. For example say a bunch of different IP's from various networks are sending a ton of traffic great. let's block them or maybe we limit the rate at which we actually accept packets from them. If it's one country that makes our job easier let's block their IP range redirect it to somewhere else where it fails. These things generally are layer 4 unless you are using a browser/script which will appear as a browser at which point layer 7, Layer 7 a WAF can probably deal with it blocking IP's and requests, layer 4 has been around forever it's not new far from it, also CloudFare service isn't terribly expensive (20-200 per month). DDOS is literally the tactic of the unskilled or frustrated.. "I tried everything and the kitchen sink ".

sh4moon - November 1, 2018, 1:55 pm

yeah, flooding a target with packets isn't the most effective way to do it. you're better off using some exploit or vulnerability. look up application layer attacks like rudy and slowloris. they're more effective in my opinion.

wirelin3 - November 1, 2018, 3:22 pm

As sh4moon said, DOS works a lot better if you can find something that makes the server work or hang.

Webservers are pretty good these days at handling static requests.

__Digital__ - November 1, 2018, 3:24 pm

DDOS is not to be spoken of here anymore. However for information like the others have told you

once you exceed the number of threads and processes the webserver can handle you will down it. In the end you will need to collapse the upload/download streams at the same time which will cause the server to go offline.

Things you will need to know:

1. Firewall evasion
2. Dos deflate evasion
3. Cloudflare detection
4. Apache/Nginx information

If the server administrator has configured things correctly you will not be able to drop them.

XPRMX - November 1, 2018, 5:07 pm

(Nov 1, 2018 03:24 PM)___Digital___ Wrote: [\[CITE\]](#) DDOS is not to be spoken of here anymore. However for information like the others have told you once you exceed the number of threads and processes the webserver can handle you will down it. In the end you will need to collapse the upload/download streams at the same time which will cause the server to go offline.

Things you will need to know:

1. Firewall evasion
2. Dos deflate evasion
3. Cloudflare detection
4. Apache/Nginx information

If the server administrator has configured things correctly you will not be able to drop them.

Thank you for this information. I did not ask how to ddos however most of the replies seemed to have dodged my question. You did not fully answer it but thank you