

Forum:[Hack Forums](#)

Thread: [DDoS \[What\]](#) [\[How\]](#)

?lvNet™ - April 27, 2013, 11:40 am

Hey guys,

Today im gonna teach u guys everything I know about DDoS. This is a guide for newbs to learn about DDoS and for them to stop opening threads about what it is.

To start everything off let me give you guys a good idea of what DDoS stands for, how it works, and methods of DDoS. Hope you guys enjoy!

DDoS stands for Distributed Denial Of Service there is also DoS which is Denial Of Service. This is used to take internet's with a IP Address (Internet Protocol Address). DDoS is a bunch of computers attacking a specific target while DoS is just 1 computer.

DDoS and DoS pretty much just send packets or memory to a internet connection then the connection cant take it and cant load any legitimate packets. Think of it as opening utorrent and torrenting a ton of stuff while watching tons of movies and having tons of links open, they take up space and over load your router. DDoS is usually performed with booters, stressers, botnets, or just a lot of people attacking with a DoS tool.

There are many unique and well known attack methods they all take down internets/websites using various methods. For example the most known and used method is UDP which is just you sending a huge amount of packets overloading the server and taking it down. Also theres SYN which just uses all the resources of a connection so no resources are left for legitimate traffic. And another well known attack method is SLOWLORIS, which is used to fake a bunch of connections to a website which hogs all the resources. The methods can also be spoofed which means it will be sending forged requests so the attack will be harder to blacklist. Most common spoofed attacks are SUDP and SSYN. All these attacks are categorized in the groups Layer 7 and Layer 4 attacks.

Layer 7 Attacks:

Spoiler ([Click to View](#))

ARME - Exploits apache and perl exhausts the memory of servers denying server to users

RUDY - Like SSYN but slower mimics user with slow internet

SLOWLORIS - Makes connections on a site and hogs resources

GET - Gets the data on the site to hog the upload speed

POST - Posts data on the site to hog the download speed

HEAD - Not to sure about this one but I think its GET and POST

And many more these attacks. Layer 7 attacks are used to take down websites.

Layer 4 Attacks:

Spoiler ([Click to View](#))

UDP - Sends huge amounts of packets

SUPD - Same as UDP but Spoofed

UDP-Lag - Like UDP except short bursts to lag the target

SSYN - Same as SYN except spoofed

SYN - Sends packets and leave small spots which confuses and overloads the server.

And others these attacks are used to attack everything websites and home connections.

To DDoS you can buy a booter/stresser or make a botnet. And to DoS you can find a program that will attack.

WARNING: DoSing from your internet connection might get you into major trouble! USE A VPN!

Note: I do not encourage DDoS or DoS this is for educational purposes only!

Hope you guys enjoy if I missed or messed something wrong please post and ill fix it.

Wide - April 27, 2013, 11:43 am

Nice tutorial man, it can help some people here

Flyn - April 27, 2013, 12:09 pm

Nice explanation for the "newbies" :)

Envy8 - April 27, 2013, 1:17 pm

Quote:Layer 7 Attacks:

Spoiler (Click to Hide)

ARME - Exploits apache and perl exhausts the memory of servers denying server to users

RUDY - Like ARME but slower mimics user with slow internet

SLOWLORIS - Makes connections on a site and hogs ports

GET - Uses get protocol to flood site

POST - Uses post protocol to flood site

HEAD - Floods page views (f5 over and over)

And many more these attacks. Layer 7 attacks are used to take down websites. Layer 7 attacks are actually application level attacks.

Layer 4 Attacks:

Spoiler (Click to Hide)

UDP - Sends huge amounts of udp packets

UDP is spoofed. Otherwise it will get automatically blocked. That's why things like LOIC only work if you have a strong enough connection to take down the target before you get blocked. You're thinking of DrDos, which is an ICMP flood (ie pinging over and over)

UDP-Lag - Like UDP except short bursts to lag the target

SSYN - Same as SYN except distributed

SYN - Sends a request, doesn't reply to ack. Wastes resources

And others these attacks are network based attacks.

Come on lol. Half that shit wasn't true :P

?lvNet™ - April 27, 2013, 3:28 pm

(Apr 27, 2013 01:17 PM)Envy8 Wrote: [\[CITE\]](#) Come on lol. Half that shit wasn't true :PThen send me the attack methods and how they work.

"The Anonymous" - April 27, 2013, 3:34 pm

Which method is the best to take down websites?

?lvNet™ - April 27, 2013, 3:39 pm

(Apr 27, 2013 03:34 PM)"The Anonymous Wrote: [\[CITE\]](#) Which method is the best to take down websites?As stated in the thread layer 7 attacks are mainly for websites but UDP and SSYN work just as well.

Zabuza? - April 27, 2013, 3:44 pm

You need to improve on your grammar and punctuation for people to take you seriously. And some of this info is not properly explained and only partially true. So, you do need to improve on a few things, but otherwise, it's pretty good. I'm sure it'll help some of the n00bs out there :P. Thanks for posting!

"The Anonymous" - April 27, 2013, 3:44 pm

Okay. Thanks for the advise. Great and HQ tutorial.

?IvNet™ - April 27, 2013, 4:00 pm

(Apr 27, 2013 03:44 PM)ceoff Wrote: [\[CITE\]](#) You need to improve on your grammar and punctuation for people to take you seriously. And some of this info is not properly explained and only partially true. So, you do need to improve on a few things, but otherwise, it's pretty good. I'm sure it'll help some of the n00bs out there :P. Thanks for posting!Looked through it and the grammar seems fine, also if somethings wrong please tell me what's wrong and whats right.

Envy8 - April 27, 2013, 4:56 pm

SSYN will take down any website stronger than udp if they have ddos mitigation. if not, use udp. If you know any weakness or its apache version, use a l7 that works

?IvNet™ - April 27, 2013, 4:58 pm

(Apr 27, 2013 04:56 PM)Envy8 Wrote: [\[CITE\]](#) SSYN will take down any website stronger than udp if they have ddos mitigation. if not, use udp. If you know any weakness or its apache version, use a l7 that worksI updated with the SYN. But wat about my other "errors"?

Envy8 - April 27, 2013, 5:00 pm

read the post I made. I bolded the corrections.

SouqlRS - April 27, 2013, 7:18 pm

Thanks for the tutorial, now I know what the attack types are. :)

But you didn't list TCP? What's the difference between duo and tcp?

?IvNet™ - April 27, 2013, 7:38 pm

(Apr 27, 2013 07:18 PM)SouqlRS Wrote: [\[CITE\]](#) Thanks for the tutorial, now I know what the attack types are. :)

But you didn't list TCP? What's the difference between duo and tcp?Im pretty sure TCP is SYN or is similar to SYN

Whiisp3r - April 27, 2013, 8:26 pm

what bots can i use? or stressers or whatever. im new to all this stuff. so basically, all i need is an IP address and i can overload someones router causing them to D/C, right? thats what my understanding of it is so far.

Understalker - April 27, 2013, 8:27 pm

Not a bad tutorial at all, good job men

killamaster7888 - April 27, 2013, 9:02 pm

(Apr 27, 2013 08:26 PM)Whiisp3r Wrote: [\[CITE\]](#) what bots can i use? or stressers or whatever. im new to all this stuff. so basically, all i need is an IP address and i can overload someones router causing them to D/C, right? thats what my understanding of it is so far.

All you need is the IP to send packets to someone's router. Bots infected people with botnets.

Stressers are bought. Stressers are the easiest to use. Stressers use servers bought by the owners instead of bots. You could DoS a weak home connection with programs such as LOIC.

?IvNet™ - April 27, 2013, 9:04 pm

(Apr 27, 2013 08:26 PM)Whiisp3r Wrote: [\[CITE\]](#) what bots can i use? or stressers or whatever. im new to all this stuff. so basically, all i need is an IP address and i can overload someones router causing them to D/C, right? thats what my understanding of it is so far. Bots as in people that download and execute ur virus, look into botnet. And for booters/stressers look in the marketplace stress testing section.

Dizzy. - April 27, 2013, 9:59 pm

(Apr 27, 2013 08:26 PM)Whiisp3r Wrote: [\[CITE\]](#) what bots can i use? or stressers or whatever. im new to all this stuff. so basically, all i need is an IP address and i can overload someones router causing them to D/C, right? thats what my understanding of it is so far.

[BAM!](#)

There's a link to the marketplace for Stressers/Booters.

Personally I am using Olympus Stresser. Click on my signature to check it out.

Upgraded - April 27, 2013, 11:14 pm

Tutorial looks good.

Learned some new attack methods.

Will be good for beginners.

?IvNet™ - May 9, 2013, 7:20 pm

Still seeing some people asking about DDoS and DoS and booters. Please advice anyone to read this for help.

Clubs - May 10, 2013, 3:46 am

"SYN - Is like UDP but will bypass DoS migration if the target has it"
Seriously?

Skwer - May 10, 2013, 3:57 am

Thanks for explaining this, realy helped me!

reypupil18 - May 10, 2013, 6:41 am

Nice Tutorial, it helps me very much. Thank you :)

Finlandia Vodka - May 21, 2013, 5:13 am

Nice tutorial. Helped me a lot. Thank you :D

Fly By Night - May 21, 2013, 5:21 am

Tutorial looks good, Thanks mate. I'll link this to my newb friend.

Anon?M ID - May 21, 2013, 5:25 am

this is a HQ guide.

thanks for the share :D

AnonymousPirate - May 21, 2013, 8:41 am

awesome. thanks for the insight :) appreciated

Tom1337 - May 21, 2013, 8:52 am

Nice tutorial man it's explained nicely, good for the noobs :P

Evazed™ - May 21, 2013, 10:22 am

Good TuT for beginners, didn't see too many grammar issues, but i'm sure it will help out noobs.

?IvNet™ - May 21, 2013, 6:20 pm

(May 21, 2013 10:22 AM)iSellVPS Wrote: [\[CITE\]](#) Good TuT for beginners, didn't see too many grammar issues, but i'm sure it will help out noobs.Thanks for digging this thread out :3 And thanks for the compliment.

WinzR - May 21, 2013, 6:56 pm

Which method is the best to take down websites?

?IvNet™ - May 21, 2013, 7:11 pm

(May 21, 2013 06:56 PM)WinzR Wrote: [\[CITE\]](#) Which method is the best to take down websites? UDP can get the job done but if not try slowloris or SYN/SSYN.

Goodies - May 21, 2013, 7:12 pm

Many if these are not in-depth at all :/ but informative nonetheless. Thanks!

?IvNet™ - May 21, 2013, 7:17 pm

(May 21, 2013 07:12 PM)Goodies Wrote: [\[CITE\]](#) Many if these are not in-depth at all :/ but informative nonetheless. Thanks!As long as new members can understand it they'll catch on and maybe be more interested so they can do research of there own.

FroStorm - May 21, 2013, 7:19 pm

Nice explanation, I actually learned something about the attack types from this.