

Forum:[Hack Forums](#)

Thread: [Hacking Tutorial | DDoS and DoS | Everything explained | DDoS Scripts |](#)

SIM-2223238 - May 23, 2015, 3:36 pm

DDoS Tutorial | Everything Explained

With using Control+F you can navigate easily trough the thread

Sections

DoS/DDoS

What is DDoS actually?

Is it illegal? Will I get easily caught?

How to DDoS?

Spoofing

How to prevent a DDoS Attack?

DDoS Ampflication.

Layer 4 and Layer 7

Scripts.

Websites that allows spoofing.

DoS/DDoS

DoS (Denial of Service)

DDoS (Distributed Denial Of Service)

They both have a large difference, DoS is sending from one location, and DDoS is sending from multiple locations.

What is DDos actually?

DDoS is basicly sending out packets, and preventing the usert from connecting to the destination. Basicly the user is trying to connect 1.1.1.1, And the attacker is sending packets to 1.1.1.1 to prevent the user from connecting.

When the host isnt being ddosed :

User > Testing Connection > 1.1.1.1 > Succesfully connected.

When a DDoS attack is active :

User > Testing Connection > Connection failed > Timeout on 1.1.1.1

Is it illegal? Will I get easily caught?

In some ways, DDoS is legal, but mostly DDoS is illegal, DDoS is also called Stress-testing, that means you are testing your server, to see If your server can handle a large amount of bandwidth in. But DDoS is mostly illegal, and for illegal purposes used, like attacking homeconnections without permission.

Is it easy to get caught? No, depends on where you are sending the attack from, you can hide your location with a VPN (Virtual Private Network).

How to DDoS/DoS

A denial of service attack is basicly sending out packets from your location to a destination, to prevent a user connecting to the destination.

You can DoS simply with using Control+R and type in CMD.exe, then type something like ping

(host), this is basically ping the destination.

Pinging won't do much, So you can buy a server and send packets from that, that will make you getting caught a lower chance, most hosts doesn't allow DDoS attacks, and will simply cancel your dedicated server/VPS.

You need a host that allows spoofing, So your destination doesn't know where to send the abuse report to, this will prevent you from getting your server canceled Not all hosts allow spoofing

Spoofing

What is spoofing you ask? Spoofing is basically hiding your host so the destination doesn't know, where the packets come from, Here is how spoofing looks like :Spoiler [\(Click to View\)](#)

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/7/72/IP_spoofing_en.svg/2000px-IP_spoofing_en.svg.png[/img]

How to prevent DDoS attacks?

Preventing DDoS attacks, isn't that simple you think it is, There are a lot of different ways to stop DDoS attacks, You can ask for DDoS Protection by your host, or you can get mitigation, mitigation is basically spreading all the packets to a set of servers so your main server doesn't get too much packets in, a reverse proxy can be used also.

How to block XMLRPC attacks?

Simply block the Wordpress Useragent, and make them redirect to a blank page.

DDoS Amplification

What is DDoS amplification you ask? Well it's basically an amplification of your DDoS attacks, there are a lot of different methods to use for amplification attacks, You double your DDoS attacks using an amplification method.

Here is a list of different amp (amplification) methods :

[\(Click to View\)](#)NTP

SNMP

MSSQL

DNS

SSDP

tFTP

Chargen

OVH

NETBIOS

QUAKE

Layer 4 and Layer 7

What is the difference about Layer 4 and Layer 7 you ask?

Layer 4 is basically sending out data/packets.

Layer 7 is sending out fake users, to a webserver.

List of Layer 4 and Layer 7 methods.

Layer 4 [\(Click to View\)](#)NTP

SNMP

MSSQL

DNS

SSDP

tFTP

Chargen
OVH
NETBIOS
QUAKE
UDP
TCP

Layer 7 ([Click to View](#))ARME

GET
HEAD
POST
Rand
RUDY
XMLRPC
Goldeneye
Pyloris

Scripts

Well, you need scripts also before DDoSing, so here is a thread where a large amount of scripts got posted :)

<https://hackforums.net/showthread.php?tid=4230629>

Compile using chmod 777 (file)

Scanning and Filtering.

Scanning and filtering, is really important for your amplification methods.

Scanning is basically searching around the world, for IPs that your amplification method can use, to double the attack amount.

How do you filter you ask me?

Here are some filter scripts, made by QuezzStresser.

<http://quez-stresser.com/joomlafilter.txt>

<http://quez-stresser.com/mssqlfilter.txt>

<http://quez-stresser.com/xmlrpcfilter.txt>

<http://quez-stresser.com/chargenfilter.txt>

Use them with installing PHP.

Filtering is testing the timeout on the IPs you scanned, the lower the timeout the higher your amp rate is.

Websites that allow spoofing.

<http://www.ecatel.info>

<https://www.slaskdatacenter.pl>

<http://blazingfast.io> | Layer 7 only.

use OVH for scanning.

Did you like my tutorial thread? Please leave a thanks, Give me some other subjects, I should write a tutorial about.

I dont believe ddos is hacking.....

Delevingne - May 23, 2015, 3:44 pm

wow please dont hack me with the ddos exploit.

OT: seems like a nice thread.

Perfectionist - May 23, 2015, 4:08 pm

Nice thread, but could you make the spoofing image a bit smaller?

Comedic - May 23, 2015, 4:21 pm

Very well written thread, Aggron. ?

Luciferum - May 23, 2015, 7:35 pm

Good tutorial, but this is not "Hacking", good though! ?

Katie Stevens - May 23, 2015, 7:39 pm

really nice TUT OP!! <3 Cheers

imcullenm - May 23, 2015, 7:40 pm

This was very detailed man! Stay High quality. Great job.

Atharva - May 23, 2015, 9:42 pm

Informative thread.

Thanks for the share.

Can you make a tutorial on scanning and filtering?

Thanks.

hahdbwoannniabs - May 23, 2015, 9:46 pm

(May 23, 2015 03:36 PM)Aggron Wrote: [\[CITE\]](#) How to DDoS/DoS

A denial of service attack is basicly sending out packets from your location to a destination, to prevent a user connecting to the destination.

You can DoS simply with using Control+R and type in CMD.exe, then type something like ping (host), this is basicly pinging the destination.

Pinging wont do much, So you can buy a server and send packets from that, that will make you getting caught a lower chance, most hosts doesnt allow DDoS attacks, and will simply cancel your dedicated server/VPS.

You need a host that allows spoofing, So your destination doesnt know wher e to send the abuse report to, this will prevent you from getting your server canceled Not all hosts allow spoofing

Spoofing

What is spoofing you ask? Spoofing is basicly hiding your host so the destination doesnt know, where the packets come from, Here is how spoofing looks like :Spoiler [\(Click to View\)](#)

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/7/72/IP_spoofing_en.svg/2000px-IP_spoofing_en.svg.png[/img]

You have no idea what you're talking about. The entire point of spoofing is the fact that without spoofing, DoS wouldn't be possible in the first place. TCP/UDP/SSYN/XSYN/etc DoS is achieved when the server receives a packet from an IP that doesn't actually exist, then the server attempts to respond to the packet by sending a packet to the nonexistent IP and waits for a response. This means that the server will be waiting for something that doesn't even exist. So many of these packets are sent that it blocks actual people from accessing the server.

SIM-2223238 - May 24, 2015, 4:36 am

(May 23, 2015 09:46 PM)nothing.nobody Wrote: [\[CITE\]](#) You have no idea what you're talking about. The entire point of spoofing is the fact that without spoofing, DoS wouldn't be possible in the first place. TCP/UDP/SSYN/XSYN/etc DoS is achieved when the server receives a packet from an IP that doesn't actually exist, then the server attempts to respond to the packet by sending a packet to the nonexistent IP and waits for a response. This means that the server will be waiting for something that doesn't even exist. So many of these packets are sent that it blocks actual people from accessing the server. Why the hell wouldn't be DoS possible, without spoofing? Spoofing is basically hiding the source.

DoS is basically sending traffic to a location, If I would ping you now, and you monitor all incoming traffic, You would see my IP right?
Spoofing is to hide the source.

moonlimer - May 24, 2015, 4:43 am

nice tut, precise and easy to understand. thanks

hahdbwoannniabs - May 24, 2015, 5:55 am

(May 24, 2015 04:36 AM)Aggron Wrote: [\[CITE\]](#) Why the hell wouldn't be DoS possible, without spoofing?
Spoofing is basically hiding the source.

DoS is basically sending traffic to a location, If I would ping you now, and you monitor all incoming traffic, You would see my IP right?
Spoofing is to hide the source.

Sigh... I'm doing my best to explain this to you without being vulgar. You can't DoS with hosts that don't allow spoofing, and the reason isn't because you'll get tracked, it's because DoS is not achievable without packet spoofing. Sending "traffic" to a location isn't DoS at all, otherwise I'd be DoS'ing HF right now according to your definition because I'm connecting to it.

Don't make threads attempting to explain things you don't even know yourself.

Crory - May 24, 2015, 6:06 am

Vouch for Aggron. Nice Tutorial for beginner.

Regards,
~Crory

NerdNational - July 5, 2015, 2:32 am

Well written so that even the most simple can understand. I just wondering why there isn't a example on how to create one for the people who wouldn't know. but other then that 10/10

MafiaServ - July 5, 2015, 5:13 am

Nice elaborated tutorial, covered up a lot of DDoS related questions. Scripts, filters and host's info also given.

Job well done OP. Appreciated. ?

SIM-2223238 - July 5, 2015, 6:22 am

Need more information to be posted on the thread? PM me with questions.

int main() - July 5, 2015, 6:45 am

I'm sorry, but this is a very very poor explanation.

Th3PonyWizard - July 5, 2015, 7:04 am

A lot of spelling issues.

Quote:DDoS is basically sending out packets, and preventing the user from connecting to the destination.

Basically the user is trying to connect 1.1.1.1, And the attacker is sending packets to 1.1.1.1 to prevent the user from connecting. what if I'm attacking the DNS server, so the user is stuck trying to connect to hostname instead of IP?

what if I'm staying within the threshold of the server's concurrent bandwidth? That's still an attack. The user still connects. I'm just lagging the connection process.

Quote:In some ways, DDoS is legal, but mostly DDoS is illegal Geez. 10/10 Wording.

Quote:You need a host that allows spoofing, So your destination doesn't know where to send the abuse report to, this will prevent you from getting your server canceled Not all hosts allow spoofing Every host "allows" spoofing. Spoofing is done within the networking layers (3rd one, specifically) has no relation to the host whatsoever

Quote:What is spoofing you ask? Spoofing is basically hiding your host so the destination doesn't know, where the packets come from, Here is how spoofing looks like : You also demonstrated Amplification / Bounce-back theory in the same picture without bothering to mention it. Spoofing at it's generic definition is merely editing out the source IP header of the packet. the IP doesn't have to exist.

Quote:Preventing DDoS attacks, isn't that simple you think it is, There are a lot of different ways to stop DDoS attacks, You can ask for DDoS Protection by your host, or you can get mitigation, mitigation is basically spreading all the packets to a set of servers so your main server doesn't get too much packets in, a reverse proxy can be used also. SHIT EXPLANATION.

Quote:Here is a list of different amp (amplification) methods : You'll throw me a list of meaningless protocols and write amplification, but you won't explain a single thing. Bravo!

Quote:What is the difference about Layer 4 and Layer 7 you ask?

Layer 4 is basically sending out data/packets.

Layer 7 is sending out fake users, to a webserver. "basically send out data/packets" explanation of somebody that has no idea what he's writing about fake users? the fuck you're on about? no no and no

to be blunt

you have absolutely no idea what you're on about, it's sorta clear you learnt everything you know based off using booters without actual networking background

Enter Down - July 5, 2015, 7:42 am

```
[root@we ~]# gcc scansnmp.c -o scansnmp -pthread
scansnmp.c:32: warning: data definition has no type or storage class
scansnmp.c: In function 'flood':
scansnmp.c:37: warning: cast from pointer to integer of different size
scansnmp.c: In function 'main':
scansnmp.c:155: warning: cast to pointer from integer of different size
```

how to excus the file .c scanner ? help me

NervyGunSage - July 5, 2015, 8:21 am

nice not bad good work mate.

BlankDreams - July 8, 2015, 12:55 pm

Cool And simple TUT ,Maybe you would like to go deeply with volumetric DDOS and application DDOS ,Ports ,Changing the method ,Making sure the attack is being going through the security of the target ,Getting zombies etc

Jamiechang1 - July 9, 2015, 10:03 am

How do you use the filter scripts with PHP? New here.

XxTheRealModzxX - July 9, 2015, 6:28 pm

Good job keep up the good work:D :wow:

Undoxability - July 9, 2015, 6:40 pm

Very nice tutorial mate! Will use!

Sennheiser - July 9, 2015, 6:47 pm

(May 24, 2015 04:36 AM)Aggron Wrote: [\[CITE\]](#) Why the hell wouldnt be DoS possible, without spoofing?

Spoofing is basicly hiding the source.

DoS is basicly sending traffic to a location, If I would ping you now, and you monitor all incoming traffic, You would see my IP right?

Spoofing is to hide the source.

Why not spoof a vpn?

So when they hit the ip im spoofing it wont do anything??????

SIM-2223238 - July 9, 2015, 6:50 pm

(Jul 9, 2015 06:47 PM)Sennheiser Wrote: [\[CITE\]](#) Why not spoof a vpn?

So when they hit the ip im spoofing it wont do anything??????

What the fuck are you trying to say?

Sennheiser - July 10, 2015, 12:14 am

(Jul 9, 2015 06:50 PM)Aggron Wrote: [\[CITE\]](#) What the fuck are you trying to say?

I wanna spoof my vpn ip so when i connect to skids they see 6.9.6.9 <3

why can't I? Assuming the server allows spoofing?

Since you can ddos with spoofed ips?

Or is there something missing here?

SIM-2223238 - July 10, 2015, 3:11 am

(Jul 10, 2015 12:14 AM)Sennheiser Wrote: [\[CITE\]](#) I wanna spoof my vpn ip so when i connect to skids they see 6.9.6.9 <3

why can't I? Assuming the server allows spoofing?

Since you can ddos with spoofed ips?

Or is there something missing here?

You cannot spoof your VPN?

Sennheiser - July 10, 2015, 7:59 am

(Jul 10, 2015 03:11 AM)Aggron Wrote: [\[CITE\]](#) You cannot spoof your VPN?
But why is that?

If we can spoof ips for a ddos attack to hide the server, why not a vpn?

SIM-2223238 - July 10, 2015, 8:02 am

(Jul 10, 2015 07:59 AM)Sennheiser Wrote: [\[CITE\]](#) But why is that?

If we can spoof ips for a ddos attack to hide the server, why not a vpn?
Its hard to explain, but its just not possible.

Sennheiser - July 10, 2015, 8:07 am

(Jul 10, 2015 08:02 AM)Aggron Wrote: [\[CITE\]](#) Its hard to explain, but its just not possible.
Image doe, spoofing ip for vpn how troll it would be <3

Unkn0wnScript - July 10, 2015, 10:28 am

Nice post :) Really clears things up ;)

OGMaco - July 11, 2015, 9:56 am

lol nice thread bro learned something again

paradox305 - November 18, 2015, 2:50 am

(May 23, 2015 09:46 PM)hahdbwoannniabs Wrote: [\[CITE\]](#) You have no idea what you're talking about. The entire point of spoofing is the fact that without spoofing, DoS wouldn't be possible in the first place. TCP/UDP/SSYN/XSYN/etc DoS is achieved when the server receives a packet from an IP that doesn't actually exist, then the server attempts to respond to the packet by sending a packet to the nonexistent IP and waits for a response. This means that the server will be waiting for something that doesn't even exist. So many of these packets are sent that it blocks actual people from accessing the server.

I TOO COUNT ON YOU .SPOOFING SOUNDDDS GOOD ONLY WHEN THERE IS NO IP IN EXISTENCE WHICH SENDS THE PACKETS TO THE DESTINATION SERVERS

GOD OF SARADOMIN - November 18, 2015, 3:42 am

nice tutorial bro very helpful thx

Landchester_Turtle - December 4, 2015, 6:16 am

How do you get the people to preform a ddos attack?

SIM-2223238 - December 4, 2015, 9:57 am

(Dec 4, 2015 07:16 AM)Landchester_Turtle Wrote: [\[CITE\]](#) How do you get the people to preform a ddos attack?

Touch their wieners a little bit.

GOD OF SARADOMIN - December 4, 2015, 10:37 am

if i want to hate website which layer exactly i should use ?

BigDap - December 8, 2015, 5:07 pm

>needs XMLRPC filter

>site is gone

8uB2iH4uS4oM3bE2h - January 10, 2016, 2:23 pm

(Jul 10, 2015 08:07 AM)Sennheiser Wrote: [\[CITE\]](#) Image doe, spoofing ip for vpn how troll it would

be <3

If its possible then you still couldn't connect anywhere because response from the server goes to spoofed IP.

SIM-2223238 - January 10, 2016, 2:31 pm

(Jan 10, 2016 03:23 PM)8uB2iH4uS4oM3bE2h Wrote: [\[CITE\]](#) If its possible then you still couldn't connect anywhere because response from the server goes to spoofed IP.
you really dont understand him do you?

8uB2iH4uS4oM3bE2h - January 10, 2016, 3:41 pm

I guess no..

TiOneDDoSso - January 11, 2016, 10:12 am

(May 24, 2015 05:55 AM)hahdbwoannniabs Wrote: [\[CITE\]](#) Sigh... I'm doing my best to explain this to you without being vulgar. You can't DoS with hosts that don't allow spoofing, and the reason isn't because you'll get tracked, it's because DoS is not achievable without packet spoofing. Sending "traffic" to a location isn't DoS at all, otherwise I'd be DoS'ing HF right now according to your definition because I'm connecting to it.

Don't make threads attempting to explain things you don't even know yourself.

You are right and wrong. Suppose i have 1 gbps port and victim can handle max 20 mbps by sending just 30 mbps victim modem can't handle the bandwidth received and this cause a denial of service . As you see in the example Ip header modification (spoofing) isn't needed at all.

Another crazy and stupid example will be victim site hosted in a server with 5 GB of hdd ,if victim site has a page that called in certain method cause error in error log by sending an huge amount of request you can saturate memory causing denial of service .

Third and last stupid example will be a site that has 100 GB of max bandwidth monthly, downloading 1 GB file 100 times cause denial of service because of bandwidth exceeded.

Obviously in 2016 limit of bandwidth and portspeed (a part of home modems) are bigger, but you can't absolutely say that isn't possible to do DoS without spoofing .

Sorry for bad english and best regards ?

Mr.Police - January 12, 2016, 8:09 am

I dont know why, but the most of these "last know" booters etc. aint working anymore..anyone know reason why they are so weak ? is there a new way of protection or what ? I was thinking to buy 5 top-best booters on HF and activate them on same time so I can get results, what do you think would I success ? anyway...corrupted media are my targets :D

Thespento - January 12, 2016, 1:07 pm

thank mate i could now understand what is Ddos more i was what the hell is that XD :P well i like your TUT

8uB2iH4uS4oM3bE2h - January 13, 2016, 8:46 am

(Jan 12, 2016 09:09 AM)Mr.Police Wrote: [\[CITE\]](#) I dont know why, but the most of these "last know" booters etc. aint working anymore..anyone know reason why they are so weak ? is there a new way of protection or what ? I was thinking to buy 5 top-best booters on HF and activate them on same time so I can get results, what do you think would I success ? anyway...corrupted media are my targets :D

Most of these are scams, better buy or crack vps because you can modify attacks as you like. That allows you bypass firewall and crash server without having huge bandwidth. Ofc with huge

bandwidth like 10Gbps would be much easier.. But also its easy to drop these stressers.

Mr.Police - January 13, 2016, 10:13 am

(Jan 13, 2016 09:46 AM)8uB2iH4uS4oM3bE2h Wrote: [\[CITE\]](#) Most of these are scams, better buy or crack vps because you can modify attacks as you like. That allows you bypass firewall and crash server without having huge bandwidth. Ofc with huge bandwidth like 10Gbps would be much easier.. But also its easy to drop these stressers.

Thank you for those kind of information. Im gonna try to do something like that to :D

ra2cod - February 25, 2016, 3:10 pm

Hello ..

i have a little Question please ... there is a University website if we try to ddos normally the ip got banned But ... if too much students open the website at same time ... of course there is no ban ... so the Question is here Can we DDOS Attack using http Requests and not TCP/IP Requests??? cause in tcp/ip there is ban thing ... by the way , the Firewall used is WDS i Hope someone Can Answer on this .

Thanks :)

ScooterDeLobos - February 25, 2016, 4:14 pm

(Feb 25, 2016 04:10 PM)ra2cod Wrote: [\[CITE\]](#) Hello ..

i have a little Question please ... there is a University website if we try to ddos normally the ip got banned But ... if too much students open the website at same time ... of course there is no ban ... so the Question is here Can we DDOS Attack using http Requests and not TCP/IP Requests??? cause in tcp/ip there is ban thing ... by the way , the Firewall used is WDS i Hope someone Can Answer on this .

Thanks :)

You're getting your terminologies/technologies mixed up. HTTP is TCP/IP, but on a higher layer of the OSI model (look it up). What you're trying to do will require the use leasing, lining up, and brute force through many, many proxies and different software.

Here-- <http://hackforums.net/showthread.php?tid=646865>

Missedcalls - February 25, 2016, 5:11 pm

It's well put together. I'd say it's a good place to start for any novice.

Reece Morgan - February 25, 2016, 7:55 pm

Quote:A denial of service attack is basicly sending out packets from your location to a destination, to prevent a user connecting to the destination.

You can DoS simply with using Control+R and type in CMD.exe, then type something like ping (host), this is basicly pinging the destination.

Pinging wont do much, So you can buy a server and send packets from that, that will make you getting caught a lower chance, most hosts doesnt allow DDoS attacks, and will simply cancel your dedicated server/VPS.

Please refer to the replies from this thread: <https://hackforums.net/showthread.php?tid=5180764>

@Jupiter - February 25, 2016, 10:15 pm

Posting here for the read tomorrow. Looks nicely put OP. Can't wait to read it

?MIN?M - February 26, 2016, 4:08 am

What a great day to be high quality. Lol. Bookmarked.

SIM-2223238 - February 26, 2016, 5:31 am

Thanks for supporting the thread, feel free to ask any question.

Echtaar - February 26, 2016, 5:37 am

Thaaaaaaaaannnnnnkkksssssss !!!

ra2cod - February 26, 2016, 2:20 pm

(Feb 25, 2016 05:14 PM)ScooterDeLobos Wrote: [\[CITE\]](#) You're getting your terminologies/technologies mixed up. HTTP is TCP/IP, but on a higher layer of the OSI model (look it up). What you're trying to do will require the use leasing, lining up, and brute force through many, many proxies and different software.

Here-- <http://hackforums.net/showthread.php?tid=646865>
Well to be Honest i am not so good in this thing so if u can Explain more and thanks or if u want PM me with more infos (but about Http is TCP/IP i know what u are meaning)

Thank you :)

motherrussia711 - March 7, 2016, 1:46 pm

very nice sir!

Chaorii - March 7, 2016, 6:07 pm

Nice thread with a lot of information in details. Good job.

Brain Dead - March 8, 2016, 4:39 am

Nice, could you maybe make the spoofing image a bit smaller?

JK1337 - March 8, 2016, 8:08 am

Very well written!

Nice!

Deveser - March 8, 2016, 8:15 am

Very well written thread!

thanks a lot bro

dracau18 - March 8, 2016, 9:02 am

Your thread is very well written, you can learn a lot of thing if you read it entierly

redlightrouter - March 8, 2016, 10:06 am

(May 23, 2015 04:08 PM)Perfectionist Wrote: [\[CITE\]](#) Nice thread, but could you make the spoofing image a bit smaller?

Just put " width="500" " in front of the img source (in inspect element ofcourse)

jackvale - March 18, 2016, 5:07 am

DDoS is not hacking but this tutorial is awesome for biggner for DDoser.

dellman - April 4, 2016, 3:36 am

Incredible tut! Starting reading some but realised that I have work to do so saving this one for later. Been interested in DDoS since my brother started buying them for Minecraft server attacks. Thought it's an interesting approach and certainly can be useful!

Thanks for the share.

Taeyeon - April 4, 2016, 2:20 pm

thanks for the share very informative

fl0cka - July 24, 2016, 7:24 pm

good tutorial, thank you for sharing

THC - July 25, 2016, 11:42 am

OP you should update the link to <http://quezstresser.com/chargenfilter.txt> etc, the old domain listed in your tut is no longer up!

Otherwise nice tutorial, pretty good for some of the L33t ass beginners.

ComplexSkills - August 6, 2016, 6:16 pm

Test my vpn, heres my Skype: jack.flexy

Root Kit - August 6, 2016, 11:03 pm

Thank you now i know what DDoS is :D :D

ambitions101 - August 7, 2016, 7:59 am

here are some IPs to practice. 166.137.102.50 and 54.165.241.61 have fun

.Unknown. - August 7, 2016, 12:29 pm

This was very helpful, thanks.

RouterNets - October 20, 2016, 8:35 am

(May 23, 2015 07:35 PM)LulzLegion Wrote: [\[CITE\]](#) Good tutorial, but this is not "Hacking", good though! ?

ddos can be considered as hacking at a certain point of veiww. you exploit a vulnerability by scanning the ipv4 range and if the routers or servers are vulnerable to the exploit, they are either bruteforced or password obtained and added to a botnet. that makes ddos considered as hacking nowadays.

BannedOffline - October 20, 2016, 11:06 pm

(Oct 20, 2016 08:35 AM)RouterNets Wrote: [\[CITE\]](#) ddos can be considered as hacking at a certain point of veiww. you exploit a vulnerability by scanning the ipv4 range and if the routers or servers are vulnerable to the exploit, they are either bruteforced or password obtained and added to a botnet. that makes ddos considered as hacking nowadays.

Pls oh nooo can't handle the cringe ??????