

Forum:[Hack Forums](#)

Thread: [\[TUT\] The BEST Way To Attack HOME CONNECTIONS! || Dos || nMaP](#)

terminal - September 9, 2012, 6:51 am

The MOST EFFECTIVE DoS Method!

1.

The tools you will need for this tutorial is as follows:

nMap - <http://nmap.org/dist/nmap-6.01-setup.exe>

A DoS Tool -

<http://sourceforge.net/projects/loic/>

(I am suggesting LOIC because its free and easy to use. In no way do I condone the use of LOIC)

2.

Harvest an IP from a victim, you can do this using an IP Grabber which you can host on SPAM. (PM me for the PHP Script!)

3.

Once you have your IP address that you want to attack, open up nMaP. Enter the IP in the target box and enter this into the command box:

Code nmap -T4 -A -v -Pn IP 456.123.784.678

4.

Hit Scan!

5.

As the default profile for a scan is 'Intense' it will take around 4 minutes to complete the scan. Once the scan is done, search through the scan results until you find a list of the vulnerable ports, these are the ports we will attack!

6.

Open up LOIC and enter the victims IP in the IP box. Then click 'Lock On'. Make the TCP/UDP message 30, the method TCP and the thread 900. For the port box, enter one of the vulnerable ports from the nMaP scan.

7.

Hit IMMA CHARGING MAH LAZOR!

8.

Sit back and relax for a while.

9.

To find out if your target has been taken down ping there IP address through CMD:

Code ping 456.123.784.678

The IP: 456.123.784.678, is entirely fictional, I have not knowingly published this IP seeking an attack.

I am NOT RESPONSIBLE for anything you do regarding the material is this tutorial!

AND FOR THE LOVE OF GOD, USE A VPN!

alignment - September 9, 2012, 6:53 am

Nice tutorial,
Well written.

Thanks for this.

a-snow - September 9, 2012, 9:35 am

Thank you for writing this.. This is really helpful

chubbz lmfao - September 9, 2012, 10:02 am

nice share

going to try this soon...

Salvatore - September 9, 2012, 10:39 am

Easy, clean and nice tutorial. Thanks for the share :)

Pvm_Polo - September 9, 2012, 11:45 am

Very nice tutorial and well written thank you

terminal - September 9, 2012, 11:00 pm

Feel free to PM me if you need any help with this, as I am at school at the moment, my replies will be a little slow.

wezio - September 10, 2012, 1:49 am

When u say use a vpn, u do mean to dos from a VPN controlled computer right?

L7aj7ammo - September 10, 2012, 3:06 am

Easy, clean and nice tutorial. Thanks for the share :)

autorunman22 - September 10, 2012, 4:13 am

is there a much better software other than loic there? im just asking what else can you recommend

hobovision - September 10, 2012, 4:21 am

Need a good FREE Vpn, can someone please PM me a link or just send me a message what a good Vpn to use is.

gAAAd - September 10, 2012, 5:52 am

Was a nice tutorial until you mentioned LOIC, haha. :P

People shouldn't be using it.

Zaligo - September 10, 2012, 6:12 am

Very clear and noob friendly tutorial

Thanks

SmexyAppleE - September 10, 2012, 7:07 am

if i use booter to attack the ip i dont need vpn ya?

terminal - September 10, 2012, 7:36 am

I know people shouldn't be using LOIC, its awful!
I recommend buying a decent shell booter from the marketplace.

tueur - September 10, 2012, 8:08 am

(Sorry I speak French..)
A DoS attack is better in TCP or in UDP ?
UDP is not priority to TCP ?

terminal - September 10, 2012, 10:08 am

The open ports which are vulnerable are TCP. So in this case a TCP attack is more effective.

DataBus - September 11, 2012, 7:10 am

nice TUTorial bro keep it up :)

cheers

d4rk41g0r1thm - September 11, 2012, 3:54 pm

Thank you i always wanted to take down some home connections but never scanned for open ports
thank you

Vodkaka - September 11, 2012, 4:14 pm

i would like to try it, but you think it's possible alone, with a simple home connection ? thanks !

skywalker313 - September 11, 2012, 4:45 pm

Yup...this will work,nice and clean ;)

Zombieboy18 - September 11, 2012, 9:30 pm

Is there any other free booter other than LOIC that actually works?
And how much time does it take to take a connection down with LOIC?
Anyways, nice thread well written and organized.

-Zombieboy18

DESTRUCTO - September 11, 2012, 9:56 pm

Nice tutorial bro keep up the good work :D

terminal - September 12, 2012, 8:06 am

(Sep 11, 2012 09:30 PM)Zombieboy18 Wrote: [\[CITE\]](#) Is there any other free booter other than LOIC that actually works?

And how much time does it take to take a connection down with LOIC?
Anyways, nice thread well written and organized.

-Zombieboy18

Go to the Tools section! ?

Zombieboy18 - September 12, 2012, 12:30 pm

(Sep 12, 2012 08:06 AM)terminal Wrote: [\[CITE\]](#) Go to the Tools section! ?Well, i did either they dont work, or they dont PM you with link...

-Zombieboy18

St4lker - September 15, 2012, 1:34 am

hey nice tutorial man but i dont understand nmap i dont see anyport in the results, can you help me though skype? my skype is: ukhst4lker

illuminator - September 15, 2012, 2:21 am

loic was that backdoored anonymous tool right ?

so besides getting an backdoor on my system, what other use does it have to ddos some random person ?

rshack190 - September 15, 2012, 3:15 am

legit, lol that's funny as hell and im just posting this for 10 posts ;)

trackme1 - September 15, 2012, 6:53 am

nice share im going to try this on some people thanks

dudekid39 - September 15, 2012, 11:04 am

easy clean and nice tutorial thx for the share

Snapchats hmu - September 15, 2012, 2:11 pm

cool and good TUT and going to try soon :))

Valiance - September 15, 2012, 2:16 pm

LOIC is extremely weak, you can purchase a booter via the marketplace that hits much harder. Nice tut though.

500 - September 15, 2012, 4:30 pm

Easy, clean and nice tutorial. Thanks for the share :)

Swirl - September 16, 2012, 11:03 am

Whenever I try the scan it always says "All scanned ports on xx are filtered. Too many fingerprints mach this host to give specific os details.

herrdeutschland - September 16, 2012, 1:15 pm

thanx dude for this nice tutorial keep up the good work

St4lker - September 17, 2012, 10:16 am

can somebody help me plz... i dont get the ports.. if i enter that command in nmap i get this (btw i tryde my own ip adress to test nmap):

Quote:C:\nmap>nmap -T4 -A -v -Pn IP (MY IP ADRESS)

Starting Nmap 6.01 (<http://nmap.org>) at 2012-09-17 19:09 West-Europa (zomertijd)

NSE: Loaded 93 scripts for scanning.

NSE: Script Pre-scanning.

Failed to resolve given hostname/IP: IP. Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges. If the machine only has an IPv6 address, add the Nmap -6 flag to scan that.

Initiating Parallel DNS resolution of 1 host. at 19:09

Completed Parallel DNS resolution of 1 host. at 19:09, 0.04s elapsed

Initiating SYN Stealth Scan at 19:09

Scanning dhcp-XXX-XXX-XXX-XXX.XX.XX (these X's is my host) (MY IP ADRESS) [1000 ports]

SYN Stealth Scan Timing: About 29.05% done; ETC: 19:11 (0:01:16 remaining)

SYN Stealth Scan Timing: About 59.05% done; ETC: 19:11 (0:00:42 remaining)

Completed SYN Stealth Scan at 19:11, 101.97s elapsed (1000 total ports)

Initiating Service scan at 19:11

Initiating OS detection (try #1) against dhcp-XXX-XXX-XXX-XXX.XX.XX (these X's is my host) (MY IP ADDRESS)

Retrying OS detection (try #2) against dhcp-XXX-XXX-XXX-XXX.XX.XX (these X's is my host) (MY IP ADDRESS)

Initiating Traceroute at 19:11

Completed Traceroute at 19:11, 0.04s elapsed

NSE: Script scanning (MY IP ADDRESS)

Initiating NSE at 19:11

Completed NSE at 19:11, 0.00s elapsed

Nmap scan report for dhcp-XXX-XXX-XXX-XXX.XX.XX (these X's is my host) (MY IP ADDRESS)

Host is up (0.0050s latency).

All 1000 scanned ports on dhcp-XXX-XXX-XXX-XXX.XX.XX (these X's is my host) (MY IP ADDRESS) are filtered

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE (using proto 1/icmp)

HOP RTT ADDRESS

1 3.00 ms dhcp-XXX-XXX-XXX-XXX.XX.XX (these X's is my host) (MY IP ADDRESS)

NSE: Script Post-scanning.

Read data files from: C:\nmap

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 108.76 seconds

Raw packets sent: 2046 (92.996KB) | Rcvd: 14 (932B)

C:\nmap>

Please help me add me on skype: st4lker or just pm or post here. thanks in advance!

terminal - September 17, 2012, 11:42 am

Failed to resolve given hostname/IP: IP. Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges. If the machine only has an IPv6 address, add the Nmap -6 flag to scan that.

There is your answer!

St4lker - September 17, 2012, 1:16 pm

i did but then it doesnt work at all! can someone please help me via skype: ukhst4lker is my skype name

this is what i get if i add nmap -6:

Quote:C:\nmap>nmap -6 -T4 -A -v -Pn IP (MY IP ADDRESS)

Starting Nmap 6.01 (<http://nmap.org>) at 2012-09-17 22:19 West-Europa (zomertijd)

NSE: Loaded 93 scripts for scanning.

NSE: Script Pre-scanning.

Failed to resolve given IPv6 hostname/IP: (MY IP ADDRESS). Note that you can't use '/mask' or '[1-4,7,100-]' style ranges for IPv6.

Failed to resolve given IPv6 hostname/IP: (MY IP ADDRESS). Note that you can't use '/mask' or '[1-4,7,100-]' style ranges for IPv6.

NSE: Script Post-scanning.

Read data files from: C:\nmap

WARNING: No targets were specified, so 0 hosts scanned.

Nmap done: 0 IP addresses (0 hosts up) scanned in 2.11 seconds

Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

C:\nmap>

what should i do or did i do wrong?

richiss972 - September 17, 2012, 4:03 pm

Im going to try soon good TUTo :))

camcamcode08 - September 17, 2012, 8:57 pm

thanks for sharing this mate can i have the php script?

Hacker 4949 - September 17, 2012, 10:36 pm

Ill try when i want.

Thanks fo tut.

yazumi - September 18, 2012, 3:35 am

thanks alot, great tutorial, clear and simple steps

n0tizie - September 18, 2012, 3:52 am

hey can i get the script? thanks my friend

RedChaos - September 19, 2012, 7:36 pm

I brand new to this thanks for the TUT man!

??_?™ - September 19, 2012, 8:16 pm

nice script, ill try it soon. thanks a lot

Austerity - September 21, 2012, 4:54 am

Thank you for sharing this tut, testing out now.

ToXic73 - September 21, 2012, 6:24 pm

Nice tut, what kind of time would I be looking at to take down a small website?

lebackoji - September 21, 2012, 6:29 pm

(Sep 11, 2012 07:10 AM)X0rCode Wrote: [\[CITE\]](#) nice TUTORial bro keep it up :)

cheers

was staring at the .GIF for past 10 mins :/

Just tried this out, took mates internet down :P thanks <3 edit

For educational purposes I did the above.

Hey Look Behind You - September 21, 2012, 9:17 pm

A very detailed and nice tutorial, Thank you for sharing :)

Dimeblade - September 22, 2012, 9:41 am

Amazing Tutorial. Thankx for the post. :D

power4gear - September 22, 2012, 12:06 pm

My victim is behind a firewall. All the ports are filtered, no other information. What are my options? Thanks.

konstentine - September 22, 2012, 2:04 pm

Nice tutorial,
Well written.

Thanks for this.

F0xDi3 - January 9, 2015, 4:11 pm

Imao i read multiple places how loic is back doored...

woahxx - January 10, 2015, 1:30 am

The part about scanning for vulnerable ports was very useful for me, thanks man!

roleeswagger - January 10, 2015, 4:24 am

Nice tutorial don't worry about the ip since we are in ipv4 no one can reach that xD

FxGrunn - January 10, 2015, 6:28 am

Easy and nice tutorial, thanks for sharing!

mafiaanonymous - January 10, 2015, 2:11 pm

Nice very good is working +1rep Thank you :)

moose_ - January 11, 2015, 1:37 am

Can you give me the php script please

ObiWanKanBlowMe - January 11, 2015, 1:41 am

(Jan 9, 2015 05:11 PM)F0xDi3 Wrote: [CITE](#) Imao i read multiple places how loic is back doored... And a little birdie told me you're a dumb ass grave digger with no knowledge beyond Internet Explorer. On top of that, LOIC uses your own bandwith and comes from your router, not a public source.

Quit grave digging and confusing new members that this method still works.

Slut.

crhater - April 2, 2015, 9:14 am

Hi guys

What could I do if I don't find any open ports? My scans always find only closed and filtered ports...

Thanks for your advices

Code Host is up (0.072s latency).

Not shown: 994 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

5001/tcp	closed	complex-link	
----------	--------	--------------	--

5030/tcp	closed	surfpas	
----------	--------	---------	--

5054/tcp closed rlm-admin
5100/tcp closed admd
5101/tcp closed admdog
64680/tcp closed unknown

nobider - January 22, 2017, 7:02 am

(Sep 9, 2012 06:51 AM)terminal Wrote: [\[CITE\]](#) The MOST EFFECTIVE DoS Method!

1.

The tools you will need for this tutorial is as follows:

nMap - <http://nmap.org/dist/nmap-6.01-setup.exe>

A DoS Tool -

<http://sourceforge.net/projects/loic/>

(I am suggesting LOIC because its free and easy to use. In no way do I condone the use of LOIC)

2.

Harvest an IP from a victim, you can do this using an IP Grabber which you can host on SPAM. (PM me for the PHP Script!)

3.

Once you have your IP address that you want to attack, open up nMaP. Enter the IP in the target box and enter this into the command box:

Code nmap -T4 -A -v -Pn IP 456.123.784.678

4.

Hit Scan!

5.

As the default profile for a scan is 'Intense' it will take around 4 minutes to complete the scan. Once the scan is done, search through the scan results until you find a list of the vulnerable ports, these are the ports we will attack!

6.

Open up LOIC and enter the victims IP in the IP box. Then click 'Lock On'. Make the TCP/UDP message 30, the method TCP and the thread 900. For the port box, enter one of the vulnerable ports from the nMaP scan.

7.

Hit IMMA CHARGING MAH LAZOR!

8.

Sit back and relax for a while.

9.

To find out if your target has been taken down ping there IP address through CMD:

Code ping 456.123.784.678

The IP: 456.123.784.678, is entirely fictional, I have not knowingly published this IP seeking an attack.

I am NOT RESPONSIBLE for anything you do regarding the material is this tutorial!

AND FOR THE LOVE OF GOD, USE A VPN!

can i get the tool ?

Freddy Kru?ger - January 22, 2017, 3:04 pm

(Jan 22, 2017 08:02 AM)nobider Wrote: [\[CITE\]](#) can i get the tool ?
Holy shit man are you for real?

minecrafter6969 - January 23, 2017, 12:20 am

nice tutorial! thank you for sharing

Flopppy - February 7, 2017, 2:24 pm

(Sep 10, 2012 04:13 AM)autorunman22 Wrote: [\[CITE\]](#) is there a much better software other than loic there? im just asking what else can you recommend

Might not be what you're looking for but i've recently discovered the magic behind "Tors Hammer" which is a webhost DOS tool. (Can only DOS Apache)

One of its main feature is how it does the attack through TOR, And wow is it effective. tried out on my i7 4770k Apache server with a craptop and it took the website down in a few seconds through 4G and TOR.

x4binode - February 7, 2017, 11:44 pm

Thanks for the tutorial! Good job!

?Ñåzg?! - February 8, 2017, 12:59 am

worst tutorial I have seen in a while
why would anyone even

weirdo1987 - February 17, 2017, 4:50 am

thank you for writing this! great!

Vindicta911 - February 17, 2017, 5:41 am

A noob question. What is this tutorial good for? For dosing who?

Arnette Rene - February 17, 2017, 5:42 am

(Feb 17, 2017 06:41 AM)Vindicta911 Wrote: [\[CITE\]](#) A noob question. What is this tutorial good for?
For dosing who?

Its good for getting yourself busted if it even manages to gets someone's attention.

Wilkassek - February 17, 2017, 5:55 am

Very good share, probably I will try it soon, good luck in the next time!

chrispa - March 8, 2017, 2:56 am

Good job bro. Thank you very much for this insightful tutorial

Hopsin - March 8, 2017, 5:07 am

(Mar 8, 2017 03:56 AM)chrispa Wrote: [\[CITE\]](#) Good job bro. Thank you very much for this insightful tutorial

OP is banned/closed so he cannot see your gratitude sadly. Also, this thread is published @2012!
Have a nice day mate. ?

Roxxx. - March 8, 2017, 7:48 am

Very nice thanks for share