

Forum:[Hack Forums](#)

Thread: [PDoSing \(Permanent Denial of Service\) | Linksys Routers](#)

Niggz - December 23, 2013, 12:48 pm

[img]<http://sadpanda.us/images/1845387-W76L1JO.png>[/img]

I am not going to make this a nice and neat, spiffed up tutorial with nice GFX because I feel that the information in the tutorial is good enough to get a positive feedback.

So, I was looking around HF and I couldn't seem to come up with one tutorial on PDoS'ing. Maybe it's because not a lot of people are familiar with the technique. But that is why I am making a tutorial for you guys.

What is PDoS'ing?

PDoS Stands for (Permanent Denial of Service). Like the famous DDoS Attack (Distributed Denial of Service), PDoS'ing causes the victim to get kicked offline. But a DDoS attack doesn't last very long at all. If you want to really punish your victim then you will need to go with PDoS'ing him/her as it will last permanently.

You will need Remote Administration Tool

Background knowledge of routers

Victim as a Slave

Before we get started you will need to download my Bricked Firmware File.

http://www.mediafire.com/download/egqa951cjc73ebd/dd-wrt.v24_voip_generic.bin

Step 1

Open up your RAT and start remote administrating your Victim.

Step 2

Go to their CMD and type in this:

Code ipconfig | findstr "Gateway"

You should receive an output like this:

Code Default Gateway . . : 10.0.0.1

Step 3

Go into Google Chrome or whatever their web browser is and type in their default gateway.

You will be brought to Linksys's website if you have done everything correctly.

Step 4

Enter the Saved Credentials to the site.

Now go over to the Administration Tab and under that click Firmware Upgrade.

Click on choose file click on the my Bricked Firmware File.

Now you have completed your first PDoS!

?lixir - December 23, 2013, 12:54 pm

Wheb I read the title I got a little excited. I thought you knew how to fry a remote host's hardware.

Goodies - December 23, 2013, 12:55 pm

SI0w go look up something called Sockstram. It can DEFINITELY result in PDOS.

Basically, you know the normal TCP handshake?

SYN
SYN/ACK
ACK

?

Well, the "window size" in the TCP ACK packet dictates the amount of data that can be sent/received. Sockstream actually sets this to 0 so the connection stays open, it allocates space in RAM for it, and doesn't use it. I've taken down servers with 8GB RAM and it can DEFINITELY affect hardware beyond repair :D

(Dec 23, 2013 01:54 PM)Dr. Caspers Wrote: [\[CITE\]](#) Wheb I read the title I got a little excited. I thought you knew how to fry a remote host's hardware.
Read my post below yours but above this one :)

Maf?a - December 23, 2013, 12:57 pm

Bookmarked this for later use, currently I have no one who pisses me off to this point.

?lixir - December 23, 2013, 12:57 pm

(Dec 23, 2013 01:55 PM)Goodies Wrote: [\[CITE\]](#) SI0w go look up something called Sockstram. It can DEFINITELY result in PDOS.

Basically, you know the normal TCP handshake?

SYN
SYN/ACK
ACK

?

Well, the "window size" in the TCP ACK packet dictates the amount of data that can be sent/received. Sockstream actually sets this to 0 so the connection stays open, it allocates space in RAM for it, and doesn't use it. I've taken down servers with 8GB RAM and it can DEFINITELY affect hardware beyond repair :D

Read my post below yours but above this one :)
Can this be done to a home connection with an open port? It seems like a program needs to be listening on said port in order for this to work.

That_Guy120 - December 23, 2013, 1:00 pm

what if they just restart their router? or get a new one?

Niggz - December 23, 2013, 1:02 pm

(Dec 23, 2013 02:00 PM)That_Guy120 Wrote: [\[CITE\]](#) what if they just restart their router? or get a new one?

1. Restarting there Router won't do anything.
2. They won't realize that they would have to buy a new router for a long time.

Goodies - December 23, 2013, 1:03 pm

(Dec 23, 2013 01:57 PM)Dr. Caspers Wrote: [\[CITE\]](#) Can this be done to a home connection with an open port? It seems like a program needs to be listening on said port in order for this to work. Absouleyly.

The thing is, this attack is old (2008) but is only now starting to be used and therefore does not have any security measures. It's as simple as dropping packets with a 0 window size.

The problem with that is TCP's built-in flow control and congestion control uses that, but it's VERY rare anyways :P

aaronq46 - December 23, 2013, 1:04 pm

Nice tutorial :D Is there any routers this works on other than linksys?

Elite Hacker 69 - December 23, 2013, 1:05 pm

This is pretty sweet but does it only work for Linksys routers?

I might make myself blackhat just to do this to someone if I can find out how to infect them, assuming I had a good enough reason.

Cool tutorial.

Goodies - December 23, 2013, 1:05 pm

(Dec 23, 2013 02:02 PM)Sl0w Wrote: [\[CITE\]](#) 1. Restarting there Router won't do anything.
2. They won't realize that they would have to buy a new router for a long time.
This.... lol once you flash the firmware, they're fucked xD

I know some routers that start a TFTP demon that can allow you to flash via TFTP (FTP that uses UDP rather than TCP... T = Trivial).

But something tells me people dumb enough to run a RAT aren't the best and brightest when it comes to router re-flashing...

Gj Sl0w :D I enjoyed.

Niggz - December 23, 2013, 1:13 pm

(Dec 23, 2013 02:05 PM)Bliss n Eso Wrote: [\[CITE\]](#) This is pretty sweet but does it only work for Linksys routers?

I might make myself blackhat just to do this to someone if I can find out how to infect them, assuming I had a good enough reason.

Cool tutorial.

No, it probably works on some other routers as well. I just have only tested the attack out on Linksys Routers.