

Forum:[Hack Forums](#)

Thread: [Selective Packet Denial of Service \[Evading IDS and Firewall\]](#)

Nitrate - October 18, 2013, 12:54 pm

Hello HF!

--

THIS IS A REPOST.

THE ORIGINAL DIDN'T GET THE ATTENTION EXPECTED
IT WAS POSTED IN THE TUTORIALS SECTION.

--

This is my second time posting a tutorial, I will be posting tutorials on advanced topics :D

Today Ill talk about selecting the right packets/exploiting handshakes to bring a web-server down without being noticed by an IDS or blocked by a Firewall.

Please notice that this is an advance topic (it might seem easy for some people) however its not for beginners,
ill try to keep it as easy as possible without forgetting any information.

Lets get started!

First, Ill throw in these common DoS methods :

UDP Flood - Most common, spams User Datagram protocol requests.

TCP Flood - spams Transmission Control Protocol requests.

SYN Flood - exploits the 3 way handshake, opening a lot of connections without completing the handshake.

What is a TCP 3-Way-Handshake?

[img]http://public.dm1.livefilestore.com/y2pzZbagfCVQxak1uvWFiScIFmUFFKQlpSdxcF2R-BkYXB5_EHkrLh8c0-X7FvxQoq8FTmaWIO6D0DsJoU_iB3P6SAfdjfemkO3H6IG61VN4q4/Latency_tcp.jpg?psid=1&rdrts=55798252[/img]

- 1) The user sends a SYNCHRONIZE packet to the host telling him to open a connection.
- 2) The client responds with an SYNCHRONIZE ACKNOWLEDGE packet 3) to inform the user that the SYN packet was recieved.
- 4) The user sends an ACKNOWLEDGE packet to inform the client that everything is ready and client should expect data.
- 5) Then the users sends data (HTTP GET/POST .etc)
- 6) The client replies with the results (weather it was a homepage/image request)

What does most common flooders do?

All flooders such as LOIC/HOIC/UDP Unicorn spams requests to the target with a VERY short delay in a very high speed, these tools are connection dependent in other means it will only take down servers that are weaker than your connection.

These flooders make too much mess on a server and almost all firewall can block these flooders + an IDS will detect it and you will get in further trouble.

1 request might take up 0.01% CPU (very weak) + Stores possibly 200KB of data (depending on the power of the tool)

What does Selective Packet DoS mean?

Instead of spamming requests, why don't we select the packets that only consume space and CPU? Packets that will take a lot of memory to process?

This is commonly called Layer 7 DoS.

Instead of spamming 10000 requests taking up 20% CPU and getting noticed by an IDS (if not blocked by a firewall)

We select the packets that takes up CPU, so 20 Selected-Packets consume 100% leading to a denial of service :D

How do we discover them?

Writing such exploits require very advanced knowledge about networking and programming.

Examine your target and install its software on your computer (a VM or another machine)

browse your locate site while keeping logs through wireshark and keeping notice at the CPU, send the packets you think is harmful until you make a pack of packets that consume more CPU than the usual spammed packets

Thanks! Please excuse any mistakes because its my first actual tutorial :D

PM for any questions!

DrDinosaur - October 18, 2013, 6:03 pm

Interesting information, but this is not even close to being a tutorial.

Le Spy - October 18, 2013, 6:05 pm

(Oct 18, 2013 06:03 PM)DrDinosaur Wrote: [\[CITE\]](#) Interesting information, but this is not even close to being a tutorial.

Agreed.

And, why double-post just because you're seeking attention?

Nitrate - October 19, 2013, 3:55 am

(Oct 18, 2013 06:05 PM)Hyphers Wrote: [\[CITE\]](#) Agreed.

And, why double-post just because you're seeking attention?

Sorry, I just wanted it to be more noticed because i worked hard on it.

Fat Autist12 - October 19, 2013, 8:48 pm

Very informative, though I got bored, so I didn't make it through the whole thing. Thank you for your contribution.

UserName - October 22, 2013, 4:22 pm

I am not trying to advertise my program, but if anybody is interested in a Layer 7 DoS script I posted one in python here:

<https://hackforums.net/showthread.php?tid=3810636>

ulstR - October 22, 2013, 8:02 pm

wtf is this, sorry man your tut makes no sense? when you start explain syn > syn ack that is where most advanced users will stop. For future reference firewalls do not adaptively start blocking dos attacks.. they are policy enforcement devices. I would simply use S/D RTBHR to punt you to a null interface. Not sure who the target audience is or what the purpose of this "tut" is, time to head back to the drawing board I think.

Nitrate - October 23, 2013, 2:34 pm

(Oct 22, 2013 08:02 PM)ulstR Wrote: [\[CITE\]](#) wtf is this, sorry man your tut makes no sense? when you start explain syn > syn ack that is where most advanced users will stop. For future reference firewalls do not adaptively start blocking dos attacks.. they are policy enforcement devices. I would simply use S/D RTBHR to punt you to a null interface. Not sure who the target audience is or what the purpose of this "tut" is, time to head back to the drawing board I think.

As i said this my first tutorial, I am trying to get used to making tutorials so that I can post more advanced one. but thanks for the feedback it will help for sure :)

Most Firewalls will block depending the requests recieved and the delay between them, cloudflare checks the packets to see if they are safe depending on their signature/data (if its udp) and will check to see if there is a flood or not. Layer 7 would look like legit packets so it wont get detected.