

Forum:[Hack Forums](#)

Thread: [Level 4 vs. Level 7](#)

Wolf of Wall Street - July 5, 2016, 12:45 pm

I bought a stresser but am not knowledgeable enough to know the difference between level 4 and 7. Could someone please help me out with an explanation. Thanks

Miniscule - July 5, 2016, 12:46 pm

Layer 4 is generally used for home connections, and layer 7 is used for websites. There is my short little guide on what each of them are haha.

Nerdi - July 5, 2016, 12:47 pm

(Jul 5, 2016 12:46 PM)Miniscule Wrote: [\[CITE\]](#) Layer 4 is generally used for home connections, and layer 7 is used for websites. There is my short little guide on what each of them are haha.
Simple and to the point.

Wolf of Wall Street - July 5, 2016, 1:24 pm

(Jul 5, 2016 12:46 PM)Miniscule Wrote: [\[CITE\]](#) Layer 4 is generally used for home connections, and layer 7 is used for websites. There is my short little guide on what each of them are haha.
perfect thank you

Miniscule - July 5, 2016, 1:25 pm

(Jul 5, 2016 01:24 PM)hfoldgeezer Wrote: [\[CITE\]](#) perfect thank you
No problem man, glad to help you so at least your money did not go to waste haha. ?

Keat - July 5, 2016, 5:43 pm

I always thought layer 4 and 7 was referencing the OSI model.

Phizo - July 5, 2016, 10:01 pm

(Jul 5, 2016 05:43 PM)Keat Wrote: [\[CITE\]](#) I always thought layer 4 and 7 was referencing the OSI model.

Correct. Layer 4 and layer 7 are respectively "transport" and "application" layers. Transport layer protocols include UDP, TCP, etc. Application layer protocols include HTTP, DNS, FTP, etc.

To understand layer 4 DoS completely, you need to understand the TCP/IP model (layer 4 DoS is typically a SYN flood).

To establish a session over TCP:

The client will send a SYN (synchronise) packet to the server.

The server will reply with a pair of packets: (SYN, ACK=acknowledgement)

The client replies with an ACK packet.

Briefly, a SYN flood is when the client repeatedly does the initial step (send a SYN packet), while ignoring the SYN-ACK response from the server, leaving connections half-open. Servers protect against this attack through the use of SYN cookies.

Layer 7 DoS is typically a HTTP GET/POST flood. Being the top of the OSI model, which is

constructed bottom-to-top from layer 1 initially by the client and subsequently deconstructed top-to-bottom in response, you're well past the point of a TCP session being acknowledged on both ends. When you make a request to a website, it is often through the GET and POST HTTP methods. This attack is pretty simple: you repeatedly perform requests to a website. To maximise efficacy of the attack, you want to make requests that put strain on the server (e.g. requesting large content).

People use "layer X" as a buzzword, really. In actual fact, it's very broad, as a layer encapsulates a wide range of different protocols. The attacks I mentioned are typical, and most likely what is contained in your booter.

Hopefully that provides some insight for you.

#Skyline - July 6, 2016, 5:46 am

(Jul 5, 2016 10:01 PM)Phizo Wrote: [\[CITE\]](#) Correct. Layer 4 and layer 7 are respectively "transport" and "application" layers. Transport layer protocols include UDP, TCP, etc. Application layer protocols include HTTP, DNS, FTP, etc.

To understand layer 4 DoS completely, you need to understand the TCP/IP model (layer 4 DoS is typically a SYN flood).

To establish a session over TCP:

The client will send a SYN (synchronise) packet to the server.

The server will reply with a pair of packets: (SYN, ACK=acknowledgement)

The client replies with an ACK packet.

Briefly, a SYN flood is when the client repeatedly does the initial step (send a SYN packet), while ignoring the SYN-ACK response from the server, leaving connections half-open. Servers protect against this attack through the use of SYN cookies.

Layer 7 DoS is typically a HTTP GET/POST flood. Being the top of the OSI model, which is constructed bottom-to-top from layer 1 initially by the client and subsequently deconstructed top-to-bottom in response, you're well past the point of a TCP session being acknowledged on both ends. When you make a request to a website, it is often through the GET and POST HTTP methods. This attack is pretty simple: you repeatedly perform requests to a website. To maximise efficacy of the attack, you want to make requests that put strain on the server (e.g. requesting large content).

People use "layer X" as a buzzword, really. In actual fact, it's very broad, as a layer encapsulates a wide range of different protocols. The attacks I mentioned are typical, and most likely what is contained in your booter.

Hopefully that provides some insight for you. Adding onto your post, and taking away the DoS concept.

OP, also research the OSI model.

http://www.webopedia.com/quick_ref/OSI_Layers.asp

It will benefit you, and help you understand more about networking and the internet.