

Forum:[Hack Forums](#)

Thread: [Difficulty with Layer 7 Attacks, and Layer 4 mitigation.](#)

panemon - January 30, 2014, 8:05 pm

I have quite a few questions here to ask, and have looked around on the forums for specifics on these topics, but have not found anything specifically useful to solve the problems I am having currently.

I haven't tried using these layer 7 scripts on my own connection, or servers, but have been attempting to use them on API-Booters. (I do this for security reasons.)

I have had an incredible amount of success with UDP and TCP layer 4 attacks, but have had absolutely no luck with any software/layer7 attacks. I am trying to figure out what I am doing wrong here.

Layer 7 Questions:

Obviously layer 7 attacks do not hit a specific port, or do they? I don't think that they do. Some booters leave the port open, if this is done should I just leave it at port 80 as default?

How can I test a server for vulnerabilities to these various layer 7 attacks? How do I know if they're working? When I set a slow loris attack to a server I just put in the website, or do I have to find a specific file or something on the server to specifically attack? If someone can answer this I'd like to know what you know about the various layer 7 attacks, and how you exactly use them. I am also wondering which ways I can easily test the attack to see if it's actually working or not, or if I just have to wait.

I think just putting in the website itself is not enough, it seems like I must find a forum, or a section on the website so the scripts can execute on that specific software layer, or do these scripts just automatically find something on the server to execute on the software side?

Layer 4 attack questions:

I know that there are various mitigation techniques used to check for spoofed attacks, packet sizes, and mitigation that filters attacks to be absorbed and spread in other parts of the network. (cloudflare methods)

Attacking websites with TCP/UDP:

Is there a method to check which is the best port to hit these servers on, or are there more vulnerable ports that you know of besides: 80, 443, and Packet sniffed ports you've sniffed with wire shark filters? I've used online port scanners, and tools like NMAP, but maybe I am not using them properly. It seems like even when a specific port is closed on a port scanner, I can still attack on that port anyway, and be successful, in some cases.

However, I understand that if I am attacking a specific server that has protection against the attacks, that if I was to target the provider that is feeding the connection to the server, that this is the best way to take down the server. My problem is how do I find the ISP that is hosting the server? I've looked at WHOIS records, but it just shows me the name servers for the same host within that region. If I want to find out who is feeding their bandwidth how do I go about doing this?

Leaking DNS users of a VPN on a home connection:

I know that newbies using VPN connections, and proxies to hide their real IP can leak their dns, if they're not using the right kind of encryption. VPNS using PPTP often leak DNS, and very few OpenVPNs seem to leak their DNS, but whenever I set up a OpenVPN connection to an encrypted server, I usually have to implement additional settings in my own network configurations to keep my DNS from leaking. My question is, how do I check a persons VPN/PROXY ip to find their real IP? If network administrators can do this, then I would assume that I could resolve the real IP as well. I would also like to know of ways to break through the encryption of low security/weak encryption VPNS.

I love the fact that I can check my own connection for DNS leaks, but how do I reverse this to check to see if someone else's DNS is leaking via their IP?

sudo_ - January 31, 2014, 8:36 am

Layer 7:

No they don't hit a specific port. The script everyone uses doesn't require a port, even though on the panel of the tool there is a port text field, the variable isn't taken in and used in the usage statement.

Usage statement:

Invalid parameters!

Usage: ./ghp <target url> <method (GET or HEAD or POST)> <number threads to use> <proxy list> <time> [manual ip (0 to disable)] [post parameters (%RANDOM% will be replaced with random shit)]

Layer 4:

Try to attack on an open port, by default 80.

But you can do 53 21 22, whatever. It really depends on what ports are open, I would just use 80.

For me personally,

I use <http://network-tools.com/> to lookup the DNS records of the domain to obtain the IP address then I would go onto <http://ip-lookup.net/> enter the IP address and see who owns the IP address, it should show you what datacenter owns the certain ipv4 range.

I'm not entirely sure on how to find out the IP through a proxy/vpn as the only way I think is possible is to check the traffic coming in/out using tcpdump or something similar.

ALO - January 31, 2014, 9:17 am

Layer 7 is an application layer attack, so to say it doesn't use a specific port holds a half-truth. In reference to booters though, the port you specify probably isn't taken into consideration due to the fact that it may turn an attack directed towards an application running on port 80, to disregarded junk on port 13337 (for the very leet, of course).

Network administrators (of said VPN/proxy provider) are able to refer to connection logs to find your IP, or in some cases malicious websites can view per request the faulty tunnel's "x-headers" (or so I've heard them refereced as) for the IP address that request is being sent for.

panemon - February 1, 2014, 4:14 pm

Alright, I will look further into this, if anyone else has some additional information, or information resources I could use, I would very much appreciate it. Thanks guys!