How do I secure my DNS resolver against amplification attacks?

Article Number: 66 | Rating: 1/5 from 1 votes | Last Updated: Wed, Aug 18, 2021 at 3:55 PM

When your DNS server resolves a recursive DNS lookup, it tracks down information about a domain name hosted on another DNS server by connecting to other DNS servers.Â An open DNS server is a server that resolves recursive DNS lookups for anyone on the Internet. Recursive DNS is essential to the correct functioning of the Web, but it can be open to abuse if it isn't properly secured. Attackers are able to exploit unsecured recursive DNS by running a particular type of DDOS attack â€“ the DNS Amplification Attack. The hacker sends a recursive DNS query through UDP (User Datagram Protocol), with a spoofed IP address (the victim's IP address) in the IP packet header. The DNS server then sends a response back to the spoofed IP address.Â The response packet may be many times larger than the DNS query packet, amplifying the traffic sent to the victim. In order to secure your DNS resolver against this type of attack, you should set it to not permit recursion or only accept recursion requests from trusted IPs. This does not affect being the nameserver for domain names or operating websites. If you do not need to use your server as a nameserver, then the easiest and safest option is to disable DNS functionality on your server.Â Linux distributions typically do not enable a DNS resolver by default, but Windows does. To disable DNS functionality on your Windows server: Go into the Server Manager Click 'Roles' Click 'Remove Roles' Uncheck the 'DNS Server' role Click 'Next' You will be warned that the server needs to be restarted Click 'Remove' to continue The removal will take place Click 'Close' Restart the server when convenient The DNS functionality will be removed when you restart To secure your DNS resolver on Windows (if you want to keep using it as a nameserver): Go to DNS Manager Right-click 'DNS Server' Click 'Properties' Go to the 'Interfaces' tab Select 'Only the following IP addresses' Deselect all the IP addresses except for the main IP address Go to the 'Advanced' tab Select 'Disable recursion (also disables forwarders)' Click 'OK' Your DNS resolver will now be secured To secure your DNS resolver on Linux: Edit /etc/named.conf Insert the following lines in the global options clause if you are running an authoritative-only server: # inhibit all recursion
 recursion no; Insert the following lines in the global options clause if you are running a caching or forwarding server: # allow recursion for known IP addresses only
 # use an appropriate added scope statement to limit all query results to trusted users
 allow-recursion {192.168.2.0/24}; //Change IPs as required
 allow-query {â€œlocalhostâ€•,â€•192.168.2.0/24â€•}; #personal resolver
 allow-recursion {â€œlocalhostâ€•;};
 allow-query {â€œlocalhostâ€•;}; Restart the DNS server after your configuration changes by using this command: /sbin/service named restart For Linux users, you can also install BIND, DNS software known for added security.

Posted - Tue, Mar 3, 2015 at 4:56 PM.

Online URL:
https://www.heartinternet.uk/support/article/how-do-i-secure-my-dns-resolver-against-amplification-attacks.html

PDF Generated by PHPKB Knowledge Base Script