Perancangan dan analisis secure DNS server berbasis konfirmasi nilai Hop count untuk mengatasi DNS amplification attack = Design and analysis of secure DNS server based on confirming Hop count value to mitigate DNS amplification attack

Aditya Putra, author

Abstrak

ABSTRAK
Melihat serangan DNS Amplification Attack DAA terus melakukan evolusi wujud dan ukuran, perlu dilakukan penelitian lebih lanjut tentang cara yang efektif dan implementasi yang tepat untuk menangkal serangan tersebut. Penelitian ini berfokus untuk melakukan pendekatan yang sederhana yaitu menggunakan Hop Count dari nilai TTL menggunakan konfirmasi ICMP untuk diimplementasikan di Server DNS Recursive Resolver untuk mengkonfirmasi kesamaan jarak hop antara Server DNS dengan Pengirim DNS Request.Penelitian ini dilakukan dengan menambahkan fungsi whitelist dan blacklist pada algoritma Hop-Count. Penambahan ini disinyalir dapat membuat antisipasi searngan menjadi lebih baik dengan mengurangi dampak ICMP Flooding yang disebabkan oleh konfirmasi Hop Count. Simulasi serangan dilakukan dalam topologi yang dibangun dalam GNS3 dengan memberikan variasi jarak hop count baik dari attacker maupun dari target kepada server DNS.Penelitian ini menyimpulkan bahwa algoritma ini berhasil mencegah serangan DAA secara efektif. Penambahan server yang digunakan pada penelitian ini juga memperlihatkan dampak penambahan efek serangan yang disebabkan olehnya dan berhasil dicegah dan algoritma HC berhasil mencegahnya. Penelitian ini juga berhasil mencegah potensi munculnya serangan ICMP Flooding hingga 99.
<hr>
ABSTRACT
As DNS Amplification Attack DAA attack keeps evolving in form and size, it is urge to take further research on how to prevent the attack effectively and using the proper implementation. This research focus to do a simple approach using Hop Count value based on TTL value which utilize ICMP confirmation to be implemented in a DNS Recursive Resolver Server to confirm that DNS Server and DNS Reques sender have the same hop distance.This research is done by adding whitelist and blacklist to Hop Count algorithm. This addition allegedly will reduce ICMP Flooding as the consequences of Hop Count confirmation. The simulation will run in GNS3 based topology which will vary the hop count distance from either attacker or target to DNS Server.This research concluded that our algorithm succeeded preventing the DAA. The increasing number of DNS Server used also showed the increasing of attack size, but the HC algorithm could still manage. This research also manage to prevent the potential ICMP Floodinng up to 99 .