**JOEICT (Jurnal of Education and Information Communication Technology)**
Volume 1, Nomor 1, Tahun 2017: 17 – 22

# ANALISIS DNS AMPLIFICATION ATTACK

**Norma Triyana[1)], Adrian Eka[2)]**
[1, 2)]Program Studi Pendidikan Teknologi Informasi, STKIP PGRI Tulungagung
Jalan Mayor Sujadi Timur Nomor 07, Plosokandang, Tulungagung, 66221
e-mail: normanuynuy945@gmail.com[1)], ryannyapo2@gmail.com[2)]

**ABSTRAK**

***Abstrak –*** *Dalam komunikasi data di jaringan Internet yang luas, komputer-komputer berkomunikasi dengan IP address, misalnya saat kita mengakses web melalui browser. Apabila kita mengunjungi alamat web tersebut sebenarnya kita sedang berhubungan dengan IP address yang dimilikinya. Itulah yang dilakukan oleh DNS terhadap kita. Domain Name System (DNS) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data (distributed database) di dalam jaringan komputer. DNS dapat menyebabkan kerusakan serius ke layanan jaringan dan dengan demikian akan menghambat proses akses ke sumber daya jaringan tersebut. Oleh karena itu nameserver DNS terus-menerus rentan terhadap ancaman Denial of Service (DOS) serangan*

.

**Kata Kunci**: DNS Amplifikasi, DNSSEC, DoS, DDoS Attack

**ABSTRACT**

*The data communication in Internet networking that so wide, between computer with other communicate with IP address, example when we accessing the web on browser. Maybe we visiting on web address this, in fact we connecting with IP addres that there have. That's it what DNS do for us. Domain Name System (DNS) is the system that save some information about hostname or domain name as distributed database on computer networking. DNS can affect broke seriously to network service and will be obstruct access process to source network this. Cause it DNS nameserver always susceptible of Denial of Service (DOS) attack threat.*

***Keywords****: DNS amplification, DNSSEC, DoS, DDoS Attack*

## I. PENDAHULUAN

Pada awal perkembangan internet, seorang user yang akan menghubungi komputer user lain harus menyebutkan alamat IP address komputer yang hendak dituju. Seiring dengan berkembangnya teknologi internet dan semakin banyaknya jumlah pengguna aplikasi internet, maka sangat menyusahkan jika kita harus mengingat IP address setiap user yang berupa angka ke nama yang lebih mudah diingat maupun sebaliknya.

Pada awalnya sistem penamaan IP address menggunakan sistem host.txt yang berisikan daftar kombinasi IP address dengan nama dari setiap komputer yang terhubung ke internet. Tentunya sistem penamaan IP seperti ini sangatlah tiak efektif dan sudah tidak mampu menangani kebutuhan yang ada saat ini. Oleh karena itu pada tahun 1984, Paul Mockapertis mengusulkan sistem penamaan IP yang baru yaitu menggunakan Domain Name System (DNS), sistem inilah yang digunakan hingga saat ini. [1]

## II. PEMBAHASAN

### A. *Pengertian DNS Amplifikasi, DNSSEC, Dos dan DDos Attack*

Domain Name System (DNS) adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer; misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima email untuk setiap domain.

Sebuah serangan DNS amplifikasi adalah Distributed Denial of Service (DDos) serangan di mana penyerang mengeksploitasi kerentanan dalam sistem nama domain (DNS) server untuk mengubah query awalnya kecil menjadi muatan yang jauh lebih besar, yang digunakan untuk menurunkan server korban. DNS amplifikasi adalah jenis serangan refleksi yang memanipulasi sistem nama domain publik dapat akses, membuat mereka membanjiri target dengan jumlah besar paket UDP. Menggunakan berbagai teknik amplifikasi, pelaku dapat "mengembang"

ukuran ini paket UDP, membuat serangan begitu ampuh untuk menurunkan bahkan infrastruktur Internet yang paling kuat. Dalam hal ini, refleksi dicapai dengan memunculkan respon dari resolvers DNS ke alamat IP palsu. Selama serangan amplifikasi DNS, pelaku mengirimkan permintaan DNS dengan alamat IP palsu (korban) ke DNS resolver terbuka, mendorong untuk membalas kembali ke alamat yang dengan respon DNS. Dengan berbagai pertanyaan palsu yang dikirim keluar, dan dengan beberapa resolvers DNS membalas kembali secara bersamaan, jaringan korban dapat dengan mudah kewalahan oleh banyaknya tanggapan DNS.[1]

Domain Name System Security Extensions (DNSSEC) adalah suite dari Internet Engeneering Task Force (IETF) spesifikasi untuk mengamankan beberapa jenis informasi yang diberikan oleh DNS seperti yang digunakan pada Internet Protocol jaringan (IP).[2].

Disk Operating System (Dos) adalah suatu sistem operasi komputer yang memakai interface command-line dan sering digunakan oleh pengguna komputer pada tahun 1980-an. DoS merupakan sistem operasi yang dipakai untuk mengelola semua sumber daya yang ada pada computer. [2]

Distributed Denial of Service adalah jenis serangan yang dilakukan oleh attacker/hacker terhadap sebuah komputer atau server di dalam jaringan internet dengan car menghabiskan sumber daya (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat lagi menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untk mengakses layanan dari komputer yang diserang. [1]

Paket DNS tradisional terbatas dengan panjang maksimal 512 byte di layer aplikasi. Namun, mekanisme ekstensi untuk DNS (EDNS) memungkinkan paket DNS yang lebih besar jika didukung oleh kedua resolver dan server otoritatif. Untuk berkomunikasi dukungan, resolver mengirimkan catatan source pseudo-code, OPT, yang menunjukkan ukuran paket yang didukung. Catatan OPT dapat menunjukkan dukungan DNSSEC, menunjukkan server harus mengirimkan catatan DNSSEC terkait. Penyerang memiliki pertimbangan taktis dengan menggunakan EDNS. Termasuk OPT record membutuhkan penyerang untuk menyertakan tambahan binary 11 byte dalam query. Jika server tidak mendukung EDNS, atau respon akan cocok dalam standar batas 512 byte, ukuran respon tetap sama. Dengan demikian, penggunaan EDNS akan mengurangi faktor amplifikasi yang terkait dengan query. Namun, jika hasil EDNS dukungan dalam respon yang lebih besar, mungkin mengerperkecil ukuran OPT record dan meningkatkan faktor amplifikasi. Dengan demikian, kita mengukur amplifikasi, baik dengan dan tanpa EDNS diaktifkan (menunjukkan aplikasi maksimum) layer ukuran paket 4096 byte seperti yang direkomendasikan oleh RFC 6891). [2]

### *B. Jenis-jenis Serangan DNS*

Ada tiga jenis umum dari serangan DNS yaitu :

#### *1. Cache Poisoning Attack*

Hal ini dapat terjadi setelah penyerang berhasil di suntik Data DNS berbahaya ke server DNS rekursif yang dioperasikan oleh banyak ISP. Jenis server DNS yang paling dekat dengan pengguna dari perspektif topologi jaringan, von Wallenstein menulis, sehingga kerusakan terlokalisir untuk pengguna tertentu menghubungkan ke server tersebut. Jika DNSSEC tidak praktis atau tidak mungkin, solusi lain adalah untuk membatasi rekursi pada server nama yang perlu dilindungi. Rekursi mengidentifikasi apakah server hanya akan membagikan informasi yang telah disimpan dalam cache, atau jika bersedia untuk pergi keluar di Internet dan berbicara ke server lain untuk menemukan jawaban terbaik.

Banyak serangan keracunan cache memanfaatkan fitur rekursif untuk meracuni sistem. Jadi dengan membatasi rekursi hanya sistem internal Anda, Anda membatasi paparan Anda. Sementara pengaturan ini tidak akan menyelesaikan semua kemungkinan vektor serangan cache keracunan, itu akan membantu Anda mengurangi porsi yang baik dari mereka.

#### *2. DNS attacks occur when an attacker take over a DNS server*

Pada tahun 2009, Twitter menderita serangan terpisah oleh Cyber Army Iran. Kelompok ini diubah catatan DNS dan diarahkan lalu lintas ke propaganda host di server mereka dikendalikan. Kemampuan untuk mengubah pengaturan DNS datang setelah Iran Cyber Army dikompromikan akun email Twitter staf, dan kemudian digunakan bahwa account untuk mengotorisasi perubahan DNS. Selama insiden yang Dyn Inc adalah registrar dihubungi untuk memproses permintaan perubahan. Pertahanan terhadap jenis serangan sering termasuk password yang kuat, dan ACL berbasis IP (daftar klien diterima). Selanjutnya, program pelatihan yang solid yang

berhubungan dengan rekayasa sosial juga akan efektif. Sayangnya, semua waktu dan sumber daya di dunia dapat ditempatkan ke dalam mengamankan webserver, tetapi jika seorang penyerang dapat menyerang server otoritatif dan titik catatan DNS pada alamat IP yang berbeda, ke seluruh dunia masih akan terlihat seperti Anda telah dimiliki. Bahkan itu lebih buruk karena itu satu serangan juga akan memungkinkan mereka untuk mengarahkan email atau layanan lain yang Anda tawarkan. Jadi server hosting otoritatif Anda dengan otoritas dipercaya merupakan cara paling sederhana untuk mengatasi masalah ini.

*3. The most problematic DNS attack to cancel*

Terjadi ketika seorang penyerang dikompromikan pendaftaran domain sendiri, dan kemudian menggunakan akses itu untuk mengubah server DNS yang ditugaskan untuk itu. Pada saat ini, mereka nameserver berwibawa menjawab semua pertanyaan untuk domain terpengaruh. Apa yang membuat serangan ini sangat berbahaya adalah apa yang disebut TTL (waktu alam secara global cache pada server DNS rekursif biasanya 86.400 detik, atau sehari penuh.
Kecuali operator mampu membersihkan cache, dapat mengambil seluruh hari (kadang-kadang lebih lama) untuk efek yang akan terbalik, "tulis von Wallenstein. Saran utama untuk DNS otoritatif adalah untuk meng-host server otoritatif dalam organisasi, memungkinkan untuk kontrol penuh.

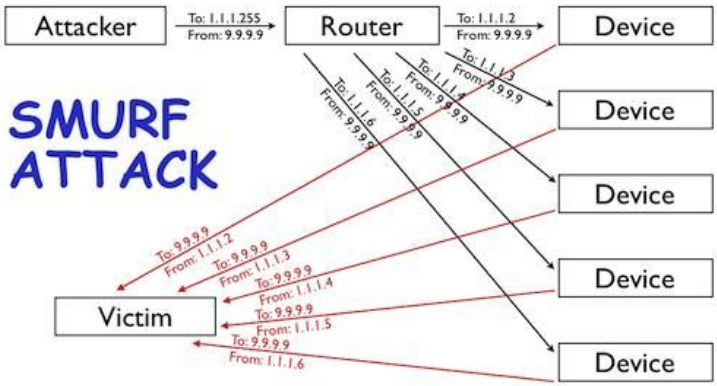
*4. DNS Flooding Attack*

Yaitu menyerang name server dengan cara membanjiri dari berbagai arah sehingga permintaan client untuk menerjemahkan alamat yang dituju menjadi terhambat dan ditolak oleh server pada akhirnya. Pada hal DNS fakta bahwa nameserver tiap zona benar-benar bertanggung jawab untuk melayani catatan zona yang dilayani dan pada gilirannya, untuk pengoperasian setiap sub-zona menyiratkan bahwa ketersediaan mereka melayani setiap permintaan. [3]

*C. Serangan Amplifikasi*

Serangan amplifikasi adalah beberapa terbesar, yang diukur dengan jumlah Gigabits per detik (Gbps). Ukuran yang dari serangan cukup untuk melumpuhkan bahkan web host besar. Bahkan dari perspektif biaya, serangan itu tidak berakhir menambah tagihan bandwidth kami karena cara di mana kita sedang dikenakan biaya untuk bandwidth grosir. DNS Amplifikasi Serangan adalah cara bagi penyerang untuk memperbesar jumlah bandwidth mereka dapat menargetkan pada korban potensial. Bayangkan Anda adalah seorang penyerang dan Anda mengontrol botnet mampu mengirimkan 100Mbps lalu lintas. Sementara yang mungkin cukup untuk mengetuk beberapa situs offline, itu adalah jumlah yang relatif sepele lalu lintas di dunia DDoS.[3]

*Smurf Attack*




Gambar 1. Alur serangan amplifikasi dengan metode smurf attack

Serangan amplifikasi asli dikenal sebagai serangan Smurf. Serangan Smurf melibatkan penyerang mengirimkan permintaan ICMP (yaitu, permintaan ping) ke alamat jaringan broadcast (yaitu, XXX.255) dari router dikonfigurasi

untuk relay ICMP ke semua perangkat di belakang router. Penyerang parodi sumber permintaan ICMP menjadi alamat IP dari korban yang dimaksud. Karena ICMP tidak termasuk jabat tangan, tujuan tidak memiliki cara untuk memverifikasi apakah sumber IP adalah sah. router menerima permintaan tersebut dan dibagikan pada semua perangkat yang duduk di belakangnya. Semua perangkat tersebut kemudian merespon kembali ke ping. Penyerang mampu memperkuat serangan oleh beberapa dari bagaimana pernah banyak perangkat berada di belakang router (yaitu, dimana penyerang menggunakan router yang tersambung dengan 5 perangkat lalu melakukan serangan ke korban beserta serangan yang 5x jauh lebih kuat., yang mana telah ditampilkan pada gambar Gambar 1).[3]

Serangan Smurf Attack adalah serangan secara paksa pada fitur spesifikasi IP yang kita kenal sebagai dirct broadcast addressing. Seorang Smurf hacker biasanya membanjiri router kita dengan paket permintaan echo Internet Control Message Protocol (ICMP) yang kita kenal sebagai aplikasi ping. Karena alamat IP tujuan pada paket yang dikirim adalah alamat broadacast dari jaringan, maka router akan mengrimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Kalau ada banyak host di jaringan, maka akan terjadi penambahan respon trafik ICMP serta permintaan dalam jumlah yang sangat besar.[3]

*1. Akibat dari serangan Smurf :*

Jika si hacker ini memilih untuk men-spoof alamat IP sumber permintaan ICMP tersebut, akibatnya ICMP trafik hanya akan memancetkan jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di spoof, jaringan ini di kenal sebagai jaringan korban (victim). Untuk menjaga agar jaringan kita tidak menjadi perantara bagi serangan Smurf, maka broadacast addressing harus dimatikan di router kecuali jika kita sangat membutuhkannya untuk keperluan multicast yang saat ini belum 100% di definisikan.

*2. Penanggulangan dari serangan Smurf*

Untuk menghindari agar jaringan kita tidak menjadi korban Smurf Attack, sebaiknya kita mempunyai upstream firewall (di hulu) yang di set untuk memfilter ICMP echo atau membatasi trafik echo agar presentasinya kecil dibandingkan trafik jaringan secara keseluruhan. [3]

*D. Serangan DOS*

Serangan Dos adalah serangan hacker melalui networking untuk menyerang suatu sistem dan juga server website. Serangan DoS sering di jumpai pada website-website terkenal khususnya pada pemerintahan. Serangan Dos ini sering di gunakan oleh hacker kelas dunia dan juga website wikileaks yang juga sering membocorkan rahasia-rahasia dokumen negara. Dos ini sendiri menyerang sebuat sitem dengan hitungan detik dan menit, karena serangannya yang cepat ini di butuhkan internet supercepat, serangan sederhana ini di miliki oleh Windows yang sering di kenal dengan nama DDos.

3. Jenis-jenis Serangan Dos:

A. Ping of Death: Ping ini digunakan untuk memeriksa utility ping untuk mengetahui IP dan jenis host yang digunakan. Ping ini sering kita jumpai di CMD pada Windows Xp. Serangan ini sudah tiak terlalu ampuh karena proses yang cukup lama dan website-website juga melakukan jupdate secara berkala.

B. UDP Flood: Serangan ini yang membuat si admin merasa terkejut karena serangan ini korban mendapatkan servernya yang terkena hang pada serangan ini

C. SYN Flooding : Serangan ini mencari kelemahan dalam sistem protocol dan serangan ini mengirimkan Syn kepada komputer target sehingga si korban terus menerima paket-paket data yang tidak di inginkan.

D. Remote Control Attack : Sering disebut sebagai mengendalikan komputer korban dari jarak jauh, penyerang ini dapat di jumpai menggunakan tools-tools terkena yang menghandalkan client.

E. Smurf Attack : Serangan yang memanfaatkan pihak ke tiga di mana si hacker menargetkan kepada si korban melalui daemon-daemon dari tools flooder. [4]

4. Cara mengatasi serangan DOS:

A. Lakukan sesering mungkin terhadap bug-bug dengan cara melakukan patch atau menambal dan back-up data secara berkala.

B. Gunakan firewall agar kemungkinan serangan ini tidak melakukan serangan-serangan data terhadap komputer.

C. Lakukan blocking terhadap IP yang mencurigakan, jika port telah termasuki maka komputer akan dikuasai. Cara megatasinya adalah gunakan Firewall di kombinasikan dengan IDS.

D. Menolak semua paket data dan mematikan service UDP. Selain itu gunakan anti virus yang dimana dapat menangkal serangan data seperti Kapersky (untuk OS berbasis Windows).

E. Lakukan filtering pada permintaan ICMP echo pada firewall.

*E. Pencegahan Serangan DNS*

Ada beberapa pencegahan serangan DNS:

A. Penggunaan terbaik praktek konfigurasi :

1. Software berjalan di lingkungan yang aman
2. Mengidentifikasi aliran data
3. ACL (Access List)
4. Stealth Arsitektur

B. Mengaktifkan DNSSec

C. Pemantauan lalu lintas DNS

1. Mengidentifikasi Log
2. Perangkat selalu diperbaharui, dan melakukan efisiensi penggunaan IP address
3. Harus mengidentifikasi aliran data yaitu menjalankan caching, resolver, server yang otoritatif. Harus memisahkan fungsi dan menonaktifkan fitur yang tidak diinginkan ini akan membantu dalam pencegahan serangan.
4. ACL digunakan untuk mengontrol informasi apa yang akan diterbitkan. Dengan identifikasi aliran data sebagai berikut :

A. Memungkinkan query (server dan tingkat zona)

B. Memungkinkan permintaan cache (tingkat server)

C. Memungkinkan perpindahan (server dan tingkat zona)

D. Memungkinkan update (tingkat zona)

E. Blackhole (tingkat server)

F. Cache negatif (tingkat zona)

5. DNSSEC digunakan untuk melindungi terhadap permintaan / request redirection. DNSSEC menciptakan rantai kepercayaan antara klien dan server otoritatif. Berdasarkan pertukaran kunci dalam catatan sumber daya ditandatangani tertentu.

6. Pengamanan DNS dengan ECC
   Dengan teknologi yang berkembang lebih cepat setiap orang mengakses internet melalui ponsel apakah itu digunakan untuk memeriksa E-Mails atau mengunjungi situs-situs aman, ECC (Elliptic Curve Cryptography) dapat diimplementasikan. ECC memberikan tingkat yang sama Security RSA dengan manfaat dari ukuran key yang kecil, perhitungan cepat, dan memori dan penghematan energi.

## KESIMPULAN

Dalam artikel kami menganalisis tentang serangan dan cara pencegahan DNS. Domain Name System (DNS) adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer; misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima email untuk setiap domain. Ada tiga jenis serangan umum pada DNS yaitu 1.) Cache Poisoning Attack, 2.) Serangan DNS terjadi ketika penyerang mengambil alih server DNS, 3.) Serangan DNS paling bermasalah untuk membatalkan. Sebuah serangan DNS amplifikasi adalah Distributed Denial of Service (DDos) serangan di mana penyerang mengeksploitasi kerentanan dalam sistem nama domain (DNS) server untuk mengubah query awalnya kecil menjadi muatan yang jauh lebih besar, yang digunakan untuk menurunkan server korban. DNS amplifikasi adalah jenis serangan refleksi yang memanipulasi sistem nama domain publik dapat akses, membuat mereka membanjiri target dengan jumlah besar paket UDP.

## DAFTAR PUSTAKA

[1] A. Alabbadi, A. Albilali, A. Almazmoomi, and O. A. Batarfi, "Journal of Environmental Science , Computer Science and Engineering & Technology Efficient Algorithm for Detecting DNS Amplification Attacks," vol. 5, no. 4, pp. 396–406, 2016.

[2] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, "DNS amplification attack revisited," Comput. Secur., vol. 39, no. PART B, pp. 475–485, 2013.

[3] A. Ali and Z. Hudaib, "DNS Advanced Attacks and Analysis," no. 8, pp. 63–74, 2014

[4] A. Anand, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 8, pp. 94–98, 2012.