Analisa Ketahanan Default Firewall Windows Server 2012 Terhadap Kemungkinan Penetration Test dan DDOS Attack

Disusun Oleh:

Henry Augusta Harsono

NIM : 1202184264

PROGRAM STUDI S1 SISTEM INFORMASI

FAKULTAS REKAYASA INDUSTRI

UNIVERSITAS TELKOM

2020

DAFTAR ISI

1.1 Latar Belakang

Server merupakan sistem komputer yang menyediakan layanan layanan tertentu seperti sistem Operasi, program aplikasi maupun data-data informasi kepada komputer lain yang saling terhubung dalam sebuah jaringan komputer.

Diantara banyak sistem Operasi yang digunakan sebagai OS dari suatu web server. Windows Server 2012 menjadi salah satu pilihan yang banyak digunakan oleh user sebagai wadah atau tempat pengimplementasian suatu server, dilansir dari w3Tech, persentase penggunaan Windows Server mencapai 29% dari total seluruh web server yang digunakan di Dunia.

Dengan banyaknya jumlah pengguna, keamanan web server tentunya harus menjadi salah satu concern dan aspek yang diperhatikan oleh pihak yang menggunakan Windows Server sebagai Sistem Operasi server mereka. Sebab, adakalanya web server dikelola oleh individu yang memiliki pengalaman minim dalam pengelolaan suatu web server, meskipun umumnya serangan yang terjadi hanya menimbulkan kesan negatif, memalukan, atau ketidaknyamanan (seperti defacing), tidak menutup kemungkinan penyerang dapat membuat masalah yang lebih serius atau bahkan merugikan.

Oleh karenanya, selain kemampuan teknis yang handal dari seorang network Administrator ataupun System Administrator, kemampuan firewall bawaan Sistem Operasi juga menjadi faktor penentu aman atau tidaknya suatu server dan jaringan komputer. Firewall peka terhadap kesalahan konfigurasi dan administrasi firewall harus dilakukan secara hati-hati. Sebab firewall merupakan garis pertahanan terdepan dari suatu server yang seharusnya dapat bertahan dengan mencegah vulnerabilities

Tulisan ini memuat analisa ketahanan firewall Windows Server 2012 terhadap kemungkinan serangan pihak luar, serta tata cara atau panduan konfigurasi yang aman agar server dapat berjalan dengan aman dan terhindar dari ancaman

1.2 Tujuan Penulisan

Tujuan penulisan makalah ini adalah untuk membahas analisa ketahanan Firewall bawaan Windows Server 2012 dari kemungkinan serangan juga saran tindakan preventif dan saran konfigurasi Firewall windows Server 2012 untuk meningkatkan keamanan Server

1.3 Batasan

Permasalahan yang dibahas pada makalah ini dibatasi pada :

- Firewall Windows Server 2012
- Analisa ketahanan Firewall Windows Server 2012 dari masalah keamanan yang berasal dari serangan pihak eksternal
- Tuning Firewall Windows Server 2012 untuk meningkatkan keamanan

BAB II
PEMBAHASAN MASALAH

A. Konsep dan Prinsip keamanan Jaringan

Keamanan Jaringan komputer sebagai bagian dari Sebuah Sistem Informasi adalah sangat penting untuk menjaga validitas dan Integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak

komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada host yang tidak terhubung kemana-mana dengan mengeksploitasi network Security. Resiko tersebut dapat dikurangi. Namun Network Security biasanya bertentangan dengan network access. karena bila network access semakin mudah maka network access semakin tidak nyaman

2

Suatu jaringan didesain sebagai komunikasi data Highway dengan tujuan meningkatkan access ke sistem komputer, Sementara keamanan dirancang untuk mengontrol akses. Penyediaan Network security adalah sebagai aksi penyeimbang antara open access dengan security

Adapun prinsip keamanan jaringan adalah sebagai berikut :

a) Kerahasiaan (Secrecy)

Secrecy berhubungan dengan hak akses untuk membaca data atau informasi dari suatu sistem komputer. Sistem komputer dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal

b) Integritas

Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem komputer. Dalam hal ini suatu sistem komputer dikatakan aman jika suatu data atau Informasi hanya dapat diubah oleh pihak yang telah diberi hak

c) ketersediaan

Availability berhubungan dengan ketersediaan data atau Informasi pada saat yang dibutuhkan

d) Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa Informasi betul-betul asli dan orang yang mengakses atau membe Informasi adalah betul-betul orang yang memiliki akses.

e) Akses kontrol

Aspek kontrol merupakan pitur-pitur keamanan yang mengontrol bagaimana user dan sistem berkomunikasi dan berinteraksi dengan system dan sumber daya yang lainnya. Akses kontro melindungi sistem dan sumber daya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah proses otentikasi berhasil dilengkapi

F. Non Repudiation

Aspek ini menjaga agar seseorang tidak menyangkal telah melakukan sebuah transaksi. Penggunaan Digital Signature, certificate dan Teknologi kriptografi

B. Sekilas Tentang Windows Server 2012

Windows Server adalah suatu merk sistem operasi yang dikembangkan oleh Microsop Corporation yang mendukung Manage-n Tingkat enterprise, penyimpanan data, aplikasi data komunikasi. Windows Server ini berperan sebagai Server atau data-center yang berperan dalam pengelolaan jaringan Server.

Secara umum, Windows Server menyediakan layanan yang Server-oriented, seperti, menghost website, manajemen sumber daya Semua pengguna dan aplikasi, manajemen pengguna, messaging, keamanan dan otorisasi dan layanan lainnya yang berkaitan deng Server. berikut beberapa kelebihan yang dimiliki oleh windows Server 2012 :

- Server Manager yang lebih mudah digunakan dari versi pendahulu
- Server Core dapat berpindah ke GUI secara langsung tanpa install ulang dan sebaliknya
- Memiliki Virtual Desktop Inprastructure yang lebih kompatibel atau sesuai dengan O.S sebelumnya
- Administrator lebih mudah mengontrol seluruh kegiatan. komputer Client karena adanya aplikasi Hyper-V
- Memudahkan Client Server untuk berbagi File (File-sharing) di dalam jaringan karena adanya pitur Server Message Block.
- Terdapat berbagai tool lainnya yang dapat memudahkan administrator manajemen sistem seperti tools untuk menambahkan roles dan Feature, konfigurasi dan manajemen server. remote administration dan yang lainnya

Adapun kekurangan dari Windows Server 2012 adalah sebagai berikut :

- Harganya mahal
- Tidak support komputer yang menggunakan Itanium
- Sulit digunakan karena ada penambahan pitur baru yang digunakan

C. Windows Server vs Linux Server

Pada bagian ini akan dijelaskan secara singkat perbandingan antara Windows Server jika dibandingkan dengan Linux Server tentunya sebagai bahan pertimbangan terutama dari segi keamanan yang merupakan salah satu topik pada makalah ini, Secara umum perbedaan yang terdapat pada Linux Server dan Windows Server dapat dilihat pada tabel dibawah :

Scipt Languages	proprietary	Open-source
Web Servers	Miarosopt IIS	Apache, Nginx, etc
Databases	MS SQL	MySQL
	Microsopt Access	MariaDB
Administrative software	Plesk	cPanel, Plesk, Conpixx
misc	Exchange	Wordpress
	.NET-App	Joomla
	Sharepoint.	dll.
	etc	
	Windows	Linux

Dari segi keamanan VPS Linux memiliki sistem operasi berbasis UNIX yang menawarkan keamanan yang lebih baik terhadap virus spyware, malware dan yang lainnya.

VPS Windows dianggap cukup aman bilamana dikonfigurasi dengan baik dan benar, sebab pada dasarnya semua sistem operasi dibangun dengan mengikuti standar yang memang ditetapkan oleh user secara luas, namun memang windows lebih banyak memiliki celah jika dibandingkan dengan sistem Operasi yang berbasis Unix seperti Linux

Selain itu hak akses yang ketat juga menyebabkan Linux secara umum lebih aman dari windows, misalnya jika kita ingin mengCopy dan mengedit file di komputer dengan OS Linux, maka kita harus memiliki hak akses terlebih dahulu, bahkan jika kita lupa password login, sangat sulit untuk masuk kembali ke komputer kita selain dengan melakukan Install ulang

D. KETAHANAN FIREWALL WINDOWS SERVER 2012

Sebelum memulai pembahasan pokok, kita akan mengenali terlebih dahulu konsep dan cara kerja firewall, dan bagaimana Firewall windows Server 2012 terhadap berbagai kemungkinan Ancaman, khususnya pada DDOS Attack dan Penetration Testing, kedua ancaman yang tadi disebutkan merupakan 2 ancaman yang dijadikan studi kasus pada pembahasan kali ini.

Sebelum membahas bagaimana firewall bereaksi terhadap DDOS Attack dan Penetration Testing, ada baiknya kita bahas kedua ancaman tersebut untuk mendapatkan pemahaman yang komprehensif dan maksimal.

I PENETRATION TEST dan DDOS Attack

a) Penetration Test

Penetration Testing atau biasa disebut Pentest adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan komputer untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Orang yang melakukan kegiatan ini disebut sebagai penetration tester

Latar belakang diperlukannya pentest adalah untuk memastikan bahwa sistem dan rancangan arsitektur yang diimplementasikan sudah aman dari segala jenis vulnerabilities dan celah yang memungkinkan terjadinya pencurian data, dan ancaman keamanan lainnya.

Dapat dikatakan bahwa penetration Testing merupakan salah satu komponen penting dari security audit. Secara umum, Langkah-langkah penetration testing adalah sebagai berikut

- Langkah pertama adalah perencanaan, pada tahap ini scope, waktu, jumlah tim, dokumen legal, dan kesiapan resource dibicarakan dan didiskusikan di tim

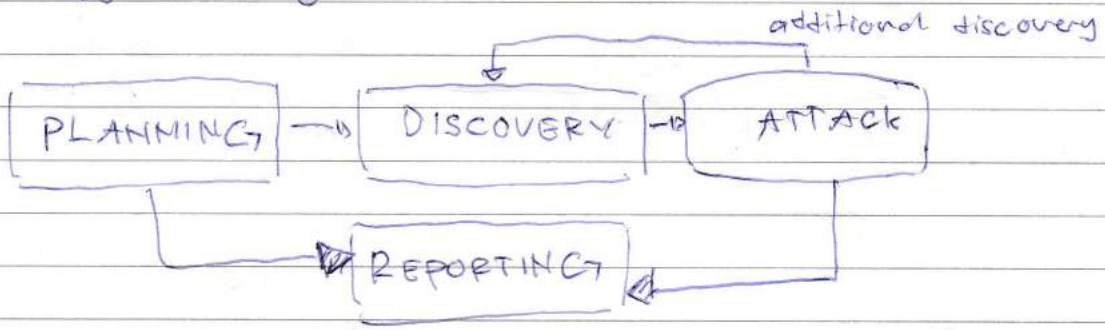
- Langkah berikutnya adalah Information Gathering dan Analysis, pada tahap ini semua informasi yang berkaitan dengan sistem target dikumpulkan, banyak alat yang dapat digunakan untuk membantu proses ini seperti misalnya adalah netcraft.com, kemudian dilakukan network survey untuk mengumpulkan informasi domain, server, nmap, host, firewall dan lain-lain

- Langkah selanjutnya adalah vulnerability detection atau pencarian celah keamanan, setelah mengetahui informasi tentang sistem, barulah pencarian celah keamanan bisa dilakukan, baik secara manual ataupun otomatis

- Setelah melakukan vulnerability detection, maka dilakukan percobaan penyerangan, pada proses ini dilakukan adalah dengan melakukan social engineering dan pengujian physical Security dari sistem

- Tahap berikutnya adalah analisis dan pembuatan Laporan, disini biasanya dilaporkan tentang langkah kerja yang dilakukan celah keamanan yang ditemukan serta usulan perbaikan. Tahap selanjutnya adalah tindak lanjut, yang dilakukan bersama system administrator untuk memperbaiki sistem

Metodology diatas dapat diringkas atau digambarkan dengan menggunakan gambar dibawah



6) DDOS Attack

Distributed Denial of Service atau yang disingkat dengan DDoS adalah salah satu jenis cyber-attack yang menyasar website, layanan online, maupun jaringan dengan cara membanjirinya dengan fake trappic yang sangat banyak. Motif utamanya adalah agar

· Server atau jaringan ~~and~~ tidak mampu mengakomodasi lalu lintas tersebut. Sehingga menyebabkan website/layanan anda down dan tidak bisa beroperasi.

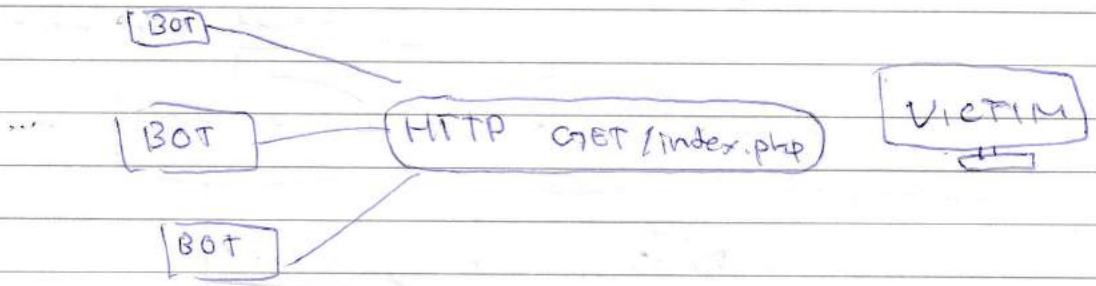
Berhasil atau tidaknya teknik DDoS dipengaruhi oleh kemampuan server menampung seluruh request yang diterima dan juga kinerja firewall saat ada reques yang mencurigakan

Konsep sederhana DDoS attack adalah ~~mempetegas~~, membanjiri jaringan dengan banyak data. Konsep Denial of Service bisa dibagi menjadi 3 tipe penggunaan, yakni sebagai berikut :

- Request flooding,
  Teknik ini membanjiri jaringan menggunakan banyak request. Akibatnya, pengguna lain yang terdaftar tidak dapat dilayani
- Trappic Flooding
  Teknik ini membanjiri lalu lintas dengan banyak data yang berakibat pengguna lain tidak dapat dilayani

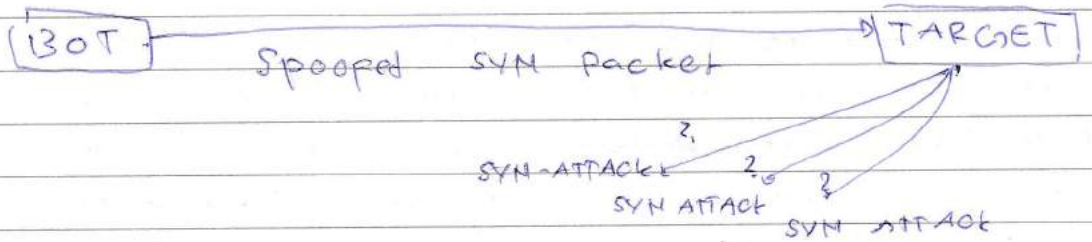
Sedangkan jika dikategorikan berdasarkan layer OSI, Jenis ada serangan pada layer aplikasi, protokol dan numerik

- DDOS Layer Aplikasi



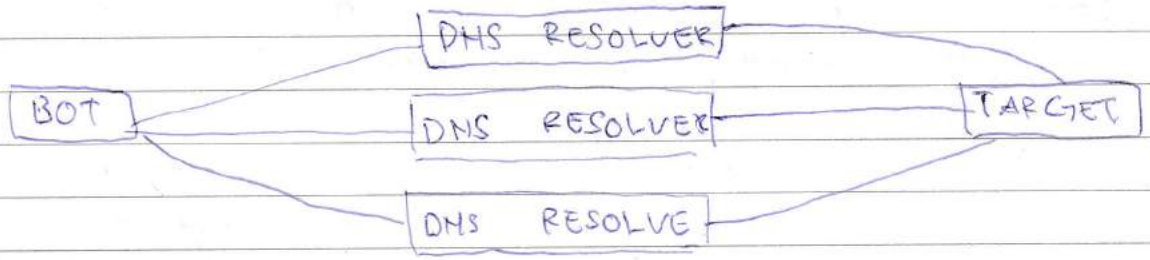
Target dari serangan ini adalah layer dimana halaman website direkasekusi di sisi server dan sangat ringan jika hanya melayani 1 request namun menjadi masalah jika melayani banyak request secara bersamaan.

- -DDOS protokol



Serangan ini mengeksploitasi TCP dengan cara mengirimkan paket SYN dengan spoof alamat IP dalam jumlah besar. Setiap koneksi yang masuk akan ditanggapi oleh server yang menunggu proses koneksi berjalan, namun tidak pernah terjadi. Sehingga proses di server mengasi overload

- Volumetrik DDOS



Tujuan dari serangan DDoS ini adalah menghabiskan semua bandwith yang tersedia antara target dan jaringan Internet. Caranya adalah dengan membuat lalu lintas yang sangat padat, seperti penggunaan botnet.

Tipe serangan yang lainnya adalah Cached DDOS, NTP Amplikasi DNS Flood, UDP FLOOD, dan masih banyak yang lainnya.

II KETAHANAN FIREWALL WINDOWS SERVER 2012 DARI DDoS ATTACK dan PENETRATION TESTING

a) Mekanisme kerja Firewall Windows server 2012

Firewall adalah software berupa sistem keamanan yang berguna untuk melindungi komputer dari berbagai gangguan dan ancaman pada jaringan. Firewall bekerja untuk memonitor, mengkontrol, dan selayaknya saklar yang menutup komputer dengan jaringan Internet yang luas jangkauan

Firewall pada windows Server 2012 beroperasi salah set dengan memantau dan memblokir semua informasi, baik keluar atau masuk ke sistem, yang tidak memenuhi rules yang telah dikonfigurasi, Penerapan firewall dibagi menja 2 kategori, yaitu firewall jaringan dan firewall host, fir Jaringan adalah firewall yang memantau informasi yang kel atau masuk sebuah jaringan, Sedangkan firewall host adala firewall yang memantau informasi yang keluar/masuk Sebuah komputer tanpa memperdulikan jaringan tempat komputer tersebut diletakkan.

Di Makalah ini ~~kakan~~ dibahas analisa ketahanan firew windows Server 2012 dari penetration dan DDoS Attack berdasarkan cara kerja dan fitur pada windows Server 2012 yang dapat mendeteksi serangan kepada sistem.

1) Port Scan Detection

Port scanner merupakan aplikasi yang digunakan untuk melihat informasi atau status dari protocol dan port yang terbuka dari sebuah perangkat, Dengan aplikasi ini ~~kaitan~~ bisa jadi merupakan sebuah awal dari simulasi serangan terhadap resource di jaringan, ketia informasi protocol dan port sudah didapat, maka hacker bisa memanfaatkan untuk melakukan eksploitasi dari protocol atau port tersebut, misalnya DDoS,

kemungkinan dilakukannya port scanning ini sudah ditutup oleh windows Server 2012 dengan adanya port scan Detection, bahkan fitur ini sudah tersedia sejak windows Server 2003, kemungkinan DDOS Attack yang berawal dari port scanning sudah ditutup

2) Packet Filtering

Packet filtering adalah fitur bawaan dari firewall windows server 2012. meskipun perlu dikonfigurasi lebih lanjut untuk meningkatkan efektifitas dan keamanan sistem, namaun secara default fitur ini sudah cukup aman untuk menahan DDoS Attack

Dengan konfigurasi packet filtering yang sesuai, maka DDoS Attack bisa dicegah, diantara atribut yang dapat digunakan untuk membuat pemfilteran packet

- alamat IP sumber
- alamat IP tujuan
- Protokol IP
- Port TCP IP dan UDP Sumber
- port TCP IP dan UDP Tujuan
- Antar muka tempat datangnya paket
- Antar muka tempat tujuan paket

3) IDS (Intrution Detection System)

IDS adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan kegiatan yang mencurigakan didalam sebuah jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan yang berhubu dengan traffic jaringan maka IDS akan memberikan peringa kepada sistem atau administrator jaringan.

Dalam banyak kasus, IDS pada windows Server 2012 juga dapat merespon terhadap anomali traffic dan memblokir alamat IP tertentu dari usaha mengakses Jaringan.

IDS pada windows Server 2012 dapat menggunakan beberapa pendekatan berbeda dalam mendeteksi anomali atau ketidakwajaran traffic dari IP tertentu. diantara pendekatannya adalah :

- NIDS (Network IDS)
  IDS jenis ini ditempatkan pada titik strategis di jaringan untuk mengawasi trappic yang menuju device di perangkat
- HIDS (Host Intrution Detection System)
  IDS jenis ini berjalan pada host yang berdiri sendiri atau perlengkapan dalam jaringan, HIDS dapat mengawasi paket yang berasal dari dalam maupun luar sebatas pada salah satu alat saja
- dll

4) Stateful Inspection

Sistem ini menelusuri packet yang diterima dengan aktivitas aktivitas sebelumnya. packet yang diterima kemudian diperiksa dalam database packet, jika packet berkonotasi positip atau tidak menimbulkan resiko bahaya, maka ia akan diteruskan ke sistem yang meminta. Setelah firewall selesai memeriksa paket, ia akan merespon dengan salah satu atau 3 cara : accept. reject dan drop

5) Proxy Service

Proxy service adalah aplikasi yang bekerja sebagai penghubung antara sistem jaringan. Aplikasi proxy berada di dalam firewall dan bertugas untuk memeriksa packet yang saling ditukarkan dalam jaringan.

Sistem proxy service pada Windows Server bisa dikatakan epektif untuk melindungi sistem dari DDoS attack. Sebab semua informasi yang diperiksa secara tersentralisasi. cara kerja ini bisa dikatakan canggih karena proxy service berusaha menciptakan hubungan antar jaringan yang mirip. Proxy seolah menghubungkan jaringan secara langsung, padahal ia hanya berusaha meng copy mekanisme yang mirip.

BAB III

Kesimpulan dan Penutup

3.1 Kesimpulan

Firewall pada windows Server dapat melindungi dan menjaga jaringan dan perangkat yang menggunakannya, dari DDoS Attack dan juga penetration test jika dilakukan konfigurasi secara lebih baik dan tepat guna. ~~meski~~ Sebab pengaturan bawaan Windows Firewall di Windows Server 2012 tidak cukup untuk menghadap DDoS Attack dan penetration yang dilakukan dengan teknik yang advance. Selain itu konfigurasi juga harus terus menerus diperbaharui dengan mempertimbkan aspek keamanan yang menyesuaikan dengan skalab dari sistem

~~DA~~

DAFTAR PUSTAKA

- Mulyana, Eueung, Onno W Purbo, "Firewall : Sekuriti Internet Computer Network Research Group, ITB, Bandung (2000)
- Roji, Muhammad Fatkhur, "SISTEM KEAMANAN INTERNET DENGAN IPTABLES FIREWALL". DINAMIKA 11 (2010)
- Asisten Lab sisgar, "Modul Praktikum Dasisop" Lab sisgar, Bandung, 2020