PENERAPAN SISTEM IDS SURICATA DAN IPTABLES PADA SERANGAN DDOS

SKRIPSI

disusun oleh

Bayu Nugraha

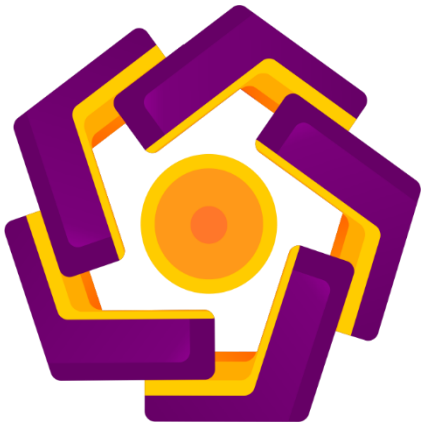
14.11.7812

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018

PENERAPAN IDS SURICATA DAN IPTABLES PADA SERANGAN DDOS

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Bayu Nugraha

14.11.7812

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018

PERSETUJUAN

SKRIPSI

PENERAPAN IDS SURICATA DAN IPTABLES PADA SERANGAN DDOS

yang dipersiapkan dan disusun oleh

Bayu Nugraha

14.11.7812

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 Mei 2018

Dosen Pembimbing,

Sudarmawan, MT
NIK. 190302035

PENGESAHAN

SKRIPSI

PENERAPAN IDS SURICATA DAN IPTABLES PADA SERANGAN DDOS

yang dipersiapkan dan disusun oleh

Bayu Nugraha

14.11.7812

telah dipertahankan di depan Dewan Penguji
pada tanggal 25 April 2018

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Melwin Syafrizal, S.Kom, M.Eng **NIK. 190302105**	
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	
Sudarmawan, MT **NIK. 190302035**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 8Mei 2018

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T
NIK. 190302038

iii

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 8 Mei 2018

Bayu Nugraha
14.11.7812

MOTTO

Rasulullah *shallallahu 'alaihi wa sallam bersabda*,

طَلَبُ الْعِلْمِ فَرِيضَةٌ عَلَى كُلِّ مُسْلِمٍ

*Menuntut ilmu itu **wajib** atas setiap muslim".* **(HR. Ibnu Majah. Dinilai *shahih* oleh Syaikh Albani dalam *Shahih wa Dha'if Sunan Ibnu Majah* no. 224)**

Rasulullah *shallallahu 'alaihi wa sallam bersabda*,

وَمَنْ سَلَكَ طَرِيقًا يَلْتَمِسُ فِيهِ عِلْمًا سَهَّلَ اللَّهُ لَهُ بِهِ طَرِيقًا إِلَى الْجَنَّةِ

"*Siapa yang menempuh jalan untuk mencari ilmu, maka Allah akan mudahkan baginya jalan menuju surga.*" **(HR. Muslim, no. 2699)**

Rasulullah *shallallahu 'alaihi wa sallam bersabda*,

الْمُؤْمِنُ الْقَوِىُّ خَيْرٌ وَأَحَبُّ إِلَى اللَّهِ مِنَ الْمُؤْمِنِ الضَّعِيفِ وَفِى كُلٍّ خَيْرٌ احْرِصْ عَلَى مَا يَنْفَعُكَ وَاسْتَعِنْ بِاللَّهِ وَلاَ تَعْجِزْ وَإِنْ أَصَابَكَ شَىْءٌ فَلاَ تَقُلْ لَوْ أَنِّى فَعَلْتُ كَانَ كَذَا وَكَذَا وَلَكِنْ قُلْ قَدَرُ اللَّهِ وَمَا شَاءَ فَعَلَ فَإِنَّ لَوْ تَفْتَحُ عَمَلَ الشَّيْطَانِ

"Seorang mukmin yang kuat lebih baik dan lebih Allah cintai daripada seorang mukmin yang lemah, dan masing-masing berada dalam kebaikan. Bersungguh-sungguhlah pada perkara-perkara yang bermanfaat bagimu, mintalah pertolongan kepada Allah dan janganlah kamu bersikap lemah. Jika kamu tertimpa sesuatu, janganlah kamu katakan: 'Seandainya aku berbuat demikian, pastilah akan demikian dan demikian' Akan tetapi katakanlah: 'Qoddarallah wa maa syaa fa'ala (Allah telah mentakdirkan hal ini dan apa yang dikehendakiNya pasti terjadi)'. Sesungguhnya perkataan 'Seandainya' membuka pintu perbuatan setan." **(HR. Ahmad 9026, Muslim 6945, dan yang lainnya).**

Ibnu Qayyim Al-Jauziyah *rahimahullah* berkata,

وَنَفْسُكَ إِنْ أَشْغَلْتَهَا بِالحَقِّ وَإِلاَّ اشْتَغَلَتْكَ بِالبَاطِلِ

"Jika dirimu tidak disibukkan dengan hal-hal yang baik, pasti akan disibukkan dengan hal-hal yang batil

Ibnu Sirin –*rohimahulloh*-

"Sungguh ilmu ini adalah agama kalian, maka lihatlah darimana kalian mengambil agama kalian". **(*Muqoddimah Shahih Muslim* 1/14).**

PERSEMBAHAN

Segala puji bagi Allah Subhanahu wa Ta'ala. Yang atas limpahan rahmat dan ridho-Nya telah memberikan kesehatan, kelancaran sehingga penulis dapat menyelesaikan penelitian ini dengan sangat baik. Sholawat serta salam semoga senantiasa tercurahkan kepada Nabi Muhammad Shallallahu 'Alaihi wa Sallam. Penelitian tentang **Penerapan Sistem IDS Suricata dan Iptables Pada Serangan Ddos**. Yang penulis persembahkan kepada:

1. Kedua orang tua tercinta, Bapak N.qoliq dan Bu Eli Ramadhaniah, yang telah menjadi orangtua terhebat, tak lelah memberikan doa, dukungan dan nasehat kepada penulis sehingga terciptanya penelitian ini.
2. Adikku Hezky Wardhan Putra dan Abyakta Chandra Subkhi yang selalu ku rindukan yang semoga Allah menjaga dan merahmati keduanya.
3. Keluarga Besar Mbah Soidi yang selama ini mendukung dan memberi nasehat kepada penulis.
4. Bapak Sudarmawan, MT. selaku dosen pembimbing yang senantiasa membimbing dengan penuh kesabaran dan selalu memberikan solusi agar skripsi ini dapat terselesaikan dengan baik.
5. Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah memberikan banyak materi, sehingga dapat dijadikan sebagai ilmu-ilmu yang menunjang penelitian ini.
6. Terimakasih untuk Rafi alias Odon yang telah memimjamkan Laptop selama 2 Bulan lebih untuk membantu mengerjakan skripsi penulis.
7. Untuk group BAP yang selalu ribut dan terkadang menjadi hiburan bagi penulis dalam mengerjakan skripsi.
8. Agung Wahyudi selaku sahabat dari SMK hingga sekarang yang selalu ada saat diminta bantuan.
9. Rizky Mahardhyka teman dari SD hingga sekarang, Gildan Prastowo, Sulthan Ariq yang terkadang laptopnya dipinjam untuk mengerjakan skripsi, Diski Rahmanto dan Syahmi Perkasa teman kost penulis selama di

Yogyakarta yang selalu ada pada setiap minta bantuan selama tinggal di Yogyakarta.

10. Khairul Azhar yang telah membantu proses dalam mendokumentasikan naskah skripsi ini dan yang telah banyak membantu.
11. Sahabat serta rekan - rekan di TI-04 yang selama ini telah berbagi pengalaman dan keceriaan penulis dalam banyak hal suka maupun duka yang telah menjadi bagian yang tak terpisahkan dan terlupakan dalam menuntut ilmu dalam beberapa tahun terakhir ini.
12. Fathur, Mas Hilal, Mas Andi, Ihsan, Rofiq, Feri Harmas Firman, Iqbal, Mas Dede, Pak Heri dan Harris yang selalu menyemangati, mendukung dan menghibur penulis selama masa pengerjaan skripsi ini hingga selesai.
13. Sahabat serta rekan-rekan Ikhwan dan para Asatidz yang bermanhaj Salaf di Yogyakarta yang memberi nasehat dan dukungan yang bermanfaat bagi penulis.

Seluruh pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu sehingga skripsi ini dapat terselesaikan.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT karena atas limpahan rahmat, hidayah serta inayah-Nya penulis masih diberi kesempatan dan kemudahan untuk menyelesaikan skripsi ini. Shalawat beserta salam semoga senantiasa tercurahkan kepada Nabi Muhammad SAW, kepada keluarganya, para sahabatnya, hingga kepada umatnya hingga akhir zaman, amin.

Skripsi ini disusun dalam rangka memenuhi salah satu syarat kelulusan perguruan tinggi Program Studi Strata-1 Informatika di Universitas AMIKOM Yogyakarta. Selain itu skripsi ini juga bertujuan agar pembaca dapat menambah pengetahuan tentang Implementasi Tanda Tangan Digital MD5 dan Enkripsi Algoritma RSA pada Resep Dokter Digital. Penulis juga mengucapkan terima kasih yang setulus-tulusnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Sudarmawan, S.T, M.T selaku dosen pembimbing, Dekan Fakultas Sains dan Teknologi, dan Ketua Program Studi S1 Informatika yang senantiasa memberikan bimbingan, waktu, dan arahan dalam pembuatan skripsi ini.
3. Segenap dosen dan staf Universitas AMIKOM Yogyakarta yang telah memberikan banyak ilmu dan pengalaman.
4. Kedua Orangtua yang tak pernah lelah mendoakan, memberikan nasehat dan dukungan.
5. Sahabat serta rekan-rekan 14-S1TI-04 yang memberikan banyak dukungan dan berbagi pengalaman.
6. Seluruh pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu sehingga skripsi ini dapat terselesaikan.

Semoga Allah SWT memberikan balasan yang berlipat ganda kepada semuanya. Penulis juga memohon maaf apabila dalam penyusunan skripsi ini masih banyak kekurangan dan masih jauh dari kata sempurna. Demi perbaikan

selanjutnya, saran dan kritik yang membangun akan penulis terima dengan senang hati. Akhirnya, hanya kepada Allah SWT penulis serahkan segalanya. Semoga skripsi ini dapat menambah pengetahuan dan memberikan manfaat bagi para pembacanya maupun diri penulis sendiri serta dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 8 Mei 2018

Bayu Nugraha

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Pengguna internet setiap hari semakin meningkat, mulai dari anak-anak hingga orang dewasa. Karena mengakses jaringan internet saat ini sangat mudah dan murah, bisa melalui PC / Laptop dan Smarthphone.

Untuk melakukan semua itu maka di perlukan seorang Server dan Server administrator untuk memperhatikan keamanan data di Server terebut. Jadi harus diawasi untuk orang yang tidak bertanggung jawab yang disusupi ke Server.

Untuk mengamankan dan mencegah serangan Ddos (Distributed Denial Of Service) perlu menerapkan sistem dalam jaringan menggunakan Suricata sebagai Network Intrusion Detection System (NIDS) dan aplikasi Iptables. Setelah analisis --hashlimit-upto dengan nilai 100000 stabil untuk diterapkan dalam sistem. Hasilnya sebelum menggunakan sumber daya Iptables CPU 1 adalah 97,1% dan CPU 2 63,7%, setelah diterapkan --hashlimit-upto 100000 kemudian CPU 1 menjadi 60,6% dan CPU 2 adalah 59,9%.

Kata Kunci : IDS Suricata, Iptables, Hashlimit.

ABSTRACT

Everyday internet users are increasing, ranging from children to adults. Because accessing the internet network today is very easy and cheap, can be through PC / Laptop and Smarthphone.

To do all that then in need of a Server and Server administrator to pay attention to data security on the Server terebut. So it should be watched for irresponsible people infiltrated to the Server.

To secure and prevent Ddos attacks (Distributed Denial Of Service) need to implement system in network using Suricata as Network Intrusion Detection System (NIDS) and Iptables application. After a --hashlimit-upto analysis with a value of 100000 is stable to be applied in the system. The result before using Iptables resources CPU 1 is 97.1% and CPU 2 63.7%, after applied --hashlimit-upto 100000 then CPU 1 to 60.6% and CPU 2 is 59.9%.

Keyword : *IDS Suricata, Iptables, Hashlimit.*