ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program studi Informatika

disusun oleh

Rachmat

19.11.2638

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program studi Informatika

Disusun oleh

Rachmat

19.11.2638

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI

yang disusun dan diajukan oleh

Rachmat

19.11.2638

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 28 Februari 2023

Dosen Pembimbing,

Sudarmawan S.T, M.T

NIK. 190302035

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI

yang disusun dan diajukan oleh

Rachmat

19.11.2638

Telah dipertahankan di depan Dewan Penguji
pada tanggal 28 Februari 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Irma Rofni Wulandari, S.Pd., M.Eng **NIK. 190302329**	
Ahlihi Masruro, M.Kom **NIK. 190302148**	
Sudarmawan, S.T., M.T **NIK. 190302035**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Februari 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rachmat
NIM : 19.11.2638

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI

Dosen Pembimbing : Sudarmawan S.T, M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 28 Februari 2023

Yang Menyatakan,

Rachmat

PERSEMBAHAN

Alhamdulillah hirobbil ‘alamin, segala puji kepada Allah SWT berkat rahmat serta anugrah, dan karunianya sehingga skripsi ini dapat diselesaikan dengan lancar dan baik. Oleh karenanya penulis mengucapkan terimakasih kepada :

1. Ucapan rasa syukur dan terimakasih kepada Allah SWT, atas petunjuk dan diberikan kelancaran dalam proses penelitian.
2. Untuk kedua orang tua, yang telah mendoakan dan memberikan support dari materi hingga mampu menyelesaikan skripsi ini
3. Dosen Pembimbing, yang selalu memberikan arahan dan memberikan waktunya agar skripsi ini cepat terselesaikan.
4. Rasa terimakasih kepada teman-teman atas saran dan arahannya selama dalam proses pengerjaannya.

KATA PENGANTAR

Assalmu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur peneliti panjatkan kehadiran Allah SWT karena atas rahmat dan karunia-Nya, sehingga peneliti masih diberikan kesehatan dan kemudahan hingga penyusunan naskah skripsi ini dapat berjalan dengan baik dan lancar.

Skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perguruan tinggi program studi Strata 1 Informatika Universitas Amikom Yogyakarta. Dibuatnya skripsi ini salah satunya bertujuan untuk memberikan informasi dan menambah pengetahuan kepada pembaca mengenai keamanan serta monitoring jaringan.

Saya menyadari bahwa dalam proses penyusunan laporan ini tidak pernah lepas dari dorongan dan bantuan dari berbagai pihak, yang telah memberi bantuan kepada saya baik berupa pemikiran, tenaga, peran serta maupun berwujud barang dan uang. Dalam kesempatan ini saya mengucapkan terima kasih kepada pihak-pihak yang telah banyak membantu dalam pelaksanaan dan penyusunan laporan diantara-Nya :

1. Bapak Prof. Dr. Suyanto, M.M., selaku rektor Universitas Amikom Yogyakarta.
2. Bapak Sudarmawan S.T, M.T selaku dosen pembimbing yang telah memberikan bimbingan, saran dan masukannya dalam menyelesaikan naskah skripsi ini.
3. Hanif Al Fatta,S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Ibu Windah Mega Pradnya D,M.Kom selaku ketua Program Studi Informatika Universitas Amikom Yogyakarta.
5. Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu, dan pengalaman selama masa perkuliahan.
6. Kedua Orang tua yang telah memberikan bantuan dukungan serta doa.

7. Teman-teman dan sahabat yang telah memberikan arahan, motivasi dan bantuan dalam pengerjaan skripsi ini.
8. Semua pihak yang telah membantu sampai selesaikan-Nya penyusunan skripsi .

penulis menyadari sepenuhnya, bahwa skripsi ini tidak luput dari berbagai kekurangan, baik dari segi bahasa, sistematika penulisan maupun penyajian materi. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari berbagai pihak. Semoga skripsi ini dapat bermanfaat bagi penulis pada khususnya dan bagi pembaca serta dapat digunakan sebagai referensi untuk penelitian.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Wonomulyo, 16 Januari 2023

Rachmat

NIM. 19.11.2638

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

INTISARI

Pada era seperti sekarang ini kebutuhan akan akses internet semakin dibutuhkan. Seiring berkembangnya waktu keamanan dunia internet juga perlu diperhatikan karena dapat mengancam keamanan pada jaringan tersebut. Router berperan penting terutama untuk menghubungan ke jaringan intenet. Sering kali router dijadikan target serangan yang dilancarkan guna mencari celah keamanan didalamnya. Router yang terhubung langsung ke ip publik lebih rentan terkana serangan karena langsung dapat diakses di jaringan internet. Serangan yang paling banyak merupakan *exploit* yaitu mencari kelemahan pada router dengan memanfaatkan port yang terbuka dan kelemahan pada *firewall* sehingga seseorang dapat lebih mudah masuk ke sistem. Agar dapat mengamankan router bisa menggunakan rule pada *firewall.*

Penggunaan *Instrusion Detection System (IDS)* dan *Port Blocking* biasa digunakan untuk mengamankan router dari serangan orang tidak bertanggung jawab yang memanfaatkan kerentanan pada router. *Instrusion Detection System (IDS)* digunakan untuk mendeteksi jika terdapat serangan pada perangkat sedangkan *Port Blocking* digunakan untuk memblokir serangan tersebut serta membantu mengijinkan perangkat diakses oleh jaringan tertentu. Terdapat juga monitoring pada router yang dapat digunakan untuk memantau jika ada problem dari router tersebut baik dari trafik yang digunakan maupun terdapat serangan bisa langsung dilihat dari aplikasi monitoring tersebut.

Hasil dari penelitian ini adalah untuk membuat keamanan dan perlindungan router dari serangan *exploit* yang memanfaatkan port terbuka terutama dari pihak luar yang ingin mengakses router, sehingga memproteksi router dari ancaman seperti *port scanning, DDOS, dan brute force*. Serta menerapkan monitoring server yang digunakan untuk memantau kondisi jaringan. Setelah firewall diterapkan tingkat keberhasilan melakukan port scanning, ddos, dan brute force adalah 0.

Kata Kunci : *Exploit, firewall, Instrusion Detection System (IDS), Port Blocking, port scanning, DDOS, brute force.*

ABSTRACT

In the current era the need for internet access is increasingly needed. As the development of the security time of the internet also needs to be considered because it can threaten security on the network. The router plays an important role especially to connect to the Intenet Network. Often routers are targeted by attacks launched to find security gaps in it. Routers that are connected directly to the public IP are more vulnerable to attack because they can be directly accessed on the internet network. The most attack is an exploit that is looking for weaknesses in the router by utilizing open ports and weaknesses in the firewall so that someone can more easily enter the system. In order to secure the router, you can use a rule on the firewall.

The use of the Instrusion Detection System (IDS) and Port Blocking is commonly used to secure the router from irresponsible attacks that utilize vulnerability to the router. Instrusion Detection System (IDS) is used to detect if there is an attack on the device while the blocking port is used to block the attack and helps allow the device to be accessed by certain networks. There is also a monitoring on a router that can be used to monitor if there is a problem from the router both from the traffic used and there is an attack can be directly seen from the monitoring application.

The results of this study were to create security and protection of routers from exploit attacks that utilize open ports, especially from outsiders who want to access routers, thus protecting routers from threats such as port scanning, DDOS, and Brute Force. And implement server monitoring used to monitor network conditions. After the firewall is applied to the level of success in doing port scanning, ddos, and brute force ports are 0

Keywords *: Exploit, firewall, Instrusion Detection System (IDS), Port Blocking, port scanning, DDOS, brute force*