Jurnal Teknologi, Kesehatan, dan Sosial (JUTEKS)
Journal homepage: https://journal.universitasbumigora.ac.id/index.php/juteks/
Published by Universitas Bumigora, Mataram, Indonesia, ISSN: XXXX-XXXX.

Analisa Penerapan Network Access Control (NAC) Untuk Keamanan Jaringan

Husrikal Fauzi, Lilik Widyawati, Khairan Marzuki
Universitas Bumigora, Mataram, Indonesia

Abstrak

Keamanan jaringan merupakan aspek kritis dalam pengelolaan sistem informasi, terutama dengan semakin kompleksnya infrastruktur teknologi informasi dan meningkatnya ancaman siber, dalam upaya untuk mengamankan jaringan dari ancaman yang terus berkembang, Penerapan Network Access Control(NAC) menjadi salah satu opsi untuk pengamanan data pada suatu jaringan, sebelum suatu perangkat mengakses jaringan perlu adanya persetujuan dari network access control, dan NAC akan memblokir segala bentuk penyerangan. Metodologi yang diterapkan dalam penelitian ini adalah Network Development Life Cycle (NDLC) . Terdapat 3(tiga) tahapan yang digunakan yaitu Analsis, Desain, dan Simulai Prototipe. Berdasarkan hasil uji coba yang telah dilakukan yang di ujikan ke perangkat server yang uji cobakan dengan 3 (tiga) serangan yaitu serangan DDOS, serangan brute force dengan protokol SSH dan brute force dengan protokol FTP percobaan dilakukan sebelum dan sesudah penerapam system keamanan yang diterapkan yaitu Network Acces Control dengan Packet Fence Kesimpulan dari penelitian ini adalah penerapan Network Acces Control menggunakan tool packet fence berhasil memblokir tiga jenis serangan yang ditujukan ke perangkat server secara realtime. Jenis serangan yang digunakan yaitu Distributed Denial of Service (DdoS), bruteforce dengan protokol SSH dan bruteforce dengan protolkol FTP.

Abstract

Network security is a critical aspect of information system management, especially given the increasing complexity of IT infrastructure and the rising number of cyber threats. To safeguard networks against evolving threats, implementing Network Access Control (NAC) has become one of the key options for securing data within a network. Before a device is allowed to access the network, it must first be authorized by the NAC system, which can block any form of attack. This study adopts the Network Development Life Cycle (NDLC) methodology, consisting of three main phases: Analysis, Design, and Prototype Simulation. Based on testing conducted on a server device, the system was subjected to three types of attacks: Distributed Denial of Service (DDoS), brute force attacks via SSH, and brute force attacks via FTP. These tests were performed both before and after implementing the security system—Network Access Control using PacketFence. The results show that the implementation of Network Access Control with PacketFence successfully blocked all three types of attacks on the server in real time. The study concludes that NAC with PacketFence is effective in protecting servers against DDoS and brute force attacks using both SSH and FTP protocols.

Informasi Artikel

Kata Kunci: Keamanan; Network Access Control (NAC); Packet Fence.

Keywords: *Security; Network Access Control (NAC); Packet Fence.*

Riwayat Artikel:
Diterima : 02-05-2025
Direvisi : 16-05-2025
Disetujui : 28-05-2025

Corresponding Author:
Husrikal Fauzi,
Email: husrikalfauzy@gmail.com

Vol. 1, no. 1, hlm. 47-56, Mei 2025
DOI: 10.30812/juteks.v1i1.5187

How to cite:
H. Fauzi, L. Widyawati & K. Marzuki , "Analisa Penerapan Network Access Control (NAC) Untuk Keamanan Jaringan" *Jurnal Teknologi, Kesehatan, dan Sosial (JUTEKS)*, vol. 1, no. 1, hlm. 47-56, Mei 2025.

1. PENDAHULUAN

Seiring dengan berkembangnya pengetahuan dan teknologi. Saat ini teknologi telah digunakan hamper di setiap kegiatan. Tentunya hal ini berdampak positif bagi kehidupan manusia dalam menjalankan aktivitasnya. Hal ini dikarenakan teknologi dapat mempermudah manusia untuk mendapatkan informasi. Hal itu pula yang kemudian menimbulkan berbagai macam tindak serangan terutama pada komputer atau jaringan server, sehingga pelu adanya pengamanan pada komputer, data server dan jaringan server, salah satu Upaya pengamanan jaringan denganmenggunakan penerapan Network Access Control (NAC).

Berdasarkan penelitian terdahulu telah menerapkan beberapa sistem keamanan jaringan Network Access Control (NAC), Penelitian yang dilakukan oleh [1] meneliti mengenai perencanaan Network Access Control (NAC), sebagai mekanisme pengawasan dan pengendalian akses endpoints dalam jaringan Compnet, kemudian penelitian oleh [2] Membangun Network Access Control (NAC) dengan menggunakan platform forescout akan memudahkan seorang administrator dalam mengontrol dan memonitoring kondisi jaringan dengan mudah, fitur policy pada platform forescout ini mengkombinasikan berbagai macam kondisi untuk keamanan jaringan seperti antivirus host intrusion dan network worm.

Berdasarkan penelitian sebelumnya pada sistem keamanan jaringan telah menerapkan Network access Control untuk mengamankan sistem jaringan komputer Network Security Protokol memberikan kemudahan kepada administrator untuk management network. Belum terdapat penelitian mengenai Keamanan Jaringan dengan Menerapakan Network Access Control (NAC). Berdasarkan hal tersebut mendorong penulis unyuk mengetahui dan menganalisa bagaimana kinerja NAC, dengan menggunakan penerapan Network Access Control (NAC), dengan melakukan uji coba penyerangan dengan menggunakan beberapa jenis serangan, mengimplementasikan sistem Network Access Control (NAC) yang digunakan sebagai cara untuk mengendalikan akses internal user pada jaringan, adapun tools yang dapat diterapkan seperti ForeScout CounterAct, Cisco System, Packet Fence. Sistem ini mengharuskan pengguna internal untuk terlebih dahulu menyelesaikan proses otentikasi dan memverifikasi "kesehatan" titik akhir sebelum mereka dapat terhubung ke jaringan. Oleh karena itu, hanya pengguna internal dengan sistem yang diautentikasi dan patuh yang berhak mengakses jaringan sesuai dengan izin mereka.

Terkait hal tersebut terdapat manfaat dari penelitian ini yak itu untuk meningkatkan keamanan network server control dari beberapa serangan. Dengan adanya penelitian Network Access Control (NAC) diharapkan dapat menjaga keamanan dan dapat menjalankan beberapa sistem keamanan jaringan tanpa perlu takut diretas.

2. METODE PENELITIAN

Metodologi yang diterapkan pada penelitian ini adalah Network Development Life Cycle (NDLC). (NDLC) adalah serangkaian proses yang digunakan dalam pengembangan dan manajemen jaringan komputer. NDLC adalah metodologi yang membantu organisasi merencanakan, merancang, mengimplementasikan, dan mengelola jaringan komunikasi mereka dengan efektif dan efisien. NDLC mirip dengan siklus pengembangan perangkat lunak tetapi fokusnya adalah pada pengembangan dan perawatan jaringan. Pada metodologi NDLC terdapat enam tahapan yaitu analisis, desain, simulasi, implementasi, monitoring dan manajemen. Penelitian ini hanya menggunakan 3 (tiga) tahapan NDLC, yaitu analisis, desain dan simulasi prototipe. [3] Metode ini sangat cocok digunakan untuk menganalisis dan merancang penelitian yang bertemakan Jaringan [4–7].

2.1 Tahap Analisa

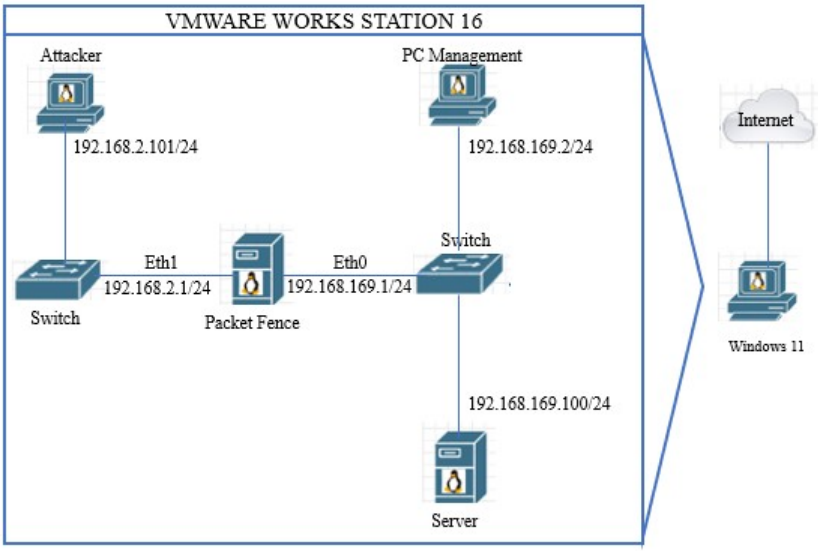
Pada tahap ini, akan dilakukan analisis mendalam terhadap kebutuhan teknis jaringan. Mereka akan memeriksa arsitektur yang ada (jika ada), menganalisis lalu lintas jaringan yang diharapkan, dan mengevaluasi teknologi yang sesuai untuk digunakan.

2.2 Tahap Desain

Pada tahapan ini dilakukan beberapa pembuatan desain dari penelitian ini dianataranya desain topologi virtualisasi dan rancangan kebutuhan perangkat keras dan perangkat lunak.

A. Topologi

Dalam rancangan uji coba akan disimulasikan secara virtualisasi menggunakan VMWare Workstation yang dijalankan pada 1 (satu) komputer dengan sistem operasi Windows 11 sebagai host machine (VM). Di dalam VMWare workstation terdapat 4 (empat) VM, 1 (satu) difungsikan sebagai host router, 1 (satu) VM sebagai PacketFence Network Access Control (NAC) sebagai sistem keamanan, 1 (satu) sebagai Server dan 1 (satu) lagi dialokasikan sebagai Attacker yaitu kali Linux. Dalam topologi virtualisasi disajikan berupa desain dari keadaan sebenarnya yang dirancang oleh penulis, dimana rancangan topologi virtualisasi dapat dilihat pada Gambar 1 dibawah ini.



Gambar 1. Topologi Virtualisasi

B. Rancangan Penglamatan IP

Tabel 1. Rancangan Pengalamatan IP

No	Perangkat	IP Address	Netmask	Keterangan
1.	Server	192.168.169.100	255.255.255.0	
2.	Attacker	192.168.2.101	255.255.255.0	Eth0
3	PacketFence	192.168.169.1	255.255.255.0	Eth0
		192.168.2.1	255.255.255.0	Eth1
4	Router	192.168.169.254	255.255.255.0	Eth0

C. kebutuhan perangkat keras dan perangkat lunak

Tabel 2. Kebutuhan perangkat

Perangkat Keras		Perangkat Lunak
1. Spesifikasi Perangkat	Processor AMD Rizen 5 5000H with Nvidia Geforce GTX	VMWare Workstation 16.0 Pro
Packet Fence NAC:	Random Access Memori 8 GB	Packet Fence ZEV versi 11.2.0
	Hard Disk 97.7 GB	OS Kali Linux
	Papan Ketik	Mesin pencarian

Perangkat Keras	Perangkat Lunak
	Tetikus
2. Spesifikasi Perangkat Router:	Processor AMD Rizen 5 5000H with Nvidia Geforce GTX Random Access Memori 256 MB Hard Disk 128 MB Papan Ketik Tetikus
3. Spesifikasi Perangkat Server:	Processor AMD Rizen 5 5000H with Nvidia Geforce GTX Random Access Memori 2 GB Hard Disk 20 GB Papan Ketik Tetikus
4. Spesifikasi Perangkat Attacker	Processor AMD Rizen 5 5000H with Nvidia Geforce GTX Random Access Memori 2 GB Hard Disk 20 GB Papan Ketik Tetikus

D. Tahap simulation prototyping

Pada bagian ini skenario pengujian yang digunakan yaitu pengujian ke web server dengan melakukan simulasi penyerangan pada konfigurasi dan instalasi yang telah dibuat sebelumnya yang menggunakan skenario pengujian sebagai berikut:

1. **Skenario tanpa sistem keamanan Network Access Control(NAC)**
   Skenario uji coba tanpa sistem keamanan Network Access Control(NAC) yang menghubung menggunakan satu jaringan Dalam melakukan skenario uji coba serangan pada server ini skenario pertama yaitu melakukan pengujian keamanan jaringan terhadap melalui perangkat Attacker dengan menggunakan beberapa tipe serangan yaitu Brute force dan DDOS dan dilakukan percobaan skenario untuk uji coba serangan.
2. **Skenario menggunakan sistem keamanan Network Access Control(NAC)**
   Skenario uji coba menggunakan sistem keamanan Network Access Control(NAC) yang menghubung menggunakan dua alamat jaringan. Network Access Control(NAC) sebagai sistem keamanan jaringan dan jalur pengiriman data. Dan Skenario pengujian dilakukan dengan pengujian keamanan jaringan terhadap server melalui perangkat Attacker dengan menggunakan serangan Brute force dan DDOS

3. HASIL DAN PEMBAHASAN

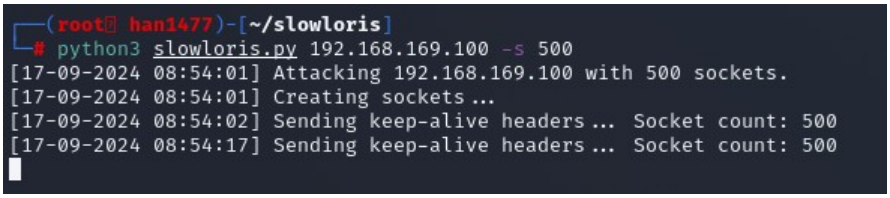
3.1 Hasil Uji Coba

Uji coba ini akan dilakukan dengan beberapa tahapan yaitu tahapan terkait sebelum dan sesudah penerapan Packet Fence NAC, terdapat 3 (tiga) jenis serangan yang digunakan dalam skenario uji coba ini meliputi Distributed Denial of Service DDoS, Brute force dengan protokol SSH, dan Brute force dengan protokol FTP yang akan di ujikan ke peraangkat server.

A. Serangan Distributed Denial of Service DDoS

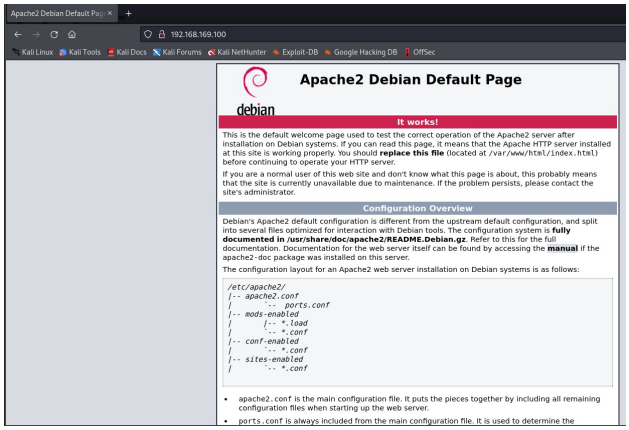
Dalam serangan Distributed Denial of Service (DdoS) tools yang digunakan adalah slowloris, slowloris digunakan untuk mengeksploitasi cara server menangani koneksi HTTP dengan tujuan untuk menyebabkan server menjadi tidak responsif atau down.

Pada Gambar 2 di bawah adalah bentuk penyerangan perintah slowloris serangan DDoS dari alamat IP penyerang 192.168.2.101 ke alamat IP tujuan 192.168.169.100.



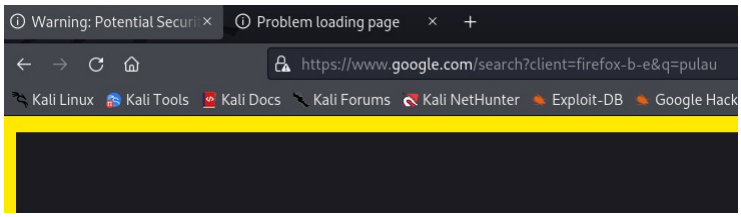
Gambar 2. Serangan sebelum aktif Packet Fence

Terlihat pada Gambar 3 di bawah perangkat Attacker berhasil terhubung ke jaringan server melalui mesin perintah.



Gambar 3. Hasil serangan sebelum aktif packet fence

Pada Gambar 4 di bawah menunjukan perangkat attacker tidak berhasil mengakses perangkat jaringan server melaliu mesin pencari

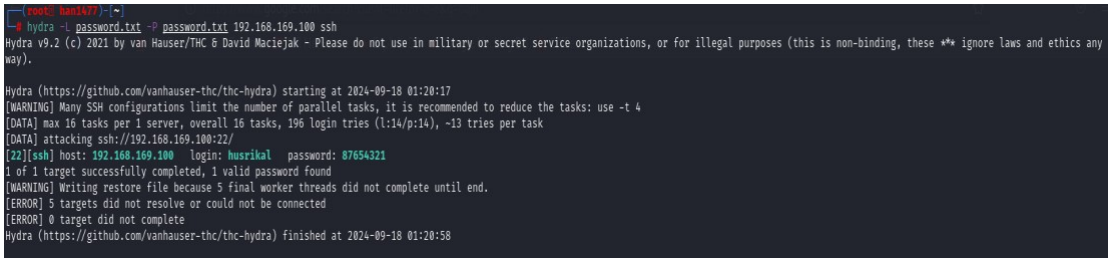


Gambar 4. Hasil serangan sebelum aktif packet fence

B. Serangan Brute Force

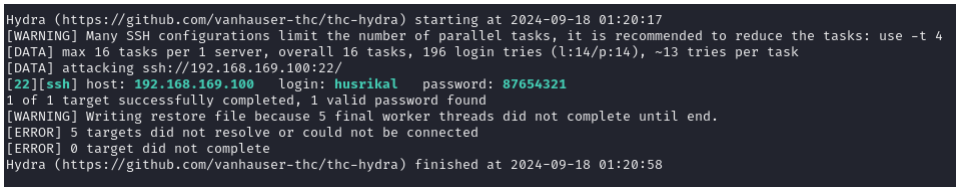
Uji coba yang akan dilakukan selanjutnya adalah serangan brute force untuk mendapatkan username dan password dari perangkat server

1. **Serangan brute force SSH**
   Pada Gambar 5 di bawah adalah bentuk penyerangan menggunakan tool hydra, hydra adalah alat yang digunakan untuk menguji keamanan sistem dengan cara mencoba berbagai kombinasi username dan password pada berbagai protokol jaringan, serangan Brute force dengan protokol SSH dari alamat IP penyerang 192.168.2.101 ke alamat IP tujuan 192.168.169.100 dan berhasil mendapatkan hotname dan password pada file packet dalam perangkat server.



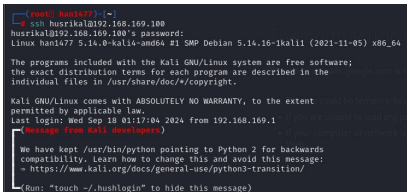
Gambar 5. Serangan Brute force SSH sebelum aktif Packet Fence

Gambar 6 di bawah menunjukkan hasil uji coba pertama serangan Brute force pada rentang waktu 01:20:17 mendapatkan hasil yaitu username "husrikal" dan password "87654321" yang password dan yang username tersebut sama dengan username dari perangkat server dari wordlist yang telah dibuat.



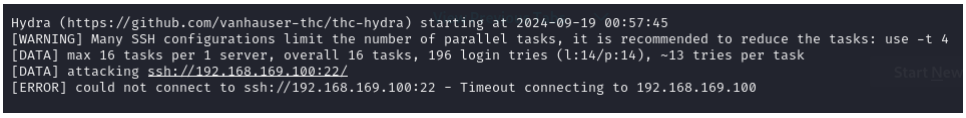
Gambar 6. Hasil serangan Brute Force SSH sebelum aktif Packet Fence

Gambar 7 di bawah menunjukkan perangkat attacker telah berhasil mengakses data yang terdapat pada server dengan menggunakan username dan password yang didapatkan pada peroses penyerangan.



Gambar 7. Hasil serangan Brute Force SSH sebelum aktif Packet Fence

Gambar 8 dibawah ini menampilkan hasil uji coba penyerangan melalui perangkat attacker ke perangkat server setelah aktif Packet Fence, dapat dilihat perangkat berhasil terblokir dan tidak mendapatkan username dan password dari perangkat attacker.

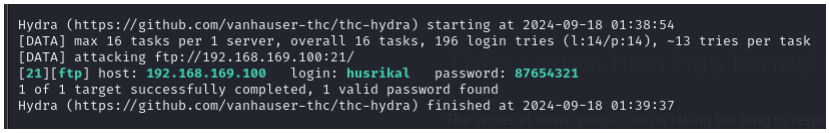


Gambar 8. Hasil penyerangan Brute force SSH setelah aktif Packet Fence

2. **Serangan Brute Force FTP**
Pada Gambar 9 di bawah adalah bentuk penyerangan menggunakan tool hydra, hydra adalah alat yang digunakan untuk menguji keamanan sistem dengan cara mencoba berbagai kombinasi username dan password pada berbagai protokol jaringan, serangan Brute force dengan protokol FTP dari alamat IP penyerang 192.168.2.101 ke alamat IP tujuan 192.168.169.100 dan berhasil mendapatkan hotname dan password pada file packet dalam perangkat server.

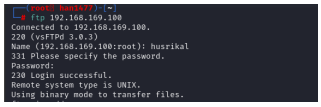
Gambar 9. Serangan brute force FTP sebelum akttif Packet Fence

Gambar 10 di bawah menunjukkan hasil uji coba pertama serangan Brute force pada rentang waktu 01:38:54 mendapatkan hasil yaitu username "husrikal" dan password "87654321" yang password dan yang username tersebut sama dengan username dari perangkat server dari wordlist yang telah dibuat.



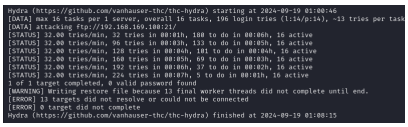
Gambar 10. Hasil serangan brute force FTP sebelum aktif Packet Fence

Gambar 11 di bawah menunjukkan perangkat attacker telah berhasil mengakses data yang terdapat pada server dengan menggunakan password yang didapatkan pada peroses penyerangan



Gambar 11. Hasil serangan brute force FTP sebelum aktif Packet Fence

Gambar 12 di bawah menunjukkan hasil uji coba serangan Brute force pada rentang waktu 01:00:46 tetapi tidak berhasil mendapatkan hotname dan password pada file packet dalam perangkat server



Gambar 12. Hasil serangan brute force FTP setelah akttif Packet Fence

3.2 Hasil Analisis

A. Analisis serangan Distributed Denial of Service DDoS

Berdasarkan hasil skenario pengujian serangan DDoS perangkat server sebelum dan setelah diaktifkan NAC, didapatkan hasil peningkatan pengamanan jaringan server. Hasil analisa dari serangan DDoS dapat dilihat pada Tabel 3 dibawah ini.

B. Serangan Brute force

Serangan menggunakan teknik brute forcedengan protokol SSH yang dilakukan pada perangkat server sebelum menjalankan NAC menunjukkan bahwa serangan berhasil dilakukan, termasuk username dan password yang cocok untuk mengakses dan login ke dalam server melalui user admin. Sebaliknya setelah NAC diaktifkan maka aktivitas serangan Brute force dengan protokol SSH yang masuk ke server gagal dilakukan, termasuk username dan password yang cocok untuk dapat mengakses ke Form login berdasarkan seperti yang terlihat pada Tabel 4 dibawah ini.

Tabel 3. Analisis serangan Distributed Denial of Service DDoS

Uji coba	Perangkat Server Sebelum aktif packet fence	Sesudah aktif packet fence
1	Lalu lintas jaringan menjadi terhambat atau terhenti, dan pengguna tidak dapat mengaakses situs web	Lalu lintas jaringan tetap berjalan dan setabil pengguna dapat mengaakses situs web
2	Lalu lintas jaringan menjadi terhambat atau terhenti, dan pengguna tidak dapat mengaakses situs web	Lalu lintas jaringan tetap berjalan dan setabil pengguna dapat mengaakses situs web
3	Lalu lintas jaringan menjadi terhambat atau terhenti, dan pengguna tidak dapat mengaakses situs web	Lalu lintas jaringan tetap berjalan dan setabil pengguna dapat mengaakses situs web
4	Lalu lintas jaringan menjadi terhambat atau terhenti, dan pengguna tidak dapat mengaakses situs web	Lalu lintas jaringan tetap berjalan dan setabil pengguna dapat mengaakses situs web
5	Lalu lintas jaringan menjadi terhambat atau terhenti, dan pengguna tidak dapat mengaakses situs web	Lalu lintas jaringan tetap berjalan dan setabil pengguna dapat mengaakses situs web

Tabel 4. Keterangan Serangan Brute force SSH

Uji coba	Perangkat Server Sebelum aktif packet fence	Setelah aktif packet fence
1	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
2	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
3	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
4	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
5	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui

Serangan menggunakan teknik brute force dengan protokol FTP yang dilakukan pada perangkat server sebelum menjalankan NAC menunjukkan bahwa serangan berhasil dilakukan, termasuk username dan password yang cocok untuk mengakses dan login ke dalam server melalui user admin. Sebaliknya setelah NAC diaktifkan maka aktivitas serangan Brute force dengan protokol FTP yang masuk ke server gagal dilakukan, termasuk username dan password yang cocok untuk dapat mengakses ke Form login berdasarkan seperti yang terlihat pada Tabel 5 di bawah ini

Tabel 5. Keterangan Serangan Brute force SSH

Uji coba	Perangkat Server Sebelum aktif packet fence	Setelah aktif packet fence
1	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
2	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
3	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
4	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui
5	Usernsme dan password file pada perangkat server dapat diketahui	Usernsme dan password file pada perangkat server tidak dapat diketahui

4. KESIMPULAN

Berdasarkan uji coba yang telah dilakukan, dapat disimpulkan bahwa Network Acces Control NAC dengan mengaktifkan beberapa tool Packet Fence untuk mengamankan perangkat server, Network Access Control NAC berhasil melindungi perangkat Server dari 3 serangan, yaitu DDOS, bruteforce dengan protocol SSH, dan bruteforce dengan Protocol FTP, yang diujikan melalui perangkat attacker. Selain itu, diperoleh perbandingan sebelum dan sesuda diimplementasikan Network Access Control dengan perlindungan yang diberikan Packet Fence NAC ketika terjadinya serangan, sedangkan sebelum penerapan Packet Fence, perangkat attacker berhasil mendapat informasi yang diinginkan dari pengujian yang telah dilakukan.

UCAPAN TERIMA KASIH

Dengan selesainya skripsi ini, penulis ingin mengucapkan terima kasih kepada pihak – pihak yang telah banyak membantu dalam penyelesaian skrpsi ini. Dalam Bapak Dr. Ir. Anthony Anggrawan, M.T., Ph.D selaku Rektor Universitas Bumigora.

1. Bapak Dr. Ir. Anthony Anggrawan, MT., Ph.D. selaku Rektor Universitas Bumigora
2. Ibu Dr. Khasnur Khidjah, M.Cs , selaku Wakil Rektor I Universitas Bumigora
3. Bapak Dr. Galih Hendro Martono, M.Kom, selaku Dekan Fakultas Teknik
4. Bapak Dr. Dadang Priyanto, M.Kom, selaku Ketua Program Studi S1 Ilmu Komputer
5. Ibu Lilik Widyawati, M.Kom, dan bapak Khairan Marzuki, S.T., M.kom selaku Dosen Pembimbing dalam mengerjakan skripsi ini
6. Kedua orang tua dan saudara tercinta yang telah memberikan segala jenis dukungan dan doa sehingga saya mampu mencapai pada titik ini
7. Sahabat-sahabat, teman-teman yang telah memberikan bantuan dan memberikan semangat dalam menyelesaikan penulisan skripsi ini.

DAFTAR PUSTAKA

[1] D. K. Heryadi and A. S. Budiman, "Optimasi Keamanan Pada Jaringan Multi-Endpoint Access Menggunakan Network Access Control Berbasis Cisco ISE," *JIKA (Jurnal Informatika)*, vol. 5, pp. 313–324, Oct. 2021. Number: 3.

[2] M. Syani, R. M. Tresna, E. A. Firdaus, and F. F. Nugraha, "PENERAPAN NETWORK ACCESS CONTROL AUTENTIKASI INTERNAL NETWORK SECURITY PROTOKOL 802.1 X," *NUANSA INFORMATIKA*, vol. 16, pp. 77–86, July 2022.

[3] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System," *IEEE Internet of Things Journal*, vol. 8, pp. 5744–5761, Apr. 2021.

[4] I. Butun and P. Osterberg, "A Review of Distributed Access Control for Blockchain Systems Towards Securing the Internet of Things," *IEEE Access*, vol. 9, pp. 5428–5441, 2021.

[5] F. Ghaffari, E. Bertin, J. Hatin, and N. Crespi, "Authentication and Access Control based on Distributed Ledger Technology: A survey," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, (Paris, France), pp. 79–86, IEEE, Sept. 2020.

[6] J. A. Gomez-Hernandez, J. Camacho, J. A. Holgado-Terriza, P. Garcia-Teodoro, and G. Macia-Fernandez, "ARANAC: A Bring-Your-Own-Permissions Network Access Control Methodology for Android Devices," *IEEE Access*, vol. 9, pp. 101321–101334, 2021.

[7] N. Kashmar, M. Adda, and M. Atieh, "From Access Control Models to Access Control Metamodels: A Survey," in *Advances in Information and Communication* (K. Arai and R. Bhatia, eds.), vol. 70, pp. 892–911, Cham: Springer International Publishing, 2020. Series Title: Lecture Notes in Networks and Systems.

[Halaman ini sengaja dikosongkan.]