FORENSIC SERANGAN *BRUTE FORCE* PADA *PUBLIC CLOUD* DENGAN METODE RULE BASE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :
M. KADAPI
09011181520119

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

FORENSIC SERANGAN BRUTE FORCE PADA PUBLIC CLOUD DENGAN METODE RULE BASE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu
Syarat Memperoleh Gelar Sarjana
Komputer

OLEH :
M. KADAPI
09011181520119

Indralaya, 31 Desember 2020

Pembimbing I	Pembimbing II
Deris Stiawan, M.T., Ph.D.	**Ahmad Heryanto, S.Kom., M.T.**
NIP.197806172006041002	**NIP. 198701222015041002**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi,M.T
NIP.196612032006041001

Dipindai dengan CamScanner

HALAMAN PERSETUJUAN

Pada hari Kamis 31 December 2020 telah dilaksanakan ujian sidang tugas ahir oleh Sarjana Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : M. Kadapi

Nim 09011181520119

Judul : Forensic Serangan Brute Force pada *Public Cloud* dengan Metode *Rule Base*

Tim Penguji :

1. **Ketua**

   Kemahyanto Exaudi, M.T. (.....)

2. **Sekretaris**

   Aditya Putra Perdana P, M.T. (.....)

3. **Penguji**

   Huda Ubaya, M.T. (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi,M.T
NIP.196612032006041001

Dipindai dengan CamScanner

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: M. Kadapi
NIM	: 09011181520119
Program Studi	: Sistem Komputer
Judul Skripsi	: Forensic Serangan Brute Force pada Public Cloud dengan Metode Rule Base

Hasil Pengecekan *Software iThenticate/Turnitin* : 17 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil *penjiplakan/plagiat.* Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Demikian Surat Pernyataan ini saya buat dengan sebenar-benarnya.

Palembang, 5 Januari 2021

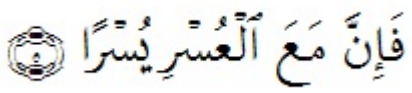
Yang menyatakan,

M. Kadapi

NIM. 09011181520119

Dipindai dengan CamScanner

HALAMAN PERSEMBAHAN



"Karena sesungguhnya sesudah kesulitan itu ada kemudahan"

Tugas Akhir ini saya persembahkan untuk :

- ***Kedua Orang tuaku, Adik-adik saya, dan seluruh keluarga saya***
- ***Dosen Pembimbing dan Penguji***
- ***Sahabat – sahabat saya***
- ***Teman Seperjuangan Sistem Komputer 2015***
- ***Almamaterku***

KATA PENGANTAR

Alhamdulillahhirabbil'alamin Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul "**Forensic Serangan Brute Force pada Public Cloud dengan Metode Rule Base**" di susun untuk memenuhi sebagian persyaratan kelulusan untuk memperoleh gelar Sarjana Komputer pada Jurusan Sistem Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis menyadari keterbatasan dan kelemahan yang ada dalam menyelesaikan tesis ini sehingga penulis ingin meyampaikan ucapan terimakasih kepada pihak-pihak yang telah memberikan dukungan, bimbingan dan motivasi kepada penulis untuk menyelasaikan tugas akhir ini, kepada:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga tugas akhir penulisan ini dapat berjalan dengan lancar.
2. Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi dan semanga.
3. Bapak Jaidan Jauhari, S.Pd, M.T. selaku dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., sebagai Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, Ph.D. selaku Dosen Pembimbing 1, dan Bapak Ahmad Heryanto, M.T selaku Dosen Pembimbing 2. selaku Dosen Pembimbing tugas akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan tugas akhir.
6. Bapak Huda Ubaya, S.T., M.T, Bapak Sarmayanta Sembiring, S.Si., M.T, selaku dosen penguji tugas akhir dan Bapak Kemahyanto Exaudi,

M.T. selaku ketua sidang, dan Bapak Aditya Putra Perdana P, M.T. selaku Sekretaris Sidang yang telah memberikan kritik dan saran serta ilmu yang bermanfaat sehingga tulisan ini menjadi lebih baik.

7. Dosen-dosen pengajar yang telah memberikan ilmu bermanfaat kepada penulis selama menuntut ilmu di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mba Winda Kurnia Sari dan Mba Renny selaku Administrator Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberi kemudahan dalam pengurusan administrasi.
9. Seluruh teman-teman Jurusan Sistem Komputer Angkatan 2015 yang telah membantu dan memberikan semangat pada masa-masa perkuliahan.
10. Semua pihak yang telah memberi dukungan kepada penulis dan tidak bisa disebutkan satu-persatu.

Akhir kata, penulis menyadari bahwa tugas akhir ini masih banyak kekurangan baik dari isi maupun susunan. Semoga tugas akhir ini dapat bermanfaat untuk kita semua.

Indralaya, Januari 2021

Penulis

FORENSIC SERANGAN BRUTE FORCE PADAPUBLIC CLOUD DENGAN METODE RULE BASE

M. Kadapi (09011181520119)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
E-mail : muhammadkadapi21@gmail.com

ABSTRAK

Owncloud X merupakan perangkat lunak cloud infrastructure as a service (IAAS) berbasis penyimpanan. Serangan brute force dapat digunakan untuk mencari password akun dari pengguna owncloud. Penelitian ini membahas tentang analisis forensik serangan brute force yang terjadi pada owncloud dengan menggunakan rule base. Langkah-langkah penelitian ini adalah membangun topologi cloud, melakukan skenario akses normal pada cloud menggunakan beberapa perangkat yang berbeda, melakukan serangan brute force pada cloud dan uji coba skenario pengujian gabungan (dilakukan akses normal ke cloud ketika serangan brute force dilakukan). Berdasarkan pengujian yang telah dilakukan, Serangan brute force ke owncloud memiliki pola-pola parameter port destination bernilai 80, protokol tcp, window size bernilai 4320, flags bernilai PA, time to live (ttl) bernilai 252, dan panjang internet protocol (ip) dengan rentang nilai 74-1023. Dari hasil pengujian yang telah dilakukan, metode rule base mendapatkan nilai akurasi sebesar sebesar 97,97%.

Kata kunci : ***Cloud, Brute Force, Rule Base, Forensik Cloud***

FORENSIC SERANGAN BRUTE FORCE PADAPUBLIC CLOUD DENGAN METODE RULE BASE

M. Kadapi (09011181520119)
Dept. of Computer Engineering, Faculty of Computer Science, Sriwijaya University
E-mail : muhammadkadapi21@gmail.com

ABSTRACT

Owncloud X is a storage-based infrastructure as a service (IAAS) cloud. The brute force attack can be used to find an account password from owncloud users. This research discusses analysis of brute force attack forensic that occur in owncloud using the rule base method. The steps of this research are build cloud topology, perform normal access to the cloud using various devices, perform brute force attack to the cloud, and perform access normal to the cloud while brute force attack occurs. Based on the test results, The brute force attack has a pattern variable value destination port 80, tcp protocol, window size 4320, flags "PA", time to live (ttl) 252, and ip length 74-1023. Based on implementing fuzzy logic on the test to detect brute force attack, The rule base method gets an accuracy value of 97.97%.

Keywords: ***Cloud, Brute Force, Rule Bae, Cloud Forensic***

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1. Latar Belakang

Brute Force adalah suatu serangan yang menggunakancara sangat sederhana untuk menemukan solusinya, yaitu dengan cara mencoba semua kemungkinan yang ada. Dengan kata lain semakin banyak kemungkinannya maka semakin lama proses pencarian solusinya[1]. Brute Force adalah algoritma yang dapat menemukan semua solusi karenaalgoritma ini mencoba semua kemungkinan solusi yang ada dan mengandalkan faktor keberuntungan (Lucky) untuk menemukan solusinya, namun jika faktor keberuntungan (Lucky) tersebut tidak didapat maka algoritma ini adalah worst-algorithm (algoritma yang terlalu lama memakan waktu untuk memecahkan suatu masalah).

NIST (National Institute of Standards and Technology), Cloud Computing adalah sebuah bentuk layanan yang membuka peluang untuk dapat diakses di manapun, memberikan kenyamanan, serta akses jaringan yang on – demand untuk penggunaan sumber daya komputasi terkonfigurasi (misalya jaringan, server, penyimpanan, aplikasi dan layanan) yang dapat dengan cepat dijalankan dengan upaya pengelolaan yang minim atau dengan menggunakan penyedia jasa layanan [2].

Owncloud merupakan salah satu perangkat lunak berbagi berkas gratis (lisensi AGPL) dan bebas, menyediakan pengamanan yang baik, memiliki tata cara yang baik bagi pengguna aplikasi untuk membagi dan mengakses data yang secara terintegrasi dengan perangkat teknologi informasi yang tujuannya mengamankan, melacak, dan melaporkan penggunaan data. Owncloud memiliki cara kerja yang cukup sederhana yaitu satu komputer yang digunakan sebagai server lokal dengan harddisk berkapasitas luas. Kemudian klien hanya mendapat akses untuk dapat menyimpan data di server owncloud, mereka bisa menyimpan data, berbagi data dari komputer masing-masing.

Pada penelitian sebelumnya[3], membahas tentang analisis forensik serangan brute force yang terjadi pada owncloud dengan menggunakan logika fuzzy. Berdasarkan pengujian yang telah dilakukan, owncloud x memiliki celah

pada application programming interface (API) Owncloud Share (OCS) sehingga dapat dilakukan serangan brute force ke cloud.

Berdasarkan latar belakang masalah tersebut, maka pada penelitian tugas akhir ini penulis akan melakukan pembuktian pola serangan *Brute Force* dengan menggunakan metode *Rule Base*. Dengan metode ini semoga dapat menghasilkan data yang akurat untuk mendapatkan pola serangan data forensic.

1.2. Tujuan

Adapun tujuan dari penelitian ini yaitu :

1. Mengenali pola serangan *brute force* pada *cloud*.
2. Menerapkan metode *rule base* untuk menganalisa suatu data.

1.3. Manfaat

Adapun manfaat yang dapat diambil dari dilakukannya penelitian ini adalah:

1. Dapat mengetahui pola serangan *brute force* pada *cloud*.
2. Dapat membedakan paket serangan dengan paket normal pada serangan *brute force.*

1.4. Rumusan Masalah

Rumusan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Bagaimana mengenali pola serangan *brute force?*

2. Bagaimana melakukan analisis serangan *brute force* yang terjadi pada cloud dengan metode *rule base?*

1.5. Batasan Masalah

Batasan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Penelitian yang dilakukan *cloud* bersifat publik.
2. Metode yang digunakan untuk menganalisa akurasi data dengan menggunakan metode *rule base.*
3. Data yang digunakan didapat dari server *cloud* dan penyerang.
4. Penggunaan sistem *snort* dalam membuktikan adanyaserangan pada *cloud.*

1.6. Metodologi Penelitia

Penelitian ini akan melewati beberapa tahapan :

1. Tahap Pertama (Perumusan Masalah)

   Dalam tahap ini penulis menentukan permasalahan yang ada di *cloud computing* yaitu keamanan yang terjadi pada *cloud computing* untuk mengidentifikasi serangan yang terjadi dan membuktikan serangan tersebut.

2. Tahap Kedua (Studi Pustaka / Literatur)

   Pada tahap ini penulis akan mencari informasi yang di perlukan melalui media pembelajaran seperti jurnal ilmiah, buku, internet serta artikel-artikel terkait yang mendukung penulisan proposal tugas akhir ini.

3. Tahap ketiga (Perancangan)

   Tahap ini ialah tahap perancangan sistem yang akan dibuat sesuai dengan rumusanmasalah penelitian. Dalam tahap ini melakukan instalasi operation system, membangun jaringan cloud dan konfigurasi cloud tersebut.

4. Tahap Keempat (Pengujian)

   Pada tahap ini dilakukan pengujian dari sistem yang dirancang. Ditahap ini seragan *brute force* akan diuji menggunakan linux ubuntu pada *cloud.*

5. Tahap Kelima (Analisa)

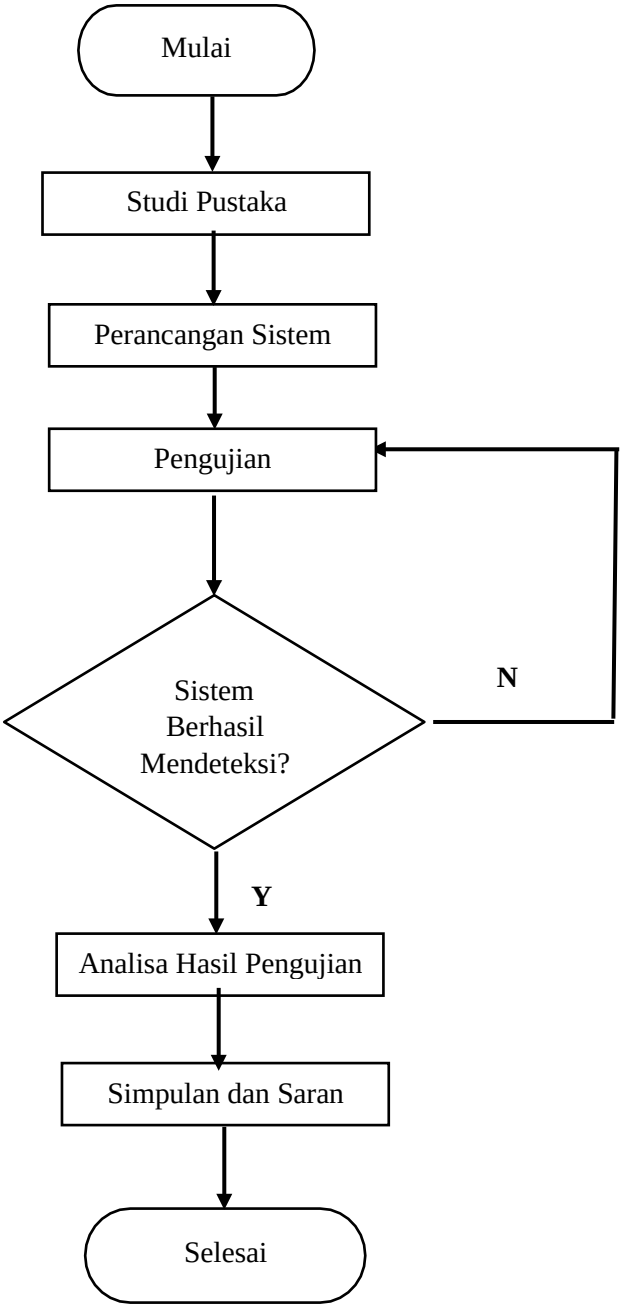
   Hasil dari pengolahan data pada tahap sebelumnya, akan dianalisa sesuai identifikasi permasalahan. Tahapan ini bertujuan untuk mendapatkan data objektif dari analisa hasil pengolahan data serta dapat dilakukannya pengembangan pada penelitian sebelumnya.

6. Kesimpulan dan Saran

   Hasil dari pengujian dari metode pengujian kemudian analisa dan dibuat saran sebagai referensi apabila penelitian ini dilanjutkan dan dibuat kesimpulan dari hasil penelitian.

Pada Gambar 1.1 berikut ditampilkan metodologi penelitian secara visual dalam bentuk diagram air yang merepresentasikan proses pelaksanaan penelitian

:



Gambar 1.1 Diagram Air Metodologi Penelitian

1.7. Sistematika Penulisan

Untuk lebih memudahkan dalam menyusun tugas akhir ini dan memperjelas isi dari setiap bab yang ada pada laporan ini, maka dibuatlah sistematika penulisan sebagai berikut.

BAB I PENDAHULUAN

Pada Bab I akan berisikan latar belakang masalah, tujuan, manfaat, perumusan masalah dan batasan masalah serta metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bab II akan berisi dasar teori *Brute Force Attack, Cloud Computing, Rule Base, Snort* yang berkaitan dengan penelitian.

BAB III METODOLOGI

Pada Bab III akan membahas penjelasan secara bertahap mengenai proses penelitian yang dilakukan dan perancangan sistem.

BAB IV PENGUJIAN DAN ANALISA

Pada Bab IV menjelasakan mengenai hasil dari pengujian yang telah dilakukan selama penelitian tugas akhir. Hasil dari pengujian itu akan dianalisis dari data yang didapatkan.

BAB V KESIMPULAN DAN SARAN

Pada Bab V berisi kesimpulan akhir dari bab-bab pembahasan penelitian yang telah dilakukan dan juga berisi saran yang diperlukan untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

[1] I. H. Sembodo and A. D. B. Force, "Password Cracking menggunakan Brute Force Attack IF2211 Strategi Algoritma," 2014.

[2] P. Mell, T. Grance, and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology."

[3] T. Akhir, "Forensik Serangan Brute Force pada Public Cloud Menggunakan Logika Fuzzy," 2019.

[4] P. K. Sharma, P. S. Kaushik, P. Agarwal, P. Jain, S. Agarwal, and K. Dixit, "Issues and challenges of data security in a cloud computing environment," *2017 IEEE 8th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2017*, vol. 2018-January, pp. 560–566, 2017, doi: 10.1109/UEMCON.2017.8249113.

[5] M. Ali, M. Ali, S. U. Khan, and A. V Vasilakos, "Security in Cloud Computing :OpportunitiesandChallengesSecurityincloudcomputing : Opportunities and challenges," *Inf. Sci. (Ny).*, vol. 305, no. February 2015, pp. 357–383, 2017, doi: 10.1016/j.ins.2015.01.025.

[6] M. Ali, S. U. Khan, and A. V Vasilakos, "Security in cloud computing: Opportunities and challenges," vol. 305, pp. 357–359, 2015.

[7] F. Version, *ENISA Threat Landscape Report 2017*, no. January. 2018.

[8] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks : Survey and research challenges," *Digit. Investig.*, vol. 7, no. 1–2, pp. 14–27, 2010, doi: 10.1016/j.diin.2010.02.003.

[9] R. N. Cronk, P. H. Callahan, and L. Bernstein, "Rule-Based Expert Systems for Network Management and Operations: An Introduction," *IEEE Network*, vol. 2, no. 5. pp. 7–21, 1988, doi: 10.1109/65.17975.

[10] D. Stiawan, S. Sandra, E. Alzahrani, and R. Budiarto, "Comparative analysis of K-Means method and Naïve Bayes method for brute force attack visualization," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 177–182, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905286.

[11] E. A. Winanto, A. Heryanto, and D. Stiawan, "Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means," *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.