PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN KALI LINUX DI LINGKUNGAN GOOGLE CLOUD PLATFORM

M. Fikri Zulfi, Oka Alvansyah, Ahmad Yusuf Al-Hafiz, Dedy Kiswanto
Ilmu Komputer, Universitas Negeri Medan
Jl. William Iskandar Ps. V Medan,Indonesia
fikrizulfi5.4233250003@mhs.unimed.ac.id

ABSTRAK

Keamanan jaringan menjadi hal yang penting bagi pengguna komputer, baik personal maupun or-ganisasi, dalam melakukan pertukaran informasi dan data menggunakan jaringan. Penelitian ini ber-tujuan untuk mengevaluasi keamanan jaringan pada VM yang di-host di Google Cloud dengan menggunakan penetration testing tools, Nmap dan Metasploit. Penelitian ini mengidentifikasi celah keamanan yang ada dan mengevaluasi dampaknya terhadap keamanan sistem Penelitian keamanan jaringan ini menggunakan metode bruteforce attack dalam serangan sibernya, yaitu dengan melakukan percobaan dengan cara menyerang sistem komputasi awan yang digunakan. Pada penelitian tersebut, penulis mendapatkan hasil dimana penulis berhasil masuk ke dalam sistem jaringan melalui port SSH yang terbuka. Untuk keamanan Google Cloud pada penelitian ini cukup tidak aman untuk keamanannya karena rentannya port SSH yang dimiliki komputasi awan tersebut dapat dieksploitasi oleh pengguna yang tidak bertanggung jawab.

Kata kunci : *Keamanan Jaringan, Kali Linux, Google Cloud Platform*

1. PENDAHULUAN

Kebutuhan akan pertukaran informasi dan data merupakan hal yang sangat penting. Oleh karena itu, dalam pelaksanaannya diperlukan tingkat keamanan tertentu agar pertukaran informasi dan data tersebut dapat berjalan dengan lancar. Keamanan Jaringan menjadi hal yang penting bagi pengguna komputer, baik personal maupun organisasi, dalam melakukan pertukaran informasi dan data dengan menggunakan jaringan.[1] Masalah keamanan menjadi hal yang sangat penting untuk dibahas, terutama di era yang serba digital dan minimalis ini. Keamanan perlu diperhatikan untuk memberikan rasa aman ketika menggunakan perangkat tersebut, Jaringan sebagai media komunikasi memerlukan sistem keamanan untuk mencegah dan membatasi kejadian-kejadian yang tidak diinginkan, seperti gangguan virus dan spam.[2].

Setelah meninjau penelitian sebelumnya mengenai keamanan jaringan, peneliti melakukan penelitian baru mengenai keamanan jaringan menggunakan Kali Linux dengan memanfaatkan Google Cloud. Penelitian ini dilatarbelakangi oleh fakta bahwa penelitian sebelumnya tidak memfokuskan sistem cloud mereka dengan menggunakan Google Cloud Platform. Oleh karena itu, penelitian ini bertujuan untuk melihat seberapa baik keamanan jaringan ketika menggunakan Google Cloud Platform. Tujuan dari penelitian ini adalah untuk menguji keamanan jaringan pada lingkungan cloud untuk mengidentifikasi kerentanan dan mengukur seberapa rentan sistem terhadap serangan.

Google Cloud Platform digunakan karena Google Cloud menawarkan berbagai manfaat keamanan yang membuat para peneliti tertarik untuk menguji keamanannya. Manfaat tersebut antara lain fitur keamanan yang canggih, termasuk enkripsi data, kontrol akses berbasis identitas, dan pemantauan keamanan.

2. TINJAUAN PUSTAKA

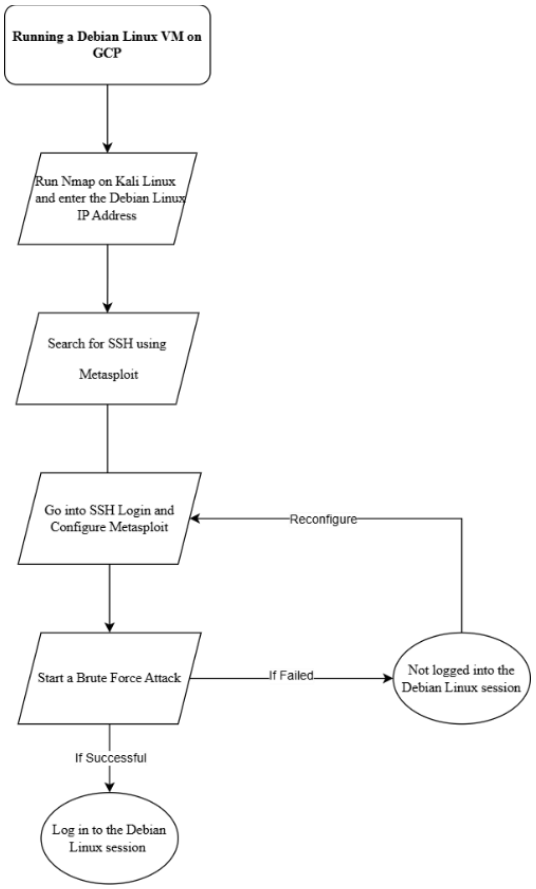
Kali Linux merupakan sistem operasi yang bersifat open source yang dapat digunakan untuk keamanan jaringan pada sebuah sistem dan jaringan komputer.[3] Kali Linux adalah pintu baru bagi spesialis keamanan *white-hat* untuk memperkuat keamanan perusahaan dan organisasi. Kali adalah distribusi berbasis keamanan dari keluarga linux yang memiliki platform Debian. Karena memiliki lebih dari 600+ aplikasi keamanan pra-instal, maka perlu untuk menyimpan catatan aktivitas jaringan oleh sistem dan ke sistem. Karena kali linux adalah alat yang ampuh untuk keamanan server.[4] Keamanan merupakan isu penting dalam paradigma komputasi awan yang mempengaruhi adopsi teknologi komputasi awan. Penyedia cloud bertanggung jawab untuk menggunakan dan menerapkan mekanisme keamanan yang berbeda, untuk memastikan bahwa data dan aplikasi diamankan. *Phishing* data, kehilangan data, downtime, kelemahan kata sandi, pengungkapan data, dan ancaman lain yang terkait dengan jaringan, keamanan, dan aplikasi masih terjadi di banyak perusahaan. Masalah dan tantangan keamanan ini menyebabkan penurunan penerimaan teknologi komputasi awan.[5]

Cloud Computing merupakan teknologi yang memiliki banyak keunggulan. Karena model komputasi ini memungkinkan pengguna untuk memanfaatkan sumber daya seperti jaringan, server, penyimpanan, aplikasi, dan layanan di dalam sistem jaringan awan, di sisi lain, sumber daya tersebut juga dapat dibagi dan digunakan secara kolaboratif. Selain itu, komputasi awan juga memiliki keunggulan untuk

dapat meningkatkan fleksibilitas dan kemampuan proses komputer secara dinamis tanpa perlu mengeluarkan biaya yang besar untuk membuat infrastruktur baru. Hal ini juga akan mengurangi biaya pelatihan tenaga ahli baru serta lisensi perangkat lunak baru.[6] Salah satu jenis serangan yang sering digunakan adalah serangan Brute Force, yang termasuk dalam kategori kejahatan siber. National Institute of Standards and Technology (NIST) sering menganalisis bukti digital dalam kasus-kasus tersebut.[7] Berbagai peneliti telah meneliti dan memberikan banyak solusi untuk mencegah serangan ini. Salah satu cara terbaik untuk mendeteksi serangan adalah melalui *Intrusion Detection System*.[8] Makalah ini berfokus pada analisis komprehensif dari berbagai serangan siber. Analisis serangan siber dilakukan dengan menggunakan kali Linux. Banyak alat yang ada di kali Linux yang dieksplorasi dalam makalah ini.[10]

3. METODE PENELITIAN

Penelitian keamanan jaringan ini menggunakan metode bruteforce attack dalam serangan sibernya, yaitu dengan melakukan percobaan dengan menyerang sistem cloud computing yang digunakan. Brute force adalah metode serangan yang digunakan untuk mendapatkan akses ke suatu akun, sistem, atau data dengan mencoba semua kombinasi password atau kunci enkripsi yang mungkin hingga ditemukan kombinasi yang benar.



Gambar 1. *Flowchart* pengujian

Proses ini diawali dengan menjalankan SSH Debian Linux di Google Cloud Platform, lalu catat IP eksternal, kemudian buka terminal Kali Linux lalu cari IP tersebut dengan menggunakan tool Nmap, setelah itu buka metasploit dan cari SSH lalu identifikasi login ssh.

Di Metasploit, peneliti mengkonfigurasinya sesuai dengan keinginan Anda, seperti menggunakan dokumen teks yang berisi berbagai kata sandi acak yang digunakan untuk menyerang menggunakan brute-force, lalu jalankan brute-force tersebut.

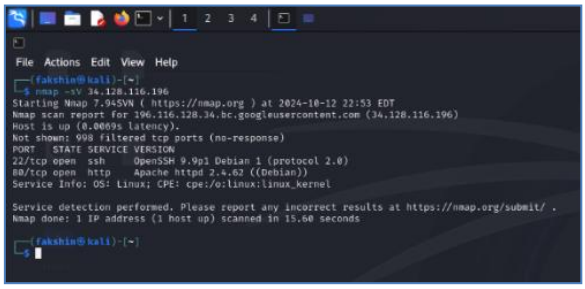
4. HASIL DAN PEMBAHASAN

Pengujian keamanan jaringan adalah proses penting untuk mengidentifikasi dan mengatasi kerentanan dalam sistem. Dalam percobaan ini, penulis menggunakan Kali Linux untuk menguji *instance VM* berbasis Debian yang di-host di Google Cloud. Metode yang digunakan antara lain pemindaian dengan Nmap dan serangan brute force menggunakan Metasploit.

4.1. Pemindaian dengan Nmap

Setelah menyiapkan instance VM dengan sistem operasi Debian, langkah pertama yang dilakukan adalah melakukan pemindaian menggunakan Nmap. Perintah yang digunakan adalah:

nmap -sV 34.128.116.196



Gambar 2. Menggunakan nmap untuk mencari port terbuka

Hasil pemindaian menunjukkan bahwa port 22 (SSH) dan port 80 (HTTP) terbuka. Hal ini mengindikasikan bahwa SSH dan layanan web berjalan dan dapat diakses dari luar.

4.2. Identifikasi *Vurnerability*

Dari hasil pemindaian, layanan SSH menjadi fokus utama karena sering menjadi target serangan. Beberapa kerentanan yang umum terjadi pada layanan SSH antara lain penggunaan password yang lemah dan pengaturan yang tidak aman. Oleh karena itu, penulis memutuskan untuk melanjutkan pengujian pada layanan SSH.

4.3. Pengujian dengan Metasploit

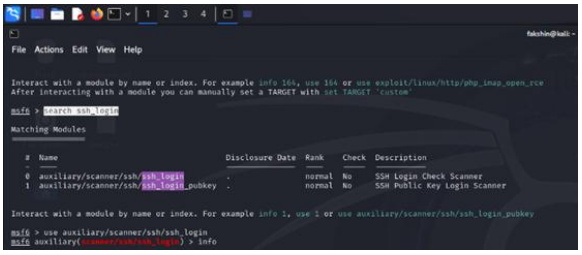
Setelah mengidentifikasi target, penulis melanjutkan dengan menggunakan Metasploit untuk melakukan serangan brute force terhadap layanan SSH. Berikut adalah langkah-langkah yang dilakukan:

4.4. Msfconsole

Gambar 3. Menjalankan metasploit

4.5. Search ssh_login

Di Metasploit, perintah search ssh digunakan untuk mencari modul-modul yang terkait dengan protokol SSH (Secure Shell). Protokol ini sering digunakan untuk mengakses sistem secara aman dari jarak jauh, dan dalam konteks Metasploit, modul yang terkait dengan SSH dapat mencakup eksploitasi, pemindai, atau muatan yang dirancang untuk berinteraksi dengan layanan SSH.



Gambar 4. Mencari modul ssh_login

4.6. use auxiliary/scanner/ssh/ssh_login

Gambar 5. Menggunakan *use auxiliary/scanner/ssh/ssh_login*

set VERBOSE true
set STOP_ON_SUCCES true
set RHOST 34.128.116.196
set USER_FILE Desktop/username.txt
set PASS_FILE Desktop/pass.txt
set VERBOSE true

Mengatur mode verbose ke true berarti Metasploit akan memberikan output yang lebih detail saat menjalankan modul. Hal ini berguna untuk memantau proses dan mendapatkan informasi yang lebih jelas tentang apa yang sedang dilakukan, seperti kemajuan pemindaian atau hasil yang ditemukan.

4.7. set STOP_ON_SUCCES true

Dengan mengatur parameter ini menjadi true, Metasploit akan menghentikan proses pengujian setelah berhasil menemukan kombinasi kredensial yang valid. Ini berguna untuk menghemat waktu dan sumber daya jika Anda sudah mendapatkan akses yang diperlukan, sehingga tidak perlu mencoba kredensial lainnya.

4.8. set RHOSTS [ip external]

Parameter RHOST (Remote Host) digunakan untuk menentukan alamat IP target yang ingin Anda uji. Dalam kasus ini, Anda menetapkan RHOST ke 34.128.116.196, yang berarti semua pengujian atau pemindaian akan diarahkan ke alamat IP tersebut.

4.9. set USER_FILE Desktop/username.txt

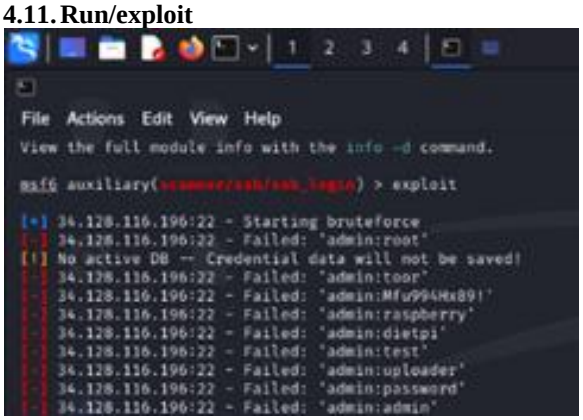
Parameter ini digunakan untuk menentukan file yang berisi daftar nama pengguna yang akan diuji. Dalam contoh ini, Desktop/username.txt adalah jalur ke file yang berisi nama-nama pengguna yang akan digunakan dalam pengujian.

4.10. set PASS_FILE Desktop/pass.txt

Parameter ini digunakan untuk menentukan file yang berisi daftar kata sandi yang akan diuji bersama dengan nama pengguna. Desktop/pass.txt adalah jalur ke file yang berisi kata sandi yang akan diuji bersama dengan nama pengguna dari USER_FILE.

Gambar 6. Mengonfigurasi parameter

4.11. Run/exploit



Gambar 7. Jalankan penyerangan

Setelah menjalankan serangan, Metasploit berhasil menemukan kombinasi nama pengguna dan kata sandi yang valid dari file yang disediakan. Hasilnya menunjukkan:

4.12. Succes'username:password'

Gambar 8. Brute-force berhasil

4.13. Sessions

Dalam konteks Metasploit, "sesi" merujuk pada koneksi yang berhasil dibuat setelah berhasil mengeksploitasi atau mendapatkan akses ke sebuah target. Ketika Anda berhasil melakukan brute force dan mendapatkan kredensial yang valid, Metasploit dapat membuka sesi baru untuk interaksi lebih lanjut dengan sistem target.

4.14. Mengakses sesi

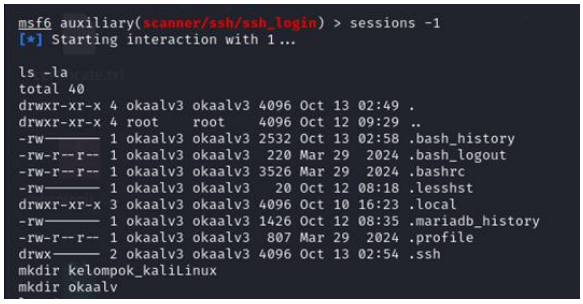
Sessions -i [session-number]

Gambar 9. Mengakses sesi

4.15. Menjelajahi sistem target

Setelah mengakses session tersebut, Anda dapat melakukan berbagai aksi untuk mengeksplorasi sistem target lebih lanjut: Sebagai contoh, disini penulis akan membuat sebuah direktori menggunakan kali linux yang sudah terkoneksi atau sudah berhasil login ke dalam debian linux di instance google cloud vm.

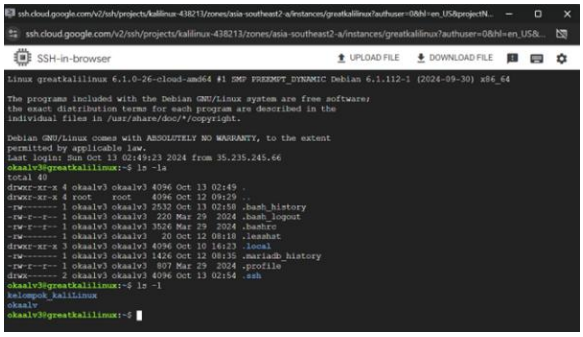
```
mkdir kelompok_kaliLinux
mkdir okaalv
```



Gambar 10. Membuat direktori dari kali linux

Hasil pada kali linux ketika diberi command ls -1

Gambar 11. Yang terjadi pada kali linux



Gambar 12. Yang terjadi pada ssh *vminstances* google cloud platform

Pengujian ini menunjukkan bahwa sistem target memiliki kerentanan yang signifikan yang dapat dieksploitasi melalui metode yang relatif sederhana. Berikut ini adalah analisis dari hasil yang diperoleh:

4.16. Kerentanan dalam Layanan SSH

Layanan SSH yang terbuka dan konfigurasi yang tidak aman meningkatkan risiko akses yang tidak sah. Penggunaan kata sandi yang lemah merupakan titik lemah yang dapat dieksploitasi oleh penyerang. Hal ini menggarisbawahi pentingnya menggunakan praktik manajemen kata sandi yang baik.

4.17. Pentingnya Pemindaian Rutin

Hasil pemindaian menunjukkan bahwa banyak organisasi yang mungkin tidak menyadari kerentanan yang ada dalam infrastruktur mereka. Oleh karena itu, melakukan pemindaian dan audit keamanan secara teratur sangat penting untuk mendeteksi dan mengatasi potensi risiko sebelum dieksploitasi.

4.18. Rekomendasi Keamanan

Berdasarkan temuan-temuan tersebut, beberapa rekomendasi untuk meningkatkan keamanan sistem antara lain:

a. Penggunaan Kata Sandi yang Kuat
   Mendorong penggunaan kata sandi yang kompleks dan tidak mudah ditebak.
b. Konfigurasi SSH yang aman
   Nonaktifkan autentikasi berbasis kata sandi dan beralih ke autentikasi kunci publik.
c. Audit dan Pemantauan
   Menerapkan audit dan pemantauan akses secara berkala untuk mendeteksi perilaku yang mencurigakan.

Pada penelitian, penulis menemukan hasil dimana penulis berhasil masuk ke dalam sistem jaringan melalui port SSH yang terbuka. Untuk keamanan Google Cloud pada penelitian ini cukup tidak aman untuk keamanannya.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa pengujian penetrasi menggunakan Kali Linux di Google Cloud Platform (GCP) efektif dalam mengidentifikasi kerentanan keamanan jaringan, seperti port yang terbuka, versi aplikasi yang rentan, dan kelemahan otentikasi. Alat-alat seperti Nmap dan Metasploit digunakan untuk menemukan potensi eksploitasi melalui serangan brute force dan eksekusi kode jarak jauh. Meskipun GCP menyediakan infrastruktur yang aman, kesalahan konfigurasi oleh pengguna tetap menjadi faktor utama yang menyebabkan kerentanan.

Dampak dari penelitian ini adalah untuk memberikan wawasan tentang pentingnya konfigurasi yang tepat dalam menjaga keamanan jaringan di lingkungan cloud serta menunjukkan keefektifan penggunaan Kali Linux untuk mengidentifikasi dan mengevaluasi kerentanan dalam pengaturan jaringan cloud.

DAFTAR PUSTAKA

[1] Setyawan. F, Rasyidah, and Amnur H, " Keamanan Jaringan Wireless Dengan Kali Linux " JITSI : Jurnal Ilmiah Teknologi Sistem Informasi., vol. 3, pp. 16-22, Maret 2022.

[2] Andrianti. D. A," ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN MENGGUNAKAN IPFIRE UNTUK MENANGKAL WEBSITE YANG TAK DIINGINKAN PADA YAYASAN ADIL GRUP " Jusikom : Jurnal Sistem Komputer Musirawas., vol. 6, pp. 142-154, Desember 2021.

[3] Andrian, " Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux " Generation Journal., vol. 4, pp. 2580-4952, Juli 2020.

[4] Sinha. V. A, " Evaluation of Network Security on basis of Virtualization Techniques in Kali Linux Environment" Turkish Journal of Computer and Mathematics Education., vol. 12, pp. 591-595, Januari 2021.

[5] Salman. Z, " Securing Cloud Computing: A Review " International Journal of Computing and Digital Systems., vol. 10, pp. 16-22, April 2021.

[6] Dwi. A, and Ujianto. E. I. H, " Analisis Sistem Keamanan Pada Cloud Computing Menggunakan Metode Attack-Centric (Security System Analysis of Cloud Computing Using Attack-Centric Method) " Progresif: Jurnal Ilmiah Komputer., vol. 5, pp. 115-125, Mei 2023.

[7] Pamungkas. C, " Analysis of Brute Force Attacks Using National Institute of Standards and Technology (NIST) Methods on Routers (Case study: Faculty of Engineering UNIMMA) Journal of Informatics, Information System, Software Engineering and Applications (INISTA)., vol. 5, pp. 115-125, Mei 2023.

[8] Nadeem M, " Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System" IEEE., vol. 9, pp. 16-22, November 2021.

[9] Rahman. R, " Keamanan Jaringan Cloud-Native dan Implementasi Solusi Keamanan Menggunakan Cloud Computing " Technology Sciences Insights Journal., vol. 1, pp. 11-21, Maret 2024.

[10] Rani. K, " Comprehensive Analysis of Various Cyber Attacks" IEEE Mysore Sub Section International Conference(MysuruCon)., vol. 1, pp. 16-22, Maret 2021.