(2024), 2 (11): 151-162 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

ANALISIS PENYERANGAN *BRUTEFORCE* TERHADAP *SECURE SHELL* (SSH) MENGGUNAKAN METODE *PENETRATION TESTING*

Renal Alwan Febrian [1], Yusuf Muhyidin [2], Dayan Singasatia [3]
Program Studi Teknik Informatika S1, Fakultas Teknik, Sekolah Tinggi Teknologi Wastukancana
Jl. Cikopak No.53, Sadang, Purwakarta, Jawa Barat, Indonesia
renalalwan18@wastukancana.ac.id

Abstract (English)
This research aims to analyze brute force attacks on Secure Shell (SSH) using the Hydra tool. Brute force attacks are a serious threat to information security, particularly in educational institutions connected to the internet. The research results indicate that brute force attacks successfully targeted SSH services, uncovering weak username and password combinations. Mitigation suggestions include using strong passwords, using non-standard ports, limiting failed login attempts, using public key-based authentication, system updates, and using firewalls. This research provides insights into brute force attacks on SSH and offers practical recommendations to enhance information system security in educational institutions.

Article History
Submitted: 15 Juli 2024
Accepted: 18 Juli 2024
Published: 25 Juli 2024

Key Words
brute force attacks, Secure Shell (SSH), Hydra, information security, mitigation, education.

Abstrak (Indonesia)
Penelitian ini bertujuan untuk menganalisis serangan *bruteforce* terhadap *Secure Shell* (SSH) menggunakan alat *Hydra*. Serangan *bruteforce* merupakan ancaman serius bagi keamanan informasi, khususnya dalam lembaga pendidikan yang terhubung dengan internet. Hasil penelitian menunjukkan bahwa serangan *bruteforce* berhasil dilakukan terhadap layanan SSH, menemukan kombinasi *username* dan *password* yang lemah. Saran mitigasi termasuk penggunaan kata sandi yang kuat, penggunaan *port* non-standar, pembatasan upaya *login* yang gagal, penggunaan autentikasi berbasis kunci publik, pembaruan sistem, dan penggunaan firewall. Penelitian ini memberikan wawasan tentang serangan *bruteforce* pada SSH dan memberikan rekomendasi praktis untuk meningkatkan keamanan sistem informasi di institusi pendidikan.

Sejarah Artikel
Submitted: 15 Juli 2024
Accepted: 18 Juli 2024
Published: 25 Juli 2024

Kata Kunci
serangan *bruteforce*, *Secure Shell* (SSH), *Hydra*, keamanan informasi, mitigasi, pendidikan.

1. Latar Belakang

Di era digital saat ini, teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari, mempengaruhi berbagai aspek termasuk komunikasi, bisnis, dan layanan publik. Salah satu teknologi yang memainkan peran penting dalam infrastruktur informasi adalah jaringan komputer. Jaringan komputer memfasilitasi pertukaran data antara perangkat dan pengguna di seluruh dunia dengan cepat dan efisien. Namun, dengan kemajuan teknologi juga muncul tantangan baru, terutama dalam hal keamanan informasi. Serangan *cyber* menjadi ancaman yang semakin nyata, dengan serangan yang semakin kompleks dan beragam. Salah satu metode serangan yang umum dilakukan adalah serangan *brute force*, di mana penyerang mencoba kombinasi kata sandi secara berulang untuk mendapatkan akses tidak sah ke sistem atau layanan tertentu.

Serangan *bruteforce* berjalan melalui semua kemungkinan kombinasi karakter legal secara berurutan sampai mereka menemukan input yang benar. Semakin lama kata sandi, semakin banyak waktu yang biasanya diperlukan untuk menemukan input yang benar. Serangan *bruteforce* yang paling umum menggunakan kamus kata sandi yang berisi jutaan kata untuk diuji. Serangan *bruteforce* yang berhasil tidak hanya memberi peretas akses ke data, aplikasi, dan sumber daya,

tetapi juga dapat berfungsi sebagai titik masuk untuk serangan lebih lanjut beberapa tanda dapat ditafsirkan sebagai indikator serangan *bruteforce*.(Menteng et al., 2023).

Cisco memperingatkan tentang lonjakan global dalam serangan *brute-force* yang menargetkan berbagai perangkat, termasuk layanan Jaringan Privat Virtual (VPN), antarmuka autentikasi aplikasi web, dan layanan SSH, setidaknya sejak 18 Maret 2024."Semua serangan ini tampaknya berasal dari node keluar TOR dan serangkaian terowongan dan *proxy* anonim lainnya," kata *Cisco Talos* .Serangan yang berhasil dapat membuka jalan bagi akses jaringan yang tidak sah, penguncian akun, atau kondisi penolakan layanan, perusahaan keamanan siber menambahkan.*Cisco Talos* menggambarkan upaya penyerangan brutal tersebut sebagai penggunaan nama pengguna generik dan *valid* untuk organisasi tertentu, dengan serangan yang tanpa pandang bulu menargetkan berbagai sektor di seluruh wilayah geografis.(Cisco Talos),2024).

Badan Siber dan Sandi Negara (BSSN) melalui 71 titik honeypot-nya mendeteksi adanya serangan SSH (*secure shell attack*) sepanjang 2020 di Indonesia. Menurut Ketua Indonesia *Honeynet Project* Dr Charles Lim, SSH attack merupakan serangan yang menyerang pada layanan yang digunakan administrator, bukan layanan umum biasa. SSH attack sudah lama populer di kalangan peretas lantaran SSH layaknya pintu gerbang ke semua layanan.Jika penyerang berhasil masuk ke SSH, menurut Charles, mereka dapat melakukan apa pun terhadap sistem yang disusupi. Mereka bisa menyiapkan perangkat yang terinfeksi untuk dimanfaatkan sendiri atau justru ditawarkan kepada peretas lain.Menurut Charles, SSH memiliki kerentanan yang memungkinkan peretas dengan gampangnya masuk ke layanan. Ini lantaran otentikasi pengguna hanya memerlukan *username* dan *password*. Apalagi, menurut Charles, kata sandi bisa diserang dengan teknik *brute force* peretas menebak acak dengan bantuan kamus kata sandi.(BSSN),2021)

Secure Shell (SSH) adalah sebuah protokol jaringan yang digunakan untuk mengamankan komunikasi data antara dua perangkat yang terhubung melalui jaringan. Dalam konteks ini, Namun, meskipun SSH memiliki protokol keamanan yang kuat, ia tetap rentan terhadap berbagai jenis serangan, salah satunya adalah serangan *bruteforce*. Serangan *bruteforce* adalah metode yang digunakan oleh penyerang untuk mendapatkan akses dengan mencoba berbagai kombinasi *username* dan *password* hingga menemukan yang benar. Metode ini sering kali dilakukan secara otomatis menggunakan skrip atau perangkat lunak khusus, yandapat mencoba ribuan hingga jutaan kombinasi dalam waktu singkat.*Hydra* adalah alat yg digunakan untuk melakukan serangan *bruteforce* terhadap berbagai layanan jaringan. Ini adalah alat yang sangat populer dalam komunitas keamanan siber dan sering digunakan oleh peneliti keamanan dan profesional untuk menguji kekuatan kata sandi dan mengidentifikasi kelemahan dalam konfigurasi layanan jaringan.

Penetration testing, atau uji penetrasi, adalah teknik yang digunakan untuk mengidentifikasi dan mengevaluasi kerentanan keamanan dalam sistem jaringan. Dengan melakukan *penetration testing*, organisasi dapat memahami titik lemah dalam sistem mereka dan mengambil langkah-langkah untuk memperbaikinya sebelum penyerang nyata dapat mengeksploitasinya. Metode ini bukan hanya membantu dalam menemukan kelemahan yang ada, tetapi juga mengukur efektivitas dari sistem keamanan yang sudah diterapkan.

Penelitian ini bertujuan untuk menganalisis serangan *bruteforce* terhadap SSH menggunakan metode *penetration testing*. Melalui analisis ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam tentang bagaimana serangan *bruteforce* dilakukan, dampaknya terhadap keamanan sistem, serta langkah-langkah pencegahan yang dapat diambil untuk mengurangi risiko serangan tersebut. Penelitian ini juga akan membahas alat dan teknik yang digunakan dalam

penetration testing untuk mensimulasikan *serangan bruteforce*, serta strategi mitigasi yang efektif untuk melindungi SSH dari ancaman serupa di masa mendatang. Dengan demikian, penelitian ini berkontribusi terhadap peningkatan keamanan jaringan, khususnya dalam konteks penggunaan SSH, dan menyediakan panduan praktis bagi administrator sistem dalam melindungi infrastruktur mereka dari serangan *bruteforce*.

2. Kajian Pustaka

2.1 Jaringan Komputer

Keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidaklangsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. selain itu, untuk menjaga data pada sistem komputer supaya aman dari berbagai ancaman.(Ryan Permana et al., 2019).

2.2 Virtual Box

Virtual Box adalah salah satu aplikasi virtualisasi (*Hypervisor*) yang dapat di-install pada komputer baik yang berbasis Intel maupun AMD, tanpa memerlukan fitur *processor* yang dibangun dalam hardware baru seperti Intel Vt-x atau AMD-V. Bahkan, *Virtual Box* dapat digunakan pada hardware/processor lama yang tidak mendukung *hardware virtualization* . Virtual Box dapat di-install pada Sistem Operasi *Windows*, *Mac*, *Linux*, atau *Solaris*, baik yang 32 bit maupun 64 bit (Host OS), dan menjalankan berbagai Sistem Operasi (Guest OS) sebanyak yang dikehendaki, berdampingan dengan aplikasi lainnya.(Gratianus & Larosa, 2020).

2.3 Kali Linux

Kali Linux adalah sebuah distribusi *Linux* yang digunakan untuk uji penetrasi dan keamanan jaringan. Dalam penelitian yang disebutkan, *Kali Linux* digunakan sebagai salah satu alat untuk melakukan pengujian keamanan pada Sistem Informasi Sekolah MTsN 8 Bantul. Meskipun dalam beberapa kasus *Kali Linux* tidak berhasil menemukan celah keamanan, namun masih merupakan salah satu alat yang penting dalam melakukan uji penetrasi. *Kali Linux* dilengkapi dengan berbagai tools dan fitur yang dapat digunakan untuk mengidentifikasi celah keamanan, melakukan penetrasi, dan mengamankan sistem informasi.(Silmina et al., 2022).

2.4 Secure Shell

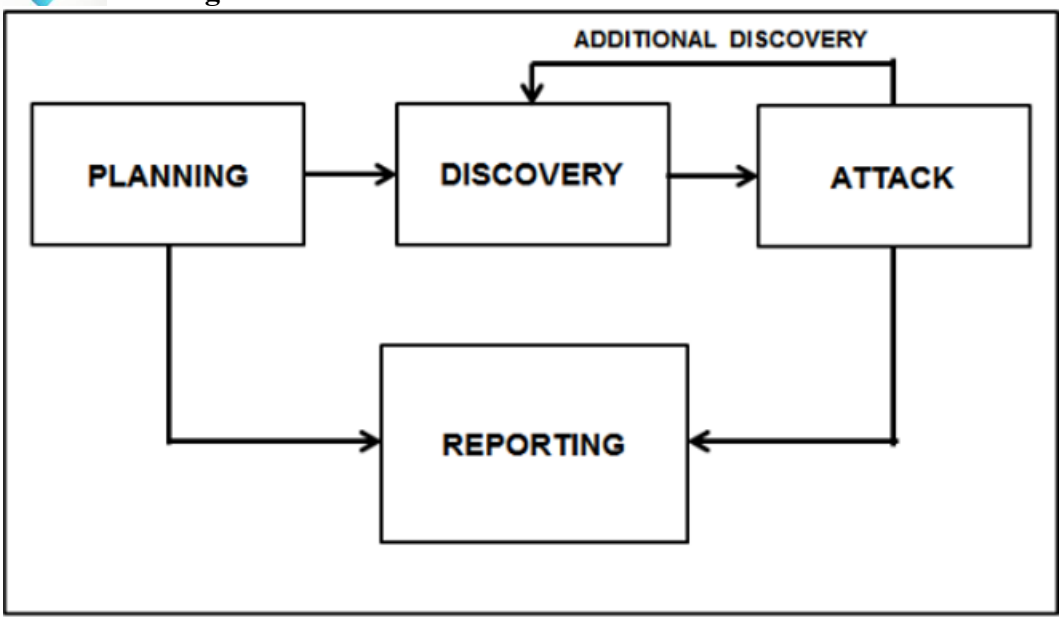
Secure Shell (SSH) adalah sebuah protokol jaringan yang memungkinkan pertukaran data yang aman antara dua perangkat melalui koneksi terenkripsi. SSH digunakan untuk mengakses perangkat jarak jauh dan melakukan *transfer file* secara aman melalui jaringan. Protokol ini menggunakan enkripsi untuk melindungi data yang dikirim antara *server* dan klien, sehingga mencegah akses yang tidak sah terhadap informasi sensitif. SSH juga memungkinkan pengguna untuk mengelola perangkat jarak jauh dengan aman melalui koneksi yang terenkripsi.(Heni Jusuf, 2019).

2.5 Brute Force

Brute Force merupakan teknik dalam mencocokkan kata atau string pada teks dengan *pattern* di tiap karakter dimulai dari kiri ke kanan. Teknik ini digunakan untuk mencari solusi dengan cara menguji semua kemungkinan secara sistematis. bekerja dengan membandingkan karakter satu per satu antara teks dan pola dari kiri ke kanan. Langkah-langkah pencocokkan dilakukan secara terstruktur dengan mengurutkan tiap solusi satu per satu untuk menemukan solusi terbaik. Contoh penerapan algoritma *brute force* adalah dalam mencocokkan *string* dengan *pattern*, di mana

langkah pertama adalah melakukan pencocokkan karakter satu per satu antara *string* dan *pattern*.(Ramadhoni et al., 2022).

2.6 Penetration Testing



Gambar 2. 1 Tahapan Penetration Testing

Penetration testing adalah metode sistematis untuk menilai ketahanan sistem *blockchain* terhadap serangan berbahaya. Ini melibatkan mensimulasikan serangan dunia nyata pada sistem *blockchain* menggunakan teknik khusus seperti rekognisi sistem, injeksi data, penolakan layanan, dan peretasan akun. Tujuan dari tes ini adalah untuk menemukan kerentanan dalam sistem dan memungkinkan pengembang untuk memperbaiki kelemahan-kelemahan tersebut sebelum penyerang dapat mengeksploitasi mereka. *Penetration testing* juga dapat digunakan untuk menilai kepatuhan regulasi dan keamanan. Hasil dari tes ini dapat digunakan untuk meningkatkan keamanan keseluruhan sistem *blockchain* dengan mengidentifikasi dan memperbaiki kerentanan potensial.(Kaushik & El Madhoun, 2023).

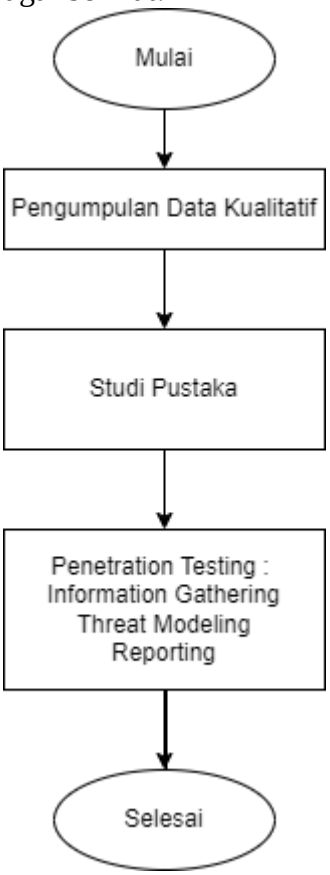
2.7 Hydra

Hydra adalah *cracker login* jaringan paralel yang dibangun di berbagai sistem operasi seperti *Kali Linux, Parrot,* dan lingkungan pengujian penetrasi utama lainnya. *Hydra* bekerja dengan menggunakan pendekatan yang berbeda untuk melakukan serangan *brute force* untuk menebak kombinasi nama pengguna dan kata sandi yang tepat. *Hydra* biasanya digunakan oleh penguji penetrasi bersama dengan serangkaian program seperti *crunch, cupp* dll, yang digunakan untuk menghasilkan daftar kata. *Hydra* kemudian digunakan untuk menguji serangan menggunakan daftar kata yang dibuat oleh program ini. (Sampurna, 2022)

3. Metode

3.1 Alur Penelitian

Dalam penelitian ini, pendekatan yang digunakan oleh penulis adalah analisis kualitatif yang bersifat deskriptif. Pendekatan ini dipilih karena permasalahan yang ingin diungkapkan lebih menekankan pada deskripsi keadaan objek yang diteliti. Adapan penulis membuat tahapan analisis sistem keamanan jaringan sebagai berikut:



Gambar 3. 1Alur Penelitian

3.2 Metode Pengumpulan Data

Metode Pengempulan data yang penulis gunakan dalam penelitian ini sebagai berikut :

1. Studi Pustaka

   Di dalam penelitian ini penulis melakukan pengumpulan data dengan melihat referensi dari berbagai sumber seperti berupa skripsi dan jurnal yang berkaitan dengan keamanan jaringan.

3.3 Alat Dan Bahan Penelitian

1. Spesifikasi perangkat keras (*Hardware)* yang dilakuna pada penelitian ini sebagai berikut:

Tabel 3. 1 Spesifikasi Hardware

No.	Spesifikasi	Keterangan
1	Laptop Asus	-
2	Sistem Operasi	Kali - Linux
3	Processor	Intel Celeron
4	Ram	4 GB

2. Spesifikasi perangkat lunak (*Software)* dalam penelitian ini menggunakan sebagai berikut:

Tabel 3. 2 Spesifikasi Software

No.	Kebutuhan	Keterangan	Fungsi
1.	Sistem Operasi	Kali - Linux	Untuk mengontrol operasi – operasi dasar dan termasuk untuk menjalankan perangkat lunak untuk percobaan *Penetration Testing* Pada *Secure Shell* yang dituju.

3.4 Penetration Testing

Pada tahap ini menjelaskan penelitian yang melewati beberapa tahapan alur penelitian yang dilalui yang dijelaskan pada gambar dibawah ini :

Gambar 3. 2 Tahap Penelitian Penetration Testing

3.4.1 Information Gathering

Selama fase ini, penulis mengumpulkan data secara manual melalui wawancara dan dokumentasi dari pihak-pihak terkait, atau informasi yang dapat diakses oleh pihak-pihak terkait dari sistem yang sedang diuji, sehingga pengumpulan data biasanya diklasifikasikan sebagai *passive penetration testing*.

3.4.2 Threat Modelling

Di tahap ini akan penulis akan mulai mencoba menyerang *Secure Shell* (SSH) untuk mendapatkan *username* dan *password.* Teknik serangan yang akan penulis lakukan adalah *bruteforce* dengan menggunakan *tools hydra.*

3.4.3 Reporting

Pada tahap akhir ini penulis menyimpulkan hasil dari penyerangan *brute force* terhadap SSH, Kerentanan apa saja yang teridentifikasi selama pengujian, dan memberikan rekomendasi

langkah pencegahan seperti malakukan keamanan tambahan autentikasi kunci public-privat atau pembatasan akses

4. Hasil dan Pembahasan

4.1 Hasil Pemngumpulan Data

Didalam penelitian ini, penulis melakukan pemgumpulan data dengan menggunakan metode kualitatif yaitu dengan cara observasi dan studi pustaka berikut adalah hasil :

4.1.1 Studi Pustaka

Hasil dari studi pustaka yang penulis lakukan adalah untuk memperkuat penelitian dengan mencari berbagai referensi dari buku dan jurnal untuk mempelajari mengenai konsep dan teknik penyerangan *bruteforce* menggunakan metode *penetration testing.*

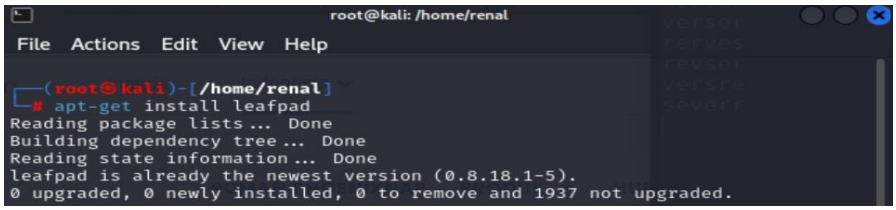
4.2 Information Gathering

Ditahap ini peneliti saudah mengetahui *IP-Address* yaitu 192.168.1.61 setalah mengetahui penulis melakukan *ping* untuk memverifikasi apakah *ip* tersebut aktif dan berfungsi setelah melakukan *ping* maka langkah selanjutnya adalah melakukan *nmap* terhadap *ip* yang dituju untuk mengetahui *port* apa saja yang terbuka untuk menentukan layanan yang sedang berjalan.

4.3 Threat Modelling

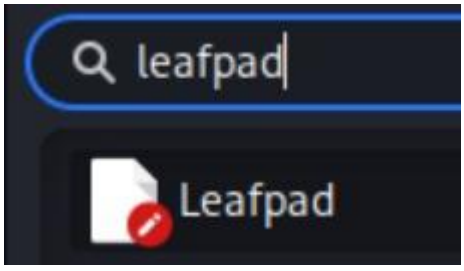
Ditahap ini penulis mulai melakukan serangkaian simulasi penyerangan *bruteforce* terhadap *Secure shell* (SSH) dengan menggunakan beberapa tools untuk penyerangan.

4.3.1Instalisasi leafpad



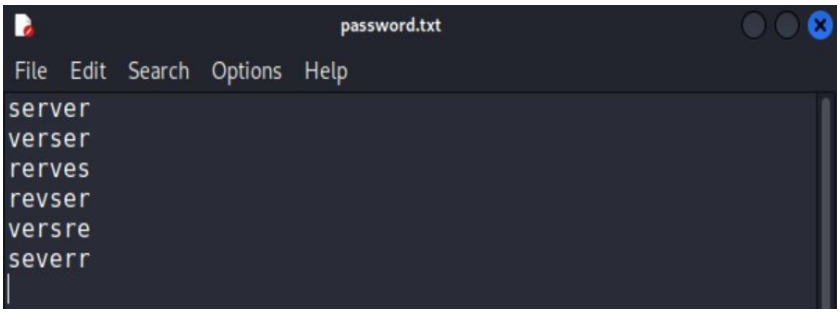
Gambar 4. 1 Install Leafpad

Ditahap ini penulis meng-*Install leafpad* untuk kebutuhan serangkaian *username* dan *password* untuk kebutuhan penyerangan terhadap *secure shell*.



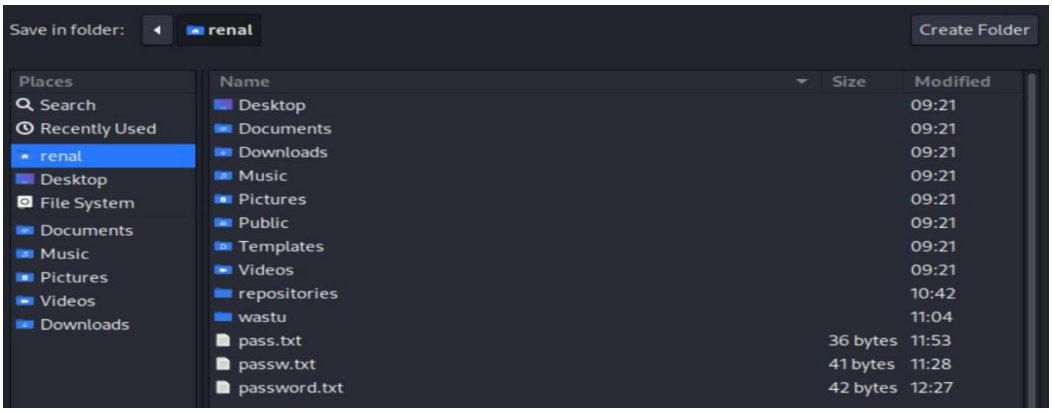
Gambar 4. 2 Leafpad

Setelah berhasil meng-*install* penulis bisa menemukan *leafpad* dibagian menu *search engine* untuk menggunakannya.



Gambar 4. 3 Membuat serangkaian Wordlist

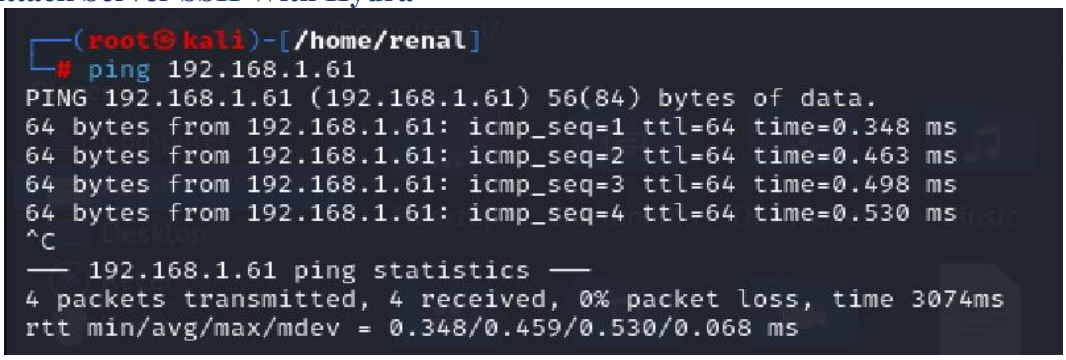
Setelah penulis menggunakan *leafpad* maka penulis bisa membuat *password palsu* dengan memasukkan *password* yang sebenarnya didalam *wordlist*.



Gambar 4. 4 Directory

Setelah penulis membuat serangkaian *password* lalu save dengan nama file yang diingin dengan diakhiri ".txt" lalu dissave di*directory/home/renal*.

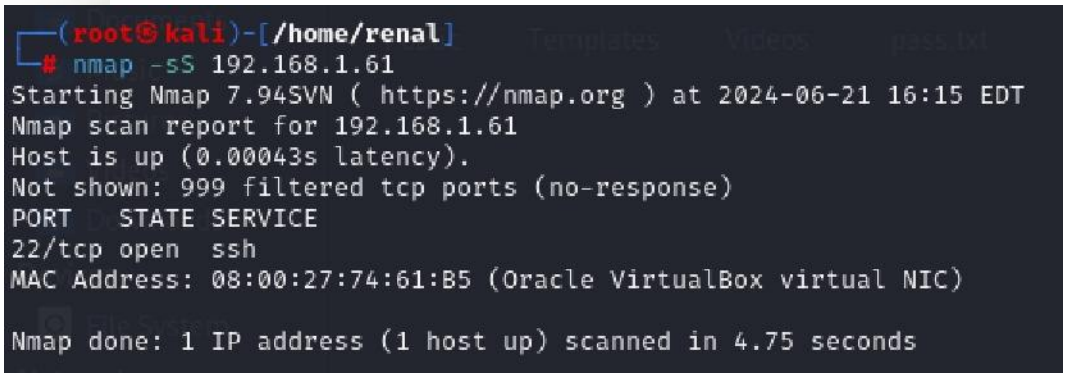
4.3.2 Attack Server SSH With Hydra



Gambar 4. 5 Ping IP-Address

Perintah ini mengirimkan paket ICMP Echo Request ke alamat IP 192.168.1.61.Setiap baris setelah perintah menunjukkan penerimaan Balasan Gema ICMP dari alamat IP target. Outputnya menunjukkan ukuran balasan (64 byte), alamat IP pengirim (192.168.1.61), nomor urut

paket (icmp_seq), TTL (Time to Live yaitu 64), dan putaran -waktu perjalanan (waktu) dalam milidetik. Ini menunjukkan ping berhasil dan semua paket mencapai tujuan dan kembali tanpa kehilangan apa pun. Nilai RTT menunjukkan koneksi yang sangat cepat dan stabil ke alamat IP 192.168.1.61.

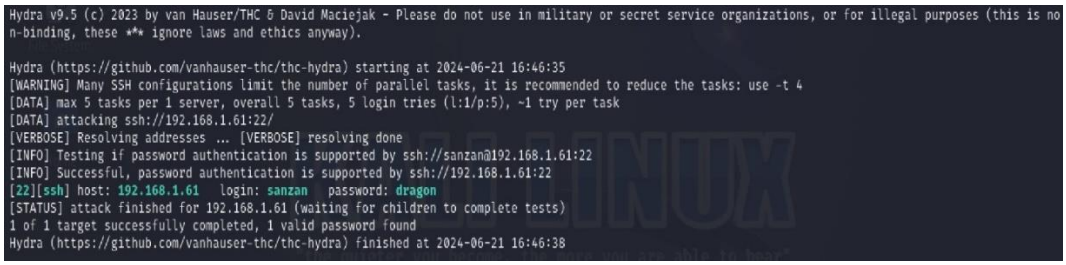


Gambar 4. 6 Nmap IP-Address

Output ini menunjukkan bahwa alamat IP 192.168.1.61 memiliki port 22 terbuka, yang biasanya digunakan untuk akses SSH (Secure Shell). Alamat MAC menunjukkan bahwa perangkat tersebut adalah mesin virtual yang berjalan di Oracle VirtualBox. Pemindaian menunjukkan bahwa 999 port TCP yang tersisa telah difilter, artinya port tersebut tidak merespons pemindaian.

Gambar 4. 7 Perintah Menggunakan Hydra

Perintah tersebut memerintahkan hydrauntuk mencoba login ke layanan SSH pada alamat IP 192.168.1.61 menggunakan nama pengguna sanzandan kata sandi yang tercantum dalam file /home/renal/pass2.txt.



Gambar 4. 8 Hasil Bruteforce SSH

Setelah melakukan serangan *bruteforce* pada layanan SSH di alamat IP 192.168.1.61. Didapatkan hasil id *login* dan *Password* yeng berarti serangan tersebut berhasil.

4.3.3 Reporting

Secara default SSH client & server melakukan komunikasi menggunakan *port* TCP 22, tetapi penggunaan port TCP tersebut bisa diganti dengan *port non-standard*. Misalnya menggunakan *port-port* yang tidak diketahui oleh orang lain selain diri kita sendiri. Tujuannya tentu saja untuk menghindari percobaan pembobolan sistem via SSH, karena port yang kita gunakan tidak terpikirkan oleh orang lain.

Perubahan konfigurasi *port* ini dilakukan di sisi SSH *server*, sedangkan dari sisi SSH *client* cukup menyesuaikan *port* yang digunakan pada saat *remote login* dilakukan. Dengan syarat *port non standard* yang dipilih belum digunakan oleh aplikasi lain di SSH *server*. Berikut adalah langkah-langkah untuk melakukan perubahan port SSH *server*.

Berdasarkan hasil pengujian terhadap SSH pada *port* 22 setelah melakukan pengujian hasilnya bisa dilihat pada tabel yang merangkum hasil dari setiap gambar beserta penjelasannya dalam konteks serangan *bruteforce* terhadap SSH:

Tabel 4. 1 Reporting

Gambar	Deskripsi	Penjelasan
Gambar 4.5	Ping IP-Address	Perintah ping 192.168.1.61 mengirimkan paket ICMP Echo Request ke alamat IP 192.168.1.61. Output menunjukkan penerimaan balasan ICMP dari target dengan ukuran 64 byte, TTL 64, dan waktu perjalanan (rata-rata 0.459 ms). Koneksi sangat cepat dan stabil.
Gambar 4.6	Nmap IP-Address	Perintah nmap -sS 192.168.1.61 menunjukkan bahwa alamat IP 192.168.1.61 memiliki port 22 terbuka untuk SSH. Alamat MAC menunjukkan perangkat berjalan di Oracle VirtualBox. 999 port lainnya difilter, tidak merespons pemindaian.
Gambar 4.7	Perintah Menggunakan Hydra	Perintah hydra -v -l sanzan -P /home/renal/pass2.txt 192.168.1.61 ssh menjalankan Hydra untuk mencoba login ke SSH pada alamat IP 192.168.1.61 menggunakan nama pengguna sanzan dan kata sandi dari file /home/renal/pass2.txt.
Gambar 4.8	Hasil Bruteforce SSH	Hasil serangan brute force menunjukkan bahwa Hydra berhasil menemukan kombinasi username sanzan dan password dragon untuk login ke layanan SSH pada alamat IP 192.168.1.61.

Penjelasan Tabel

- Gambar 4.5: Menunjukkan proses pengecekan koneksi menggunakan perintah ping. Semua paket mencapai tujuan dan kembali tanpa kehilangan, menunjukkan koneksi yang stabil dan cepat.
- Gambar 4.6: Menunjukkan hasil pemindaian *port* menggunakan nmap. Hanya *port* 22 yang terbuka (untuk SSH), dan 999 *port* lainnya difilter.

- Gambar 4.7: Menunjukkan penggunaan alat *bruteforce Hydra* untuk mencoba berbagai kombinasi *password* terhadap layanan SSH. Gambar
- 4.8: Menunjukkan bahwa serangan *bruteforce* berhasil dengan ditemukan kombinasi *username* dan *password* yang *valid*, yaitu sanzan dengan *password* dragon.

Dari hasil di atas, kita dapat melihat bagaimana serangan *bruteforce* SSH dilakukan dan bagaimana hasilnya dapat digunakan untuk mendapatkan akses tidak sah ke sistem. Langkah-langkah mitigasi yang direkomendasikan meliputi penggunaan kata sandi yang kuat, konfigurasi *server* untuk membatasi upaya login yang gagal, dan penggunaan autentikasi berbasis kunci publik. Pada penelitian ini peneliti berhasil mengumpulkan hasil hasil yang dibutuhkan untuk menyimpulkan hasil dari penelitian di *web* SMAN 1 Wanayasa. Berikut ini adalah hasil yang ditemukan oleh peneliti pada saat fase pengujian:

1. Pada saat pengujian serangan SQL *injection* terhadap *web* SMAN 1 Wanayasa, *web* telah masuk ke dalam kategori aman. Karena *web* telah melindungi diri nya dengan WAF (*web application firewall*) berupa Imunify360 yang telah berhasil mencegah serangan atau kegiatan yang mencurigakan pada *web*.
2. Pada tahap pemindaian celah, *web* ini masih memiliki beberapa *port* yang terbuka, hal ini bisa dimanfaatkan oleh penyerang untuk melakukan eksploitasi untuk mengambil, memanipulasi atau merusak data yang terdapat pada *web* SMAN 1 Wanayasa.

Jadi pada intinya, *web* ini telah berhasil melindungi diri terhadap serangan SQL *injection.* Akan tetapi, masih terdapat celah celah lain dalam *web* SMAN 1 Wanayasa yang memungkinkan untuk dilakukan eksploitasi.

5. Kesimpulan

Dari hasil pengujian dan analisis yang telah dilakukan terhadap layanan SSH pada alamat IP 192.168.1.61, dapat diambil beberapa kesimpulan penting: Pengujian dengan perintah ping menunjukkan bahwa koneksi ke alamat IP 192.168.1.61 sangat stabil dan cepat, di mana semua paket ICMP mencapai tujuan dan kembali tanpa kehilangan apa pun, dengan waktu perjalanan rata-rata (RTT) sekitar 0.459 ms. Hasil pemindaian menggunakan nmap menunjukkan bahwa *port* 22, yang biasanya digunakan untuk akses SSH, terbuka pada alamat IP 192.168.1.61, sementara 999 *port* lainnya difilter dan tidak merespons pemindaian, dan alamat MAC perangkat menunjukkan bahwa ini adalah mesin *virtual* yang berjalan di *Oracle VirtualBox*.

6. Daftar Pustaka

Ryan Permana, Dochi Ramadhani, & Isnania Lestari. (2019). *Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak*.

Gratianus, F., & Larosa, N. (2020). PEMANFAATAN VIRTUAL BOX DALAM PRAKTIKUM ADMINISTRASI SERVER MENGGUNAKAN TEKNIK DHCP PADA MIKROTIK ROUTER OS. In *Jurnal METHODIKA* (Vol. 2, Issue 1).

Silmina, E. P., Firdonsyah, A., & Amanda, R. A. A. (2022). ANALISIS KEAMANAN JARINGAN SISTEM INFORMASI SEKOLAH MENGGUNAKAN PENETRATION TEST DAN ISSAF. *Transmisi*, *24*(3), 83–91. https://doi.org/10.14710/transmisi.24.3.83-91

Heni Jusuf. (2019). *Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online*.

Ramadhoni, A. T., Santi, I. H., Kirom, S., Islam, U., & Blitar, B. (2022). PENERAPAN ALGORITMA BRUTE FORCE PADA APLIKASI SIDAYKO BERBASIS ANDROID. In *Jurnal MNEMONIC* (Vol. 5, Issue 1).

Kaushik, S., & El Madhoun, N. (2023). Analysis of Blockchain Security: Classic attacks, Cybercrime and Penetration Testing. In *MobiSecServ* (Vol. 2023). https://hal.science/hal-04299951

Sampurna, M. R. (2022). *Implementasi Hydra, FFUF, dan WFUZZ dalam Brute Force DVWA*. *1*(2). https://jurnal.netplg.com/