Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-10

Penerapan dan Pengujian Keamanan SSH Pada Server Linux menggunakan Hydra

Daryn Ramadhani Az Zahra*, Fauzan Perdana Ilham, Herlambang Nurasyid Ramdhani, Aep Setiawan

Sekolah Vokasi, IPB University

Abstrak: Saat ini, teknologi internet berkembang dengan pesat, dan memastikan keamanan operasi jaringan menjadi krusial untuk mengatasi meningkatnya ancaman serangan siber. Penelitian ini bertujuan untuk menganalisis implementasi dan pengujian keamanan SSH pada server Linux menggunakan Hydra untuk mendeteksi kerentanan yang mungkin dieksploitasi oleh penyerang. Metodologi yang digunakan mencakup pengumpulan data melalui tinjauan literatur dan observasi langsung terhadap praktik implementasi sistem keamanan pada SSH di server Linux. Temuan penelitian menunjukkan adanya kerentanan dalam sistem login, seperti kata sandi yang mudah ditebak dan periode timeout login yang singkat. Namun, dengan langkah mitigasi seperti membuat kata sandi yang kuat, memperpanjang periode timeout login, dan memanfaatkan alat manajemen log terpusat seperti ELK Stack atau Splunk, keamanan sistem dapat ditingkatkan secara signifikan. Studi ini menekankan pentingnya evaluasi keamanan yang berkelanjutan dan implementasi praktik terbaik dalam manajemen akses SSH untuk melindungi server Linux dari ancaman siber.

Kata kunci: Keamanan *SSH,* Pengujian Pentrasi, Keamanan Siber, *Hydra, Server Linux*

DOI:
https://doi.org/10.47134/pjise.v1i3.2627
*Correspondence: Daryn Ramadhani Az Zahra
Email: razzdaryn@apps.ipb.ac.id

Received: 01-05-2024
Accepted: 15-06-2024
Published: 31-07-2024

Abstract: Currently, internet technology is advancing rapidly, and ensuring the security of network operations is crucial to address the escalating threats of cyber-attacks. This research aims to analyze the implementation and security testing of SSH on Linux servers using Hydra to detect vulnerabilities that may be exploited by attackers. The methodology employed includes data collection through literature review and direct observation of security system implementation practices on SSH in Linux servers. The research findings indicate vulnerabilities in the login system, such as easily guessable passwords and short login timeout periods. However, with mitigation measures such as creating strong passwords, extending login timeout periods, and utilizing centralized log management tools such as ELK Stack or Splunk, system security can be significantly enhanced. This study emphasizes the importance of continuous security evaluation and the implementation of best practices in SSH access management to protect Linux servers from cyber threats.

Keywords: *SSH Security, Penetration testing, Cyber Security, Hydra, Linux Server*

Pendahuluan

Dalam era kemajuan teknologi internet yang pesat, menjaga keamanan dalam jaringan kerja sangat penting untuk mengatasi meningkatnya ancaman serangan siber. Suatu jaringan membutuhkan seorang kepala keamanan yang handal, terutama dalam menangani serangan peretas. Keamanan komputer bertujuan melindungi informasi yang tersimpan di dalamnya. Jaringan tanpa keamanan yang memadai sangat berisiko karena mudah diakses dan diserang oleh para peretas. Penetration testing adalah salah satu cara untuk mendeteksi kelemahan yang mungkin dieksploitasi oleh peretas, dengan mencoba menembus celah keamanan pada server. Jika berhasil, peretas dapat mengakses dan memanipulasi data yang tersimpan di dalam server tersebut. Oleh karena itu, penetration testing dilakukan oleh sejumlah ahli, termasuk kepala jaringan, untuk memastikan keamanan jaringan tersebut.

Carapaling akurat untuk mengevaluasi sikap keamanan informasi organisasi adalah dengan mengamati bagaimana organisasi tersebut berdiri melawan serangan, cara terbaik untuk memastikan bahwa sistem aman adalah dengan mencoba pengujian penetrasi, pengujian penetrasi sering kali memungkinkan analisis keamanan menemukan kerentanan baru (Zeebaree et al., 2020). SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. 1. Kelemahan protokol SSH yang ada pada berbagai sistem operasi (dalam bentuk openSSH) adalah diperbolehkannya login root langsung. (Boss E, 2012). Dalam proses ini, peretas mencoba mengakses sistem pengguna melalui teknik enumeration, yang melibatkan berbagai cara untuk memecahkan password yang dihasilkan dari hash generator. Untuk melakukan enumeration, berbagai tools open-source seperti Hydra, Medusa, dan John The Ripper digunakan. Dalam pengujian ini, penggunaan tool Hydra untuk meretas password akan disimulasikan, dan langkah-langkah mitigasi terhadap serangan akan diimplementasikan.

Metodologi Penelitian

Pengumpulan data dilakukan untuk mendukung penelitian mengenai analisis "Penerapan dan Pengujian Keamanan SSH Pada Server Linux Menggunakan Hydra", dengan melaksanakan studi literatur dilakukan untuk mencari beberapa data yang terkait mengenai cara membuat dan menerapkan sistem keamanan untuk mendukung sistem keamanan pada server Linux. Dalam hal ini peneliti mengumpulkan dan melakukan analisis terhadap beberapa literatur yang berasal dari buku-buku referensi, jurnal, maupun internet yang terkait dengan penerapan keamanan sistem pada server Linux.

Metodologi lain yang dilakukan adalah teknik observasi yang dieksekusi terhadap praktik implementasi keamanan sistem pada SSH di server Linux. Dengan kombinasi pengumpulan data melalui studi literatur dan observasi langsung, penelitian ini bertujuan untuk memperoleh pemahaman yang komprehensif mengenai penerapan dan pengujian keamanan SSH pada server Linux menggunakan Hydra.

Hasil dan Pembahasan

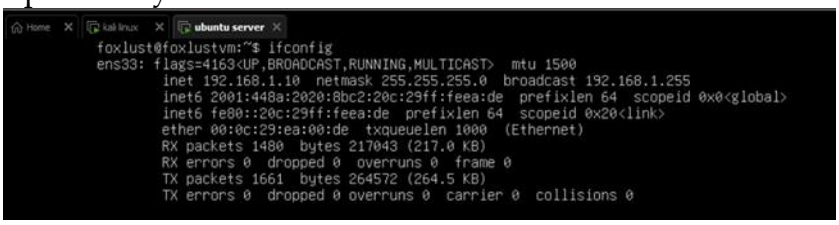
Penelitian ini bertujuan untuk mengevaluasi keamanan SSH dalam sistem dan juga memastikan keamanan Linux tidak mudah diretas. Dalam rangka mencapai tujuan tersebut, serangkaian langkah-langkah telah diimplementasikan dan dievaluasi. Langkah pertama melibatkan konfigurasi pada dua sistem operasi yang
digunakan, yaitu Kali Linux dan Ubuntu.

Tabel 1: Spesifikasi OS pada Viirtual Box

OS	Kali Linux	Ubuntu Server
Versi	2024.1	24.04
RAM	8 GB	8 GB
CPU	2 Core	2 Core
Penyimpanan	60 GB	60 GB
Jaringan	Bridge Local	Bridge Local

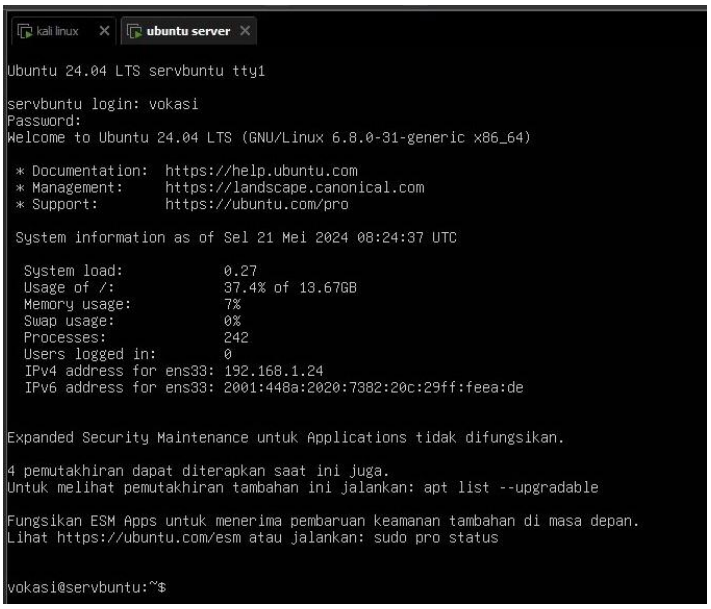
Linux Ubuntu (Target *Bruteforce*)

Dengan menggunakan command **ifconfig**, dapat terlihat bahwa IP pada Linux Ubuntu adalah **192.168.1.10**. IP inilah yang menjadi target serangan *Bruteforce* yang akan dilakukan pada aplikasi Hydra.



Gambar 1. Pengecekkan IP Pada Linux Ubuntu (target)

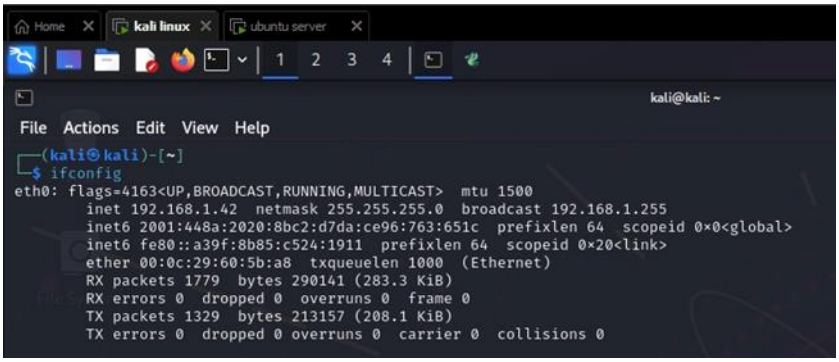
Kemudian pada **login screen** dibawah dapat terlihat bahwa username yang digunakan untuk login pada Linux Ubuntu adalah **vokasi**.



Gambar 2. Login Linux dengan user 'vokasi'

Username inilah yang nantinya akan digunakan untuk mencoba serangan *Bruteforce* pada aplikasi Hydra. Hydra akan mencoba login dengan menggunakan kombinasi username **vokasi** dan password yang telah tersedia pada list **rockyou.txt.**

Linux Kali (Attacker)



Gambar 3. Pengecekkan IP pada Kali Linux (attacker)

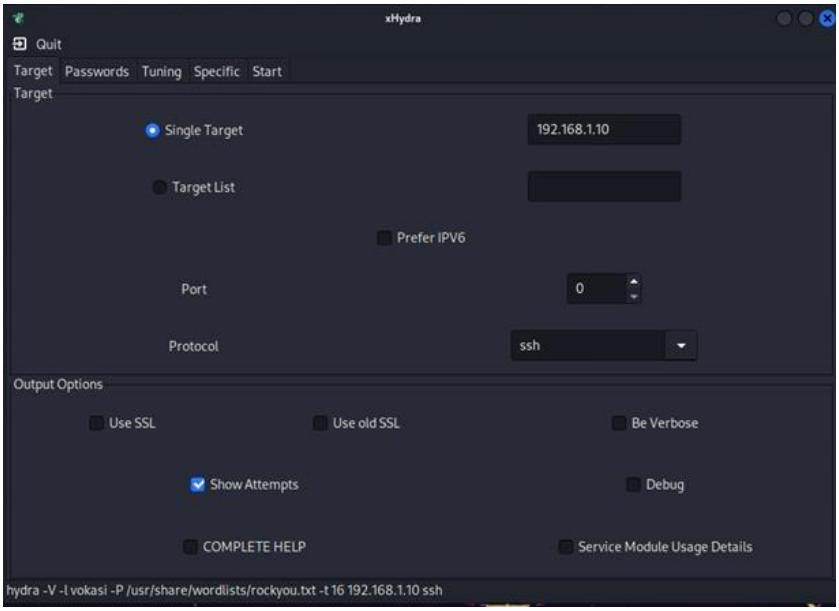
Pada gambar diatas, dapat terlihat bahwa IP pada Linux Kali adalah **192.168.1.42**. IP Inilah yang akan menjadi *attacker* atau penyerang dengan menggunakan teknik *Bruteforce* terhadap Linux Ubuntu.

Hydra

Linux Kali dibekali dengan aplikasi atau *tool* bawaannya, yaitu Hydra. Hydra sendiri merupakan salah satu tool yang populer digunakan dalam pengujian penetrasi atau ethical hacking untuk menguji keamanan sistem, khususnya dalam konteks pengujian kekuatan kata sandi atau serangan *password.*

Gambar 4. Logo Hydra

Tool ini dapat digunakan untuk melakukan serangan *Bruteforce*, di mana *tool* akan mencoba semua kemungkinan kombinasi kata sandi secara otomatis untuk mencoba mendapatkan akses ke sistem yang dilindungi oleh kata sandi.

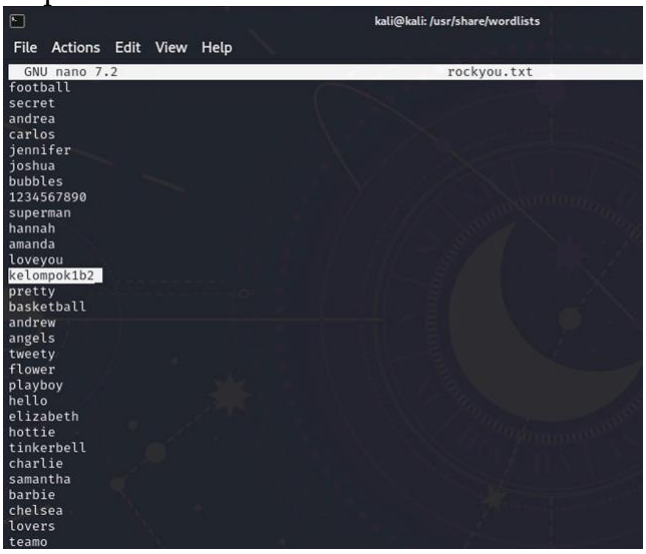


Gambar 5. Tampilan Tool Hydra

Hydra dapat digunakan untuk berbagai protokol dan layanan, termasuk SSH, FTP, HTTP, SMB, dan banyak lagi. Ini adalah alat yang sangat fleksibel dan kuat yang memungkinkan pengujian keamanan sistem dengan mencoba berbagai kata sandi yang mungkin digunakan oleh penyerang untuk mendapatkan akses yang tidak sah ke sistem.

Rockyou

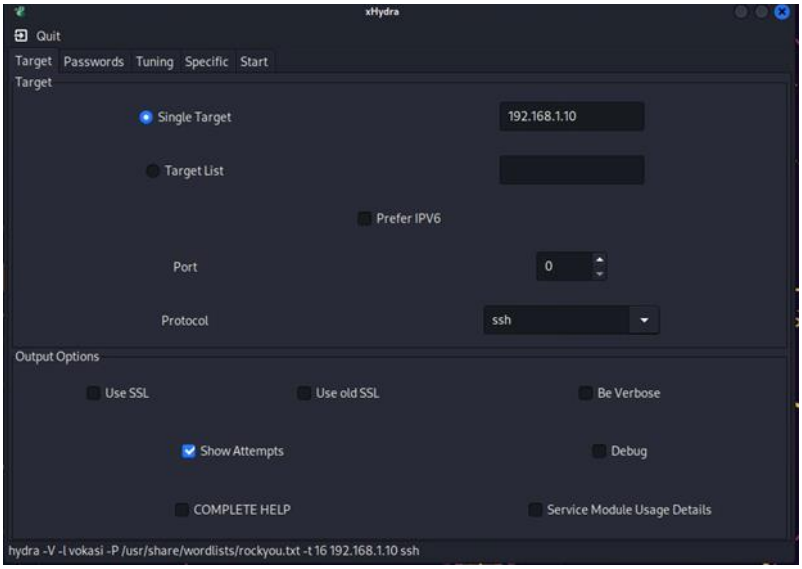
Rockyou adalah daftar kata yang berisi lebih dari 14 juta atau lebih tepatnya **14,344,403** daftar kata sandi yang bocor karena pelanggaran data. Pada tahun 2009, sebuah perusahaan bernama RockYou diretas. Hal tersebut tidak akan menjadi masalah besar jika saja mereka tidak menyimpan semua kata sandi mereka dalam keadaan tidak terenkripsi, dalam bentuk teks biasa agar dapat dilihat oleh penyerang. Penyerang mengunduh daftar semua kata sandi dan membuatnya tersedia untuk umum. Oleh karena itu, Rockyou biasanya digunakan oleh peretas untuk memecahkan file atau menebak kata sandi.



Gambar 6. Preview isi rockyou

Gambar diatas merupakan cuplikan isi dari **rockyou.txt.** Telah disisipkan password asli dari Linux Ubuntu yaitu **kelompok1b2** di antara lebih dari 14 juta daftar password pada **rockyou.txt.**

1. Menjalankan Hydra

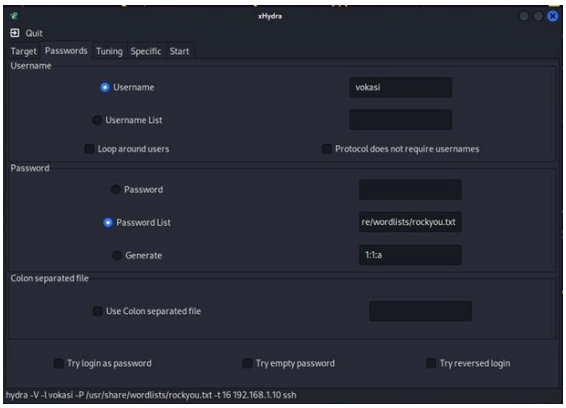


Gambar 7. Halaman Utama Aplikasi Hydra

Untuk melakukan B*ruteforce* pada Linux Ubuntu, jalankan aplikasi Hydra pada Linux Kali. Gambar diatas merupakan tampilan utama dari aplikasi Hydra. Pada tab **Target**, centang **Singe Target**, kemudian isi dengan IP Target yaitu **192.168.1.10**. Hal ini dilakukan karena target atau tujuan serangan hanya satu *devices* saja.

Protokol yang ingin diserang merupakan protokol SSH. Maka dari itu, pada bagian **Protocol**, pilih **ssh**. Lalu tidak lupa pula untuk mencentang **Show Attempts** agar log percobaan penyerangan akan ditampilkan.

2. Konfigurasi Pada Tab Password

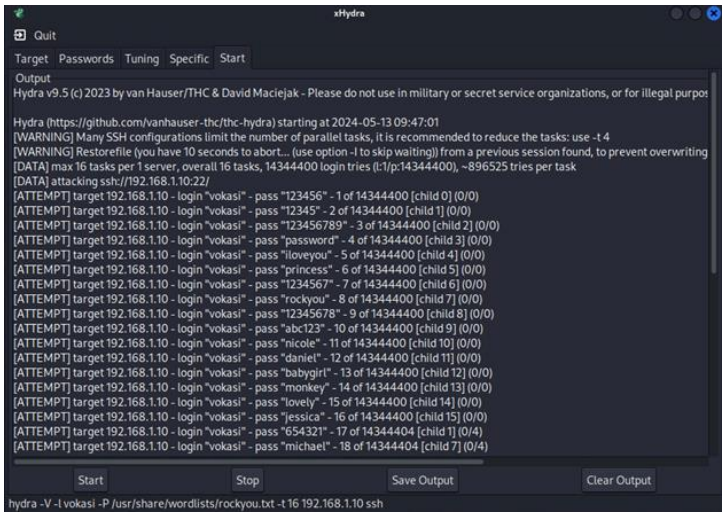


Gambar 8: Pemilihan Target Bruteforce

Pada tab **Passwords**, terdapat pilihan menggunakan **Username** atau **Username List**. Apabila ingin mencoba menebak username dari target *Bruteforce*, maka opsi ini dapat dicentang lalu memasukkan *path file* dari daftar username yang ingin ditebak. Namun, pada kasus ini username telah diketahui, jadi tidak perlu lagi untuk mencoba menebak username satu per satu. Maka dari itu, centang **Username**, kemudian masukkan username yang telah diketahui, yaitu **vokasi**.

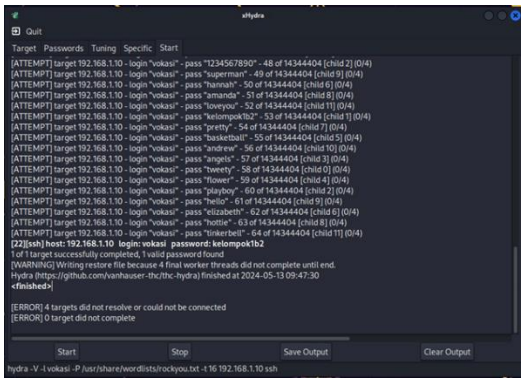
Daftar password yang ingin kita tebak adalah **rockyou.txt**. Centang **Password**, lalu masukkan direktori *path* dari file **rockyou.txt** tersebut pada kolom yang telah disediakan.

3. Memulai Serangan Bruteforce



Gambar 9. Tampilan Attempt Untuk Menyocokkan Password

Setelah semuanya telah selesai dikonfigurasi, klik **Start** pada menu tab, kemudian tampilannya akan berubah menjadi seperti gambar diatas. Untuk memulai serangan, klik **Start** pada tombol dibagian bawah kiri. Kemudian proses *Bruteforce* akan segera dilakukan. Setiap percobaan akan ditampilkan pada tab tersebut. Dapat terlihat bahwa pada setiap barisnya, Hydra mencoba untuk melakukan login menggunakan protokol SSH dengan IP **192.168.1.10** dengan setiap baris password yang tersedia pada **rockyou.txt** yang totalnya sejumlah **14.344.404** baris.



Gambar 10. Tampilan Berhasil Menyocokkan Password

Ketika proses *Bruteforce* telah berhasil, maka akan memunculkan peringatan **<finished>**. Dapat terlihat pada gambar tersebut bahwa Hydra hanya mencoba 64 kali dari total 14.344.404 daftar password yang tersedia, lalu akhirnya berhasil menemukan password yang benar, yaitu **kelompok1b2** pada percobaan yang ke-64.

Saran

Langkah-langkah pencegahan untuk setiap tahap pengujian penetrasi dapat digunakan sebagai parameter keamanan dalam pembangunan sistem berbasis SSH. Tingkat keamanan yang dihasilkan akan lebih tinggi jika tindakan pencegahan ini digabungkan dengan alat keamanan lainnya untuk menciptakan lapisan perlindungan yang berlapis. Berikut saran-saran untuk mengoptimalkan SSH:

- Nonaktifkan login root pada layanan SSH untuk mencegah serangan *bruteforce* terhadap login root.
- Batasi waktu percobaan login untuk memperlambat serangan *bruteforce.*
- Gunakan kata sandi yang kuat dengan panjang minimal 6 karakter dan terdiri dari huruf serta angka.
- Lakukan verifikasi menggunakan tanda tangan digital pada perangkat lunak yang digunakan untuk memastikan keasliannya dan mencegah penyebaran program berbahaya di sistem.
- Lakukan pembaruan perangkat lunak secara rutin.
- Konfigurasi ulang sistem log agar disimpan pada direktori dan dengan nama yang berbeda untuk menghambat proses *covering tracks.*
- Buat backup sistem log secara rutin dengan program penjadwal.
- Tambahkan perangkat keamanan sentry untuk memantau sistem log.
- Implementasikan IDS dan port sentry untuk menambahkan informasi ekstra pada sistem log dan sebagai peringatan dini jika terjadi serangan terhadap sistem.

Simpulan

Penelitian dan pengujian terhadap keamanan SSH pada server Linux dengan menggunakan alat seperti Hydra telah mengungkapkan adanya beberapa kerentanan dalam sistem login, terutama terkait dengan penggunaan password yang mudah ditebak dan waktu timeout login yang singkat. Meskipun demikian, penelitian ini juga menunjukkan bahwa dengan menerapkan berbagai langkah mitigasi, keamanan sistem dapat ditingkatkan secara signifikan.

Pembuatan password yang kuat dan memperpanjang waktu timeout login adalah langkah awal yang penting dalam mengurangi risiko akses tidak sah. Selain itu, Linux menyediakan mekanisme deteksi dan pencatatan percobaan login, yang memungkinkan administrator untuk memantau aktivitas mencurigakan melalui log sistem. Penggunaan sistem manajemen log terpusat seperti ELK Stack atau Splunk sangat dianjurkan untuk analisis real-time dan deteksi dini terhadap serangan potensial.

Langkah-langkah penguatan konfigurasi SSH juga memainkan peran krusial dalam meningkatkan keamanan. Menonaktifkan login root, menerapkan autentikasi kunci

publik, mengubah port default SSH, serta menggunakan alat seperti Fail2ban untuk memblokir alamat IP yang melakukan percobaan login berulang, adalah beberapa strategi efektif yang dapat diterapkan. Implementasi langkah-langkah ini menunjukkan bahwa meskipun terdapat kerentanan yang dapat dieksploitasi oleh alat seperti Hydra, penerapan mitigasi yang tepat dapat secara signifikan mengurangi risiko dan melindungi sistem dari akses tidak sah.

Kesimpulannya, penelitian ini menekankan pentingnya evaluasi keamanan yang berkelanjutan dan penerapan praktik terbaik dalam pengelolaan akses SSH. Dengan demikian, administrator sistem dapat memastikan bahwa server Linux tetap terlindungi dari berbagai ancaman keamanan siber. Penelitian lebih lanjut dan pengembangan alat-alat keamanan yang lebih canggih akan terus dibutuhkan untuk menghadapi ancaman yang terus berkembang di dunia maya.

Referensi

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland)*, *12*(6). https://doi.org/10.3390/electronics12061333

Boss, E., & Poll, E. (2012). *Evaluating implementations of SSH by means of model-based testing*.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver menggunakan Penetration Test. *Jurnal Informatika*, *8*(2), 183–190. https://doi.org/10.31294/ji.v8i2.10854

Hardi Wirasasmita, R., & Hizbi, T. (2015). *Efektivitas Penerapan Sistem Operasi Berbasis Linux Ubuntu Hamzanwadi V.14 Untuk Meningkatkan Hasil Belajar Mahasiswa*. *10*(1), 15–25.

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158.

Herdiana, Y., Munawar, Z., & Indah Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT : Information Communication & Technology*, *20*(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Jusuf Heni. (2015). Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online. *Bina Insani Ict Journal*, *2*(2), 75–84.

Kurniawan, A. A., & Nugroho, Y. (2019). Upaya Penetrasi dengan Enumeration menggunakan Hydra. *Journal of Technology and Informatics (JoTI)*, *1*(1), 62–64.

Likmi, S. (2020). *Penerapan Keamanan Remote Server Melalui SSH*. *4*(1), 133–138.

Nugraha, P. A., Irwansyah, M. A., & Priyanto, H. (2016). Rancang Bangun Web Server Berbasis Linux Dengan Metode Load Balancing (Studi Kasus : Laboratorium Teknik Informatika). *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *3*(1), 371–375.

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, *1*(2), 85–92.

Sakti, B., Aziz, A., & Doewes, A. (2016). Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan Penetration Testing. *Jurnal Teknologi & Informasi ITSmart*, *2*(1), 44. https://doi.org/10.20961/its.v2i1.620

Samantha, B. S., & Phanindra, M. V. (2018). an Overview on the Utilization of Kali Linux Tools. *IJRAR-International Journal of Research and Analytical Reviews*, *5*(2), 104–113.

Sugeng Santoso. (2018). Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional. *Jurnal Kajian Lemhannas RI*, *34*, 43–48.

Sunaringtyas, S. U., & Prayoga, D. S. (2021). Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On. *Edu Komputika Journal*, *8*(1), 48–56. https://doi.org/10.15294/edukomputika.v8i1.47179

Syarif, M. (2015). Vol. XII No. 2, September 2015 Jurnal Techno Nusa Mandiri. *Techno Nusa Mandiri*, *XII*(2), 21–26.

Tohirin, T. (2020). Penerapan Keamanan Remote Server Melalui Ssh Dengan Kombinasi Kriptografi Asimetris Dan Autentikasi Dua Langkah. *Jurnal Teknologi Informasi*, *4*(1), 133–138. https://doi.org/10.36294/jurti.v4i1.1262

Utama, D. A., Khairil, K., & Supardi, R. (2024). Analisis Keamanan Website Menggunakan Ptes (Penetration Testing Execution And Standart). *Jurnal Media Infotama*, *20*(1), 106–112.

Zeebaree, S. R. M., Jacksi, K., & Zebari, R. R. (2020). Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(1), 505–512. https://doi.org/10.11591/ijeecs.v19.i1.pp505-512