 ISSN:2302-8149
e-ISSN:2540-9719

Penerapan Model *Zero Trust* pada Keamanan SSH dengan Protokol *Kerberos dan OpenLDAP*

Implementing Zero Trust Model for SSH Security with kerberos and OpenLDAP

Salwa Deta Mediana, Lindawati*, Mohammad Fadhli
Teknik Elektro, Sarjana Terapan Teknik Telekomunikasi,
Politeknik Negeri Sriwijaya Palembang
Jalan Srijaya Negara Bukit Besar Palembang
*e-mail: lindawati9111@yahoo.com

(***received*:** 4 Agustus 2023, ***revised*:** 4 Agustus 2023, ***accepted*:** 5 Agustus 2023)

Abstrak

Untuk menghilangkan asumsi kepercayaan terhadap jaringan internal, penelitian ini membahas penerapan Model Zero Trust dalam keamanan SSH (Secure Shell). Pendekatan penelitian dilakukan dengan melakukan uji coba dengan mengintegrasikan protokol Kerberos dan OpenLDAP ke dalam infrastruktur SSH. Sementara OpenLDAP berfungsi sebagai direktori pusat untuk manajemen pengguna dan izin akses, Kerberos digunakan untuk autentikasi tunggal dan sumber daya keamanan seperti tiket Kerberos. Dalam penelitian ini, sistem operasi Debian digunakan sebagai sistem operasi server. Ada alasan yang kuat untuk mengamankan SSH dengan Kerberos dan OpenLDAP. Serangan protokol SSH umumnya menargetkan port standar 22 (SSH), yang digunakan oleh SSH. Untuk memastikan keamanan dan integritas sistem server, port SSH harus dilindungi dengan Kerberos dan OpenLDAP. Autentikasi tunggal Kerberos membatasi akses ke SSH, mengurangi kemungkinan serangan brute-force dan pencurian kata sandi. Integrasi OpenLDAP mempermudah manajemen pengguna dan otorisasi. Penerapan strategi Zero Trust memastikan autentikasi yang kuat dan melindungi sistem dari ancaman dari dalam. Dengan autentikasi yang kuat, otorisasi yang tepat, dan pemisahan jaringan internal dan eksternal, sistem terlindungi dari serangan baik dari dalam maupun luar jaringan. Langkah penting dalam menjaga keamanan sistem server, integritas data, dan kerahasiaan informasi adalah melindungi port 22 dan meningkatkan keamanan SSH dengan integrasi ini. Temuan penelitian menunjukkan bahwa penerapan model Zero Trust melalui integrasi protokol ini secara signifikan meningkatkan keamanan sistem, dengan peningkatan pemisahan jaringan, autentikasi, dan otorisasi.

Kata kunci: Keamanan Server, Kerberos, OpenLDAP, SSH.

Abstract

In order to remove trust presumptions towards the internal network, this study addresses the use of the Zero Trust Model in SSH (Secure Shell) security. The study approach is conducting tests by incorporating the Kerberos and OpenLDAP protocols into the SSH infrastructure. While OpenLDAP acts as a central directory for user management and permission access, Kerberos is utilized for single authentication and security resources like Kerberos tickets. As the server operating system for this investigation, Debian was used. Strong justification exists for securing SSH with Kerberos and OpenLDAP. SSH protocol assaults commonly target the standard port 22 (SSH), which is used for SSH. To ensure the security and integrity of the server system, the SSH port must be protected with Kerberos and OpenLDAP. SSH access is limited by Kerberos single authentication, which lowers the possibility of brute-force assaults and password theft. User administration and authorisation are facilitated by the integration of OpenLDAP. Implementing the Zero Trust strategy enables strong authentication and defends the system from insider threats. The system is protected from internal and external network assaults thanks to robust authentication, accurate authorisation, and isolating internal and external networks. An essential step in maintaining the security of the server system, data integrity, and information confidentiality is to secure port 22 and improve SSH

 ISSN:2302-8149
e-ISSN:2540-9719

with this integration. The research findings show that applying the Zero Trust model through this protocol integration greatly improves system security, resulting in better authentication and authorisation.

Keywords: *Server Security*, Kerberos, OpenLDAP, SSH

1 Pendahuluan

Faktor kunci dalam menjaga kerahasiaan dan integritas data yang disimpan adalah keamanan sistem server. Protokol *Secure Socket Shell* (SSH), yang berjalan pada lapisan ketujuh dalam arsitektur OSI (*Open System Interconnection*), menjadi komponen penting dalam infrastruktur keamanan server. Perangkat lunak bernama SSH sering digunakan untuk menjaga keamanan jaringan. Protokol ini memungkinkan transfer data yang dienkripsi antara server dan *client*, menyediakan koneksi data yang aman antara *port* terlindungi, serta melindungi transmisi data dari ancaman eksternal. Pengguna yang memiliki kredensial sah, seperti nama pengguna dan kata sandi pada sistem operasi server, dapat mengakses dan mengelola server secara remote serta mentransfer *file* diantara *workstation* menggunakan protokol SSH.

SSH menawarkan empat keunggulan keamanan utama, yaitu autentikasi pengguna, autentikasi host, enkripsi, dan integritas data [1]. Meskipun memiliki sistem keamanan yang kuat, kesulitan keamanan SSH terus berubah akibat serangan baru yang dilakukan oleh pihak yang tidak berwenang dan kemajuan teknologi. Pencurian data, yang sering dikenal sebagai *data breach*, merupakan salah satu masalah utama dalam keamanan sistem server. *Data breach* dapat memiliki dampak besar, termasuk pengungkapan informasi sensitif, pelanggaran privasi pengguna, dan merusak reputasi bisnis [1]. Keberhasilan serangan terhadap protokol SSH dapat menyebabkan kelemahan yang berpotensi menyebabkan terjadinya kasus *data breach*. Serangan yang berhasil pada protokol SSH dapat memberikan akses yang tidak sah ke sistem server, meningkatkan risiko pencurian data sensitif dan mungkin membahayakan perusahaan [2]. Untuk menghindari serangan yang dapat menyebabkan terjadinya kasus *data breach*, penting untuk menerapkan perlindungan yang kuat terhadap *protocol* SSH. Salah satu bentuk serangan yang harus diwaspadai adalah *brute-force attack*, dimana penyerang secara otomatis mencoba menebak kata sandi selama proses autentikasi dengan tujuan untuk mendapatkan akses yang tidak sah ke sistem server. Keamanan dan integritas data yang disimpan dalam sistem server dapat mengalami kerusakan yang signifikan akibat serangan ini, yang menimbulkan risiko yang besar terhadap terjadinya kasus *data breach*. Oleh karena itu, untuk mencegah serangan tersebut, *protocol* SSH harus dirancang dengan perlindungan yang tepat dan menggunakan teknik keamanan yang kuat.

Penelitian [3] membahas pengembangan sistem autentikasi Kerberos yang ditingkatkan untuk SDN *controller*. Masalah mengenai autentikasi *host* dalam jaringan SDN yang dapat diatur dengan skala menjadi fokus utama dalam penelitian ini. Penelitian ini menggunakan server terpusat yang menyimpan semua identitas dan kata sandi *host* untuk menilai kredensial *host* dan melakukan autentikasi *host* menggunakan protokol autentikasi Kerberos. Hasil penelitian menunjukkan bahwa dalam jaringan SDN yang dapat diatur dengan skala, metode autentikasi Kerberos dapat digunakan untuk menjamin keaslian *host*. Strategi ini dapat membantu melindungi dari ancaman jaringan dan meningkatkan keamanan jaringan.

Penelitian selanjutnya [4] menjelaskan bagaimana autentikasi Kerberos digunakan dalam sektor ritel *online* untuk mengirimkan produk kepada pelanggan. Tujuan dari proyek ini adalah menciptakan sistem autentikasi Kerberos untuk model pengiriman produk yang menjamin keandalan *client*, pemasok, dan karyawan pengantar. Hasil dari penelitian ini adalah mekanisme autentikasi Kerberos yang dapat digunakan di sektor ritel *online* untuk pengiriman barang kepada pelanggan. Proses autentikasi ini menjamin keabsahan *client*, pemasok, dan karyawan pengantar. Sistem autentikasi ini juga dapat digunakan dengan model pengiriman produk yang lebih kompleks.

Pada penelitian berikutnya [5], penekanannya adalah pada pemanfaatan konsep dari protokol Kerberos untuk meningkatkan keamanan protokol otentikasi 802.1x/EAP pada jaringan *Wire Local Area Network* (WLAN). Penelitian ini bertujuan untuk menyelesaikan masalah-masalah pada metode otentikasi WLAN yang ada, seperti serangan menebak kata sandi, serangan *replay*, dan serangan *man-in-the-middle* (MITM). Hasil dari penelitian ini adalah sebuah protokol baru yang disebut Kerberos *Extensible Authentication Protocol* (KEAP), yang meningkatkan keamanan

 ISSN:2302-8149
e-ISSN:2540-9719

otentikasi WLAN dengan menggunakan enkripsi kunci asimetris, nomor urut pesan, dan fungsi hash. Berdasarkan hasil pengujian, KEAP memiliki performa keamanan yang lebih baik dibandingkan dengan protokol otentikasi WLAN yang lebih umum digunakan, yaitu EAP-TLS.

Dengan menghilangkan asumsi kepercayaan terhadap jaringan internal, penelitian yang kami lakukan bertujuan untuk meningkatkan keamanan autentikasi *protocol* SSH dan sistem server dengan menerapkan model *Zero Trust* melalui integrasi protokol Kerberos dan OpenLDAP. Kami berharap dapat mengurangi risiko serangan dan melindungi sistem server dari kasus pencurian data yang dapat merugikan berbagai pihak dengan menerapkan langkah-langkah keamanan yang ketat untuk *protocol* SSH.

2 Tinjauan Literatur

A. Studi Literatur

Dalam penelitian ini, berbagai studi literatur relevan telah dijelajahi untuk memahami konsep Model *Zero Trust*, implementasi protokol Kerberos, serta penerapan keamanan SSH dengan mengintegrasikan protokol Kerberos dan sistem direktori OpenLDAP. Berikut adalah ringkasan beberapa penelitian terkait yang menjadi acuan dalam penelitian ini:

Tabel 1. Studi Literatur

No	Judul Penelitian	Penulis	Output
1	*A High Signature Algorithm Based on Kerberos for REST-style Cloud Storage Service*	Yuanyun Yang, Hui Li, Xiangdong C. & Yaoguang H.	Menawarkan metode LNU untuk menanggapi serangan terhadap *password-guessing attack* pada layanan penyimpanan *Cloud* [6].
2	*Securing Virtual Machine Images of Cloud by Encryption through Kerberos*	S.M. Neamul Islam & Md. Mahbubur Rahman	Menawarkan model dengan peningkatan fitur keamanan yang lebih tinggi dibandingkan dengan model lain yang sudah ada [4].
3	*Synopsis of Security: Using Kerberos Method to Secure File Transfer Sessions*	Fadi Al-Ayed & Hang Liu	Penelitian ini menyarankan penggunaan Kerberos sebagai pengganti SSL untuk melindungi dan mengkategorikan komunikasi FTP yang dienkripsi. Dengan menggunakan model pembelajaran mesin Markov, penelitian ini juga meningkatkan deteksi intrusi pada FTP. Studi ini menyimpulkan bahwa Kerberos adalah metode yang berguna untuk meningkatkan keamanan aplikasi dan protokol FTP. Implementasi Kerberos menghasilkan metode transportasi data yang lebih aman dan dapat diandalkan [7].
4	*A Fixed Network TransmissiBased on Kerberos Authentication Protocol*	M. CHALAPATHI RAO	Penelitian ini menggunakan Kerberos dalam sistem autentikasi untuk meningkatkan keamanan jaringan dan menyediakan *single sign-on*. Protokol ini juga menggunakan enkripsi untuk melindungi data yang dikirimkan melalui jaringan. Dengan Kerberos, prosedur otentikasi menjadi lebih efektif dan aman, memberikan pengalaman yang mulus dan aman bagi pengguna saat mengakses layanan jaringan [8].

Tabel 1 merupakan rangkuman dari beberapa penelitian terkait yang relevan. Setiap penelitian tersebut membahas penggunaan *protocol* Kerberos sebagai bagian dari *system* keamanan untuk melindungi berbagai layanan dan transmisi data dalam lingkungan jaringan. Penelitian-penelitian yang ada pada Tabel 1 menjadi referensi peneliti untuk memberikan landasan teori dan merancang model *framework* pada penelitian yang dilakukan.

 ISSN:2302-8149
e-ISSN:2540-9719

B. Objek Penelitian

Penelitian ini berfokus pada penerapan Model *Zero Trust* pada sistem keamanan *Secure Shell* (SSH) dengan memanfaatkan protokol Kerberos dan OpenLDAP sebagai backend autentikasi pada server Debian 11. Objek penelitian ini mencakup beberapa aspek utama yang akan diinvestigasi secara mendalam:

1) Sistem Keamanan *Secure Shell* (SSH):

Penelitian akan melibatkan analisis mendalam tentang sistem keamanan SSH, yang merupakan protokol kriptografi yang umum digunakan untuk mengamankan layanan jaringan pada lingkungan yang rentan terhadap serangan *cyber*. Pemahaman tentang fitur keamanan SSH, mekanisme autentikasi, dan aspek keamanan lainnya akan menjadi landasan untuk mengimplementasikan Model *Zero Trust* pada sistem ini.

2) Protokol Kerberos:

Objek penelitian juga akan mencakup penerapan protokol Kerberos sebagai sistem autentikasi yang kuat dalam konteks SSH. Analisis mendalam tentang protokol ini akan mencakup mekanisme *ticket-granting ticket* (TGT) dan tiket layanan, serta integrasi dengan sistem direktori OpenLDAP sebagai *backend* autentikasi.

3) Integrasi dengan OpenLDAP:

Penelitian akan mengeksplorasi proses integrasi antara protokol Kerberos dan sistem direktori OpenLDAP sebagai backend autentikasi. Pemahaman tentang pengaturan dan konfigurasi yang diperlukan untuk menghubungkan kedua sistem ini akan menjadi bagian penting dalam penerapan Model *Zero Trust*.

4) Penerapan *Model Zero Trust*:

Objek penelitian ini akan fokus pada implementasi Model *Zero Trust* pada keamanan SSH dengan mengintegrasikan protokol Kerberos dan OpenLDAP. Penerapan model ini akan melibatkan pengaturan autentikasi tunggal dan pembatasan akses berbasis otorisasi untuk meminimalkan risiko serangan dan memperkuat lapisan keamanan pada sistem.

5) Pengujian Keamanan:

Penelitian ini juga akan melibatkan pengujian keamanan yang komprehensif untuk menilai efektivitas penerapan Model *Zero Trust* pada keamanan SSH. Pengujian ini akan mencakup uji coba serangan, seperti *brute-force attack* dan *dictionary attack*, serta skenario *man-in-the-middle* untuk mengidentifikasi dan mengatasi potensi kerentanan dalam sistem.

3 Metode Penelitian

Pendekatan penelitian yang digunakan dalam studi ini melibatkan identifikasi masalah keamanan yang relevan, analisis literatur, serta pembuatan dan penerapan sebuah kerangka keamanan dalam lingkungan Debian Linux menggunakan model yang diusulkan. Selain itu, semua pengaturan dan konfigurasi yang diperlukan dilakukan, dan Kerberos serta OpenLDAP digunakan untuk menerapkan model tersebut. Data dikumpulkan menggunakan metode *Vulnerabilities Assessment and Penetration Testing* (VAPT), dan serangan eksploitasi yang dilakukan selama uji penetrasi dianalisis.

A. Pengidentifikasian Masalah

Identifikasi penelitian pada tahap ini berfokus pada masalah-masalah seperti ancaman serangan pada sistem server, kelemahan keamanan yang perlu diperbaiki, atau kesulitan dalam menjaga keamanan sistem.

B. Rancangan *Framework*

Pada tahap ini, sebuah kerangka keamanan yang akan digunakan dalam lingkungan sistem operasi Debian 11 harus dirancang. Rencana tersebut mencakup semua elemen yang diperlukan, termasuk mengintegrasikan protokol autentikasi Kerberos dan OpenLDAP, mengatur model untuk bekerja dengan protokol SSH, dan menetapkan prosedur otorisasi dan autentikasi.

C. Kerberos *Authentication Protocol*

Metode autentikasi tradisional Needham-Schroeder menjadi dasar dari sistem autentikasi Kerberos [9]. Sistem ini menggunakan pihak ketiga yang terpercaya untuk melakukan autentikasi dan pertukaran kunci antara entitas di jaringan. Enkripsi kunci simetris menjadi dasar dari Kerberos.

 ISSN:2302-8149
e-ISSN:2540-9719

Meskipun berbagai teknik enkripsi simetris dapat digunakan, Standar Enkripsi Data (DES) [10] awalnya digunakan sebagai standar interoperabilitas.

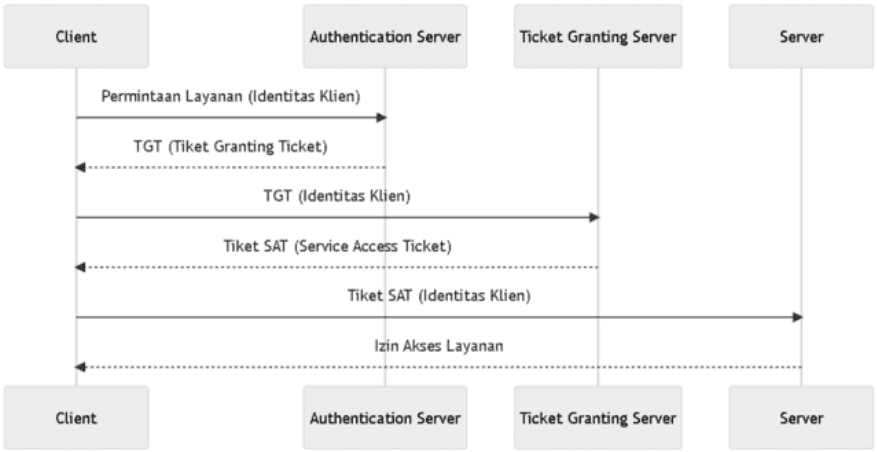
Tabel 2. Istilah-Istilah Penting pada Kerberos

Istilah	Keterangan
Authentication Server (AS)	Subprotokol dalam Kerberos yang menangani autentikasi awal dan memberikan Tiket-*Granting* Tiket (TGT) kepada *client*.
Ticket-Granting Ticket (TGT)	Tiket yang digunakan untuk memperoleh tiket layanan dan dikeluarkan oleh *Authentication Server* (AS) setelah berhasil melakukan otentikasi *client*.
Key Distribution Center (KDC)	*Database* (db), *Authentication Server* (AS), *dan Ticket Granting Server* (TGS) membentuk server autentikasi dalam Kerberos.
Ticket-Granting Server (TGS)	Server aplikasi yang menghasilkan tiket layanan sesuai permintaan dikenal sebagai *Ticket Granting Server* (TGS) dalam protokol Kerberos.
Enkripsi simetris	Enkripsi simetris adalah teknik kriptografi dimana kunci yang sama digunakan baik untuk mengenkripsi maupun mendekripsi komunikasi.
Pihak ketiga tepercaya	Entitas yang dapat dipercaya oleh kedua belah pihak dalam sebuah transaksi.
Tiket layanan	Otorisasi yang diberikan oleh TGS kepada *client* untuk menggunakan layanan jaringan.

Tabel 2 merupakan istilah-istilah penting yang ada pada protokol keamanan autentikasi Kerberos. Semua istilah mengacu pada semua komponen yang berada pada algoritma dan sistem dari protokol Kerberos. Berikut adalah karakteristik Kerberos yang sesuai dengan kerangka kerja yang telah dirancang:

1) Karena tidak perlu mengelola sistem autentikasi terpisah khusus untuk akses jaringan, penggunaan Kerberos sebagai sistem autentikasi untuk mengatur akses ke berbagai layanan aplikasi mengurangi beban administratif bagi institusi. Selain itu, pengguna juga mendapatkan manfaat dari sertifikasi jaringan yang terintegrasi, dan prosedur masuk ke Kerberos memungkinkan pengguna untuk masuk ke layanan aplikasi dengan menggunakan kredensial yang sama.

2) Karena Kerberos menggunakan enkripsi kunci simetris dan merupakan protokol yang ringan, ia lebih mudah untuk diimplementasikan dan dipelihara pada perangkat kecil dengan daya komputasi terbatas [10]. Menurut [3], proses autentikasi Kerberos akan diperlihatkan pada Gambar 1 sebagai berikut:



Gambar 1. Kerberos *Authentication Protocol Procedure*

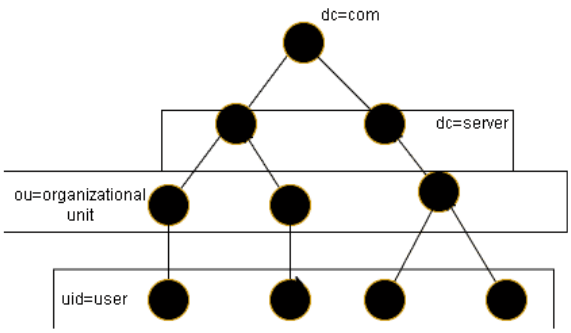
 ISSN:2302-8149
e-ISSN:2540-9719

Tahap-tahap autentikasi Kerberos:

1. *Client* harus menggunakan layanan berbasis server. Sebagai hasilnya, *client* akan menghubungi *Authentication Server* (AS) dengan permintaan. Identitas *client* dienkripsi dengan kata sandi mereka dalam permintaan ini.
2. Setelah meninjau permintaan, AS akan memberikan balasan kepada *client* berupa *Ticket Granting Ticket* (TGT) yang telah dienkripsi menggunakan kunci rahasia yang telah disediakan oleh AS.
3. TGT ini dienkripsi dengan kunci rahasia TGS dan dikirimkan oleh *client* ke TGS. Jika autentikasi *client* berhasil, TGS bertugas untuk memberikan *Service Access Ticket* (SAT).
4. TGS menghasilkan tiket SAT dan membalas kepada *client*. Tiket ini dienskripsi dengan kunci rahasia yang disediakan oleh AS.
5. *Client* mengirimkan tiket SAT dan membalas kepada *client*. Tiket ini dienkripsi dengan kunci rahasia yang disediakan oleh AS.
6. *Client* mengirimkan tiket SAT ke server yang dienskripsi dengan kunci rahasia server.
7. Sebagai balasan, server memberikan izin kepada *client* untuk mengakses layanan yang dibutuhkan. Jawaban ini menunjukkan kepada *client* bahwa layanan server yang diminta oleh *client* telah diberikan.

D. Skema OpenLDAP

Universitas Michigan di Amerika Serikat mengembangkan LDAP *(Lightweight Directory Access Protocol*), sebuah direktori informasi baru dengan entri yang setara dengan catatan dalam tabel basis data relasional [11]. Sebuah entri adalah pengelompokan dari properti *Distinguished Name* (DN). Pengelolaan terpusat informasi dan sumber daya jaringan menjadi lebih sederhana dengan model pohon hierarkis, yang menyimpan informasi objek dalam direktori sebagai kesatuan yang terpadu. Karena direktori umumnya menyimpan data yang relatif statis dalam jumlah besar dan dirancang untuk dioptimalkan dalam pencarian, maka cocok untuk membaca dan mencari informasi pendaftaran dari sejumlah besar orang. Gambar 2 merupakan contoh sederhana dari hierarki LDAP dalam sebuah jaringan:



Gambar 2. Contoh Hierarki LDAP

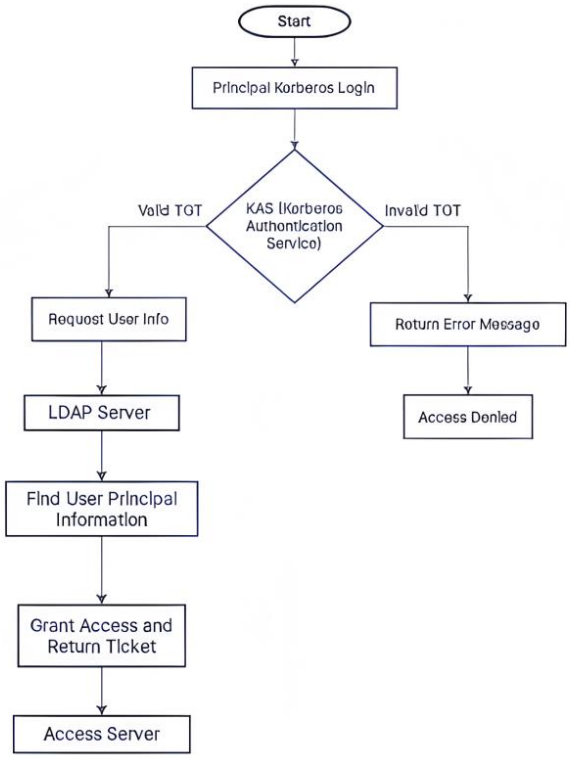
Pengguna dapat mengunjungi server LDAP untuk mendapatkan sertifikat orang lain karena server tersebut menyediakan layanan penjelajahan direktori dan layanan sistem basis data sertifikat digital dari server pusat registrasi ke server lainnya [11].

E. *Design* Pemodelan *Zero Trus*t pada Metode Autentikasi

1. *Framework Design*

Gambar 3 mengilustrasikan aturan yang menggambarkan alur langkah-langkah autentikasi dalam *framework* utama autentikasi pada sistem ini sehingga *client* dapat mengakses layanan SSH yang diminta.

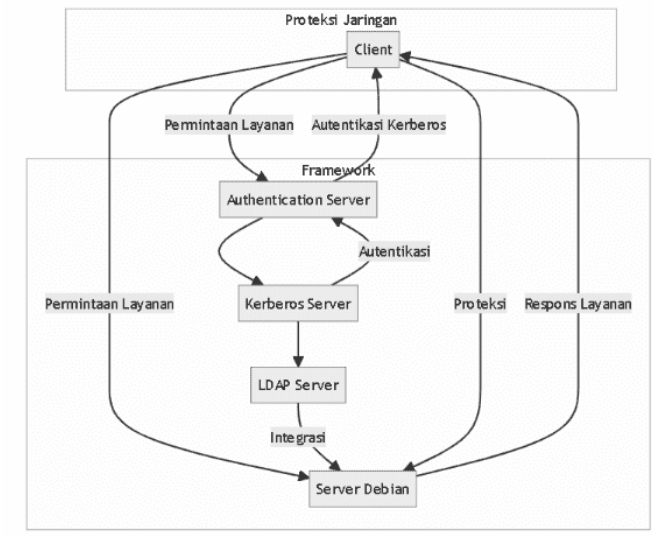
 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 3. *Design Framework* Autentikasi Keamanan

Berdasarkan Gambar 3 alur autentikasi Kerberos dimulai dengan Prinsipal Kerberos melakukan login ke sistem dengan mengirimkan permintaan *Ticket Granting Ticket* (TGT) ke *Key Distribution Center* (KDC) untuk otentikasi. KAS (*Kerberos Authentication Service*) memproses permintaan TGT dan jika berhasil, Prinsipal Kerberos dapat mengakses layanan pada server Debian. Jika TGT tidak berhasil diterbitkan, autentikasi berakhir. Selanjutnya, TGT dikirim ke layanan LDAP untuk otorisasi dan informasi tambahan tentang Prinsipal. KAS mengenkripsi informasi Prinsipal dan mengirimkan *user ticket*. Prinsipal Kerberos menggunakan *user ticket* ini untuk mengakses layanan pada server Debian. Alur ini memperlihatkan keamanan dan akses yang kuat bagi Prinsipal dengan integrasi Kerberos dan LDAP pada server Debian.

2. Prosedur Authentikasi & Permintaan Layanan



Gambar 4. Proses Autentikasi

 ISSN:2302-8149
e-ISSN:2540-9719

Alur Autentikasi pada Gambar 4 akan dijelaskan sebagai berikut:
(1) *Client* mengirim permintaan layanan ke *Authentication Server* (AS).
(2) AS menggunakan protokol Kerberos utuk melakukan autentikasi terhadap *client*.
(4) *Client* menggunakan token Kerberos untuk melakukan permintaan layanan ke Server Debian.
(5) Server Debian menerima permintaan layanan dari *client* dan menggunakan *framework* model untuk memvalidasi token Kerberos melalui integrasi dengan OpenLDAP sebagai *backend*.
(6) Jika token Kerberos valid, server Debian memberikan respons layanan kepada *client*.

F. Konfigurasi dan Pengaturan yang Diperlukan

Pada tahap ini, konfigurasi dan pengaturan penting dilakukan untuk mempersiapkan lingkungan yang sesuai dengan penerapan model keamanan *Zero Trust*. Ini melibatkan instalasi dan konfigurasi Kerberos, konfigurasi OpenLDAP, integrasi *protocol* OpenLDAP sebagai *backend protocol* Kerberos untuk menghubungkan *user entries* OpenLDAP dan *user principal* Kerberos, mengatur server Debian 11, serta memodifikasi *protocol* SSH.

G. Implementasi Model

Tahap ini melibatkan penerapan model keamanan dengan mengikuti prosedur yang telah dibuat sebelumnya. Ini mencakup mengatur integrasi *protocol* SSH dengan Kerberos dan OpenLDAP, serta autentikasi satu kali masuk (*single sign-on*), otorisasi akses, dan penerapan konsep *Zero Trust* pada infrastruktur SSH.

H. Uji Coba VAPT (*Vulnerability Assessment and Penetration Testing*)

Tahap ini melibatkan penerapan metodologi *Vulnerability Assessment and Penetration Testing* (VAPT) untuk menguji 988ystem keamanan. Dalam pengujian ini, kerentanan 988ystem diidentifikasi, pengujian penetrasi dilakukan untuk melihat sejauh mana pengguna yang tidak berwenang dapat masuk ke dalam 988ystem, dan evaluasi dilakukan untuk melihat seberapa aman sistem setelah model keamanan *Zero Trust* diimplementasikan.

I. Pengumpulan Data dan Analisis Hasil Uji Coba

Hasil dari pengujian VAPT digunakan untuk mengumpulkan data pada tahap ini. Setelah menerapkan model keamanan *Zero Trust* yang dimaksud dalam lingkungan jaringan server, data yang terkumpul menunjukkan penurunan jumlah serangan brute force, pencurian kredensial, atau masalah keamanan lainnya. Efektivitas dan keberhasilan penerapan model *Zero Trust* dengan protokol autentikasi Kerberos dan OpenLDAP dievaluasi melalui analisis data ini.

4 Hasil dan Pembahasan

Pada bagian ini Hasil dan Pembahasan akan disajikan semua data hasil dari implementasi dan percobaan yang telah dilakukan terhadap system server yang telah mengadopsi model *Framework Zero Trust*. Hasil implementasi dan uji coba ini selanjutkan akan dianalis untuk menguji keefektifan dari model *framework* keamanan system server.

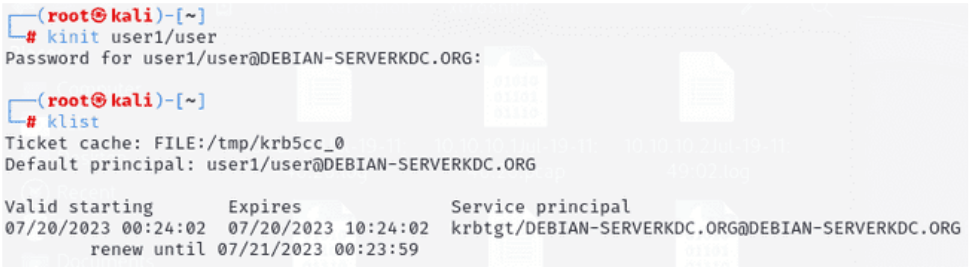
4.1 Pengujian Penerapan Model pada *Client*

Pada bagian ini akan disajikan hasil atau *output* keberhasilan pengimplementasian model *Framework Zero Trust* pada lingkungan jaringan. *Host* yang terhubung di semua lingkungan jaringan akan mengirimkan permintaan tiket Kerberos melalui *principal* yang sah ke server Kerberos untuk mengakses layanan SSH.

4.1.1 Permintaan *Ticket* Kerberos

Dengan membuat layanan pengguna Kerberos di sisi *client*, seperti *krb5-user* atau *krb5-workstation*, adalah mungkin untuk menguji implementasi sisi *client* dari model *Zero Trust*. Hal ini dilakukan untuk memungkinkan *client* meminta *Ticket Granting Ticket* (TGT) dari server *Key Distribution Centre* (KDC) yang berada di *Authentication Server* (AS) dalam lingkungan Debian. Gambar 5 adalah *client* yang berhasil meminta tiket Kerberos pada server Kerberos.

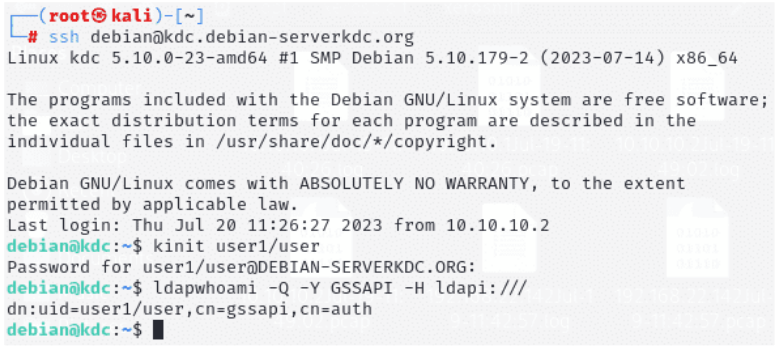
 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 5. Tiket *User* Tervalidasi

4.1.2 Permintaan Layanan SSH

Client harus menyebutkan *username* dan *host* dari pengguna yang akan diakses secara *remote* ketika meminta layanan SSH pada server *client* setelah mendapatkan tiket Kerberos yang valid yang telah dikonfirmasi oleh sistem AS.



Gambar 6. Permintaan Layanan SSH yang Berhasil

Untuk mengakses layanan SSH pada saat ini, *client* tidak akan diminta untuk memasukkan kata sandi dari *username* pengguna terkait seperti yang dapat dilihat pada Gambar 6. Selama tiket yang telah diberikan sebelumnya masih aktif, *client* tidak perlu melakukan autentikasi lagi setiap kali mereka ingin mengakses layanan SSH pada server. Hal ini karena sistem server sekarang mengenali *client* sebagai *client* yang sah. Dalam Kerberos, ini disebut sebagai sistem *Single Sign-On* (SSO). Apabila server tidak dapat memvalidasi tiket *client* untuk mengakses layanan. Maka dapat dipastikan autentikasi permintaan layanan akan ditolak oleh sistem server seperti yang ditunjukan oleh Gambar 7.

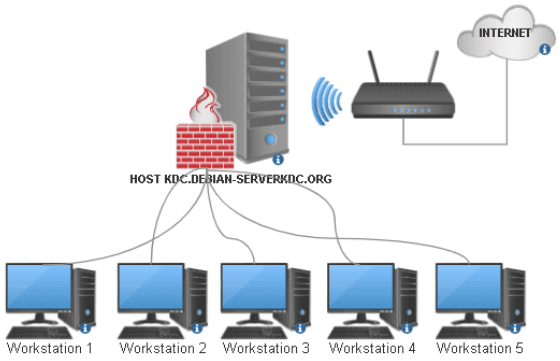
Gambar 7. Kegagalan Autentikasi

4.2 Pengujian Keberhasilan Autentikasi

Pengujian keberhasilan autentikasi dilakukan dengan skenario sebagai berikut:

(1) Terdapat 5 *client* aktif yang terhubung ke jaringan yang sama dengan server. Adapun design topologi akan digambarkan seperti pada Gambar 8.

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 8. Topologi Jaringan

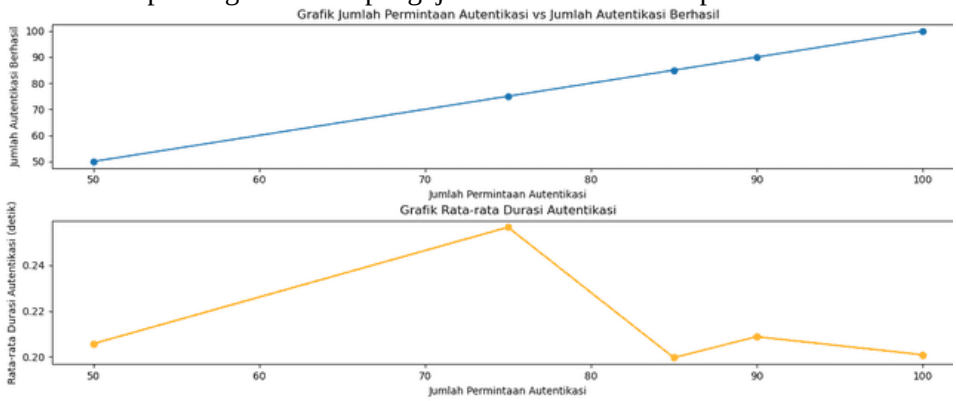
(2) *Client* masing-masing telah mendapatkan tiket Kerberos untuk permintaan layanan SSH.
(3) Jumlah permintaan yang dilakukan *client* akan tertera pada Tabel 3 beserta jumlah keberhasilan dan kegagalan permintaan yang ditangani oleh server.
(4) *Client* mengirimkan permintaan ke server dalam waktu *real-time* dan secara bersamaan.

Adapun hasil pengujian keberhasilan autentikasi dapat dilihat pada Tabel 3:

Tabel 3. Pengujian Keberhasilan Autentikasi

Client	User *principal* (@DEBIAN-SERVERKDC.ORG)	Jumlah permintaan autentikasi	Jumlah autentikasi berhasil	Jumlah autentikasi gagal	Total keberhasilan (%)	Durasi Rata-Rata
192.168.22.141/24	user2/user	50	50	0	100%	0.213s
192.168.22.142/24	user1/user	75	75	0	100%	0.225s
192.168.22.143/24	user2/user	85	85	0	100%	0.256s
192.168.22.144/24	user2/user	90	90	0	100%	0.215s
192.168.22.145/24	user1/user	100	100	0	100%	0209s

Gambar 9 merupakan grafik hasil pengujian berdasarkan hasil pada Tabel 3:



Gambar 9. Grafik Hasil Pengujian Autentikasi

Hasil pengujian keberhasilan autentikasi pada berbagai *client* yang masuk ke server ditampilkan dalam Tabel 3 Keberhasilan Autentikasi dan Gambar 9 merupakan gambaran Grafik Hasil Pengujian Autentikasi yang telah dilakukan. Terdapat lima *client* dalam tabel ini, masing-masing memiliki *user principal* yang unik. Setiap *client* melakukan sejumlah permintaan autentikasi SSH, dan hasil dari setiap percobaan dicatat untuk studi lebih lanjut.

Hasil pengujian menunjukkan bahwa semua *client* berhasil dalam menjalin koneksi autentikasi dengan server. *Client* dengan alamat IP 192.168.22.141/24 dan *user principal* user2/user melakukan 50 permintaan autentikasi, dan semuanya disetujui tanpa ada percobaan yang tidak berhasil. Pola keberhasilan serupa juga terlihat pada *client* lainnya, termasuk *client* dengan *user principal* user1/user dan alamat IP 192.168.22.142/24, yang berhasil menyelesaikan 75 permintaan autentikasi dengan sukses.

 ISSN:2302-8149
e-ISSN:2540-9719

Keberhasilan 100% dalam autentikasi server juga diraih oleh *client-client* lain, termasuk 192.168.22.143/24 dengan *user principal* user2/user, 192.168.22.144/24 dengan *user principal* user2/user, dan 192.168.22.145/24 dengan *user principal* user1/user. Tidak ada upaya yang gagal dalam autentikasi oleh kelima *client* tersebut.Hasil ini menunjukkan bahwa implementasi model *Zero Trust* dengan menggunakan Kerberos dan OpenLDAP sebagai *backend* autentikasi pada server SSH telah memberikan tingkat keberhasilan autentikasi yang sangat baik. Keberhasilan autentikasi mencapai 100% untuk semua client yang diuji, menandakan bahwa konfigurasi keamanan yang diterapkan telah efektif dalam melindungi server dari percobaan autentikasi yang tidak sah.

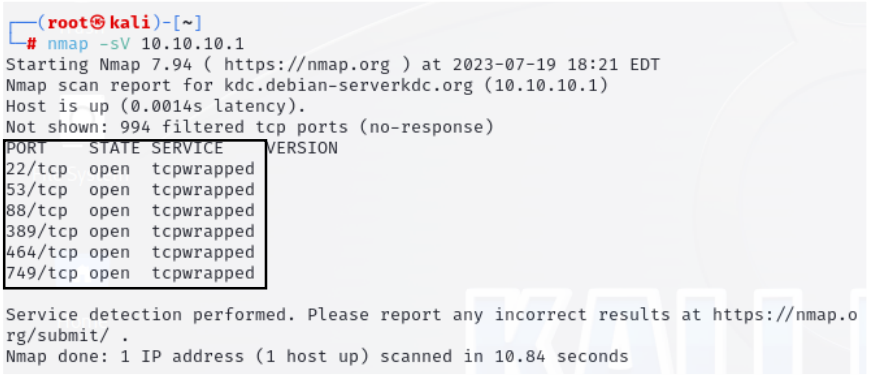
Dalam skenario pengujian ini, penerapan model *Zero Trust* telah menunjukkan bahwa menggunakan Kerberos dan OpenLDAP sebagai sistem autentikasi bersama-sama dapat memberikan tingkat keamanan yang tinggi. Tanpa adanya upaya autentikasi yang tidak berhasil, semua *client* dapat mengakses server secara sah dan berhasil. Temuan ini memberikan keyakinan bahwa model *Zero Trust* dengan autentikasi berbasis Kerberos dan OpenLDAP dapat menjadi pilihan yang andal untuk melindungi layanan autentikasi pada sistem server SSH.

4.3 Evaluasi Eksploitasi dan Keamanan Framework

Pada bagian ini akan disajikan hasil dan analisis terhadap pengujian yang telah dilakukan pada *system* server yang telah mengadopsi model *Framework Zero Trust* sebagai system keamanan server.

4.3.1 *Vulnerability Assessment Nmap* (*Network Mapper*)

Dengan menggunakan program Nmap di lingkungan Kali-Linux, pengujian kerentanan dilakukan dengan menemukan dan mengevaluasi potensi kerentanan dan kelemahan keamanan dalam sistem atau jaringan. Pada *host* 10.10.10.1/29, Nmap dapat diamati melakukan pemindaian jaringan dan pemetaan *port*. Dalam contoh ini, jaringan internal dan eksternal server dapat mengakses *port* 22/tcp, yang digunakan oleh protokol SSH dan ditampilkan sebagai terbuka (*open*) seperti yang bisa dilihat pada Gambar 10.

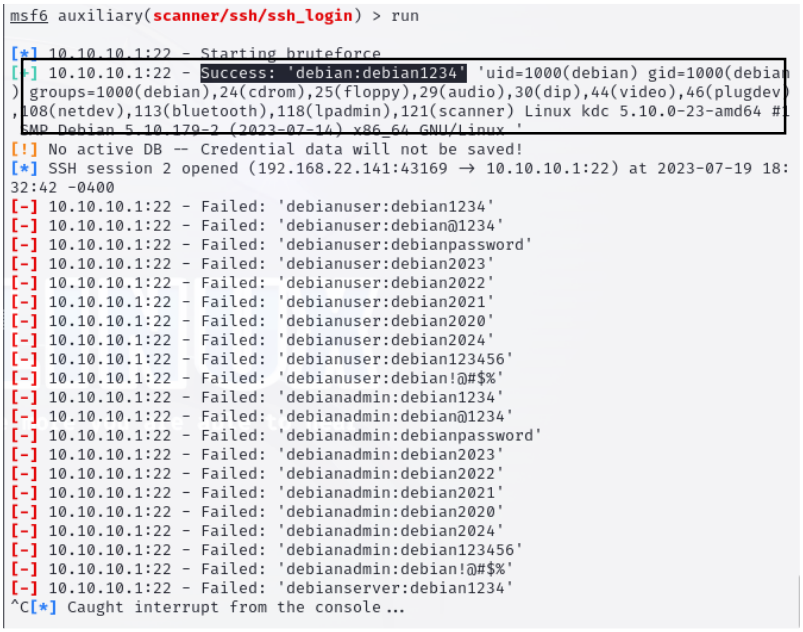


Gambar 10. *Vulnerability Assessment Nmap*

4.3.2 *Brute-Force Attack & Dictionary Attack Exploitation*

Pengujian keamanan autentikasi menggunakan metodologi *Brute-Force* Attack dan *Dictionary Attack Exploitation*. Dalam kasus ini, seorang peretas membuat dan memperoleh daftar kata kemungkinan untuk nama pengguna (*username*) dan kata sandi (*password*) untuk autentikasi SSH. Jika nama pengguna dan kata sandi korban ditemukan dalam daftar tersebut, skenario terburuk adalah peretas dapat menggunakannya untuk meminta layanan SSH pada server, meningkatkan akses pengguna, dan mendapatkan akses ke data apa pun yang ada di direktori aktif dari *host* server. Pendekatan-pendekatan yang paling umum digunakan oleh peretas untuk jenis eksploitasi ini adalah Metasploit, Hydra, dan Nmap, yang digunakan dalam pengujian. Gambar 11 menampilkan hasil eksploitasi sebelum menerapkan Model *Zero Trust* dalam lingkungan server.

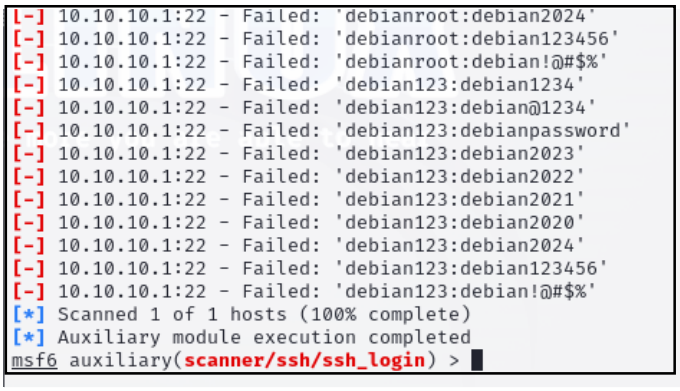
 ISSN:2302-8149
e-ISSN:2540-9719



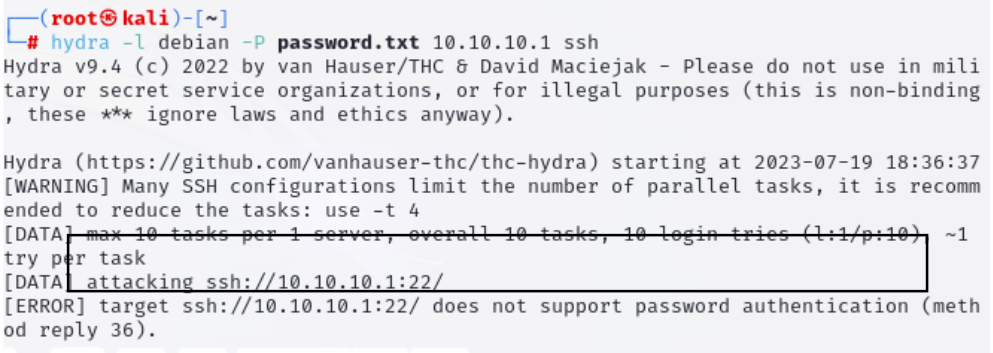
Gambar 11. *Brute-Force* Sebelum Model *Zero Trust* Diimplementasikan

Berdasarkan hasil yang ditunjukkan pada Gambar 11, peretas berhasil mencocokkan dengan tepat semua *username* dan *password* yang diprediksi dari pengguna target. *Username* yang diperoleh dalam kasus ini adalah "**debian**" dan *password* pengguna adalah "**debian1234**". Yang mengindikasikan penggunaan *password-based authentication* sebagai metode autentikasi sangat rentan terhadap serangan *password guessing* dengan metode *brute-forced attack*.

Sedangkan untuk hasil eksploitasi pada s*ystem* server yang telah diimplementasikan model *framework* dapat dilihat pada Gambar 12 melalui tiga metode uji coba eksploitasi *password guessing*.



(a)



(b)

 ISSN:2302-8149
e-ISSN:2540-9719

```
┌──(root㉿kali)-[~]
└─# nmap 10.10.10.1 -p 22 --script ssh-brute --script-args userdb=username.txt,passdb=password.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 18:39 EDT
Nmap scan report for kdc.debian-serverkdc.org (10.10.10.1)
Host is up (0.00092s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_ssh-brute: Password authentication not allowed

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

(c)

Gambar 12. (a) Metasploit *Brute-Force* Gagal; (b) Hydra *Brute-Force* Gagal; (c) *Brute-Force/Dictionary Attack* Gagal

Berdasarkan *output* dari Gambar 12 telah dilakukan pada *host* KDC dengan alamat kdc.debian-serverkdc.org dengan menggunakan uji coba *brute force* dan *dictionary attack* menggunakan program seperti Metasploit, Hydra, dan Nmap. Uji coba ini bertujuan untuk menebak identitas SSH dan *password* yang akan digunakan oleh peretas untuk mengakses sistem.

Dengan menggunakan alat-alat peretasan tersebut, beberapa kombinasi login dan *password* diuji selama proses pengujian. Namun, menurut hasil uji coba, tidak ada dari upaya peretasan tersebut yang berhasil, dan keamanan sistem tidak dapat dikompromikan. Hasil ini menunjukkan bahwa model *Zero Trust* yang diterapkan pada sistem, yang menggunakan Kerberos dan OpenLDAP sebagai backend autentikasi, telah berhasil mencegah percobaan peretasan melalui brute force dan *dictionary attack*.

Model Zero Trust mendorong pendekatan yang ketat terhadap autentikasi dan otorisasi dalam hal keamanan. Dengan menerapkan model ini, sistem menuntut autentikasi yang kuat sebelum memberikan akses ke layanan atau sumber daya yang diinginkan. Selain itu, penggunaan OpenLDAP sebagai sistem direktori pusat memberikan manajemen pengguna dan otorisasi akses yang efektif, dan Kerberos sebagai protokol autentikasi tunggal memastikan bahwa hanya pengguna yang diizinkan yang dapat mengakses sistem.

Berdasarkan temuan dari penelitian ini, menerapkan model *Zero Trust* dengan Kerberos dan OpenLDAP telah menciptakan sistem yang aman dan dapat bertahan dari serangan *brute force* dan *dictionary*. Keberhasilan ini menunjukkan nilai dari strategi keamanan yang ketat untuk menjaga integritas dan kerahasiaan data pada sistem server.

4.3.3 *Man-in-the-Middle Attack* (MITM)

Ancaman keamanan yang terkait dengan proses autentikasi berbasis *username* dan *password* juga mencakup eksploitasi *Man-in-the-Middle* (MITM) selain risiko dari serangan *brute-force* dan *dictionary*. Sebuah serangan MITM dilakukan antara *host* 10.10.10.1/29 dan salah satu *host* aktif 192.168.1.142/24 untuk menunjukkan bahwa koneksi antara *client* dan server terintegrasi dengan benar dan aman terenkripsi. Hasil dari eksploitasi MITM setelah lingkungan server mengimplementasikan Model *Zero Trust* ditampilkan dalam Gambar 13.

1	0.000000	192.168.22.142	10.10.10.1	SSH	90 Client: Encrypted packet (len=36)
6	0.000000	10.10.10.1	192.168.22.142	SSH	90 Server: Encrypted packet (len=36)
15	1.000000	192.168.22.142	10.10.10.1	SSH	90 Client: Encrypted packet (len=36)
28	1.000000	10.10.10.1	192.168.22.142	SSH	106 Server: Encrypted packet (len=52)
45	2.000000	10.10.10.1	192.168.22.142	SSH	130 Server: Encrypted packet (len=76)
66	2.000000	10.10.10.1	192.168.22.142	SSH	154 Server: Encrypted packet (len=100)
91	3.000000	192.168.22.142	10.10.10.1	SSH	90 Client: Encrypted packet (len=36)
120	3.000000	10.10.10.1	192.168.22.142	SSH	90 Server: Encrypted packet (len=36)
153	4.000000	192.168.22.142	10.10.10.1	SSH	90 Client: Encrypted packet (len=36)
190	4.000000	10.10.10.1	192.168.22.142	SSH	90 Server: Encrypted packet (len=36)
231	5.000000	192.168.22.142	10.10.10.1	SSH	90 Client: Encrypted packet (len=36)
276	5.000000	10.10.10.1	192.168.22.142	SSH	90 Server: Encrypted packet (len=36)
325	5.000000	192.168.22.142	10.10.10.1	SSH	90 Client: Encrypted packet (len=36)

Gambar 13. Komunikasi Terenkripsi antar *Host*

Hasil dari percobaan ini seperti yang terlihat pada Gambar 13 menunjukkan bahwa serangan MITM oleh Xerosploit berhasil dicegah oleh model *Zero Trust* dengan penerapan Kerberos dan OpenLDAP. Setiap koneksi antara *host* dan *client* harus melewati prosedur autentikasi yang kuat sesuai dengan kontrol keamanan ketat yang ada dalam model *Zero Trust*. Selain itu, penggunaan Kerberos sebagai protokol autentikasi tunggal memastikan kerahasiaan dan keamanan komunikasi

 ISSN:2302-8149
e-ISSN:2540-9719

antar *host*. Temuan dari investigasi ini menunjukkan bahwa sistem server yang menggunakan model *Zero Trust* mampu bertahan dari serangan MITM berbahaya. Penggunaan Kerberos dan OpenLDAP sebagai elemen penting dalam model keamanan ini telah membuktikan keefektifannya dalam menggagalkan upaya peretasan dan menjaga integritas sistem.

5 Kesimpulan

Berdasarkan hasil pengujian dan analisis, dapat dikatakan bahwa integrasi model *Zero Trust* dengan Kerberos dan OpenLDAP pada sistem server Debian 11 telah berhasil meningkatkan tingkat keamanan dan melindunginya dari berbagai serangan, seperti serangan *brute-force*, *dictionary attack*, dan potensi serangan *man-in-the-middle* (MITM). Dengan mensyaratkan setiap *client* yang mencari layanan SSH untuk melewati prosedur autentikasi yang kuat melalui Kerberos, model *Zero Trust* dengan Kerberos dan OpenLDAP berhasil melindungi proses autentikasi, seperti yang ditunjukkan oleh pengujian keberhasilan autentikasi pada *client*. Akibatnya, tidak ada kegagalan selama percobaan autentikasi. Hal ini menunjukkan bahwa penggunaan strategi keamanan ini secara efektif mencegah upaya menebak *username* dan *password* SSH melalui serangan *brute force* dan dictionary. Pengujian keberhasilan autentikasi pada server juga menghasilkan temuan yang memadai. Autentikasi server dilakukan dalam setiap interval waktu yang ditentukan tanpa ada kesalahan. Telah terbukti bahwa arsitektur *Zero Trust* dengan Kerberos dan OpenLDAP melindungi server dari berbagai serangan yang dapat menyebabkan kebocoran data dan kerusakan infrastruktur. Penggunaan Xerosploit dalam eksperimen man-in-the-middle (MITM) menunjukkan seberapa efektifnya model *Zero Trust* dalam melindungi sistem dari serangan MITM yang berbahaya. Pengendalian keamanan yang ketat, autentikasi tunggal menggunakan Kerberos, dan penggunaan OpenLDAP sebagai sistem direktori pusat telah berhasil menggagalkan upaya peretasan dan menjamin kerahasiaan dan integritas komunikasi antar host. Secara keseluruhan, sistem server telah terlindungi dengan baik dari berbagai serangan, seperti serangan *brute-force*, *dictionary attack*, dan serangan *man-in-the-middle*, berkat integrasi Kerberos dan OpenLDAP dalam model *Zero Trust*. Pendekatan ini memberikan keyakinan bagi pengguna sistem bahwa data dan informasi mereka akan aman dan terlindungi dengan menerapkan langkah-langkah keamanan yang ketat dan menghilangkan asumsi kepercayaan dalam jaringan internal. Konsep *Zero Trust* berhasil menjaga keamanan dan integritas sistem server dalam menghadapi berbagai tantangan keamanan siber yang terus berkembang.

Referensi

[1] Tohirin, "Penerapan Keamanan *Remote Server* melalui SSH dengan Kombinasi Kriptografi Asimetris dan Autentikasi Dua Langkah Tohirin Program Studi Pascasarana Sistem Informasi, STIMK LIKMI," *Jurnal Teknologi Informasi*, vol. 4, no. 1, 2020.

[2] A. W. Wastumirad and M. I. Darmawan, "Implementasi *Honeypot* menggunakan Dionaea dan Kippo sebagai Penunjang Keamanan Jaringan Komunikasi Komputer," *J Teknol*, vol. 9, no. 1, pp. 80–91, Nov. 2021, doi: 10.31479/jtek.v9i1.119.

[3] H. Mutaher and P. Kumar, "*Security-enhanced SDN controller based kerberos authentication protocol*," in *Proceedings of the Confluence 2021: 11th International Conference on Cloud Computing, Data Science and Engineering*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 672–677. doi: 10.1109/Confluence51648.2021.9377044.

[4] H. Li, Y. Niu, J. Yi, and H. Li, "*Securing offline delivery services by using kerberos authentication*," *IEEE Access*, vol. 6, pp. 40735–40746, Jul. 2018, doi: 10.1109/ACCESS.2018.2856904.

[5] Yi M, Hongyun N, "*The Improvement of Wireless LAN Security Authentication Mechanism Based on Kerberos*," Sichuan Institute of Electronics and Institute of Electrical and Electronics Engineers, *2018 International Conference on Electronics Technology (ICET) : May 23 -May 27,2018, Chengdu, China*.

 ISSN:2302-8149
e-ISSN:2540-9719

[6] Y. Yang, H. Li, X. Cheng, X. Yang, and Y. Huo, "*A High Security Signature Algorithm Based on Kerberos for REST-style Cloud Storage Service*," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 0176–0182. doi: 10.1109/UEMCON51285.2020.9298140.

[7] H. Arabnia, L. Deligiannidis, M. Q. Yang, "*Synopsis of Security: Using Kerberos Method to Secure File Transfer Sessions*," American Council on Science and Education, IEEE Computer Society, and Institute of Electrical and Electronics Engineers., *2016 International Conference on Computational Science and Computational Intelligence : CSCI 2016 : proceedings : 15-17 December 2016, Las Vegas, Nevada, USA*.

[8] M. C. Rao, "*A Fixed Network Transmission Based on Kerberos Authentication Protocol*." [Online]. Available: www.ijert.org

[9] P. K. Shukla, G. S. Mishra, P. G. Shambharkar, P. Rusia, and V. Kapoor, "*Implementation comparison of Kerberos passwords by RC-5 encryption type analysis with RC-4 encryption*," in *ITNG 2009 - 6th International Conference on Information Technology: New Generations*, 2009, pp. 1581–1582. doi: 10.1109/ITNG.2009.304.

[10] L. Ning L, W. Qing W, and D. Zhongliang, "*Authentication Framework Of Iiedns Based On Ldap & Kerberos*," *Proceedings IC-BNMT : 2010 3rd IEEE International Conference on Broadband Network & Multimedia Technology : October 26-28, Beijing, China*. IEEE Press, 2010.

[11] Z. Wang and Y. Wang, "*Research and design of campus network unified identity authentication system based on Kerberos*," in *Advanced Materials Research*, 2012, pp. 1086–1089. doi: 10.4028/www.scientific.net/AMR.546-547.1086.