BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berkembangnya internet, banyak instansi kantor ataupun perusahaan yang menggunakan internet untuk memperlancar arus komunikasi informasi di dalamnya. Data-data perusahaan merupakan informasi yang bersifat rahasia dan harus dijaga keamanannya. Di sisi lain, mudahnya akses untuk mendapat informasi tersebut menyebabkan munculnya masalah baru yaitu dapat di manfaatkan informasi atau data penting oleh pihak yang tidak bertanggung jawab demi kepentingannya sendiri. Ancaman dalam dunia teknologi merupakan hal yang lazim dihadap. Pengamanan perlu dilakukan pada semua lini, tidak hanya pengamanan pada sisi perimeter atau sisi pembatas dengan dunia luar dengan menggunakan firewall, namun juga pada sisi endpoint (perangkat pengguna). Terkait dengan pengamanan tersebut, pada beberapa industri diciptakan standar kepatuhan (*compliance*) untuk menyeragamkan standar keamanan yang harus dipenuhi oleh perusahaan. Misalnya compliance khusus industri keuangan, compliance khusus industri kesehatan, hingga compliance yang dibuat oleh pemerintah untuk menjaga keamanan data pengguna yang berlaku multi sektor (Patricia, 2021).

Compliance (kepatuhan) merupakan standar yang wajib dipenuhi sebuah perusahaan, standar ini terkait dengan industry dimana bisnis perusahaan

bergerak. Standar kepatuhan ini selain membantu dalam pengelolaan resiko ia juga akan berpengaruh kepada kredibilitas perusahaan. File *Integrity Monitoring* (FIM) merupakan salah satu standar kepatuhan yang harus dipenuhi dalam beberapa standar industri. Salah satunya adalah standar kepatuhan dalam dunia pemerintahan yang biasa dikenal dengan PCI DSS. *File Integrity Monitoring* (FIM) merupakan aktifitas memonitor integritas sebuah file untuk menjaga keutuhan suatu file dari perubahan yang tidak terotorisasi, yang merupakan indikasi adanya ancaman. Pada penulisan ini implementasi File *Integrity Monitoring* (FIM) akan dilakukan menggunakan aplikasi Wazuh. Salah satu aplikasi *open source* yang cukup dikenal dalam perlindungan keamanan di endpoint (Harahap & Hutrianto, 2021).

Seorang penyerang akan menyerang sistem jaringan dengan maksud guna mengalahkan layanan keamanan pada fasilitas jaringan tersebut. Dengan mempertimbangkan fakta bahwa jaringan public pada awalnya dirancang untuk keterbukaan tanpa mempertimbangkan keamanan, jelas diikuti meningkatnya pula serangan *cybercriminals* dari tahun ketahuan. Untuk itu perlu sekali dilakukan monitoring server guna memastikan data-data penting yang dianggap rahasia tetap aman dan tidak tidak dirusak maupun dicuri oleh penjahat siber. Maka diperlukan sebuah tools yang dapat memantau perkembangan yang terjadi dalam sebuah server. Dimana akan ada sebuah server yang bertugas melakukan monitoring terhadap suatu server dengan teknologi cloud computing. *Cluod computing* sendiri sangat tergantung pada teknologi virtualisasi, yaitu konsep pembuatan versi virtual dari sesuatu yang bersifat fisik, misalnya sistem operasi, perangkat storage

atau penyimpanan data atau sumber daya jaringan. Web server seringkali menjadi target dari berbagai jenis serangan baik yang sifatnya minor maupun major sehingga berakibat fatal. Akan tetapi, adakalanya website dijadikan pintu oleh peretas (*hacker*) untuk menembus web server. Salah satu contoh eksploitasi pada web server yang sering terjadi adalah serangan DoS .Teknologi virtualisasi ini juga memiliki tujuan untuk memaksimalkan kinerja server serta menghindari pemborosan. Salah satu *tools* yang digunakan untuk monitoring adalah Wazuh (Fitri Nova et al., 2022).

Wazuh merupakan perangkat berbasis *Open Source* yang berfungsi sebagai sistem deteksi intrusi berbasis host *(endpoint).* Wazuh melakukan analisis log, pemeriksaan integritas, pemantauan registri Windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif. Wazuh merupakan perangkat yang menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau host pada sistem operasi dan juga pada tingkat aplikasi (Sandra, 2020).

Beberapa penelitian dilakukan, seperti terkait implementasi remote site pada *virtual private network* berbasis mikrotik. Penelitian tersebut berfokus pada permasalahan yaitu penggunaan email dan pertukaran data melalui flashdisk cenderung lemah dalam mengantisipasi keamanan jaringan. Metode yang digunakan pada penelitian tersebut menggunakan *Virtual Private Network* yang merupakan teknik pengamanan jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet, teknologi ini menggunakan protokol *Point to Point*

Tunneling Protocol (PPTP) dengan cara remote site yang dapat menyediakan sarana transfer data dan jaringan yang lebih aman. Hasil dari penelitian tersebut adalah jaringan VPN walaupun mempunyai packet loss lebih banyak namun mempunyai round trip yang kecil dan dapat mendownload data lebih cepat serta terbukti lebih aman. Virtual Private Network (VPN) merupakan salah satu cara untuk melindungi pertukaran data informasi melalui Jaringan internet, khususnya dengan menggunakan Protokol Secure Socket *Tunneling Protokol* (SSTP) dapat membuat komunikasi antar beberapa Jaringan melalui sebuah *Tunneling* yang melewati Jaringan internet dengan aman (Prayogi Wicaksana et al., 2021).

Berdasarkan laporan keamanan diperoleh hasil penelitian mengenai pertahanan ancaman keamanan yang digunakan oleh organisasi bahwa tingkat pertahanan keamanan di perusahaan atau organisasi di dunia meningkat dari tahun 2014 ke tahun 2015 pada bidang *Encryption/Privacy/Data Protection*, *Authentication dan Data Loss Prevention*. Didasari kepada kesadaran para profesional IT *security* akan rentannya keamanan pada bidang tersebut seperti terjadi serangan-serangan dan pencurian data pribadi pada perusahaan maupun organisasi yang bersifat penting. Penelitian ini berfokus pada masalah kebutuhan akan keamanan data yang baik tetapi tidak mengurangi kecepatan terhadap akses data tersebut. Berdasarkan observasi yang telah dilakukan, sudah menggunakan *Virtual Private Network* dengan teknologi PPTP, tetapi teknologi sudah ditinggal pergi oleh Microsoft. Sedangkan kebutuhan akan keamanan data, tetapi cepat dalam transfer data diperlukan. Dari hasil pengamatan di tempat penelitian diperoleh akar masalahnya yaitu tidak semua produk jaringan support terhadap

teknologi V*irtual Private Network*. Pengambilan file / data tidak bisa dilakukan secara realtime dalam ruang tertentu. Kurangnya tenaga IT yang menguasai tentang Networking Security. Berdasarkan deskripsi diatas, penulis akan melakukan penelitian dengan judul : "**PERANCANGAN DAN IMPLEMENTASI TEKNOLOGI SISTEM MONITORING MENGGUNAKAN WAZUH 4.0 DAN METODE VIRTUAL PRIVATE NETWORK (VPN) L2TP UNTUK PENINGKATAN KEAMANAN SERVER DALAM PELAYANAN PUBLIK PADA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA PADANG**".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana layanan Dinas Kependudukan Dan Pencatatan Sipil bias diakses layanan luar?
2. Bagaimana mengatasi jaringan pada Dinas Kependudukan Dan Pencatatan Sipil Kota Padang dapat lebih stabil?
3. Bagaimana cara mengatasi permasalahan jaringan yang sering terputus koneksi sehingga dapat berefek kepada kinerja karyawan?

1.3 Hipotesis

Hipotesa merupakan jawaban ataupun dugaan sementara terhadap latar belakang dan rumusan masalah yang ada. Pada sub bab ini penulis menguraikan dugaan sementara yang didapat sebagai berikut:

1. Diharapkan dengan menggunakan monitoring Wazuh 4.0 dapat memberikan kemudahan kepada pihak IT dalam proses monitoring website dan pengontrolan jaringan pada dinas kependudukan dan pencatatan sipil kota padang.
2. Diharapkan dengan VPN dapat memberikan peningkatan keamanan jaringan pada Dinas Kependudukan Dan Pencatatan Sipil Kota Padang sehingga tidak ada lagi masalah pemblokiran jaringan oleh orang yang tidak bertanggung jawab.
3. Diharapkan dengan menggunakan monitoring wazuh dan VPN dapat memberikan kemudahan kepada pihak capil dalam mengakses informasi lebih cepat dan lebih banyak dalam proses penggunaan jaringan, sehingga mengurangi terjadinya masalah koneksi terputus.

1.4 Batasan Masalah

Adapun batasan-batasan masalah yang terdapat dalam penelitian ini yaitu:

1. Penelitian ini hanya membahas bagaimana proses monitoring jaringan pada dinas kependudukan dan pencatatan sipil kota padang dengan menggunakan aplikasi wazuh 4.0.
2. Menggunakan VPN untuk proses peningkatan keamanan jaringan.

1.5 Tujuan Penelitian

Adapun tujuan penelitian yang dilakukan yang dilakukan penulis berdasarkan latar belakang masalah yang telah diuraikan diatas diantaranya yaitu:

1. Mengusulkan proses monitoring yang baik sehingga tidak ada lagi masalah peretasan jaringan yang terjadi pada dinas kependudukan dan pencatatan sipil kota padang.
2. Meningkatkan keamanan jaringan dengan menggunakan VPN sebagai alat bantu dalam proses keamanan jaringan.
3. Memberikan kemudahan kepada pihak Capil Kota Padang dalam mengatasi permasalahan ketidakstabilan jaringan pada kantor.

1.6 Manfaat Penelitian

Adapun manfaat penelitian yang dilakukan penulis sebagai berikut:

1. Bagi pengguna dapat memudahkan dalam bertukar informasi dan transformasi data.
2. Bagi penulis mendapatkan tambahan ilmu dalam merancang jaringan dan keamanan jaringan pada Dinas Kependudukan Dan Pencatatan Sipil Kota Padang.
3. Bagi Instansi dapat memberikan wawasan baru dan manfaat untuk membantu proses keamanan jaringan dan dapat memberikan kemudahan dalam permasalahan jaringan.