BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi yang pesat telah menjadikan jaringan komputer sebagai kebutuhan utama dalam berbagai aspek kehidupan, seperti pendidikan, pekerjaan, hingga hiburan. Semakin tingginya ketergantungan terhadap jaringan komputer juga menyebabkan meningkatnya lalu lintas data yang melintasi berbagai sistem dan perangkat. Kondisi ini membuka lebih banyak peluang bagi pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan kejahatan siber. Menurut laporan dari Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2019 terdapat lebih dari 290 juta serangan siber yang terdeteksi di Indonesia. Ancaman siber tidak hanya semakin banyak, tetapi juga semakin kompleks dan canggih. Bahkan negara maju seperti Amerika Serikat pun mengalami kerugian besar akibat serangan siber, sebagaimana dilaporkan oleh *Federal Bureau of Investigation* (FBI) yang mencatat kerugian hingga 3,5 miliar dolar pada tahun yang sama. Oleh karena itu, kebutuhan akan sistem keamanan jaringan yang tangguh menjadi semakin mendesak, khususnya pada sisi server yang rentan terhadap berbagai jenis serangan seperti *Denial of Service* dan *Brute Force* (Mardiansyah et al., 2021).

Pada penelitian yang dilakukan oleh Fadhlirrahman Baso dan Muhammad Ardiansyah yang berjudul Implementasi Metode *Port Knocking* pada *MikroTik RouterOS* untuk Mendukung Keamanan Jaringan. Menjelaskan bahwa keamanan jaringan menjadi aspek vital untuk mencegah akses tidak sah ke layanan kritis,

salah satunya melalui implementasi *Port Knocking*, metode yang menutup *port* tertentu dan hanya membukanya setelah urutan ketukan (*knock sequence*) yang telah ditentukan dilakukan. Penelitian ini menguji implementasi *Port Knocking* pada *MikroTik RouterOS* untuk mengamankan port layanan seperti Winbox (8291) dan *World Wide Web* (80), di mana hasilnya menunjukkan bahwa metode ini berhasil memblokir akses *ping* dan *remote* kecuali bagi pengguna yang telah melakukan autentikasi dengan urutan ketukan yang benar (misal: port 2001, 2002, 2003). Dengan demikian, *Port Knocking* tidak hanya meningkatkan keamanan jaringan terhadap serangan *spoofing* atau *brute force* tetapi juga mempertahankan fleksibilitas akses bagi pengguna terotorisasi, menjadikannya solusi efektif untuk sistem berbasis *MikroTik* (Baso & Ardiansyah, 2023).

Pada penelitian yang dilakukan oleh Eka Putra F, Amir Hamzah, Agel W, dan Firmansyah Kusuma R pada tahun 2023. Dengan judul Implementasi Sistem Keamanan Jaringan *Mikrotik* Menggunakan *Firewall Filtering* dan *Port Knocking*. Menjelaskan bahwa keamanan jaringan menjadi isu krusial di era digital, terutama dengan meningkatnya serangan siber yang dapat mengancam sistem informasi. *Mikrotik*, sebagai salah satu perangkat jaringan yang banyak digunakan oleh berbagai instansi, memiliki berbagai fitur keamanan, namun tetap rentan terhadap serangan jika tidak dikonfigurasi dengan baik. Salah satu metode yang dapat diterapkan untuk meningkatkan keamanan jaringan *Mikrotik* adalah dengan menggunakan *Firewall Filtering* dan *Port Knocking*. *Firewall Filtering* berfungsi untuk memblokir akses pada port yang rentan terhadap serangan, sementara *Port Knocking* menambahkan lapisan keamanan dengan mewajibkan pengguna mengetuk *port* dalam urutan tertentu sebelum mendapatkan akses ke jaringan.

Penelitian tersebut bertujuan untuk mengimplementasikan kedua metode tersebut guna meningkatkan perlindungan jaringan terhadap ancaman seperti *Denial of Service* (DoS) dan eksploitasi *port* terbuka. Melalui pendekatan deskriptif dan analisis literatur, penelitian ini menunjukkan bahwa kombinasi *Firewall Filtering* dan *Port Knocking* mampu mengurangi risiko serangan dengan menyaring lalu lintas jaringan dan menyembunyikan akses *port* dari pihak yang tidak berwenang (Eka Putra et al., 2024).

Pada penelitian yang dilakukan oleh Zai D, dan Suharsono T dengan judul Penggunaan Metode *Port Knocking*, *Port Blocking*, dan *ARP* Untuk Melaksanakan Keamanan Jaringan *router MikrotikOS* pada tahun 2023. Menjelaskan bahwa perkembangan teknologi sampai saat ini terus berkembang. Perkembangan tersebut berdampak pada keamanan sistem yang ada di dalamnya. Sehingga Organisasi menjadi lebih rentan terhadap ancaman atau serangan jaringan atau keamanan informasi yang disebabkan oleh berbagai sumber baik dari aktivitas personil internal atau serangan peretas. Oleh karena itu, pada penelitian ini akan melakukan pengamanan pada *router mikrotik* dengan menggunakan metode *port knocking*, *port blocking* dan *ARP* yang merupakan sebuah program khusus yang dibuat pada keamanan jaringan *mikrotik router os*, pada penelitian ini bertujuan untuk membuat sebuah keamanan pada *router mikrotik* dalam sebuah jaringan dengan membuat 3 *rule Port knocking*, *Port blocking*, dan *ARP* dan membuat langkah - langkah pengetukan *port knocking* supaya hanya klien yang mengetahui kode otentikasi yang bisa mengakses *port service* tersebut. Berdasarkan penelitian tersebut dapat disimpulkan bahwa metode *port knocking*, *port blocking* dan *ARP* telah berhasil membuat sebuah keamanan jaringan dimana *port services* hanya bisa diakses oleh

pengguna yang ditentukan dengan melakukan beberapa langkah - langkah yang telah dibuat (Zai & Suharsono, 2023).

Pada penelitian yang dilakukan oleh Dermawan A, pada tahun 2024 dengan judul Analisa Perbandingan Optimalisasi *Port Knocking* Dan *Honeypot* Dengan *Iptables*. Pada Server Untuk Keamanan Jaringan menjelaskan bahwa Keamanan jaringan merupakan aspek krusial dalam melindungi sistem dari berbagai ancaman siber yang terus berkembang. Salah satu metode yang digunakan untuk meningkatkan keamanan adalah teknik *port knocking* dan *port blocking*, yang berfungsi untuk menyembunyikan atau membatasi akses ke port tertentu pada suatu sistem. Teknik ini bertujuan untuk mencegah serangan dari pihak yang tidak berwenang, seperti *brute force attack* dan *port scanning*, yang sering digunakan untuk mengeksploitasi kelemahan jaringan. Namun, dalam implementasinya, teknik ini memiliki beberapa tantangan, seperti kompleksitas konfigurasi, keterbatasan fleksibilitas akses bagi pengguna sah, serta potensi gangguan koneksi jika terjadi kesalahan konfigurasi. Oleh karena itu, diperlukan penelitian lebih lanjut untuk mengevaluasi serta mengoptimalkan penerapan metode ini, khususnya dalam lingkungan jaringan yang lebih luas, seperti institusi pendidikan. Dengan adanya penelitian ini, diharapkan dapat ditemukan metode yang lebih efektif dan efisien dalam meningkatkan keamanan jaringan tanpa mengorbankan aksesibilitas bagi pengguna yang berhak.

Komisi Pemilihan Umum (KPU) Kabupaten Tanah Datar adalah lembaga independen yang bertanggung jawab atas penyelenggaraan pemilihan umum di Kabupaten Tanah Datar, Sumatera Barat. Pembentukan KPU di tingkat kabupaten/kota, termasuk Tanah Datar, merupakan bagian dari reformasi politik

Indonesia pasca lengsernya Presiden Soeharto pada 21 Mei 1998. Pada masa itu, desakan publik untuk segera melaksanakan pemilu baru guna menggantikan hasil Pemilu 1997 yang dianggap tidak kredibel sangat kuat. Sebagai respons, pemerintah membentuk KPU sebagai lembaga penyelenggara pemilu yang independen, terpisah dari pemerintah, untuk memastikan pelaksanaan pemilu yang jujur dan adil. KPU Kabupaten Tanah Datar dibentuk untuk menyelenggarakan pemilu di tingkat kabupaten, termasuk pemilihan anggota legislatif daerah dan kepala daerah, dengan tujuan memastikan proses demokrasi berjalan sesuai prinsip-prinsip yang telah ditetapkan. Sejak pembentukannya, KPU Kabupaten Tanah Datar telah berperan dalam berbagai pemilu, seperti pemilu legislatif, pemilu presiden, dan pemilihan kepala daerah. Sebagai lembaga penyelenggara pemilu, KPU Kabupaten Tanah Datar memiliki tanggung jawab untuk menjaga integritas data dan kelancaran komunikasi jaringan selama proses pemilu. Namun, dalam pelaksanaannya, terdapat beberapa tantangan yang dapat mengancam keamanan jaringan, seperti potensi serangan dari pihak yang tidak bertanggung jawab, terbukanya akses *port* yang rentan terhadap eksploitasi, serta belum optimalnya sistem keamanan jaringan yang digunakan.

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu **"ANALISA DAN IMPLEMENTASI KOMBINASI TEKNIK KEAMANAN JARINGAN DENGAN MENGGUNAKAN METODE *PORT KNOCKING* DAN *HONEYPOT* PADA PERANGKAT *ROUTER MIKROTIK* YANG TERPASANG DI KOMISI PEMILIHAN UMUM KABUPATEN TANAH DATAR".**

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, dapat disimpulkan permasalahan yang akan dibahas pada laporan ini sebagai berikut:

1. Bagaimana implementasi metode *Port Knocking* dan *Honeypot* dapat meningkatkan keamanan jaringan pada perangkat *router Mikrotik* yang terpasang di KPU Kabupaten Tanah Datar?
2. Bagaimana dengan adanya *Honeypot* dapat meragukan pihak penyerang?
3. Bagaimana penggunaan *Port Knocking dan Honeypot* pada *router Mikrotik*, dapat mengatasi masalah yang dihadapi KPU Kabupaten Tanah Datar dalam implementasi sistem keamanan jaringan?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut:

1. Diharapkan dengan mengimplementasikan metode yang digunakan dapat meningkatkan keamanan jaringan *Mikrotik* di KPU Kabupaten Tanah Datar dengan mencegah akses tidak sah ke layanan jaringan.
2. Diharapkan metode *Port Knocking* dan *Honeypot* mampu membatasi akses ke layanan jaringan hanya bagi pengguna yang memiliki otorisasi yang sah.
3. Diharapkan penggunaan *Port Knocking dan Honeypot* pada *Mikrotik Router OS* dapat meningkatkan kemampuan deteksi dan respons terhadap serangan siber di KPU Kabupaten Tanah Datar

1.4 Batasan Masalah

Untuk menghindari penyimpangan maupun perluasan dari pokok masalah dalam penelitian ini, peneliti memberikan batasan masalah dengan hanya menggunakan satu laptop dan satu perangkat *mikrotik* untuk melakukan implementasi *Port Knocking* dan *Honeypot*. Hal ini mungkin tidak cukup untuk menguji keamanan jaringan secara menyeluruh. Selain itu, terdapat keterbatasan dalam keakuratan informasi, seperti *IP address server* dan perangkat lainnya, yang disebabkan oleh fakta bahwa informasi tersebut merupakan rahasia instansi dan tidak dapat diungkapkan kepada peneliti. Penelitian ini akan dilakukan pada KPU Kabupaten Tanah Datar, dengan perancangan yang nantinya akan diimplementasikan pada perangkat *Mikrotik* yang menggunakan sistem operasi *Router OS,* serta diuji coba menggunakan *software PuTTy*

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini, tujuan yang ingin dicapai diantaranya adalah:

1. Untuk merancang dan mengimplementasikan metode *Port Knocking* dan *Honeypot* pada *router Mikrotik* untuk meningkatkan keamanan jaringan di Komisi Pemilihan Umum (KPU) Kabupaten Tanah Datar.
2. Untuk melakukan pengujian terhadap hasil implementasi menggunakan *software PuTTY* untuk memastikan bahwa hanya pengguna yang memiliki otorisasi yang dapat mengakses layanan jaringan.
3. Untuk menilai efektivitas penggunaan *Port Knocking* dan *Honeypot* dalam memperkuat sistem keamanan jaringan perusahaan, dan mengevaluasi peran

MikroTik dalam menghadapi ancaman jaringan serta mengelola trafik data secara optimal.

1.6 Manfaat Penelitian

Adapun manfaat atau benefit yang didapat dari penelitian ini antara lain yaitu:

1. Dengan Penelitian ini diharapkan dapat memberikan solusi praktis dalam meningkatkan keamanan jaringan instansi, sehingga dapat melindungi data sensitif dan menjaga kontinuitas operasional.
2. Meningkatkan keamanan jaringan di Komisi Pemilihan Umum (KPU) Kabupaten Tanah Datar dengan menerapkan metode *Port Knocking* dan *Honeypot* untuk mencegah akses tidak sah.
3. Membantu organisasi dalam memahami pentingnya konfigurasi *firewall* dan teknik autentikasi *port* sebagai bagian dari strategi keamanan jaringan.

1.7 Gambaran Umum Objek Penelitian

Dalam bagian ini diuraikan informasi objek penelitian sebagai gambaran umum yang berisikan sekilas tentang objek penelitian, visi & misi, dan struktur organisasi.

1.7.1 Sekilas tentang Komisi Pemilihan Umum

Komisi Pemilihan Umum (KPU) adalah lembaga independen di Indonesia yang bertugas menyelenggarakan pemilihan umum (pemilu) secara nasional, termasuk pemilihan presiden dan wakil presiden, pemilihan anggota legislatif (DPR, DPD, DPRD), serta pemilihan kepala daerah (Pilkada). KPU dibentuk sebagai bagian dari reformasi politik setelah runtuhnya pemerintahan Orde Baru

pada tahun 1998, dengan tujuan memastikan pemilu yang transparan, jujur, dan adil. Sebagai bagian dari struktur organisasi KPU, terdapat KPU di tingkat provinsi dan kabupaten/kota yang bertanggung jawab atas penyelenggaraan pemilu di wilayah masing-masing. Salah satunya adalah KPU Kabupaten Tanah Datar, yang berperan dalam mengoordinasikan pelaksanaan pemilihan umum di tingkat kabupaten. Tugas utama KPU Kabupaten Tanah Datar meliputi perencanaan, pelaksanaan, dan pengawasan jalannya pemilu, termasuk pengelolaan data pemilih, logistik pemilu, serta penghitungan suara.

1.7.2 Visi dan Misi dari Komisi Pemilihan Umum Kab. Tanah Datar

Adapun Visi dan Misi dari Komisi Pemilihan Umum Kabupaten Tanah Datar antara lain:

1. Visi

Menjadi Penyelenggara Pemilihan Umum yang Mandiri, Professional, dan Berintegritas untuk Terwujudnya Pemilu yang LUBER dan JURDIL.

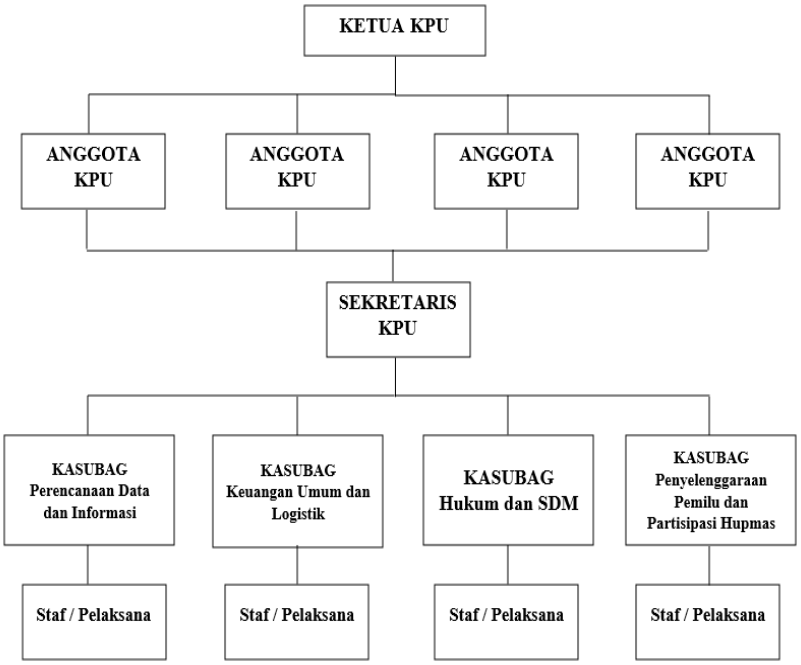
2. Misi

1) Meningkatkan kualitas penyelenggaraan Pemilihan Umum (Pemilu) yang efektif dan efisien, transparan, akuntabel, serta aksesible.
2) Meningkatkan integritas, kemandirian, kompetensi dan profesionalisme penyelenggara Pemilu dengan mengukuhkan *Code of Conduct* penyelenggara Pemilu.
3) Menyusun regulasi di bidang Pemilu yang memberikan kepastian hukum, progresif, dan partisipatif.
4) Meningkatkan kualitas pelayanan Pemilu untuk seluruh pemangku kepentingan.

5) Meningkatkan partisipasi dan kualitas pemilih dalam Pemilu, Pemilih berdaulat Negara kuat.
6) Mengoptimalkan pemanfaatan kemajuan teknologi informasi dalam penyelenggaraan Pemilu.

1.7.3 Struktur Organisasi Komisi Pemilihan Umum Kab. Tanah Datar

Dengan adanya struktur organisasi diharapkan akan dapat diketahui dengan jelas mengenai tugas, wewenang, dan tanggung jawab di KPU Kabupaten Tanah Datar. Adapun struktur organisasi KPU dapat dilihat pada gambar 1.1 sebagai berikut:



Sumber: Komisi Pemilihan Umum Tanah Datar

Gambar 1.1 Struktur Organisasi KPU Kab. Tanah Datar

1.7.4 Tugas dan Wewenang KPU

Berikut adalah uraian dari tugas serta wewenang pada KPU:

1. Tugas KPU
   a. Merencanakan program dan anggaran serta menetapkan jadwal.
   b. Menyusun tata kerja KPU, KPU Provinsi, KPU Kabupaten/Kota, PPK, PPS, KPPS, PPLN, dan KPPSLN.
   c. Menyusun Peraturan KPU untuk setiap tahapan pemilu.
   d. Mengkoordinasikan, menyelenggarakan, mengendalikan, dan memantau semua tahapan pemilu.
   e. Menerima daftar pemilih dari KPU Provinsi.
   f. Memutakhirkan data pemilih berdasarkan data pemilu terakhir dengan memperhatikan data kependudukan yang disiapkan dan diserahkan oleh pemerintah dan menetapkannya sebagai daftar pemilih.
   g. Membuat berita acara dan sertifikat rekapitulasi hasil penghitungan suara serta wajib menyerah kepada saksi Peserta Pemilu dan Bawaslu.
   h. Mengumumkan calon anggota DPR, Calon Anggota DPD dan Pasangan Calon terpilih serta membuat berita acaranya.
   i. Menindaklanjuti dengan segera putusan Bawaslu atas temuan dan laporan adanya dugaan pelanggaran atau sengketa Pemilu.
   j. Menyosialisasikan Penyelenggaraan Pemilu dan/atau yang berkaitan dengan tugas dan wewenang KPU Kepada Masyarakat.
   k. Melakukan evaluasi dan membuat laporan setiap tahapan Penyelenggaraan Pemilu.

l. Melaksanakan tugas lain dalam penyelenggaraan Pemilu sesuai dengan ketentuan peraturan perundang-undangan.

2. Wewenang KPU

a. Menetapkan tata kerja KPU, KPU Provinsi, KPU Kabupaten/Kota, PPK, PPS, KPPS. PPLN, dan KPPSLN.

b. Menetapkan peraturan KPU untuk setiap tahapan Pemilu.

c. Menetapkan peserta Pemilu.

d. Menetapkan dan mengumumkan hasil rekapitulasi perhitungan suara tingkat nasional berdasarkan hasil rekapitulasi perhitungan suara di KPU Provinsi untuk pemilu Presiden dan Wakil Presiden dan untuk pemilu anggota DPR serta hasil rekapitulasi perhitungan suara di setiap KPU Provinsi untuk pemilu anggota DPD dengan membuat berita acara perhitungan suara dan sertifikat hasil penghitungan suara.

e. Menerbitkan keputusan KPU untuk mengesahkan hasil pemilu dan mengumumkannya.

f. Menetapkan dan mengumumkan perolehan jumlah kursi anggota DPR, anggota DPRD Provinsi, dan Anggota DPRD Kabupaten/Kota untuk setiap partai politik peserta Pemilu Anggota DPR, anggota DPRD Provinsi, dan Anggota DPRD Kabupaten/Kota.

g. Menetapkan standar serta kebutuhan pengadaan dan pendistribusian perlengkapan.

h. Membentuk KPU Provinsi, KPU Kabupaten/Kota, dan PPLN.

i. Mengangkat, membina dan memberhentikan anggota KPU Provinsi, anggota KPU Kabupaten/Kota, dan anggota PPLN.

j. Menjatuhkan sanksi administratif dan/atau menonaktifkan sementara anggota KPU Provinsi, anggota KPU Kabupaten/Kota anggota PPLN, anggota KPPSLN, dan sekretaris Jenderal KPU yang terbukti melakukan tindakan yang mengakibatkan terganggunya tahapan penyelenggaraan Pemilu yang sedang berlangsung berdasarkan putusan Bawaslu dan/atau ketentuan peraturan perundang-undangan.

k. Menetapkan kantor akuntan publik untuk mengaudit dana kampanye Pemilu dan mengumumkan laporan sumbangan dana Kampanye Pemilu.

l. Melaksanakan wewenang lain dalam penyelenggaraan Pemilu sesuai dengan ketentuan peraturan perundang-undangan.