BAB 1. PENDAHULUAN

1.1. Latar Belakang

Seiring dengan perkembangan transformasi digital yang serba terhubung, keamanan siber menjadi pondasi utama bagi kelangsungan operasional berbagai organisasi. Transformasi digital yang masif di berbagai sektor, mulai dari pemerintahan hingga industri, menuntut perlindungan menyeluruh terhadap infrastruktur digital dari berbagai ancaman. Salah satu target utama dalam infrastruktur ini adalah sistem operasi Linux, yang kini mendominasi server global dan menjadi pilihan utama bagi mayoritas layanan cloud. Berkat keandalan, skalabilitas, dan efisiensi sumber dayanya, Linux memegang peran krusial dalam ekosistem teknologi pada era digital 4.0 (Huda, 2023).

Linux dikenal karena fleksibilitas, keamanan, dan stabilitasnya. Namun, konfigurasi yang kurang tepat seperti kesalahan penempatan direktori /tmp di awal variabel path pada konfigurasi .bashrc, terdapat riwayat password user untuk akun mysql pada .bash_history, penambahan aturan setuid pada /bin/find user non administrator atau adanya kerentanan pada perangkat lunak yang belum stabil dapat membuka celah eksploitasi (Massacci et al., 2022). Salah satu metode yang digunakan oleh peretas untuk mengambil alih kendali penuh atas sistem adalah serangan peningkatan hak akses. Teknik privilege escalation merupakan metode serangan di mana peretas yang awalnya hanya memiliki hak akses sebagai pengguna biasa, memanfaatkan celah keamanan untuk mendapatkan hak akses administrator (Happe et al., 2024). Berbagai metode dapat digunakan untuk mencapai tujuan tersebut, mulai dari eksploitasi program bawaan Linux hingga manipulasi file konfigurasi seperti format .conf, .ssh, .config, dan .xml (Huang et al., 2022).

Sistem deteksi serangan yang umum digunakan saat ini, seperti Sistem Deteksi Intrusi berbasis signature atau machine learning, sering kali dinilai kurang transparan. Meskipun efektif mendeteksi keanehan pada celah konfigurasi, pendekatan ini cenderung bersifat black-box yang memberi peringatan adanya bahaya tetapi tidak mampu menjelaskan secara logis bagaimana peningkatan hak akses itu terjadi, khususnya di lingkungan Linux yang memiliki arsitektur unik (Maulani dkk., 2023). Oleh karena itu, framework seperti MITRE ATT&CK telah banyak dimanfaatkan dalam penelitian sebelumnya untuk memetakan celah keamanan (Wahyudi dkk., 2025). Namun, penggunaan framework ini sering kali masih bersifat reaktif dan belum terintegrasi dengan mekanisme penalaran logis untuk diagnosis otomatis.

MITRE ATT&CK sendiri mendokumentasikan 14 teknik Privilege Escalation yang mencakup berbagai platform seperti Linux, Windows, macOS, dan Cloud. Dari keempat belas teknik tersebut, terdapat empat teknik yang paling relevan dan paling sering dieksploitasi pada lingkungan Linux, yaitu Abuse Elevation Control Mechanism, Boot or Logon Initialization Scripts, Scheduled Task/Job, dan Create or Modify System Process. Keempat teknik ini kemudian diidentifikasi mencakup tujuh sub-teknik yang bersifat spesifik terhadap platform Linux. Selanjutnya, ketujuh sub-teknik tersebut didekomposisi lebih lanjut berdasarkan pengetahuan pakar keamanan siber menjadi sembilan jenis vulnerability konkret yang dapat dideteksi secara teknis pada sistem operasi Linux. Dekomposisi ini diperlukan karena masing-masing kerentanan memiliki pendekatan teknis yang berbeda, baik dari segi proses deteksi maupun penanganannya, sehingga membutuhkan representasi pengetahuan yang lebih granular dan dapat dinalar secara otomatis oleh mesin inferensi.

Pada penelitian ini, penggunaan sistem pakar menjadi solusi yang tepat karena kemampuannya dalam melakukan penalaran logis terhadap celah keamanan. Sistem pakar memungkinkan konversi pengetahuan skema dari framework MITRE ATT&CK ke dalam aturan yang dapat dinalar secara otomatis. Selanjutnya proses penalaran tersebut dijalankan dengan metode forward chaining yang memegang peranan penting dalam mendiagnosis celah keamanan dengan melakukan inferensi dari fakta menuju kesimpulan. Forward chaining telah terbukti berhasil diterapkan dalam masalah teknis, seperti diagnosis kerusakan perangkat keras (Sakinah dkk., 2024).

Guna mengatasi kesenjangan tersebut, penelitian ini mengusulkan pengembangan Sistem Pakar Diagnosa Privilege Escalation di Linux Menggunakan Forward Chaining Berdasarkan MITRE ATT&CK. Sistem pakar ini dirancang untuk meniru kemampuan penalaran seorang profesional dalam bidang keamanan siber dalam menganalisis fakta yang ditemukan di sistem, lalu menyimpulkan jenis teknik serangan yang terjadi (Mishchenko et al., 2024). MITRE ATT&CK akan digunakan sebagai panduan utama yang menyediakan basis pengetahuan terstruktur mengenai teknik-teknik serangan yang sering digunakan peretas. Integrasi ini memastikan bahwa diagnosis sistem tidak hanya mendeteksi adanya anomali, tetapi juga mampu mengidentifikasi nama teknik serangan secara spesifik.

Tujuan penelitian ini menghasilkan sebuah alat bantu yang efektif bagi administrator sistem untuk meminimalisir dampak serangan siber. Sistem pakar ini tidak hanya mampu mendiagnosa potensi privilege escalation, tetapi juga memberikan penjelasan transparan mengenai proses penalarannya serta merekomendasikan langkah mitigasi yang tepat. Dengan demikian, penelitian ini diharapkan dapat mengisi kekosongan dalam literatur yang ada dan memberikan kontribusi nyata dalam meningkatkan keamanan sistem.

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan masalah dalam penelitian ini yaitu :

a. Bagaimana merancang dan membangun sistem pakar berbasis forward chaining untuk mendiagnosa sembilan kerentanan *privilege escalation* yang diturunkan dari empat teknik MITRE ATT&CK pada sistem operasi Linux ?
b. Bagaimana mengimplementasikan framework MITRE ATT&CK dalam sistem pakar agar dapat mendiagnosa teknik serangan secara spesifik pada level sub-teknik Linux serta menghasilkan rekomendasi mitigasi yang tepat ?
c. Bagaimana tingkat penerimaan pengguna dan efektivitas sistem pakar yang telah dibangun berdasarkan pengujian User Acceptance Test ?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini yaitu:

a. Merancang dan membangun sistem pakar menggunakan metode forward chaining yang mampu mendiagnosa secara otomatis sembilan kerentanan *privilege escalation* yang diturunkan dari empat teknik MITRE ATT&CK pada sistem operasi Linux.
b. Menerapkan framework MITRE ATT&CK sebagai basis pengetahuan untuk memetakan teknik serangan pada sub-teknik Linux dan menghasilkan rekomendasi mitigasi keamanan yang tepat sasaran.
c. Mengetahui tingkat efektivitas dan penerimaan sistem oleh pengguna melalui pengujian fungsional dan User Acceptance Test (UAT) guna memastikan sistem layak digunakan.

1.4. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini yaitu:

a. Diharapkan penelitian ini dapat membantu meminimalisir resiko kesalahan konfigurasi.
b. Diharapkan penelitian ini dapat membantu mengurangi waktu pengecekan celah keamanan secara manual yang memakan waktu.
c. Diharapkan penelitian ini dapat menjadi referensi basis pengetahuan yang terorganisir mengenai kerentanan linux yang dapat dikembangkan oleh peneliti selanjutnya mengenai pengembangan sistem pakar dengan metode *forward chaining*.

1.5. Batasan Penelitian

Adapun batasan penelitian ini yaitu:

a. Fokus penelitian pada diagnosis celah keamanan dan pemberian rekomendasi upaya meminimalisir resiko celah keamanan. Sistem yang dibangun tidak melakukan tindakan eksekusi otomatis seperti perbaikan konfigurasi.
b. Teknik privilege escalation yang dianalisis dibatasi pada sembilan kerentanan dari hasil dekomposisi sub-teknik, yaitu Privesc SUID Find, Privesc SGID Nano, Sudo Privilege Drop, Sudo Caching, InputPlumber Lack of D-Bus Auth, Cron, Symlink Race Condition, Systemd Timers, dan RC Scripts.
c. Target diagnosis adalah Debian 12 bookworm yang dijalankan dalam lingkungan virtual menggunakan Oracle VirtualBox.