BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada awal tahun 2023, Badan Siber dan Sandi Negara (BSSN) Republik Indonesia memberi publikasi terhadap Lanskap Keamanan Siber Indonesia 2022 yang berisi kondisi keamanan siber di Indonesia sepanjang tahun 2022. Lanskap Keamanan Siber tersebut berisi hasil deteksi anomali trafik, dugaan insiden, dan ancaman-ancaman siber yang diprediksi oleh BSSN RI. Dari laporan tersebut brute-force dengan Remote Desktop Protocol (RDP) termasuk ke dalam ancaman yang diprediksi terjadi pada tahun 2023 oleh BSSN RI[12].

Di sisi lain, SSH brute-force juga meningkat di Indonesia[2]. SSH brute force merupakan tindakan untuk mengakses sistem yang menggunakan SSH protocol secara ilegal. Dari hasil deteksi anomali trafik yang dilakukan, Indonesia merupakan negara yang paling banyak menjadi negara tujuan dari anomali trafik tersebut. Anomali trafik tersebut merupakan trafik dari berbagai ancaman siber seperti MyloBot Botnet, MiningPool, Trojan, Phising, dan banyak lagi [12].

Jenis insiden siber terbanyak yang terjadi di Indonesia pada tahun 2022 berdasarkan Rekapitulasi Insiden Siber 2022 adalah web defacement dengan 2,348 kasus dari banyaknya insiden siber yang terjadi [12]. Dari hasil pemeriksaan lebih lanjut, Administrasi Pemerintahan merupakan sektor terbanyak yang mengalami insiden tersebut dengan 885 kasus. Insiden-insiden tersebut terjadi karena banyak institusi ataupun perusahaan yang tidak melakukan tindak lanjut ataupun menyikapi insiden-insiden yang terjadi.

Pada insiden-insiden yang terjadi di sektor Administrasi Pemerintahan, misconfiguration merupakan kategori insiden terbanyak dengan 37% yang mengakibatkan vulnerability pada suatu sistem. Misconfiguration berakibat kerentanan (vulnerability) yang disebabkan oleh kesalahan dalam konfigurasi. Dengan begitu, perlu adanya tindakan untuk melakukan indentifikasi terhadap penyebab dari kerentanan-kerentanan tersebut [12].

Deteksi merupakan tindakan yang perlu dilakukan untuk mengidentifikasi kerentanan-kerentanan tersebut. Dari deteksi tersebut perlu adanya sistem deteksi sebagai

tindakan awal untuk mencegah terjadinya insiden-insiden siber. Teknologi dari sistem deteksi tersebut adalah Intrusion Detection System (IDS). Dalam hal ini, IDS yang digunakan adalah Wazuh sebagai Host-based IDS dan akan diuji sistem deteksinya dengan melakukan serangan simulasi dengan metode penetration testing menggunakan Kali Linux.

Proses-proses yang dilakukan seperti implementasi sistem deteksi perlu dianalisis untuk mengindentifikasi ancaman-ancaman keamanan dalam sistem deteksi berdasarkan log. Kemudian implementasi rule dilakukan pada Wazuh untuk meningkatkan kapabilitas dalam terhadap deteksi ataupun identifikasi terhadap simulasi penetration testing. Log yang diterima Wazuh sebelum implementasi rule dan log yang diterima Wazuh sesudah implementasi rule dilakukan analisis dengan melakukan perbandingan untuk mengetahui kapabilitas Wazuh dalam mendeteksi ataupun melakukan identifikasi simulasi penetration testing yang dilakukan.

1.2 Tujuan dan Manfaat

Adapun tujuan dari penulisan Proyek Akhir ini, sebagai berikut.

1. Melakukan implementasi Wazuh sebagai host based IDS untuk mendeteksi SSH brute-force melalui penetration testing menggunakan hydra tool tool.
2. Melakukan analisis dengan melakukan perbandingan anatara log yang dideteksi Wazuh menggunakan default rule dengan log yang dideteksi Wazuh setelah implementasi rule.

Manfaat dari penulisan Proyek Akhir ini, sebagai berikut.

1. Membangun sistem deteksi dengan *Wazuh* yang berlisensi open-source.
2. Memanfaatkan implementasi *rule* untuk meningkatkan kapabilitas deteksi dari *Wazuh*.

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut.

1. Bagaimana melakukan implementasi *Wazuh* sebagai *host based IDS* untuk mendeteksi *SSH brute-force* melalui *penetration testing* menggunakan *hydra tool*.

2. Bagaimana melakukan analisis dengan melakukan perbandingan anatara *log* yang dideteksi *Wazuh* menggunakan *default rule* dengan *log* yang dideteksi *Wazuh* setelah implementasi *rule*

1.4 Batasan Masalah

Adapun batasan masalah dari Proyek Akhir ini, sebagai berikut.

1. Implementasi *IDS* dilakukan menggunakan *Wazuh*.
2. Analisis perbandingan dilakukan berdasarkan *log* yang diterima oleh *IDS*.
3. *Penetration testing* dilakukan menggunakan *hydra tool* dari *Kali Linux.*
4. Analisis, implementasi, dan *penetration testing* dilakukan dalam *VirtualBox environment*.

1.5 Metodologi

Adapun metodologi pada penelitian Proyek Akhir ini, sebagai berikut.

1. Studi Literatur

   Studi literatur dilakukan dengan mengumpulkan literatur-literatur dan kajian-kajian yang berkaitan dengan permasalahan yang ada pada penelitian Proyek Akhir ini, baik berupa buku referensi, artikel, maupun *e-journal* yang berhubungan dengan implementasi *Wazuh, brute*-force, *Penetration testing*.

2. Pengumpulan Data

   Pengumpulan data awal dilakukan dengan melakukan pengumpulan *log* yang diterima oleh *IDS* berdasarkan hasil *penetration testing hydra tool tools*.

3. Implementasi

   Implementasi dilakukan dengan melakukan implementasi *Wazuh, penetration testing* dengan *hydra tool*.

4. Simulasi

   Simulasi dilakukan dengan melakukan *penetration testing* menggunakan *hydra tool Kali Linux* untuk melakukan *SSH brute-force*.

5. Analisis

   Analisis dilakukan dengan melakukan perbandingan hasil deteksi *Wazuh* dengan *default rule* dengan hasil deteksi sudah diimplementasikan *rule*.

1.6 Sistematika Penulisan

Dalam penulisan Proyek Akhir terdiri atas lima bab, dengan keterangan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini membahas tentang teori pendukung pengerjaan Proyek Akhir, seperti penjelasan terkait IDS, Wazuh, hydra tool tools, SSH brute-force, Ubuntu, VirtualBox, Penetration testing, Kali Linux.

BAB III IMPLEMENTASI

Pada bab ini membahas tentang implementasi Proyek Akhir, alur pengerjaan Proyek Akhir, pemasangan Wazuh, beserta configuration.

BAB IV SIMULASI DAN ANALISIS

Pada bab ini membahas tentang simulasi dan analisis terhadap implementasi Wazuh, implementasi rule, beserta simulasi hydra tool tools.

BAB V PENUTUP

Pada bab ini membahas tentang kesimpulan dari pengerjaan Proyek Akhir.