BAB V
KESIMPULAN

5.1 KESIMPULAN

Hasil penelitian menunjukkan bahwa Wazuh dapat mendeteksi serangan *brute-force* terhadap protokol SSH dan RDP. Wazuh juga dapat memblokir secara sementara alamat IP komputer yang digunakan untuk melakukan penyerangan sebagai bentuk dari penanganan serangan *brute-force*.

Dalam perspektif *user*, Wazuh memiliki beberapa keunggulan dalam mendeteksi serangan *brute-force*, antara lain:

- Kemampuan mendeteksi berbagai jenis serangan *brute-force*. Wazuh dapat mendeteksi serangan *brute-force* dengan berbagai metode, termasuk:
  - Percobaan *login* yang gagal
  - Pemindaian *port* atau jaringan yang mencurigakan
  - Perubahan konfigurasi signifikan
  - Penggunaan kredensial yang mencurigakan
- Kemampuan mendeteksi serangan *brute-force* dengan cepat. Wazuh dapat mendeteksi serangan *brute-force* dengan cepat, sehingga organisasi dapat mengambil tindakan pencegahan atau mitigasi sesegera mungkin.
- Kemampuan memberikan peringatan yang jelas dan akurat. Wazuh dapat memberikan peringatan yang jelas dan akurat kepada pengguna, sehingga mereka dapat dengan mudah memahami jenis serangan yang terjadi dan mengambil tindakan yang tepat.

- Kemampuan memblokir alamat IP penyerang secara otomatis. Wazuh dapat memblokir alamat IP penyerang secara otomatis, sehingga dapat mencegah penyerang untuk melanjutkan serangan.

Namun, Wazuh juga memiliki beberapa kekurangan, antara lain:

- Kompleksitas konfigurasi. Wazuh memiliki konfigurasi yang cukup kompleks, sehingga membutuhkan waktu dan upaya untuk mempelajarinya.
- Kemungkinan *false positive*. Wazuh dapat mendeteksi serangan *brute-force* yang sebenarnya bukan serangan *brute-force*, sehingga dapat menimbulkan kebingungan bagi pengguna.

Secara keseluruhan, Wazuh merupakan SIEM yang efektif dalam mendeteksi serangan *brute-force*. Namun, organisasi perlu mempertimbangkan kompleksitas konfigurasi dan kemungkinan terjadinya *false-positive* sebelum mengimplementasikan Wazuh.

Penting untuk diingat bahwa deteksi kerentanan hanya satu bagian dari strategi keamanan yang lengkap, dan pemeliharaan rutin serta pengelolaan perangkat lunak dan sistem operasi juga krusial untuk mengurangi risiko kerentanan.

5.2 SARAN

Berdasarkan kesimpulan diatas, peneliti dapat menyarankan untuk selalu mengaktifkan *firewall* serta selalu memperbarui sistem keamanan dari sistem operasi yang digunakan. Hal tersebut dilakukan karena hampir setiap saat selalu ada celah atau metode baru yang dilakukan peretas dalam melakukan peretasan.

Peneliti juga menyarankan untuk menutup *port* yang tidak digunakan agar tidak ada penyerangan *brute-force* yang menyerang secara acak *port* yang tidak digunakan.

Untuk penelitian selanjutnya, penulis menyarankan untuk melakukan pengujian dengan metode *brute-force* yang lebih kompleks atau

dengan *tools* yang lebih mumpuni, agar dapat memperkuat klaim bahwa Wazuh sebagai implementasi SIEM adalah pilihan tepat untuk mendeteksi serangan *brute-force* pada sistem.