BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian dan pengembangan yang telah dilakukan, dan mengacu pada point Rumusan Masalah yang dipaparkan pada BAB 1, berikut adalah kesimpulan yang dapat diambil :

a. Tingkat efektivitas penerapan algoritma Naïve Bayes dalam mendeteksi serangan brute force attack berdasarkan data logs dari Honeypot Cowrie terbilang cukup baik, dengan menghasilkan nilai yang baik pula pada parameter ukur dari hasil evaluasi model yang dibangun, dimana rataan yang didapat dari 4 metrics : Accuracy, Precision, Recall, dan F1-Score diangka 0.99 atau 99%. Lalu dengan data uji prediksi menghasilkan score : Accuracy, Precision, Recall, dan F1-Score : 0.98, 0.99, 0.80, dan 0.87.
b. Parameter yang dijadikan acuan utama dalam mendeteksi serangan brute force attack melalui data logs dari honeypot cowrie, pada proses pelatihan dan uji modal adalah keys-keys penting yang didasari oleh dokumentasi langsung dari komunitas pengembang software Honeypot Cowrie. Seperti : ‘eventid’, ‘username’, ‘password’, ‘src_ip’, dan juga ‘timestamp’.
c. Tingkat keberhasilan penerapan algoritma naïve bayes dalam mendeteksi serangan brute force attack berdasarkan data logs dari honeypot cowrie terbilang cukup baik, dengan data uji baru dalam range waktu yang sudah

ditentukan, menghasilkan nilai evaluasi : Accuracy, Precision, Recall, dan F1-Score : 98% , 99% , 80%, dan 87%.

5.2 Saran

Berdasarkan hasil penelitian dan implementasi sistem, beberapa saran yang dapat diberikan dan mungkin bisa dipertimbangkan untuk pengembangan lebih lanjut adalah sebagai berikut :

a. Menggunakan Algoritma Lain atau Menggabungkan Algoritma Lainnya

   Terbukti memang algoritma naïve bayes dapat dengan baik untuk melakukan kalsifikasi jenis data serangan siber, khususnya berdasarkan data logs dari honeypot cowrie. Namun pada saat implementasi sistem diatas, penulis melakukan metoda ensamble atau stacking dimana point intinya adalah, bukan hanya Naïve Bayes yang menjadi estimator pada data predict, namun ada base modal lainnya yang dijadikan acuan lain dalam menentukan behaviour dari modal yang dibangun.

b. Penggunaan Honeypot Dengan Level Interaction Lainnya

   Penggunaan Honeypot Cowrie dalam mendeteksi serangan brute force attack terbilang cukup baik, terlebih paket ini memang didasari oleh proses development yang secara khusus untuk menjadi IDS dan IPS pada protocol SSH, dan remote session lainnya.

c. Menggunakan lebih banyak parameter

   Untuk memperkaya keberagaman hasil uji test, disarankan untuk menambahkan lebih banyak parameter lainnya yang bisa diujikan.

Menambahkan parameter disini termasuk menambahakn jumlah kuantitas data yang ada.

d. Pengembangan Interface

Bagi sebagian orang awam, design interface yang didevelop mungkin cukup membingungkan dimana kita akan disajikan sebagain langkah-langkah input dan mengeluarkan output berupa file yang otomatis terdownload. Tentu hal ini akan menjadi pertimbangan besar kedepannya, terkhusus bagi penggunan sistem dengan latar belakang non-technic.

e. Pengujian Lapangan Lebih Dalam

Karena lingkungan tempat uji terbatas pada VPS Staging pada PT Riwtech Workshop Indonesia yang memang sengaja di design untuk dilakukan uji coba simulasi penyerangan siber, akan lebih akurat dan valid apabila kedua teknologi ini di implementasikan langsung pada server Production, agar lebih mendapatkan informasi yang lebih beragam.

f. Skalabilitas Sistem

Diharapkan penelitian selanjutnya dapat mengembangkan sistem ini agar lebih mudah dipahami dan diimplementasikan dengan berbagai jenis lingkungan yang ada dengan menggunakan teknologi-teknologi lainnya seperti docker dari section containerization method, dan berbagai jenis teknologi lainnya.

Dengan diberikannya saran-saran diatas, diharapkan penelitian ini menjadi salah satu referensi untuk penelitan selanjutnya atas penggabungan teknologi informasi antara Cyber Security dan Machine Learning dalam konteks perangkat

atau media pelengkap dalam proses transformasi digital bisnis yang lebih aman dan efektif menghasilkan suatu informasi terkait bahaya ancaman serangan siber.

DAFTAR PUSTAKA

Aditya, A., Wahyuddin, P., Leo, S., Santoso, W., Wahyu, G., Wibowo, N., Khrisna, A., Rahmaddeni, W., Wahidin, A. J., Eka, G., Elisawati, Y., Rizqi, R., & Abdurrasyid,