INTERNSHIP MINGGU 1

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

CYBERSECURITY

Disusun Oleh:

Farrel Ardya Ghalyndra - 101012330102

Octlivatua Patricia Disiulina – 1301223200

Naisya Aghis Nabila- 1101223215

MULTIMEDIA APPLICATION, BIG DATA,

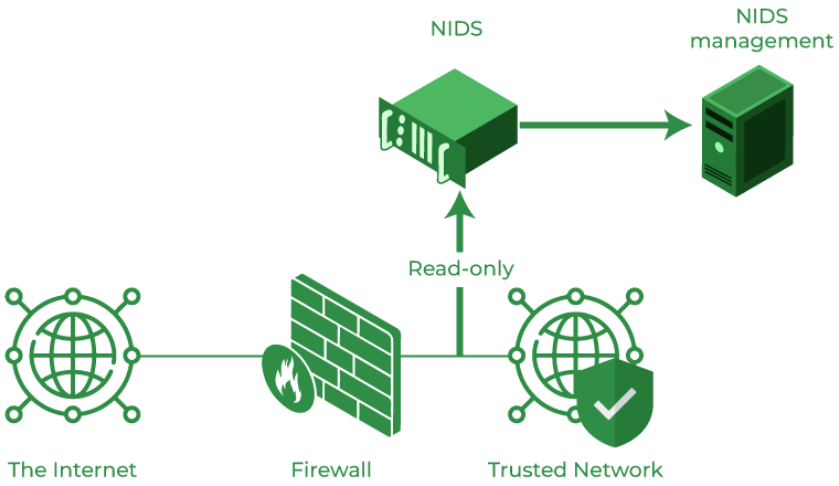
AND CYBERSECURITY LABORATORY

UNIVERSITAS TELKOM

BANDUNG

2024

NIDS (Network Intrusion Detection System)



Intrusion Detection System (IDS) adalah aplikasi perangkat lunak yang memonitor jaringan atau sistem untuk kegiatan yang berbahaya atau kegiatan intruder. Setiap kegiatan yang terdeteksi atau pelanggaran atas rule dilaporkan baik untuk administrator atau dikumpulkan secara terpusat menggunakan manajemen informasi keamanan atau security information and event management (SIEM). Ada beberapa jenis IDS, yang paling umum adalah Network Intrusion detection system (NIDS) dan Host Intrusion Detection System (HIDS). NIDS atau Network Intrusion Detection System adalah solusi yang menganalisis lalu lintas dan mencoba menemukan aktivitas yang tidak biasa, seperti pemindaian, upaya penyusupan, gerakan lateral, eksfiltrasi, pintu belakang, komando dan kontrol, dll. Hal ini pada awalnya dilakukan melalui tanda tangan, tetapi seiring berjalannya waktu beberapa solusi berevolusi menjadi NTA. XDR/ NTA mencakup fitur NIDS dengan lebih dari 80.000 aturan yang diperbarui secara berkala.

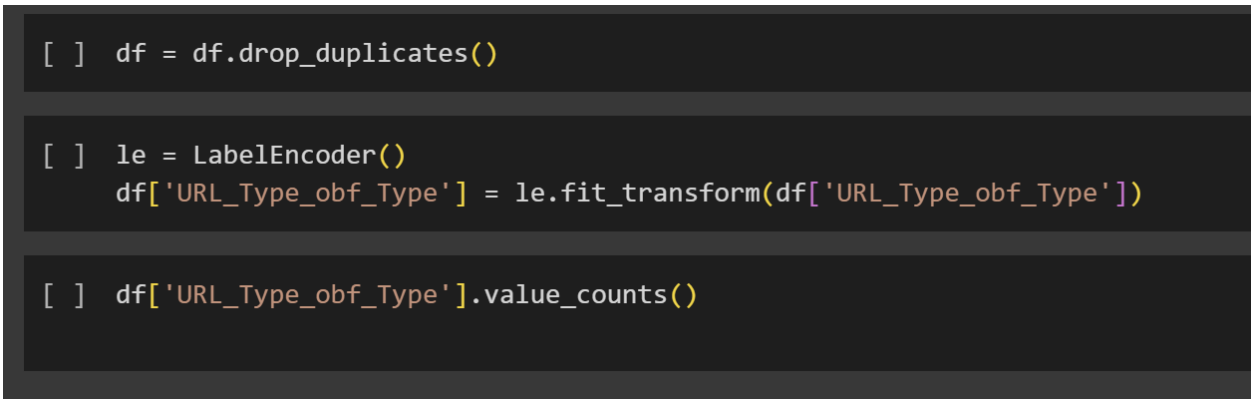
Network Intrusion detection system (NIDS) ditempatkan pada titik strategis atau titik dalam jaringan untuk memonitor lalu lintas ke dan dari semua perangkat pada jaringan . NIDS melakukan analisis lalu lintas yang lewat di seluruh subnet. Semua trafik yang masuk ke subnet akan di periksa dan dicocokkan dengan pattern atau signature yang ada di database. Setelah serangan diidentifikasi, atau perilaku abnormal dirasakan, sebuah alert atau peringatan dikirim ke administrator. NIDS dapat di instal pada subnet dimana firewall berada. Idealnya NIDS memeriksa semua lalu lintas inbound dan outbound, namun hal itu dapat membuat bottleneck yang akan merusak kecepatan keseluruhan jaringan. Ketika kita mengklasifikasikan perancangan NIDS sesuai dengan properti sistem interaktivitas, ada dua jenis: on-line dan off-line NIDS. On- line NIDS berhubungan dengan jaringan secara real time. Ini analisis paket Ethernet dan menerapkan beberapa aturan, untuk memutuskan apakah itu adalah serangan atau tidak. Off-line NIDS berhubungan dengan data yang tersimpan dan dibagikan melalui beberapa proses untuk memutuskan apakah itu adalah serangan atau tidak.

URL dataset (ISCX-URL2016)

Dataset yang sedang kami pakai terkait dengan URL berbahaya, yang sering digunakan dalam serangan siber seperti phishing atau distribusi malware. Dalam konteks IDS (Intrusion Detection System), data ini cukup berguna untuk mendeteksi URL berbahaya. Prosedur preprocessing, seperti pengkodean header kolom dan nilai kosong dan duplikat, dirancang untuk memperhalus dataset sehingga model Mechine Learning dapat menganalisis dan menginterpretasikannya dengan lebih mudah. Melalui proses ini, IDS dapat mengidentifikasi sebagian besar karakteristik tautan berbahaya dan membantu mengidentifikasi akun palsu dengan cepat dan efektif.

PROGRESS COLLAB

https://colab.research.google.com/drive/1sBoVHqshj9lv_DQggKAK6BMrRsh3Nah6?usp=sharing



Proses ini dimulai dengan mengimpor dataset baru, Spam.csv, menggunakan fungsi read_csv. Setelah data dikumpulkan, analisis eksplorasi dilakukan dengan melihat informasi umum dan statistik deskriptif dari dataset dan menghitung jumlah kosong. Selanjutnya, dataset diperluas dengan mengelompokkan bar yang berisi data yang berkorelasi dan tidak berkorelasi. Setelah proses pembersihan, kolom dengan jenis kategori, seperti URL_Type_obf_Type, dikonversi menggunakan LabelEncoder menjadi label numerik. Selanjutnya, jumlah kemunculan setiap kategori dalam kolom yang telah ditentukan sebelumnya dihitung untuk memahami distribusinya di antara kumpulan data.

REFERENSI

https://mti.binus.ac.id/2022/12/03/intrusion-detection-system/

https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset/code

https://tehtris.com/en/glossary/nids-network-intrusion-detection-system/