Capa

Índice

[1. Introdução 3](#_Toc211534254)

[2. Dados em análise 3](#_Toc211534255)

[3. KDD Process – Step 1 3](#_Toc211534256)

# Introdução

TBC

# Dados em análise

O dataset em análise pode ser encontrado no [Kaggle](https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks/data?select=cybersecurity_attacks.csv) e contém 40 mil entradas com 25 colunas correspondentes a métricas numéricas e simbólicas relacionadas com tráfego de rede.

|  |  |  |  |
| --- | --- | --- | --- |
| Métrica | Descrição | Exemplo | Numérica / Simbólica |
| Timestamp |  | 2023-05-30 06:33:58 |  |
| Source IP Address |  | 103.216.15.12 |  |
| Destination IP Address |  | 103.216.15.12 |  |
| Source Port |  | 31225 | Numérica |
| Destination Port |  | 17616 | Numérica |
| Protocol |  | ICMP |  |
| # Packet length |  | 503 | Numérica |
| Packet type |  | Data |  |
| Traffic type |  | HTTP |  |
| Payload Data |  | Text…… |  |
| Action Taken |  | Logged |  |
| Severity Level |  | Low |  |
| User Information |  | Sumar Rana |  |
| Device Information |  | Mozilla/5.0 (compatible; MSIE 8.0; Windows NT |  |
| Network Segment |  | Segment A |  |
| Geo-Location data |  | Jamshedpur, Sikkim |  |
| Proxy Information |  | 150.9.97.135 |  |
| Firewall Logs |  | Log Data |  |
| IDS/IPS alerts |  | NaN / Alert data |  |
| Log Source |  | Server |  |

# KDD Process – Step 1