Analisis Kerentanan pada Autonomous System Number di Indonesia Berdasarkan Data Shodan dengan Menggunakan Algoritma K-Means Clustering = Vulnerability Analysis of Autonomous System Number (ASN) from Indonesia Based on Exposure Data in Shodan with K-Means Clustering

Bambang Novianto, author

Abstrak

Pertumbuhan pemanfaatan internet telah meningkatkan perhatian terhadap keamanan data. Pada tahun 2014, Projek SHINE (SHodan Intelligence Extraction) telah menerbitkan laporan penilaian keamanan skala besar untuk perangkat yang terhubung ke Internet. Namun, berdasarkan laporan tersebut, jumlah informasi mengenai IP address Indonesia yang berhasil didapatkan masih sedikit. Terdapat sebanyak 7.182 IP address dari Indonesia, yaitu sekitar 0,0032% dari total 2.186.971 IP address yang berhasil dikumpulkan oleh Projek SHINE. Dalam penulisan tesis ini, penulis mengajukan inisiatif untuk melakukan analisis kerentanan semua informasi Autonomous System Number (AS Number) di Indonesia dari Shodan. Penulis telah menyusun dataset semua informasi AS Number di Indonesia antara lain 12.787 port, 79 sistem operasi, 409 produk, 3.634 domain, 145.543 IP address, dan 790 organisasi. Penulis menggunakan algoritma K-Means clustering untuk mengelompokkan AS Number ke dalam beberapa kelas sesuai dengan tingkat paparan di shodan. Berdasarkan hasil pengelompokan, penulis mendapatkan 4 kelas AS Number antara lain 1.075 AS Number di kelas: 0 (belum terdapat informasi mengenai AS Number tersebut di Shodan), 614 AS Number di kelas: 1 (tingkat paparan rendah), 9 AS Number di kelas: 2 (tingkat paparan sedang), dan 1 AS Number di kelas: 3 (tingkat paparan tinggi). Informasi ini dapat dimanfaatkan oleh Kementerian yang menangani bidang Teknologi Informasi dan Komunikasi dan Badan yang menangani Keamanan Siber di Indonesia untuk menghimbau organisasi pengelola AS Number agar mewaspadai potensi kerentanan yang dinformasikan oleh Shodan dan dimanfaatkan oleh hacker.

.....The growth of internet-enabled devices has increased interest in cybersecurity. In 2014, Project SHINE (SHodan INtelligence Extraction) published a report of large-scale security assessments for devices connected to the Internet. However, the number of IP addresses harvested from Indonesia in 2014 is very small. There were 7.182 IP address from Indonesia. It was about 0,0032% from the total 2.186.971 IP addresses. In this paper, we propose an initiative to gather all information for all Autonomous System Number (AS Number) from Indonesia in Shodan. We have gathered a dataset about all information of AS Numbers in Indonesia such as 12.787 unique ports, 79 unique operating systems, 409 unique products, 3.634 unique domains, 145.543 unique IP addresses, and 790 unique organizations. We use the K-Means algorithm to cluster all AS Numbers into several classes according to the exposure level in shodan. Based on the result, we have 4 classes of AS Numbers. There are 1.075 AS Numbers in class:0 (no information in Shodan yet), 614 AS Numbers in class:1 (exposure level = low), 9 AS Numbers in class:2 (exposure level = medium), and 1 AS Number in class:3 (exposure level = high). This information can be used to warn the organizations that manage AS Numbers in Indonesia to be aware of the security and the threats to their systems.