

ABSTRACT

IQBAL NURFARISI, APPLICATION OF DATA SECURITY ON HIGH TRAFFIC NETWORK USING INTRUSION DETECTION SYSTEM (IDS) AND INTRUSION PREVENTION SYSTEM (IPS) METHODS AT THE OFFICE OF COMMUNICATION AND INFORMATICS (DISKOMINFO) PADANG PANJANG CITY

Padang Panjang City Communication and Information Service Cyber attacks such as hacking, malware, phishing, and DDoS have the potential to disrupt services and cause theft of sensitive data. Critical data leaks can occur due to DISKOMINFO's inability to protect public and private data. The network is not strong enough to handle large data traffic, especially when the number of users increases. a structured and strategic approach to ensure that DISKOMINFO can carry out its duties efficiently and increase public trust in the services it provides. Perform regular data backups to ensure fast data recovery in cases of data leaks or loss. To handle high data traffic, update and improve network infrastructure, including increasing bandwidth. Replace outdated software and hardware with newer and more sophisticated ones. create an easily accessible public information portal with accurate and up-to-date data. DISKOMINFO can improve operational efficiency, maintain data security, and provide better services to the public and other stakeholders by implementing these solutions. Intrusion Detection System (IDS) is to have the ability to identify attack activities involving the network. If an attack is detected, they will log the attack that was carried out. Many server defense systems are manually operated by administrators, so the integrity of the system depends on how quickly the administrator can respond to a disruption. If the disruption has managed to bring the server down or the network to malfunction, which means they cannot repair the network quickly Intrusion Prevention System (IPS) is a convenience in exchanging information This is important to anticipate the threat of unauthorized misuse of resources. There are various systems. This study has been tested data security is one of the main issues in managing networks that have high traffic, such as at the DISKOMINFO Office. With the increase in cyber attacks and threats to network security, the implementation of IDS and IPS is very important to detect and prevent attacks before they can cause further damage.

Keyword : Data Security, High Traffic Network, Intrusion Detection System, Intrusion Prevention System, Padang Panjang City Communication and Information Service

ABSTRAK

IQBAL NURFARISI, PENERAPAN DATA SECURITY PADA HIGH TRAFFIC NETWORK MENGGUNAKAN METODE INTRUSION DETECTION SYSTEM (IDS) DAN INTRUSION PREVENTION SYSTEM (IPS) DI KANTOR DINAS KOMUNIKASI DAN INFORMATIKA (DISKOMINFO) KOTA PADANG PANJANG

Diskominfo Kota Padang Panjang Serangan siber seperti hacking, malware, phishing, dan DDoS berpotensi mengganggu layanan dan menyebabkan pencurian data sensitif. Kebocoran data penting dapat terjadi karena ketidakmampuan DISKOMINFO untuk melindungi data publik dan pribadi. Jaringan tidak cukup kuat untuk menangani lalu lintas data yang besar, terutama saat jumlah pengguna meningkat. Pendekatan yang terstruktur dan strategis untuk memastikan bahwa DISKOMINFO dapat melaksanakan tugasnya dengan efisien dan meningkatkan kepercayaan publik terhadap layanan yang disediakan. Melakukan backup data secara teratur untuk menjamin pemulihan data yang cepat dalam kasus kebocoran atau kehilangan data. Untuk menangani lalu lintas data yang tinggi, memperbarui dan meningkatkan infrastruktur jaringan, termasuk meningkatkan bandwidth. Mengganti perangkat lunak dan perangkat keras yang sudah usang dengan yang lebih baru dan lebih canggih. Membuat portal informasi publik yang mudah diakses dengan data yang akurat dan terkini. DISKOMINFO dapat meningkatkan efisiensi operasional, menjaga keamanan data, dan memberikan layanan yang lebih baik kepada masyarakat dan pemangku kepentingan lainnya dengan menerapkan solusi-solusi ini. Intrusion Detection System (IDS) adalah memiliki kemampuan untuk mengidentifikasi aktivitas serangan yang melibatkan jaringan. Jika serangan terdeteksi, mereka akan membuat log serangan yang dilakukan. Banyak sistem pertahanan server dioperasikan secara manual oleh administrator, sehingga integritas sistem bergantung pada seberapa cepat administrator dapat merespon gangguan. Apabila gangguan telah berhasil membuat server down atau jaringan menjadi malfungsi, yang berarti mereka tidak dapat memperbaiki jaringan dengan cepat. Intrusion Prevention System (IPS) merupakan kemudahan dalam pertukaran informasi. Hal ini yang penting dilakukan mengantisipasi ancaman penyalahgunaan sumber daya yang tidak sah. Ada berbagai sistem. Penelitian ini telah di uji coba keamanan data menjadi salah satu isu utama dalam pengelolaan jaringan yang memiliki lalu lintas tinggi, seperti di Kantor DISKOMINFO. Dengan meningkatnya serangan siber dan ancaman terhadap keamanan jaringan, penerapan IDS dan IPS sangat penting untuk mendeteksi dan mencegah serangan sebelum mereka dapat menyebabkan kerusakan lebih lanjut. Kota Padang Panjang sebagai instansi pemerintahan juga memerlukan infrastruktur jaringan yang aman untuk menjaga integritas dan kerahasiaan data publik, sehingga penelitian ini relevan untuk membantu meningkatkan keamanan sistem.

Kata Kunci : Data Security, High Traffic Network, Intrusion Detection System, Intrusion Prevention System, Diskominfo Kota Padang Panjang