# ABSTRAK

Data informasi kesehatan merupakan suatu hal yang sangat sensitif untuk disebarluaskan. Hal ini hanya perlu diketahui oleh dokter dan pihak rumah sakit. Misalnya jika informasi rekam medik pasien ini disebarluaskan maka bisa menimbulkan dampak buruk bagi si pasien, dari menjadi bahan gossip sampai bisa terkena dampak tindakan kriminal. Penelitian ini bertujuan untuk menganalisis dampak serangan MITM pada data privasi pasien yang memang tidak boleh disebarluaskan. Sejauh mana serangan ini berdampak pada privasi pasien tersebut. Terdapat tiga jenis data yaitu data HL7, data HL7 ditambahkan dengan MD5 dan data HL7 ditambah SHA512. Data kemudian dikirimkan dan diserang dengan metode serangan aktif MITM (*Man In The Middle*). Tujuan dari serangan ini adalah untuk mencuri dan memodifikasi data yang terkirim, sehingga data rekap riwayat penyakit pasien yang dilihat oleh dokter adalah data palsu yang sudah dimodifikasi oleh penyerang.

Dalam penelitian ini, pengambilan data dilakukan melalui 3 tahap skenario yaitu *phising password website* https dengan beef kali linux, kemudian dilakukan *generate* data dengan Hashcat 3.30 dan yang terakhir adalah memodifikasi data yang mengirimkan kembali ke data center.

Hasil data percobaan pada perbandingan mekanisme keamanan antara data yang tidak terlindungi dengan data yang terlindungi MD5 adalah bahwa dalam waktu 3 menit pesan yang tidak terlindungi berhasil dimodifikasi, sedangkan pesan yang terlindungi dengan hash MD5 dengan total waktu 2 menit 4,2 detik untuk melakukan *phising password* website dan *generate* hash tetapi pesan tidak berhasil dimodifikasi. Data percobaan pada perbandingan mekanisme keamanan antara MD5 dengan SHA512, menunjukkan bahwa untuk SHA512, penyerang hanya bisa melakukan *phising password* tetapi tidak bisa memodifikasi data. Sedangkan untuk MD5, selain melakukan *phising password* kemudian mencuri data, *attacker* juga mampu membaca dan memodifikasi data dengan minimum karakter data sejumlah 9 karakter dalam waktu 3 menit 3 detik, selebihnya data tetap tidak bisa di *cracked*/ dibobol sehingga tidak bisa dimodifikasi.

Kata Kunci :*MITM, phising, MD5, SHA512, HL7*

## *ABSTRACT*

*Data health information is something that is very sensitive to publish. It only needs to be known by doctors and hospitals. For example if the patient medical record information is distributed, it can cause adverse effects for the patient, of the subject of gossip to be affected by a criminal act. This study aims to analyze the impact of a MITM attack on the privacy of data of patients who did not be reproduced. The extent to which these attacks have an impact on the patient's privacy. There are three types of data are the data HL7, HL7 data is added to the MD5 and SHA512 plus HL7 Data. The data is then transmitted and attacked by the method active attack MITM (Man In The Middle). The purpose of this attack is to steal and modify the data sent, so that data recap the history of illness of patients seen by physicians is the false data that has been modified by an attacker.*

*In this study, data collection is done through three stages scenarios ie password phishing website https with beef times linux, then do generate data by Hashcat 3:30 and the last one is to modify the transmit data back to the data center.*

*The results of experimental data on comparisons between data security mechanisms that are not protected by the MD5 protected data is that within 3 minutes of unprotected messages successfully modified, while the message is protected by the MD5 hash for a total time of 2 minutes 4.2 seconds to perform password phishing website and generate hash but the message is not successfully modified. The experimental data in comparison with the security mechanisms MD5 SHA512, SHA512 showed that for, the attacker could only perform phishing password but can not modify the data. As for MD5, in addition to phishing password and then steal data, the attacker is also able to read and modify data with minimum data characters are 9 characters in 3 minutes 3 seconds, the rest of the data still can not be cracked / hacked so it can not be modified.*




*Keywords: MITM, phishing, MD5, SHA512, HL7*