p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 11 Nomor 2 Agustus 2019
Terakreditasi peringkat 3 SK. No. 28/E/KPT/2019

ANALISIS LAYANAN KEAMANAN SISTEM KARTU TRANSAKSI ELEKTRONIK MENGGUNAKAN METODE PENETRATION TESTING

Huzain Azis[1], Farniwati Fattah[2]
[1]huzain.azis@umi.ac.id, [2]farniwati.fattah@umi.ac.id
[1,2]Universitas Muslim Indonesia

Abstrak

Transaksi pembayaran ikut berkembang seiring perkembangan teknologi, saat ini teknologi mendukung transaksi pembayaran yang dilakukan secara digital, setiap jenis transaksi digital memiliki layanan keamanannya tersendiri, pada penelitian ini fokus dalam analisis layanan keamanan (*confidentiality*, *integrity* dan *availability*) menggunakan metode *Penetration Testing* pada kartu *magnetic stripe* sebagai alat transaksi pembayaran salah satu wahana permainan, kemudian membandingkan layanan keamanannya jika menggunakan alat transaksi elektronik *Radio Frequency Identification* (RFID). Hasil dari penelitian ini adalah kartu transaksi elektronik RFID memberikan layanan keamanan lebih lengkap sebagai alat transaksi elektronik pembayaran pada wahana.
Kata kunci: transaksi pembayaran elektronik, *magnetic stripe*, *radio frequency identification (*RFID*)*, *penetration testing*, layanan keamanan.

Abstract

Payment transactions developed along with technological developments, now days technology supports digital payment, each type of digital transaction has its own security services, this study focus on the analysis of security services (confidentiality, integrity and availability) using the Penetration Testing method on magnetic stripe cards as a payment transaction playground facility, then comparing security services to the Radio Frequency Identification (RFID) electronic transaction tool. The results of this study are RFID electronic transaction cards that provide a more complete security service as an electronic payment transaction.
Keywords: electronic payment transaction, magnetic stripe, radio frequency identification (RFID), penetration testing, security services.

1. Pendahuluan

Teknologi yang semakin canggih telah memberi banyak kemudahan di masa kini, baik layanan penyimpanan, pengolahan hingga pengamanan data[1][2]. Saat ini teknologi telah masuk dan berperan banyak dalam dunia transaksi, terutama pada layanan transaksi elektronik. namun masalah keamanan sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi[3]. teknologi yang digunakan sebagai alat transaksi elektronik diantaranya yaitu *Magnetic Stripe Card* dan *Radio Frequency Identification*. Contoh alat transaksi konvensional menggunakan koin seperti yang ditunjukkan pada Gambar 1 kini telah ditinggalkan secara perlahan, dan beralih ke metode pembayaran digital seperti yang di perlihatkan pada Gambar 2.

(a) (b)

Gambar 1. (a) contoh alat pembayaran dan (b) alat transaksi pembayaran konvensional

Magnetic Stripe Card adalah tipe kartu yang mampu menyimpan data dengan memodifikasi daya magnet dari partikel kecil magnetik berbasis besi pada pita dari material magnetik di

DOI: http://dx.doi.org/10.33096/ilkom.v11i2.447.167-174

p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 11 Nomor 2 Agustus 2019
Terakreditasi peringkat 3 SK. No. 28/E/KPT/2019

kartu. *Magneticstripe*, terkadang disebut *magstripe*. *Magnetic Stripe Card* umumnya digunakan pada kartu debit, kredit, maupun kartu identitas. *Radio Frequency Identification* (RFID) merupakan sebuah teknologi yang menggunakan metoda auto-ID atau *Automatic Identification*. Auto-ID adalah metode pengambilan data dengan identifikasi objek secara otomatis tanpa ada keterlibatan manusia. Auto-ID bekerja secara otomatis sehingga dapat meningkatkan efisiensi dalam mengurangi kesalahan dalam memasukkan data. Gambar 2(a) menunjukkan alat pembayaran dan Gambar 2(b) sebagai alat transaksi pembayarannya.

(a) (b)

Gambar 2. (a)contoh alat pembayaran dan (b) alat transaksi pembayaran digital

Pada keamanan informasi, dikenal istilah CIA yakni *Confidentiality*, *Integrity*, dan *Availability* sebagai jantung dari keamanan informasi[4]. Berdasarkan ISO27000, *Confidentiality* atau kerahasiaan dalam hal ini adalah informasi yang kita miliki pada sistem atau database kita yang sifatnya rahasia sehingga pengguna atau orang yang tidak berkepentingan tidak dapat melihat/mengaksesnya. *Integrity* adalah menjamin konsistensi data terhadap semua konstrain yang diberlakukan terhadap data tersebut, sehingga memberikan jaminan keabsahan data itu sendiri. sedangkan *Availability* adalah memastikan sumber daya yang ada siap diakses kapanpun oleh user, application atau sistem yang membutuhkannya.

Penetration Testing, atau pentesting merupakan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, untuk menilai apa yang mungkin didapat oleh penyerang setelah eksploitasi sukses.

Penelitian ini akan mencoba untuk menganalisis layanan keamanan dengan penerapan metode Penetration Testing pada MagneticStripeCard sebagai alat transaksi elektronik yang telah digunakan oleh beberapa penyedia usaha wisata permainan dan membandingkan layanan yang dapat diimplementasikan oleh RFID pada objek yang sama. keluaran yang diharapkan dari hasil penelitian ini adalah perbandingan layanan postur keamanan yang tersedia serta saran solusi bagi layanan keamanan yang masih rentan.

2. Metode

2.1 Security Services

Seorang professional dalam bidang keamanan informasi akan berfokus untuk mencapai dan melindungi *Confidentiality, Integrity*, dan A*vailability* (CIA)[5]. Ketiga hal tersebut merupakan prinsip dasar pada keamanan informasi. Ketika kita ingin membangun sebuah sistem yang aman, ketiga hal tersebutlah yang dijadikan sebagai acuan yang harus dicapai dan dilindungi. Berikut 3 prinsip dasar keamanan informasi tersebut satu per satu secara lebih mendalam[4].

1. *Confidentiality*

   Maksudnya secara singkat sama dengan arti katanya yaitu kerahasian. Kerahasian dalam hal ini adalah informasi yang kita miliki pada sistem/database kita, serta pengguna atau orang yang tidak berkepentingan tidak dapat melihat/mengaksesnya. Salah satu layanan *Confidentiality* adalah dengan menerapkan enkripsi. Enkripsi merupakan sebuah teknik untuk mengubah file/data/informasi dari bentuk yang dapat dimengerti (*plaintext*) menjadi bentuk yang tidak dapat dimengerti (*ciphertext*)[6],. Enkripsi harus dilakukan pada level media penyimpanan dan transmisi data. Sedangkan ilmu yang mempelajari

DOI: http://dx.doi.org/10.33096/ilkom.v11i2.447.167-174

mengenaultehnik untuk menemukan atau mengembalikan kunci rahasia disebut dengan *cryptanalysis*[7].

2. *Integirity*

   Integrity maksudnya adalah data tidak dirubah dari aslinya oleh orang yang tidak berhak, sehingga konsistensi, akurasi, dan validitas data tersebut masih terjaga. Dengan bahasa lain, *integrity* mencoba memastikan data yang disimpan benar adanya, tidak ada pengguna yang tidak berkepentingan atau *software* berbahaya yang mengubahnya.

3. *Availability*

   Maksud dari *availability* adalah memastikan sumber daya yang ada siap diakses kapanpun oleh user/application/sistem yang membutuhkannya. Sama seperti aspek integrity, rusaknya aspek availability dari sistem juga bisa diakibatkan karena faktor kesengajaan dan faktor accidental (kecelakaan).

2.2 Penetration Testing

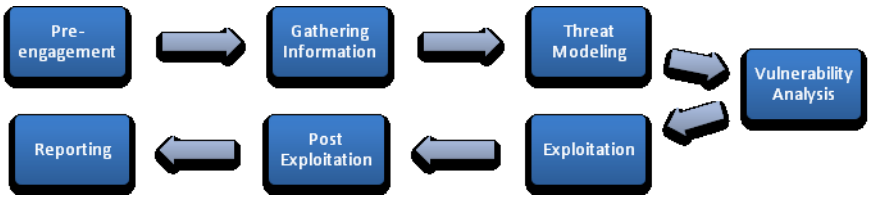
Penetration Testing, atau *pentesting*, melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan[8]. Pada pentest, penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, untuk menilai apa yang mungkin didapat oleh penyerang setelah eksploitasi sukses[9].

1. Tahapan Uji Penetrasi

   Pentesting dimulai dengan fase *pre-engagement*, yang melibatkan klien tentang tujuan mereka untuk *pentest*, memetakan lingkup (tingkat dan parameter tes), dan seterusnya. Ketika pentester dan klien menyetujui ruang lingkup, format pelaporan, dan topik lainnya, pengujian yang sebenarnya dimulai.

   Dalam fase *Gathering-Information*, *pentester* mencari informasi yang tersedia secara umum tentang klien dan mengidentifikasi cara-cara potensial untuk terhubung ke sistemnya. Dalam fase *Threat-Modeling*, penguji menggunakan informasi ini untuk menentukan nilai setiap temuan dan dampaknya bagi klien jika temuan tersebut memungkinkan penyerang untuk membobol sistem. Evaluasi ini memungkinkan *pentester* untuk mengembangkan rencana aksi dan metode serangan.

   Sebelum *pentester* dapat mulai menyerang sistem, dia melakukan *Vulnerability Analysis*[10]. Pada fase ini, pentester berupaya menemukan kerentanan dalam sistem yang dapat dimanfaatkan dalam fase *exploitation*. Eksploitasi yang berhasil dapat menyebabkan fase *Post-Exploitation*, di mana hasil eksploitasi dimanfaatkan untuk menemukan informasi tambahan, data sensitif, akses ke sistem lain, dan sebagainya. Akhirnya, dalam fase *Reporting*, *pentester* merangkum temuan untuk para eksekutif dan praktisi teknis. Gambar 3 menunjukkan tahapan-tahapan uji penetrasi.



Gambar 3. Tahapan uji penetrasi

a. *Pre-engagement*

   Sebelum pentest dimulai, pentester melakukan interaksi pre-engagement dengan klien untuk memastikan semua orang berada di halaman yang sama tentang pengujian penetrasi. Miskomunikasi antara pentester dan klien yang mengharapkan pemindaian kerentanan sederhana dapat menyebabkan situasi yang sulit karena tes penetrasi jauh lebih mengganggu.

   Tahap *pre-engagement* adalah kapan harus meluangkan waktu untuk memahami sasaran bisnis klien untuk pentest. Jika ini adalah pentest pertama mereka, apa yang mendorong mereka untuk menemukan pentester? Eksposur apa yang paling mereka khawatirkan? Apakah mereka memiliki perangkat rapuh yang perlu Anda berhati-hati saat melakukan pengujian?

b. *Gathering Information*

Selanjutnya adalah fase Gathering-Information. Selama fase ini, Anda menganalisis sumber informasi yang tersedia secara bebas[11], suatu proses yang dikenal sebagai pengumpulan *intelijen sumber terbuka (OSINT)*. Anda juga mulai menggunakan alat seperti pemindai port untuk mendapatkan ide tentang sistem apa yang ada di Internet atau jaringan internal serta perangkat lunak apa yang sedang berjalan.

c. *Threat-Modeling*

Berdasarkan pengetahuan yang diperoleh dalam fase *Gathering-Information*, Pentester beralih ke *Threat-Modeling*. Di sini berpikir seperti penyerang dan mengembangkan rencana serangan berdasarkan informasi yang dapat dikumpulkan. Sebagai contoh, jika klien mengembangkan perangkat lunak berpemilik, penyerang dapat merusak organisasi dengan mendapatkan akses ke sistem pengembangan internal mereka, di mana kode sumber dikembangkan dan diuji, dan menjual rahasia dagang perusahaan kepada pesaing. Berdasarkan data yang Pentester temukan selama pengumpulan informasi, Pentester mengembangkan strategi untuk menembus sistem klien.

d. *Vulnerability Analysis*

Selanjutnya, pentester mulai aktif menemukan kerentanan untuk menentukan seberapa sukses strategi mengeksploitasi mereka. Kegagalan yang gagal dapat merusak layanan, memicu peringatan deteksi gangguan, dan sebaliknya merusak peluang Anda untuk mengeksploitasi yang sukses. Seringkali selama fase ini, pentester menjalankan pemindai kerentanan, yang menggunakan database kerentanan dan serangkaian pemeriksaan aktif untuk membuat perkiraan terbaik tentang kerentanan yang ada pada sistem klien. Tetapi meskipun pemindai kerentanan adalah alat yang kuat, mereka tidak dapat sepenuhnya mengganti pemikiran kritis, jadi Pentester juga melakukan analisis manual dan memverifikasi hasil sendiri dalam fase ini juga.

e. *Exploitation*

Sekarang tahap ini menjalankan eksploitasi terhadap kerentanan yang Pentester temukan (terkadang menggunakan alat seperti Metasploit) dalam upaya untuk mengakses sistem klien. Seperti yang Anda lihat, beberapa kerentanan akan sangat mudah dieksploitasi, seperti masuk dengan kata sandi default.

f. *Post Exploitation*

Setelah pasca eksploitasi, tahap ini mengumpulkan informasi tentang sistem yang diserang, mencari file yang menarik, mencoba untuk meningkatkan hak istimewa Pentester jika perlu, dan seterusnya. Misalnya, Pentester mungkin membuang hash kata sandi untuk melihat apakah Pentester dapat membalikkan atau menggunakannya untuk mengakses sistem tambahan. Pentester mungkin juga mencoba menggunakan mesin yang dieksploitasi untuk menyerang sistem yang sebelumnya tidak tersedia bagi Pentester dengan *memutar* ke dalamnya.

g. *Reporting*

Fase terakhir dari pengujian penetrasi adalah pelaporan. Di sinilah Pentester menyampaikan temuan Pentester kepada pelanggan dengan cara yang berarti. Pentester memberi tahu mereka apa yang mereka lakukan dengan benar, di mana mereka perlu meningkatkan postur keamanan mereka, bagaimana Anda masuk, apa yang Anda temukan, cara memperbaiki masalah, dan sebagainya

2.3 Magnetic Stripe Card

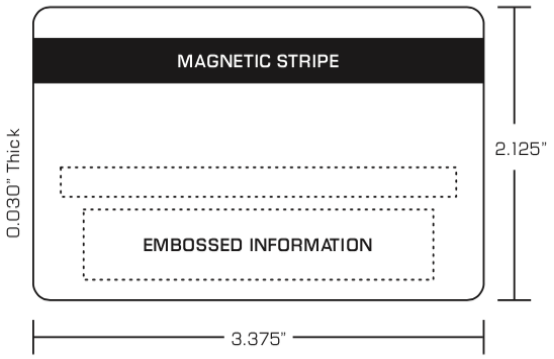
Magnetic Stipe, atau pita magnetic merupakan salah satu teknologi yang digunakan untuk menyimpan data dengan memanfaatkn medan magnet berupa pita, teknologi ini terkadang digunakan pada kartu yang disebut dengan magneticstipecard dan menggunakan magneticstripereader dan writer sebagai alat untuk menulis atau membaca informasi pada pita magnetic[12].

Kartu *Magnetic Stripe* adalah jenis kartu yang mampu menyimpan data dengan memodifikasi magnet dari partikel-partikel magnetik sis besi kecil pada bahan magnetik pada kartu. Garis magnetik, kadang-kadang disebut kartu gesek atau *magstripe*, dibaca dengan menggesek melewati kepala pembacaan magnetic[13]. Kartu strip magnetik umumnya digunakan dalam kartu kredit, kartu identitas, dan tiket transportasi. Gambar 4 Menunjukkan

p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 11 Nomor 2 Agustus 2019
Terakreditasi peringkat 3 SK. No. 28/E/KPT/2019

Ukuran kartu *Magnetic Stripe Card*. Penyimpanan pada *Magnetic Stripe Card* umumnya terdapat 3 *track*, setiap *track* memiliki ukuran penyimpanan yang berbeda. Gambar 5 menunjukkan *track* penyimpanan pada *Magnetic Stirpe Card*.



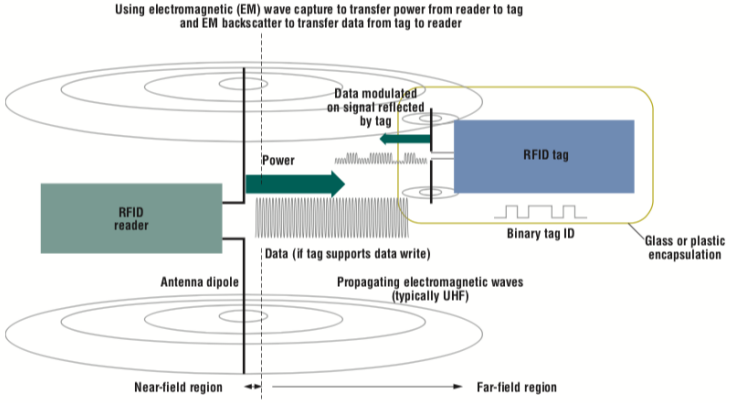
Gambar 4. Ukuran *Magnetic Stirpe Card*

	Track		Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	1	IATA	210	7 bits per character	79 alphanumeric characters
0.110"	2	ABA	75	5 bits per character	40 numeric characters
0.110"	3	THRIFT	210	5 bits per character	107 numeric characters

Gambar 5. Track Penyimpanan *Magnetic Stripe Card*

2.4 RFID.

RFID adalah teknologi penangkapan data yang dapat digunakan secara elektronik untuk mengidentifikasi, melacak dan menyimpan informasi yang sebelumnya tersimpan dalam idtag dengan menggunakan gelombang radio. RFID adalah sebuah metode identifikasi secara otomatis dengan menggunakan suatu piranti yang disebut RFID tag atau transporder. Data yang ditransmisikan dapat berupa kode–kode yang bertujuan mengidentifikasi suatu objek tertentu. Pada RFID proses identifikasi dilakukan oleh RFID reader dan RFID tag.



Gambar 6. proses pembacaan RFID[14]

RFID tag diletakkan pada suatu benda atau objek yang akan diidentifikasi. Tiap-tiap RFID tag memiliki data angka identifikasi (ID number) yang unik, sehingga tidak ada RFID tag yang memiliki ID number yang sama. Gambar 6 menunjukkan proses pembacaan pada RFID.

3. Hasil dan Pembahasan

Berikut adalah penjabaran hasil 7 langkah penerapan penetration testing

1. *Pre-engagement*

   Tahap ini merupakan tahap wawancara dengan pengelola objek penelitian, Tabel 1 menunjukkan 3 pertanyaan inti sebagai bagian proses penelitian

DOI: http://dx.doi.org/10.33096/ilkom.v11i2.447.167-174

p-ISSN 2087-1716
e-ISSN 2548-7779

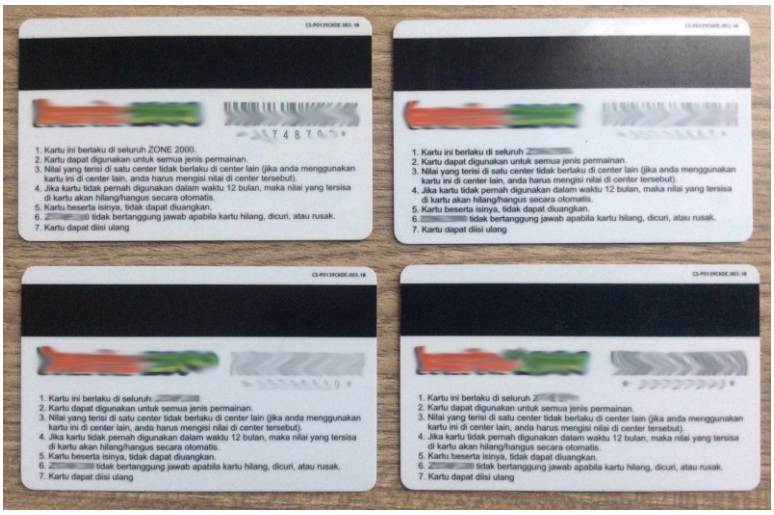
ILKOM Jurnal Ilmiah Volume 11 Nomor 2 Agustus 2019
Terakreditasi peringkat 3 SK. No. 28/E/KPT/2019

Tabel 1. Daftar inti pertanyaan tahap pre-engagement

No	Pertanyaan	Jawaban
1	kapan harus meluangkan waktu untuk memahami sasaran bisnis klien untuk pentest?	Waktu yang dapat diluangkan untuk melakukan pengujian yaitu pada: Jam\hari S S R K J S M 09.00-12.00 ok ok ok ok ok ok - 12.00-15.00 ok - - - - - - 15.00-18.00 - - - - - - - 18.00-21.30 ok - ok - - - -
2	Eksposur apa yang paling mereka khawatirkan	Keseluruhan sistem bermasalah pada saat proses pengujian
3	Apakah mereka memiliki perangkat rapuh yang perlu Anda berhati-hati saat melakukan pengujian	Daftar perangkat, fungsi dan perizinannya: No Perangkat Fungsi Izin 1 Sofware Sistem transaksi Tidak 2 Hardware Sistem pembayaran Iya

2. Gathering Information

Setelah mengetahui batasan-batasan yang dapat dilakukan dalam melakukan pengujian, data yang dikumpulkan adalah 4 kartu alat pembayaran, 2 kartu dengan saldo 50.000 dan 2 karto dengan saldo 100.000. Gambar 7 menunjukkan 4 kartu yang dikumpulkan.



Gambar 7. Data awal pengujian

3. Threat Modeling

Sebelum melihat model ancaman, hal yang dilakukan selanjutnya adalah pembacaan isi kartu magneticstripe dari data yang telah di kumpulkan. Tabel 2 menunjukkan isi pembacaan kartu objek penelitian dan Gambar 8. Merupakan kartu yang digunakan.

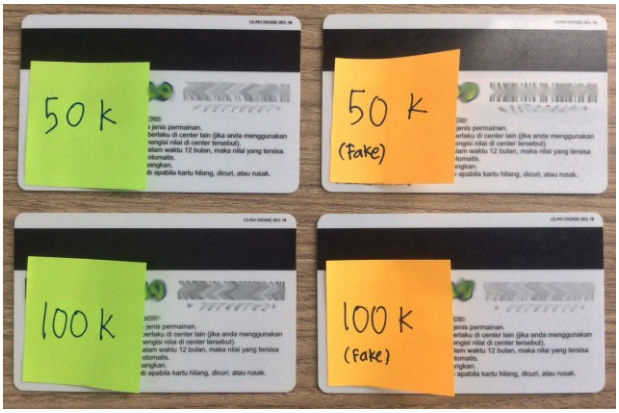
Tabel 2.Daftar hasil pembacaan kartu objek penelitian

No	Saldo	Track 1	Track 2	Track 3
1	50.000	%ATNDG349IROER?	;542876498?	;990076454?
2	50.000	%A235443SDG234?	;096375357?	;565211765?
3	100.000	%DTBF4532GF466?	;985763451?	;545533984?
4	100.000	%7KDCW388223DA?	;098876342?	;989064653?

DOI: http://dx.doi.org/10.33096/ilkom.v11i2.447.167-174

p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 11 Nomor 2 Agustus 2019
Terakreditasi peringkat 3 SK. No. 28/E/KPT/2019



Gambar 8. Data Uji

Tabel 3 menunjukkan layanan keamanan sementara pada kartu magneticstripe. Hasil pembacaan data yang di enkripsi menunjukkan bahwa layanan keamanan confidentiality ada pada kartu objek penelitian.

Tabel 3. Layanan Keamanan pada objek penelitian

No.	Layanan Keamanan	Objek Magnetic Stripe
1	*Confidentiality*	Ya
2	*Integrity*	?
3	*Availability*	?

4. *VulnerabilityAnalysis*

Berdasarkan hasil analisis awal pada pembacaan kartu, maka peluang yang dapat dilakukan yaitu pengujian pada layanan integrity dan availabilitynya.bentuk pengujiannya di tunjukkan pada Tabel 4.

Tabel 4. Daftar pengujian layanan keamanan yang akan dilakukan.

No	Layanan Keamanan	Bentuk Pengujian
1	*Integrity*	Menggandakan isi kartu pada kartu yang lain
2	*Availability*	• Mencoba kartu pada host sama dilokasi berbeda • Mencoba kartu pada host yang berbeda

5. *Exploitation*

Tahap exploitation dilakukan untuk dua layanan keamanan yaitu integrity dan availability, Tabel 5. Menunjukkan bahwa setelah proses pengujian di ketahuiisi kartu dapat dirubah, dan dapat digandakan serta kartu fake dapat digunakan layaknya kartu original.

Tabel 5.Pengujian integrity data

No	Jenis	Saldo	Track 1	Track 2	Track 3	Pengujian penggunaan
1	Original	50.000	%ATNDG349IROER?	;542876498?	;990076454?	Berhasil
2	Fake	50.000	%ATNDG349IROER?	;542876498?	;990076454?	Berhasil
3	Original	100.000	%DTBF4532GF466?	;985763451?	;545533984?	Berhasil
4	Fake	100.000	%DTBF4532GF466?	;985763451?	;545533984?	Berhasil

Tahap exploitation selanjutnya untuk menguji ketersediaan data, Tabel 6 menunjukkan percobaan yang dilakukan yaitu kartu dapat digunakan sesuai aturan yang berlaku, yaitu dapat digunakan di host yang sama dan dilokasi berbeda juga tidak dapat digunakan pada host berbeda.

Tabel 6. Pengujian avalability data

No	Jenis	Saldo	Host Sama Lokasi Berbeda	Host Berbeda
1	Original	50.000	Berhasil	Gagal
2	Fake	50.000	Berhasil	Gagal
3	Original	100.000	Berhasil	Gagal
4	Fake	100.000	Berhasil	Gagal

DOI: http://dx.doi.org/10.33096/ilkom.v11i2.447.167-174

6. *PostExploitation*

Setelah melakukan pengujian, kesimpulan selanjutnya layanan keamanan pada objek hanya terdapat pada confidentiality dan availability, namun tidak pada integrity, karena sistem masih belum membedakan kartu ori dan fake. Tabel 7 menunjukkan daftar layanan keamanan pada objek penelitian

Tabel 7. Layanan keamanan objek penelitian

No.	Layanan Keamanan	Objek MagneticStripe
1	Confidentiality	Ya
2	Integrity	Tidak
3	Availability	Ya

7. *Reporting*

Dua layanan coonfidentiality yang dimiliki oleh objek penelitian cukup untuk standar layanan keamanan, namun jika layanan keamanan integritas data juga ingin di terapkan maka saran yang dapat ditawarkan yaitu dengan mengganti penerapan penggunaan kartu magneticstripe menjadi RFID. Karena konsep keamanan pada sistem yang diterapkan pada kartu magneticstripe sama dengan RFID, perubahan sistem cukup pada sisi hardware saja tidak pada sisi softwarenya. Tabel 8 menunjukkan perbandingan layanan keamananmagneticstripe dan RFID

Tabel 8. PerbandinganLayanan Keamanan Objek penelitian

No.	Layanan Keamanan	MagneticStripe	RFID
1	Confidentiality	Ya	Ya
2	Integrity	Tidak	Ya
3	Availability	Ya	Ya

4. Kesimpulan dan Saran

Setelah melakukan analisis layanan keamanan data pada objek penelitian magneticstripe melalui 7 tahap metode penetration testing dapat di simpulkan bahwa layanan keamanan yang ada pada kartu magneticstripe adalah confidentiality dan availability, layanan keamanan tersebut cukup aman dalam penggunaan transaksi dilokasi tersebut, namun jika layanan integritas data juga ingin diterapkan maka diperlukan penggantian dari sisihardware, yaitu RFID tag untuk alat pembayarannya dan RFID reader untuk alat transaksinya.

Daftar Pustaka

[1] H. Azis, “Penerapan Modifikasi Lack Steganography Dan Layanan Message Authentication Code Pada Komunikasi Multimedia,” 2013.
[2] Y. Salim and H. Azis, “Metode Digital Watermark Pada File Penelitian Dosen,” *Ilk. J. Ilm.*, vol. 9, no. 2, pp. 161–166, 2017.
[3] F. Muharram, H. Azis, and A. R. Manga, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES),” *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.
[4] W. C. Easttom, *Computer Security Fundamentals*, 3rd ed. United States of America: PEARSON, 2011.
[5] C. Meijer and R. Verdult, “Ciphertext-only cryptanalysis on hardened Mifare classic cards,” *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 2015-Octob, pp. 18–30, 2015.
[6] W. D. Wallis, *Mathematics in the Real World*. London: Birkhausher, 2013.
[7] R. Verdult, “A Toolbox for RFID Protocol Analysis,” *CCS’15*, 2009.
[8] I. B. Ryzhkov and O. N. Isaev, “Current Status and Trends in Cone Penetration Testing of Soil,” *Springer Sci. Media New York*, vol. 52, no. 3, pp. 31–32, 2015.
[9] G. Weidmen, *Penetration Testing - A hands-on introduction to Hacking.pdf*. USA: No Starch Press, Inc., 2014.
[10] S. P. Oriyano, *CEHv9 Certified Ethical Hacker Version 9 Study Guide*. 2016.
[11] S. A. Rahalkar, *Certified Ethical Hacker (CEH) Foundation Guide*. 2016.
[12] Silicon Labs, *Magnetic Stripe Reader*. 2008.
[13] Magtek, “Dimensions - Financial Transaction Cards Magnetic Stripe Encoding - Financial Transaction Cards Card Data Format - Track 1 Card Data Format - Track 2 Card Data Format - Track 3 (ISO 4909),” *MagTek Inc. P/N 99800004 Rev. 1.03 11/0*, no. Cvv, pp. 2–3, 2011.
[14] R. Want, “An Introduction to RFID,” *IEEE CS IEEE ComSoc*, vol. 4, no. 8, pp. 25–33, 2016.

