Implementasi Metode *Penetration Testing* pada Layanan Keamanan Sistem Kartu Transaksi Elektronik Wahana Permainan

Implementation of Penetration Testing Methods in Game Vehicle Electronic Transaction Card System Security Services

Farniwati Fattah[1], Aulia Maharani[2*], Huzain Azis[3]
[1,2,3]Fakultas Ilmu Komputer, Universitas Muslim Indonesia
E-mail: [1]farniwati.fattah@umi.ac.id, [2]13020200215@umi.ac.id, [3]huzain.azis@umi.ac.id
*Penulis Korespondensi

Abstrak

Penggunaan kartu *magnetic stripe* pada wahana permainan rentan terhadap akses yang tidak sah, seperti *skimming*, yang dapat merugikan pengelola dan penyedia wahana. *Penetration testing* merupakan metode yang dapat digunakan untuk mengidentifikasi dan eksploitasi kerentanan. Pada pengujian *penetration testing* terdapat tujuh fase yang digunakan yaitu *pre-engagement, information gathering, threat modeling, vulnerability analysis, exploitation, post exploitation,* dan *reporting*. Dalam Penelitian sebelumnya menunjukkan bahwa komunikasi antara *magnetic stripe reader* dan komputer utama dilakukan melalui koneksi kabel, yang menghasilkan layanan *confidentiality* dan *availability*. Namun, pada penelitian ini, pengimplementasian *penetration testing* menggunakan koneksi nirkabel menghasilkan temuan bahwa layanan keamanan yang tersedia adalah *availability*. Oleh karena itu, dapat disimpulkan bahwa komunikasi baik melalui koneksi kabel maupun nirkabel tidak terdapat layanan keamanan *integrity*. Rekomendasi bagi penyedia layanan untuk meningkatkan kemanan kartu di lokasi tersebut dengan menerapkan enkripsi data.

Kata kunci: pengujian penetrasi, kartu strip magnetik, layanan keamanan

Abstract

The use of magnetic stripe cards on game rides is vulnerable to unauthorized access, such as skimming, which can be detrimental to ride managers and providers. Penetration testing is a method that can be used to identify and exploit vulnerabilities. In penetration testing, there are seven phases used, namely pre-engagement, information gathering, threat modeling, vulnerability analysis, exploitation, post exploitation, and reporting. Previous research shows that communication between the magnetic stripe reader and the main computer is carried out via a cable connection, which results in confidentiality and availability services. However, in this research, implementing penetration testing using a wireless connection resulted in the finding that the security services available were availability. Therefore, it can be concluded that communication whether via wired or wireless connections does not provide integrity security services. Recommendations for service providers to increase card security at these locations by implementing data encryption.

Keywords: penetration testing, magnetic stripe card, security services

1. PENDAHULUAN

Seiring perkembangan teknologi, transaksi elektronik telah menjadi metode pembayaran yang populer dan nyaman. Teknologi yang semakin canggih memberi banyak kemudahan di masa kini, baik layanan penyimpanan, pengolahan, dan pengamanan data [1]. Salah satunya pada sektor hiburan seperti wahana permainan. Namun, dengan meningkatnya penggunaan sistem transaksi

elektronik. Penyedia layanan dan pengelola wahana perlu memperhatikan masalah keamanan sistem informasi atau teknologi yang dimilikinya. Salah satu tindak kejahatan yang paling umum adalah *skimming*. Teknik *skimming* adalah tindakan atau upaya seseorang untuk meretas data yang terdapat pada strip magnetik kartu agar pelaku dapat mengetahui data dari korban. Selanjutnya setelah melakukan teknik tersebut, pelaku dapat mengakses data korban secara ilegal [2].

Sebagai upaya meminimalisir risiko terhadap layanan keamanan yang dimiliki kartu tersebut, maka langkah yang dapat dilakukan dengan mengevaluasi layanan keamanan pada kartu tersebut. Oleh karena itu perlu dilakukan pengujian berupa *penetration testing* yang dimana kegiatan tersebut dilakukan sebagai langkah untuk identifikasi dan eksploitasi kerentanan [3]. *Penetration testing*, atau *pentesting*, melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan [4]. Pada pengujian *penetration testing* terdapat tujuh fase yang digunakan yaitu *pre-engagement, information gathering, threat modelling, vulnerability analysis, exploitation, post exploitation,* dan *reporting*.

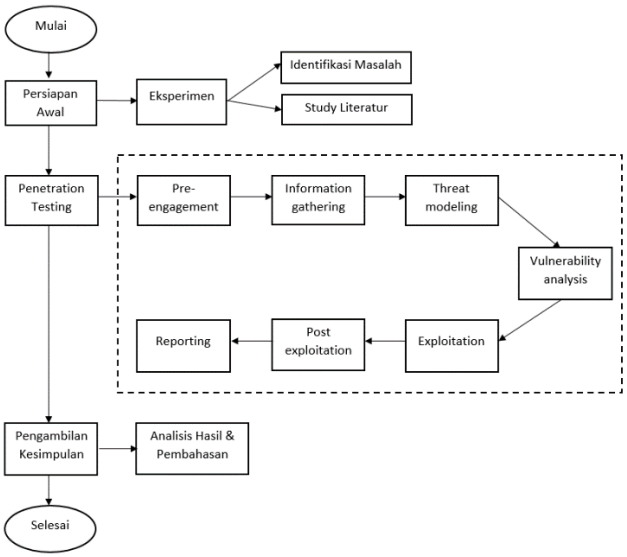
Teknologi yang digunakan sebagai alat transaksi elektronik pada wahana permainan yaitu *Magnetic Stripe Card*. *Magnetic stripe card* adalah jenis kartu yang dapat menyimpan data dengan memodifikasi daya magnet dari partikel kecil magnetik berbasis besi pada pita dari material magnetik di kartu [5]. *Magnetic stripe card* umumnya digunakan pada kartu kredit, kartu identitas, dan kartu wahana permainan. Teknologi kartu magnetik ini secara inheren tidak aman karena kartu menyimpan data-data sehingga mudah dibaca oleh alat pembaca (*magnetic stripe reader*) manapun.

Terdapat penelitian terdahulu yang serupa yang telah dilakukan, yaitu menganalisis layanan keamanan yang ada pada kartu transaksi elektronik menggunakan metode *penetration testing*. Layanan keamanan yang dianalisis antara lain adalah *confidentiality*, *integrity*, dan *availability*. Hasil dari penelitian ini menunjukkan bahwa layanan keamanan yang cukup aman pada penggunaan kartu transaksi di lokasi tersebut adalah *confidentiality* dan *availability* [6].

Berdasarkan penelitian serupa yang telah dilakukan sebelumnya, layanan keamanan (*confidentiality, integrity,* dan *availability*) menjadi hal yang menarik untuk diteliti. Cara terbaik yang dapat dilakukan dengan pengujian penetrasi, karena dengan pengujian tersebut dimungkinkan untuk menemukan kerentanan baru. Hal dasar yang menjadi perbedaan antara penelitian sebelumnya dengan peneliti yang akan diangkat adalah komunikasi antara *magnetic stripe reader* yang ada di wahana dengan komputer utama. Dimana, penelitian sebelumnya berkomunikasi menggunakan kabel sedangkan pada penelitian ini menggunakan komunikasi nirkabel. Oleh karena itu, penelitian ini bertujuan untuk merumuskan masalah tentang bagaimana cara menganalisis layanan keamanan sistem kartu transaksi elektronik pada wahana permainan terutama dalam konteks penggunaan komunikasi nirkabel, dengan mengimplementasikan metode *penetration testing*.

2. METODE PENELITIAN

Metode penelitian merupakan suatu cara atau teknik untuk memperoleh informasi dan sumber data yang akan digunakan pada penelitian. Selain itu, metodologi penelitian juga dapat diperoleh melalui media daring ataupun elekronik [7]. Tahapan penelitian yang dilakukan peneliti ditunjukkan pada Gambar 1.



Gambar 1. Tahapan penelitian

2.1 Persiapan Awal

Penelitian ini menggunakan metode eksperimen, karena penelitian ini bertujuan untuk mengetahui kerentanan kartu saat diberi beberapa serangan dengan mengikuti prosedur *penetration testing.*

2.1.1 Identifikasi Masalah

Pada tahapan pertama peneliti melakukan identifikasi masalah terlebih dahulu bertujuan untuk menganalisa celah keamanan pada kartu transaksi wahana permainan. Pada penelitian ini berusaha untuk mencoba mengidentifikasi masalah pada kartu transaksi *magnetic stripe* melalui sudut pandang layanan keamanan yang disediakan.

1. Ancaman Terhadap Sistem Informasi

   Ancaman adalah suatu tindakan atau peristiwa yang dapat merugikan perusahaan [8]. Kerugian dapat mencakup uang, tenaga, peluang bisnis, reputasi perusahaan bahkan mungkin dapat menyebabkan pailit. Menurut W. Stallings ada beberapa kemungkinan ancaman [9], yaitu:

   - *Interruption*, perangkat sistem rusak atau menjadi tidak tersedia.
   - *Interception*, pengaksesan informasi oleh pihak yang tidak berwenang.
   - *Modification*, pihak yang tidak memiliki wewenang tidak hanya mengakses informasi tetapi juga melakukan perubahan terhadap informasi.
   - *Fabrication*, penyisipan objek palsu ke dalam sistem oleh pihak yang tidak berwenang.

2. Keamanan Informasi

   Aset informasi yang terdiri dari *hardware*, *software*, sistem informasi, dan manusia merupakan aset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak hanya disandarkan pada alat atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi [10]. Prinsip keamanan informasi yaitu:

   a. *Confidentiality* (Kerahasiaan)

   Menjamin kerahasiaan data atau informasi, memastikan hanya orang berwenang yang mempunyai akses terhadap sistem informasi tersebut dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

   b. Integrity (Integritas)

Menjamin bahwa data tidak diubah tanpa adanya izin dari pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.

c. Availability (Ketersediaan)

Menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait [11].

d. Authentication (Autentikasi)

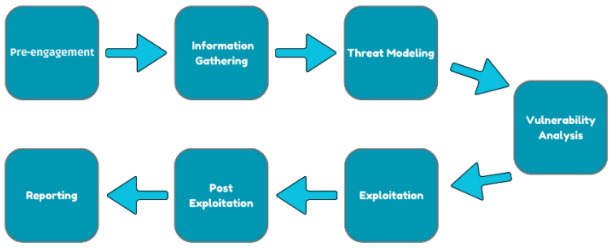
Merupakan aspek keamanan yang terjadi saat sistem dapat membuktikan bahwa pengguna yang sedang mengklaim identitas merupakan pengguna yang sah, yang memang memiliki identitas tersebut [12].

2.1.2 Studi Literatur

Tahapan kedua bertujuan untuk menyusun dasar teori yang digunakan dalam melakukan penelitian. Diantaranya mengenai *penetration testing*, *magnetic stripe car*d, dan layanan keamanan. studi literatur pada penelitian ini dilakukan dari berbagai sumber, diantaranya e-book dan jurnal penelitian.

2.2 Penetration Testing

Penetration testing, atau *pentesting*, melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan [4]. *Penetration testing* memberikan hasil terperinci mengenai ancaman keamanan yang berisiko adanya eksploitasi apabila diimplementasikan ke dalam keamanan pada organisasi. Pengujian penetrasi membantu pihak terkait untuk melakukan identifikasi kerentanan potensial yang cepat dan akurat [13]. Hasil evaluasi pengujian keamanan sistem dari metode pengujian penetrasi yang berhasil diidentifikasi atau dieksploitasi akan dikumpulkan dan diberikan kepada administrator, pemilik organisasi, atau pengelola sistem organisasi dengan tujuan memberi mereka rekomendasi untuk membuat keputusan dan memprioritaskan upaya untuk meningkatkan keamanan dan perlindungan sistem [14]. Tahapanan uji penetrasi ditunjukkan pada Gambar 2.



Gambar 2. Tahap uji penetrasi

A. *Pre-engagement*

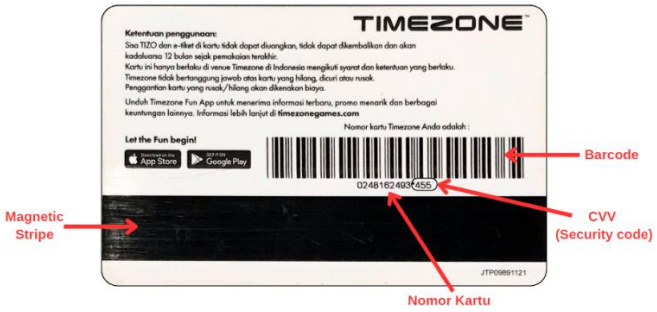
Tahap ini merupakan bagian wawancara terkait tujuan dari penelitian dan menentukan pertanyaan mengenai gambaran umum kartu [15] *magnetic stripe* dengan daftar pertanyaan disesuaikan berdasarkan kasus yang diangkat. Pada tahap ini peneliti memberikan beberapa pertanyaan umum untuk mempermudah proses wawancara mengenai kartu transaksi *magnetic stripe.*

Tabel 1. Daftar inti pertanyaan tahap *pre-engagement*

No	Pertanyaan
1	Bagaimana mekanisme dan sistem pengamanan yang diterapkan pada kartu transaksi *magnetic stripe* pada umumnya ?
2	Eksposur apa yang perlu dikhawatirkan pada kartu?
3	Apa yang menjadi risiko keamanan yang paling sering terjadi pada kartu transaksi?
4	Data apa yang umumnya tersimpan dalam kartu transaksi?
5	Apakah diperlukan prosedur pemulihan data yang baik jika terjadi pelanggaran keamanan?

B. *Information Gathering*

Tahap ini merupakan tahap pengumpulan data atau informasi yang bersifat terbuka pada pihak terkait dengan sistem yang akan diuji [16]. Pada tahap ini peneliti melakukan pengumpulan informasi berupa jenis kartu timezone, jumlah track serta track yang digunakan pda kartu tersebut. Informasi yang dikumpulkan adalah wahana permainan timezone memiliki 3 jenis kartu yaitu, welcome card, blue elit dan gold. Ketiga jenis kartu memiliki manfaat masing-masing. Pada kartu timezone, terdapat informasi yang relevan untuk proses pengujian, berupa *magnetic stripe*,*barcode*, nomor kartu, dan CVV yang terletak di bagian belakang kartu.



Gambar 3. Tampak belakang kartu timezone

Langkah selanjutnya melakukan pembacaan isi kartu menggunakan alat *magnetic stripe reader writer* untuk mengetahui isi track yang terdapat dalam kartu. Hasil dari pembacaan isi kartu menggunakan *software magcard write/read utlitiy program v2017* yaitu kartu timezone memiliki 3 track, namun hanya track 2 yang digunakan. Pada penelitian ini, peneliti menggunakan 2 jenis kartu timezone yaitu welcome card dan blue elite. Tujuan utama dari pengujian ini adalah untuk melakukan analisis terhadap pola data yang terdapat di dalam track kartu tersebut.

C. *Threat-Modeling*

Tahap ini merupakan tahap untuk melaksanakan *penetration* yang benar dengan melakukan pendekatan pemodelan ancaman agar lebih mudah menentukan serangan yang dapat terjadi dan menentukan kemungkinan serangan tersebut [17]. Pada tahap ini peneliti mengidentifikasi ancaman pada celah keamanan yang mungkin terjadi dengan melakukan pembacaan isi kartu *magnetic stripe* dari data yang telah dikumpulkan.

Tabel 2. Daftar hasil pembacaan kartu objek penelitian

No	Saldo	Jenis Kartu	*Magnetic Stripe*			Barcode	Id Kartu	CVV
			Track 1	Track 2	Track 3			
1	50.000	Welcome card	No data	;0012813170357980772?	No data	357980772	0357980772	823
2	50.000	Welcome card	No data	;0012813170357980773?	No data	357980773	0357980773	410
3	50.000	Welcome card	No data	;0012813170357980774?	No data	357980774	0357980774	179
4	50.000	Welcome card	No data	;0012813170357980775?	No data	357980775	0357980775	956
5	200.000	Blue elite	No data	;00129023902481624933?	No data	248162493	0248162493	455
6	9000	Blue elite	No data	;00129731402530137442?	No data	253013744	0253013744	795
7	20000	Blue elite	No data	;00129530702478939542?	No data	247893954	0247893954	825

Dari hasil pembacaa isi kartu, terlihat adanya pola berurutan yang memungkinkan terjadinya penggandaan atau duplikasi kartu.

D. *Vulnerability Analysis*

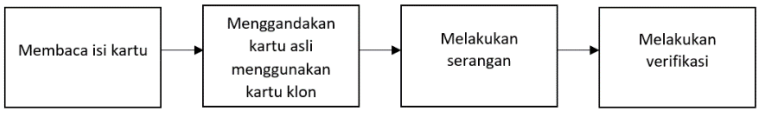
Tahap ini dilakukan pemindaian kerentanan, analisis hasil kerentanan, dan menentukan jenis serangan apa yang bisa dilakukan exploitasi [15]. Berdasarkan hasil analisis awal pada pembacaan kartu, maka peluang yang dapat dilakukan yaitu pengujian pada layanan keamanan *confidentiality*, *integrity* dan *availability*. Bentuk pengujian layanan di tunjukkan pada Tabel 3.

Tabel 3. Daftar pengujian layanan keamanan yang akan dilakukan

No.	Layanan Keamanan	Bentuk Pengujian
1	*Confidentiality*	Mencoba membuat kartu baru dengan id baru
2	*Integrity*	Mencoba menggandakan isi kartu asli pada kartu palsu
3	*Availability*	Mencoba kartu pada host yang sama dilokasi berbeda

E. *Exploitation*

Pada tahap eksploitasi, dilakukan penetrasi terhadap sistem dengan memulai simulasi serangan pada sistem yang menjadi target untuk mencari celah dalam keamanannya [18]. Pada penelitian ini tahap exploitation dilakukan untuk menguji ketiga layanan keamanan yaitu *confidentiality*, *integrity*, dan *availability*. **Gambar 4.** Menunjukan tahapan skenario pengujian yang akan dilakukan.



Gambar 4. Tahapan skenario pengujian

1. Skenario Pengujian 1

Membuat kartu baru dengan isi track 2 kartu klon sama dengan isi track 2 pada kartu asli. Bertujuan untuk menganalisis terhadap potensi duplikasi kartu asli dengan mencocokkan data yang terdapat pada track 2 dari kartu tersebut. Serangan yang dilakukan pada skenario 1 yaitu *interception*, serangan *interception* memanfaatkan kerentanan pada layanan keamanan *confidentiality*, dimana kartu timezone tidak dilengkapi dengan fitur *password* atau PIN. Hasil dari pengujian skenario 1 adalah berhasil. Maka dapat disimpulkan :

- Layanan keamanan yang terdapat pada skenario 1 yaitu *availability* karena kartu klon dapat digunakan di wahana dan dapat dilakukan pengecekan saldo pada sistem.
- Setelah kartu digunakan, tidak terdapat adanya perubahan data pada track 2.
- Saldo pada kartu asli berkurang.

2. Skenario Pengujian 2

Membuat kartu baru dengan mengubah empat digit isi track 2. Bertujuan untuk memberikan pemahaman lebih mendalam mengenai signifikasi dan fungsi spesifik dari empat digit tersebut dalam proses otentikasi dan otorisasi transaksi kartu. Serangan yang dilakukan pada skenario 2 yaitu *modification*, serangan *modification* memanfaatkan kerentanan pada layanan keamanan *integrity*, dimana data pada kartu timezone dapat diubah. Hasil dari pengujian skenario 2 menunjukkan bahwa ketiga percobaan berhasil. Maka dapat disimpulkan:

- Empat digit nomor kartu tidak mempengaruhi fungsi atau keamanan kartu,
- Layanan keamanan yang terdapat pada skenario 2 yaitu *availability* karena setelah serangan *modification* dilakukan, kartu tetap dapat digunakan di wahana dan dapat dilakukan pengecekan saldo pada sistem.
- Setelah kartu digunakan, tidak terdapat adanya perubahan data pada track 2.
- Saldo pada kartu asli berkurang.

3. Skenario Pengujian 3

Menggunakan 3 kartu klon untuk membuat kartu baru dengan mengubah beberapa digit isi track 2 pada kartu asli. Bertujuan untuk melakukan analisis terhadap peran dari perubahan beberapa digit dalam isi track 2 pada kartu. Serangan yang dilakukan dalam skenario 3 yaitu

modification, serangan *modification* memanfaatkan kerentanan pada layanan keamanan *integrity*, dimana data pada kartu timezone dapat diubah. Hasil dari pengujian skenario 3 yaitu percobaan 1 dan 2 berhasil, percobaan 3 error. Maka dapat disimpulkan:

- Pada percobaan 1 dan 2 terdapat pengamatan bahwa kartu tidak dapat mengecek saldo terlebih dahulu. Untuk memperoleh informasi saldo, langkah yang harus dilakukan dengan memainkan salah satu wahana terlebih dahulu, baru kemudian saldo dapat di cek.
- Layanan keamanan yang terdapat pada percobaan 1 dan 2 adalah *Availability*. Karena setelah serangan *modification* dilakukan, kartu tetap dapat digunakan di wahana dan dapat dilakukan pengecekan saldo pada sistem.
- Saldo pada kartu asli berkurang.
- Setelah kartu digunakan, tidak terdapat adanya perubahan data pada track 2.
- "00128", "00129", "00130" merupakan kode identifikasi kartu.
- Tidak terdapat layanan keamanan *availability* pada percobaan ke-3, karena kartu tidak dapat digunakan apabila kode identifikasi salah.

F. *Post Exploitation*

Pada tahap ini, dilakukan perbaikan dan menerapkan solusi yang tepat untuk mengatasi kerentanan [19]. Hasil pengujian dari ketiga skenario diatas menggunakan layanan keamanan *confidentiality, integrity,* dan *availability* menunjukkan bahwa aspek layanan tersebut belum sepenuhnya terimplementasi pada kartu timezone. Tabel 4. Menunjukkan solusi yang tepat untuk mengatasi kerentanan.

Tabel 4. Solusi yang tepat untuk mengatasi kerentanan

No	Layanan Keamanan	Kerentanan	Solusi
1	*Confidentialilty*	✗	Menerapkan enkripsi data
2	*Integrity*	✗	Menggunakan kartu Uniq dengan data yang tidak dapat diubah
3	*Availability*	✓	-

G. *Reporting*

Pada tahap pelaporan, pentester menyimpulkan hasil dari tahap sebelumnya, kerentanan yang teridentifikasi selama pengujian, dan memberikan rekomendasi terkait langkah untuk mengurangi kerentanan yang ditemukan dan peningkatan keamanan sistem [20]. Pada penelitian ini, mengenai pelaporan akan dibahas pada hasil penelitian.

2.3 Pengambilan Kesimpulan

Analisis Hasil dan Pembahasan

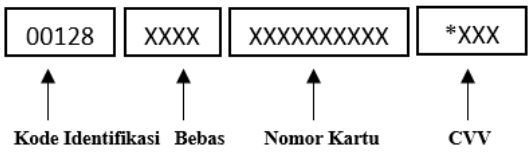
Hasil pada penelitian ini meliputi pemahaman data yang telah dikumpulkan selama penelitian, mencakup evaluasi temuan dan data yang diperoleh dari pengujian *penetration testing*. Pembahasan pada penelitian ini meliputi tahap dimana menguraikan signfikansi temuan dengan membandingkan hasil dengan standar keamanan yang ada.

3. HASIL DAN PEMBAHASAN

Tabel 5. Hasil pengujian

No.	Jenis	Saldo	Track 2	Status Pengujian
1	Asli	200.000	;0012902390248162493?	Berhasil
2	Klon	200.000	;0012902390248162493?	Berhasil
3	Asli	50.000	;0012813170357980772?	Berhasil
4	Klon 1	50.000	;0012817120357980772?	Berhasil
5	Klon 2	50.000	;0012850880357980772?	Berhasil
6	Asli	50.000	;0012813170357980772?	Berhasil
7	Klon 1	50.000	;0012913170357980772?	Berhasil
8	Klon 2	50.000	;0013013170357980772?	Berhasil
9	Klon 3	50.000	;0013114190357980772?	Gagal

Tabel 5. Menunjukkan hasil pengujian yang telah dilakukan oleh pentester, dari skenario-skenario yang telah dilakukan hanya satu yang berstatus gagal, yaitu kartu tidak dapat digunakan apabila kode identifikasi salah. Hasil pengujian secara keseluruhan mengindikasikan adanya potensi kerentanan pada kartu timezone yang dapat dieksploitasi. Solusi atas permasalahan tersebut, untuk tidak menampilkan nomor kartu pada bagian belakang kartu dan menerapkan enkripsi data.



Gambar 5. Isi track 2 pada kartu timezone

Berdasarkan hasil pembacaan kartu dan serangkaian percobaan pengujian yang telah dilakukan, informasi relevan yang dapat disimpulkan dari isi track 2 pada kartu timezone adalah sebagai berikut:

- Terdapat tiga jenis kartu dengan kode identifikasi masing-masing: kode 00128 welcome card, kode 00129 blue elite, dan 00130 kode gold.
- Empat digit setelah kode kartu tidak mempengaruhi fungsi atau keamanan kartu.
- Sepuluh digit berikutnya adalah nomor kartu, yang mengidentifikasi kartu secara khusus.
- CVV (Card Verification Value) atau kode keamanan kartu. Hanya digunakan untuk melakukan pengecekan saldo melalui aplikasi.
- Pada saat melakukan pengecekan saldo pada aplikasi, kita dapat menebak digit terakhir nomor kartu dan mencoba CVV dari 000-999.

Hasil pengujian *penetration testing* menunjukkan bahwa dua jenis ancaman, yaitu *interception* dan *modification*, berhasil dijalankan pada sistem kartu timezone. Pada ancaman *interception*, teridentifikasi bahwa kartu timezone tidak memiliki lapisan keamanan berupa PIN atau metode pengamanan lainnya. Pengguna dapat dengan mudah mengakses dan menggunakan kartu hanya dengan menggeseknya pada *magnetic stripe reader* yang ada di wahana, tanpa adanya proses validasi yang memadai. Hal ini menunjukkan bahwa kartu timezone tidak memiliki layanan keamanan *confidentiality*. Selanjutnya, dilakukan serangan *modification* dengan mengubah 5 digit awal dan digit ke-6 sampai ke-9 isi track 2 yang dapat menghasilkan kartu klon baru. Hal ini menunjukkan bahwa kartu timezone tidak memiliki layanan keamanan *integrity*.

Berdasarkan hasil di atas, dapat disimpulkan bahwa kartu *magnetic stripe* di lokasi tersebut rentan terhadap ancaman *interception* dan *modification*. Meskipun demikian, kartu tersebut memiliki layanan *availability* yang handal. Ketika mencoba mengubah lima digit awal menjadi 00131, kartu tersebut tidak dapat digunakan. Karena digit 00131 tidak termasuk dalam kode identifikasi pada kartu tersebut. Wahana permainan timezone memiliki database yang cukup baik dalam mengelola transaksi. Hal ini dibuktikan bahwa, meskipun kartu berhasil dikloning, kartu tetap dapat digunakan, dan saldo pada kartu asli berkurang sesuai dengan penggunaan yang sebenarnya. Hasil pengujian menunjukkan, wahana yang menggunakan koneksi nirkabel antara *magnetic stripe* reader dengan komputer utama hanya menyediakan layanan keamanan *availability*. Hal ini dapat mengancam keamanan data pengguna dan integritas transaksi. Rekomendasi untuk penyedia layanan adalah meningkatkan layanan keamanan pada kartu di lokasi tersebut, serta menerapkan enkripsi data.

Seluruh pengumpulan data dilakukan pada bulan Agustus tahun 2023. Saat ini terdapat jenis kartu baru yang digunakan yaitu jenis kartu smart card. Rekomendasi untuk penelitian selanjutnya yaitu dengan mencoba jenis kartu baru wahana permainan timezone yang sudah tidak terlihat adanya *magnetic stripe* sebagai bagian dari inovasi teknologi pembayaran mereka atau dengan melakukan pengujian lebih lanjut mengenai kartu yang masih menggunakan teknologi *Magnetic Stripe* dengan lokasi wahana yang berbeda.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis dan pengujian terhadap layanan keamanan sistem pada kartu transaksi elektronik wahana permainan menggunakan metode *penetration testing*, dapat disimpulkan bahwa layanan keamanan yang diterapkan pada kartu timezone masih menunjukkan adanya celah yang berpotensi untuk dieksploitasi. Karena ketiga aspek utama keamanan, yaitu *confidentiality*, *integrity*, dan *availability* belum sepenuhnya terimplementasi dengan baik pada kartu timezone.

Hal ini dibuktikan pada layanan keamanan *confidentiality* dapat dilakukan serangan *interception* karena kartu tersebut tidak memiliki lapisan keamanan berupa PIN atau metode pengaman lainnya. Pengguna dapat dengan mudah mengakses dan menggunakan kartu hanya dengan menggeseknya pada *magnetic stripe reader* yang ada di wahana, tanpa adanya proses validasi yang memadai. Pada layanan keamanan *integrity* dapat dilakukan serangan *modification* dengan mengubah 5 digit awal dan digit ke-6 sampai ke-9 isi track 2 yang dapat menghasilkan kartu klon baru. Meskipun demikian, kartu tersebut memiliki layanan *availability* yang handal. Ketika mencoba mengubah lima digit awal menjadi 00131, kartu tersebut tidak dapat digunakan. Karena digit 00131 tidak termasuk dalam kode identifikasi kartu. Wahana permainan timezone memiliki database yang cukup baik dalam mengelola transaksi. Hal ini dibuktikan bahwa, meskipun kartu berhasil dikloning, kartu tetap dapat digunakan, dan saldo pada kartu asli berkurang sesuai dengan penggunaan yang sebenarnya. Hasil pengujian menunjukkan, wahana yang menggunakan koneksi nirkabel antara *magnetic stripe reader* dengan komputer utama hanya menyediakan layanan keamanan *availability*.

Dari hasil pengujian kita dapat mengetahui perbandingan komunikasi antara *magnetic stripe reader* dengan komputer utama menggunakan kabel dan nirkabel. Hal ini dapat menjadi masukan bagi pengelola wahana untuk meningkatkan layanan keamanan lainnya. Khususnya pada aspek layanan *confidentiality* dan *integrity*. Solusi atas permasalahan tersebut, untuk tidak menampilkan nomor kartu pada bagian belakang kartu dan menerapkan enkripsi data.

DAFTAR PUSTAKA

[1] Y. Salim and H. Azis, "Sistem Penanda Kepemilikan File Dokumen Menggunakan Metode Digital Watermark Pada File Penelitian Dosen Universitas Muslim Indonesia," *Ilk. J. Ilm.*, vol. 9, no. 2, pp. 161–166, Aug. 2017, doi: 10.33096/ilkom.v9i2.125.161-166.

[2] Yulianti, "Perlindungan Nasabah Bank dari Tindakan Kejahatan Skimming di Tinjau dari Undang Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.," *Jurnal Hukum*, vol. 3, no. 2, pp. 195–204, 2020, doi: 10.31328/wy.v3i2.1663.

[3] G. Suprianto, "Penetration Testing Pada Sistem Informasi Jabatan Universitas Hayam Wuruk Perbanas," *InComTech*, vol. 12, no. 2, pp. 129–138, Aug. 2022, doi: 10.22441/incomtech.v12i2.15093.

[4] G. Weidman, *Penetration Testing a Hands-on Introduction to Hacking*. USA: no strach press, 2014.

[5] R. Muzawi and N. Sahrun, "Aplikasi Kartu Magnetik Absensi Karyawan Menggunakan Personal Computer dan Bahasa Pemrograman," *JIKB.Jur.il.kom.bis*, vol. 9, no. 2, pp. 2070–2076, Nov. 2018, doi: 10.47927/jikb.v9i2.137.

[6] H. Azis and F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," *Ilk. J. Ilm.*, vol. 11, no. 2, pp. 167–174, Aug. 2019, doi: 10.33096/ilkom.v11i2.447.167-174.

[7] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, "Pengujian Penetrasi Pada Website elearning2.binadarma.ac.id dengan Metode PTES (Penetration Testing Execution Standard)," *jicon*, vol. 11, no. 1, pp. 91–95, Mar. 2023, doi: 10.35508/jicon.v11i1.9809.

[8] Andi, *Keamanan Sistem Informasi*. Yogyakarta: IBISA, 2011.

[9] B. Rahardjo, *Keamanan Sistem Informasi Berbasis Internet*. Bandung, 2002.

[10] D. Darwis, A. Junaidi, and Wamiliana, "A New Approach of Steganography Using Center Sequential Technique," *J. Phys.: Conf. Ser.*, vol. 1338, no. 1, p. 012063, Oct. 2019, doi: 10.1088/1742-6596/1338/1/012063.
[11] M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *JIK*, vol. 6, no. 1, pp. 92–101, Jan. 2022, doi: 10.59697/jik.v6i1.144.
[12] D. Satrinia, S. N. Yutia, and I. M. M. Matin, "Analisis Keamanan dan Kenyamanan pada Cloud Computing," *Journal of Informatics and Communications Technology (JICT)*, vol. 4, no. 1, 2022, doi: 10.52661.
[13] A. A. B. A. Wiradarma and G. M. A. Sasmita, "It Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company)," *IJCNIS*, vol. 11, no. 12, pp. 17–29, Dec. 2019, doi: 10.5815/ijcnis.2019.12.03.
[14] A. Shanley and M. Johnstone, "Selection of Penetration Testing Methodologies: A Comparison and Evaluation," in *13th Australian Information Security Management Conference*, Western Australia.: Security Research Institute (SRI), Edith Cowan University, 2015, pp. 65–72, doi: 10.4225/75/57B69C4ED938D.
[15] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *JSisfotek*, pp. 1–6, Mar. 2021, doi: 10.37034/jsisfotek.v3i1.36.
[16] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force dengan Metode Penetration Testing (Studi Kasus:Rs H.Lmanambai Abdulkadir)," *JINTEKS*, vol. 4, no. 1, pp. 26–35, Feb. 2022, doi: 10.51401/jinteks.v4i1.1528.
[17] B. Parga Zen, Satria Galang Saputra, and Abdurahman, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Execution Standard (PTES)," *JSIG*, vol. 1, no. 2, pp. 43–51, Jul. 2023, doi: 10.25157/jsig.v1i2.3152.
[18] R. Umar, I. Riadi, and M. I. A. Elfatiha, "Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF," *Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 1, pp. 280–292, Apr. 2023.
[19] F. Fachri, "Optimasi Keamanan Web Server terhadap Serangan Brute-Force Menggunakan Penetration Testing," *JTIIK*, vol. 10, no. 1, pp. 51–58, Feb. 2023, doi: 10.25126/jtiik.20231015872.
[20] Y. Mulyanto and A. A. Fari, "Analisis Keamanan Login Router Mikrotik dari Serangan Bruteforce Menggunakan Metode Penetration Testing," *JINTEKS (Jurnal Informatika Teknologi dan Sains)*, vol. 4, no. 3, pp. 145–155, Agustus 2022, doi: 10.51401/jinteks.v4i3.1897.