ANALISA PENGELOMPOKAN *CYBER CRIME* PADA PENERAPAN *ELECTRONIC COMMERCE*

Juwita Artanti Kusumaningtyas[1]

[1]*Institut Agama Islam Negeri Salatiga*

Email: mee.juwita@gmail.com[1]

Abstract - The rapid development of Information Technology (IT) greatly influences human needs and activities. One influence occurs in buying and selling transactions carried out by two parties, namely consumers and producers or more online. The transaction process is E-commerce (Electronic Commerce). Internet use certainly has risks, one of which is Cyber Crime. Cyber Crime is a crime committed in the internet world involving individuals or groups. Types of Cyber Crime consist of hacking, craking, sniffing and so forth. Cyber Crime cases are grouped into 4 groups namely Interruption, Interception, Modification, and Fabrication. This study uses a literature study method that analyzes 21 journals that discuss Cyber Crime in E-Commerce. The purpose of this study is to determine the Cyber Crime that often occurs in E-Commerce. The results of this study provide recommendations that can be used for developers related to the Cyber Crime group that need to be watched out and prevented.

Keywords- **E-Commerce, Cyber Crime**

PENDAHULUAN

Teknologi informasi yang semakin berkembang secara pesat juga mempengaruhi berkembangnya suatu *E-commerce* terutama di Indonesia. Peran dari teknlogi informasi dalam sebuah bisnis juga semakin kuat yang ditunjukkan dengan keaktifan perusahaan besar multinasional untuk menggunakan internet sebagai sarana pemasaran produknya [1]. Internet sebagai salah satu implementasi dari teknologi informasi yang berkembang pesat saat ini dan masih terus dikembangkan hingga saat ini. Manfaat dari pentingnya internet sendiri sudah dirasakan oleh banyak individu maupun organisasi yang berkembang. Asosiasi Penyelenggara Jasa Internet Indonesia (APJJI) telah melakukan survey pada bulan Desember 2013 di 33 provinsi Indonesia. Survey tersebut mengatakan bahwa penggunaan internet di Indonesia mencapai 71,19 juta orang atau telah mencapai 28% dari total populasi di Indonesia [2].

Salah satu contoh pemanfaatan penggunaan internet yang sering digunakan yaitu *e-commerce. E-commerce* (*Electronical Commerce*) merupakan sebuah kegiatan transaksi jual beli yang dilakukan oleh dua pihak atau lebih yaitu dari pihak konsumen (*customers*) dan pihak produsen yang dilakukan secara *online*. Berdasarkan dari *Ministry of Science, Technology and Inovation* mengatakan bahwa *e-commerce* sendiri merupakan sebuah proses transaksi jual beli yang terjadi baik itu yang dilakukan untuk kepentingan bisnis, perorangan, pemerintah dan perusahaan perorangan lainnya yang dilakukan berbasis komputer secara *online* [3]. Penggunaan *e-commerce* yang perlu diperhatikan yaitu mengenai keamanan data dan juga keamanan *service* yang ditawarkan.

Perkembangan Teknologi Informasi (TI) secara pesat sangat mempengaruhi kebutuhan dan kegiatan manusia. Salah satu pengaruh terjadi pada transaksi jual beli yang dilakukan oleh dua pihak yaitu konsumen dan produsen atau lebih secara *online*. Proses transaksi tersebut yaitu *E-commerce* (*Electronical Commerce*). Penggunaan internet tentu terdapat resiko, sala satunya yaitu *Cyber Crime. Cyber Crime* merupakan tindakan kejahatan yang dilakukan didalam dunia internet yang melibatkan individu atau kelompok. Jenis *Cyber Crime* terdiri dari *hacking, craking, sniffing* dan lain sebagainya. Kasus *Cyber Crime* merupakan kasus yang harus diperatikan terutama untuk *developer* ataupun pengguna dari *e-commerce*. Salah satu caranya yaitu melakukan identifikasi kasus *cyber crime* yang sering terjadi dalam duni internet kemudian fokus pada pencegahannya.

Berdasarkan latar belakang diatas, maka akan dilakukan penelitian mengenai analisa pengelompokan *Cyber Crime* pada penerapan *electronic commerce*. Penelitian ini membahas mengenai studi letaratur dengan pembahasan *Cyber Crime* yang sangat sering terjadi di dalam dunia *E-Commerce*. Kasus *Cyber Crime* yang ditemukan akan dikelompokkan menjadi 4 kelompok yaitu *Interruption, Interception, Modification,* dan *Fabrication*. Penelitian ini menggunakan teknik studi literatur yang dilakukan terhadap 21 jurnal yang terkait. Teknik tersebut dilakukan untuk mengetahui kasus *Cyber Crime* yang sering terjadi di dalam dunia *E-Commerce*. Tujuan dari penelitian ini akan menghasilkan sebuah rekomendasi yang bisa digunakan oleh para *developer* untuk menjadi panduan mengenai apa saja yang harus diperhatikan jika ingin membangun sebuah *E-Commerce* khususnya dari sisi keamanan.

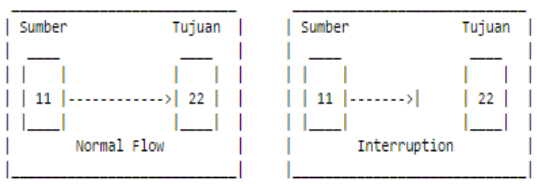
KAJIAN PUSTAKA

Menurut penelitian yang dilakukan oleh *Erikson Damanik* pada tahun 2012 [9] mengatakan bahwa kejahatan *E-Commerce* yang sering terjadi yaitu pencurian informasi transaksi yang terjadi dan data tersebut dimodifikasi sesuai dengan keinginan pelaku. Penelitian ini membahas mengenai bagaimana peranan dari *Payment Gateway* untuk mengatasi masalah yang terjadi di dalam suatu *E-Commerce*.

Menurut penelitian yang dilakukan oleh *Jian Kang* pada tahun 2005 [21] mengatakan bahwa kejahatan *E-Commerce* yang sering terjadi yaitu *Distributed Denial of Service* (DDoS). Serangan DDoS merupakan serangan yang langsung mengarah kepada server dan akan mengakibatkan server menjadi tidak beroperasi kembali sehingga tidak dapat memberikan *service* atau pelayanan dengan baik lagi. Penelitian ini membahas mengenai bagaimana meningkatkan D-WARD *Detection System* yang bisa digunakan untuk mencegah serangan DDoS pada sebuah *E-Commerce*.

A. Interruption

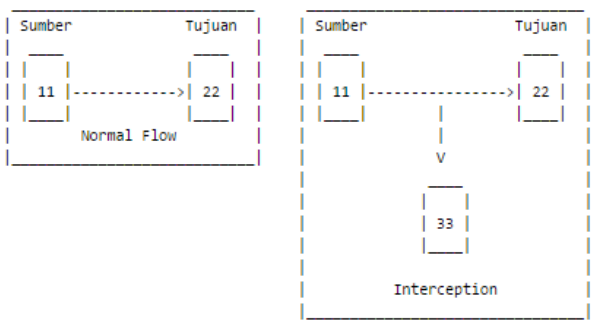
Interruption merupakan ancaman terhadap availability informasi, data yang ada dalam sistem computer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang. Contohnya adala perusakan/modifikasi terhadap piranti keras atau saluran jaringan. [28]



Gambar 1 Serangan *Interruption*

A. Interception

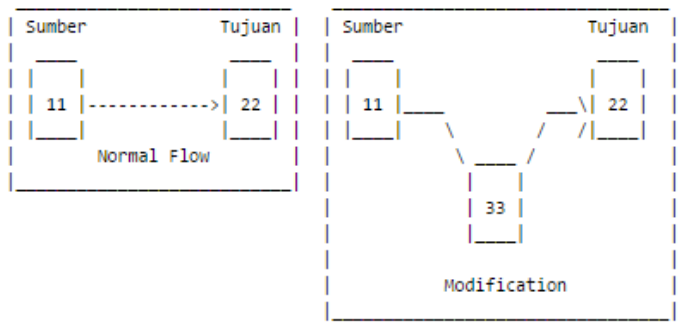
Interception merupakan ancaman terhadap kerahasiaan (secrery). Informasi yang disadap seingga seingga orang yang tidak berhak dapat mengakses computer dimana informasi tersebut disimpan. Contohnya adalah penyadapan terhadap data dalam suatu jaringan [28].



Gambar 2 Serangan *Interception*

B. Modification

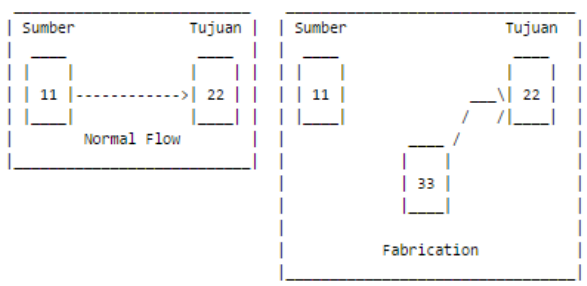
Modification merupakan ancaman terhadap integritas, Orang yang tidak berhasil menyadap lalu lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.



Gambar 3 Serangan *Modification*

C. Fabrication

Fabrication merupakan ancaman terhadap integritas, Orang yang tidak berhak berhasil meniru atau memalsukan informasi seingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki ole si penerima informasi. Contohnya adalah pengiriman pesan palsu kepada orang lain.



Gambar 4 Serangan *Fabrication*

METODE PENELITIAN

Penelitian ini dilakukan dengan beberapa tahap seperti tahap studi literatur, tahap analisa masalah, dan tahap penarikan kesimpulan. (1) Pada tahapan studi literatur dilakukan pencarian literatur terkait masalah yang akan diteliti yaitu mengenai serangan yang terjadi pada suatu *E-Commerce*. Studi literatur menggunakan sebanyak 20 literatur yang membahas mengenai serangan-serangan yang terjadi pada *E-Commerce*. (2) Tahapan selanjutnya yaitu melakukan identifikasi masalah dari studi literatur yang telah dilakukan. Masalah yang diangkat adalah serangan-serangan keamanan apa saja yang sering terjadi di dalam sebuah *E-Commerce*. Daftar serangan tersebut kemudian dikelompokkan ke dalam empat aspek serangan keamanan yaitu *Interruption, Interception, Modification, Fabrication*. (3) Tahapan selanjutnya yaitu mengambil kesimpulan dari masalah yang ditemukan. Hasil dari penelitian ini sebuah rekomendasi yang bisa digunakan oleh para *developer* untuk menjadi panduan mengenai apa saja yang harus diperhatikan jika ingin membangun sebuah *E-Commerce* khususnya dari sisi keamanan. .

PEMBAHASAN

Jurnal	I	In	M	F
Analisa dan perancangan prototipe aplikasi E-Commerce [4]		V		
Implementasi aplikasi e-commerce dengan menggunakan protokol HTTPS sebagai pendukung kemanan jaringan (Studi kasus di PD. Kharima Jaya Cimahi, Bandung) [5]		V	V	

Analisa Yuridis Tentang Hukum Asuransi Dalam Transaksi Electronic Commerce Melalui Perspektif Kitab Undang-Undang Hukum Dagang [6]		V		
Pengaruh Keamanan, Regulasi dan Sistem Pembayaran Terhadap Sistem E-Commerce pada PT. WEBA International [7]		V	V	
E-Commerce dengan memanfaatkan Sistem operasi LINUX [8]		V		
Perancangan Sistem Informasi Pembayaran Online Menggunakan Payment Gateway [9]				
E-Commerce Security [10]			V	
Pengaruh Structural Assurance dan Perceived Reputation Terhadap Trust Pengguna Internet di Sistem E-Commerce [11]		V	V	
E-Gold Sebagai Alternatif Alat Pembayaran pada E-Commerce [12]		V	V	
Analisa Penerapan Sistem Informasi Akuntansi dan Audit Electronic Data Processing Melalui		V		

Electronic Commerce dalam Mengendalikan Transaksi Pembayaran Online [13]				
Analisa Pengaruh Privasi, Keamanan, dan Kepercayaan Terhadap Niat Untuk bertransaksi secara Online di OLX.co.id [14]		V		
Optimalisasi Cyberlaw Untuk Penanganan Cybercrime pada E-Commerce [15]		V		
Kejahatan Teknologi Hacking Paypal [16]	V			
Mengamankan Transaksi di Internet : Suatu Tinjauan Terhadap Justifikasi dan Metode [17]				
Model Identifikasi Perencanaan Keamanan Pada E-Business [18]		V		
Bisnis Rental Mobil Melalui Internetx (E-Commerce) Menggunakan Algoritma SHA-1 (Secure Hash Algorithm) [19]		V	V	
DDoS – Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection [20]	V			
Protect E-Commerce Against DDoS attacks with improved D-WARD	V			

Detection System [21]				
Method and Apparatus for Recognizing and Reacting to denial of Service attacks on a Computerized Network [22]	V			
Using a High-Performance, Programmable Secure Coprocessor [23]	V		V	
Analisis Serangan Web Phishing Pada Layanan E-Commerce Dengan Metode Network Forensic Process [24]				**V**

Table 1 Pengelompokan Serangan Keamanan *E-Commerce*

Keterangan :

I = Interruption

In = Interception

M = Modification

F = Fabrication

Berdasarkan Table 1 didapatkan bahwa, dari 21 literatur yang diteliti (1) terdapat 14 literatur yang mengatakan bahwa serangan *E-Commerce* tergolong kedalam kelompok *Interruption* dimana serangan yang berikan dapat merusak data yang tersimpan di dalam server. (2) Terdapat 15 literatur yang mengatakan bahwa serangan *E-Commerce* tergolong ke dalam kelompok *Interception* dimana serangan diberikan bertujuan untuk mengetahui informasi yang dibutuhkan. (3) Terdapat 8 literatur yang mengatakan bahwa serangan *E-Commerce* tergolong ke dalam kelompok *Modification* dimana *hacker* berhasil menyadap lalu lintas informasi yang dikirim dan informasi tersebut dapat diubah sesuai dengan keinginan, dan (4) Terdapat 1 literatur yang mengatakan bahwa serangan *E-Commerce* tergolong ke dalam kelompok *Fabrication*. Adapun jenis serangan yang sering terjadi pada kasus *E-Commerce* dapat dilihat pada Table 2.

Literatur	Aspek Serangan	Serangan
[4]	Interception	Sniffing
[5]	Interception, Modification	Sniffing, Man in the Middle
[6]	Interception	Sniffing username dan password login

[7]	Interception, Modification	Hacking, Cracking
[8]	Interruption, Interception	Sniffing, Penghapusan data, Hacking
[9]	Interception, Modification	Pencurian informasi transaksi dan melakukan modifikasi
[10]	Modification	Cracking
[11]	Interception, Modification	Hacking, Cracking
[12]	Interception, Modification	Hacking, Sniffing, Cracking
[13]	Interception	Hacking
[14]	Interception	Hacking
[15]	Interception	Hacking
[16]	Interruption	DDoS
[17]	Interception	Hacking
[18]	Interception	Hacking
[19]	Interception, Modification	Hacking, Cracking
[20]	Interruption	DDoS
[21]	Interruption	DDoS
[22]	Interruption	DoS, DDoS
[23]	Interruption, Modification	Merubah Algoritma, Merusak Data
[24]	Fabrication	Phishing

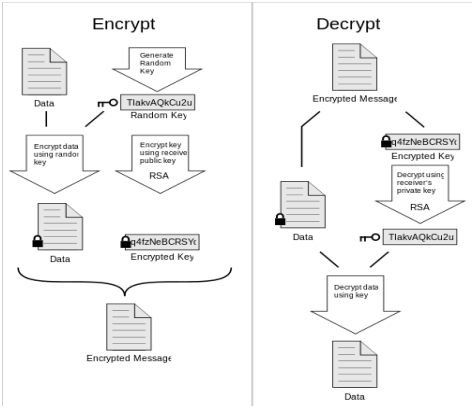
Table 2 Jenis Serangan yang Berhasil di Kelompokkan.

Berdasarkan pengelompokan serangan yang sudah dilakukan, didapatkan bahwa aspek serangan yang sering terjadi pada *E-Commerce* adalah *Interception*. Serangan *Interception* yang dilakukan berupa *hacking* dan *sniffing*. Jenis serangan tersebut dijelaskan oleh literatur (4, 5, 6, 7, 9, 11, 12, 13 ,14, 15, 17, 18, 19). Aspek serangan kedua yang sering terjadi adalah *Modification*. Serangan *Modification* yang dilakukan berupa *Man in the middle* dan *cracking*. Jenis serangan tersebut dijelaskan oleh literatur (5, 7, 9, 11, 12, 19, 23). Jenis serangan ketiga yang sering terjadi adalah *Interruption*. Serangan *Interruption* yang dilakukan berupa *DDoS* dan *DoS*. Jenis serangan tersebut dijelaskan oleh literatur (16, 20, 21, 22, 23). Jenis serangan keempat yaitu *Phishing* yang dijelaskan pada literature 24.

Jenis serangan *Interception* merupakan serangan yang dilakukan terhadap *privacy* atau kerahasiaan. Pada kasus *E-Commerce*, jenis data yang harus bersifat *privacy* diantaranya *password login*, kode pelanggan, id transaksi, dan nomor pembayaran. Masalah serangan *privacy* bisa dicegah dengan menggunakan cara *cryptography*. *Cryptography* sendiri merupakan salah satu teknik yang bekerja dengan mengodekan semua data yang tersimpan menjadi sebuah kode yang tidak bisa dibaca. Penggunaan teknik *cryptography* sendiri akan sangat membantu dalam penanganan serangan *Interception*, karena sekalipun para *hacker* berhasil masuk pada jalur informasi yang

dikirimkan, data tetap tidak bisa terbaca karena sudah dilakukan pengkodean terhadap informasi yang dikirimkan. Pemanfaatan *cryptography* yang telah digunakan kemudian digabungnkan dengan metode PGP (*Pretty Good Privacy*) dimana PGP merupakan sebuah servis yang melayani *cryptography privacy* dan *authentication* dari data yang dikirimkan.

Penerapan PGP di dalam Script PHP menggunakan fungsi tambahan yaitu OpenPGP dan GnuPGP. OpenPGP merupakan standar yang digunakan oleh PGP, sedangkan GnuPGP merupakan sebuah library dari PHP yang dapat digunakan untuk melakukan *generate key* yang dibutuhkan untuk proses enkripsi maupun dekripsinya. Proses dari PGP sendiri dapat dilihat pada Gambar 5.



Gambar 5 Proses dari PGP.

KESIMPULAN

Berdasarkan pembahasan yang sudah dijelaskan pada bagian sebelumnya, dapat disimpulkan bahwa jenis serangan yang masih sering terjadi adalah serangan *Interception*. Serangan yang tergolong kedalam kelompok *Interception* adalah *sniffing* dan *hacking*. Kesimpulan tersebut didapatkan dari hasil studi literatur yang dilakukan pada 21 literatur yang sudah pernah dilakukan. Berdasarkan kesimpulan tersebut, maka pencegahan yang bisa dilakukan adalah dengan menerapkan metode *cryptography* yang kemudian digabungkan dengan menggunakan metode PGP (*Pretty Good Privacy*) pada aplikasi *E-Commerce*.

REFERENSI

[1] Nuryanti.2013.Peran E-Commerce Untuk Meningkatkan Daya Saing Usaha Kecil dan Menengah (UKM), Universitas Riau, Pekanbaru.

[2] Marius, Parlindungan , Anggoro, Sapto. 2015. Profil Penggunaan Internet Indonesia 2014, Puskakom UI, Jakarta.

[3] Hai, Woon Tai. 2010. E-Commerce for Global Reach. PIKOM. Malaysia.

[4] Putra, Dimas Ernomo, Astuti, Endang Siti, Riyadi. 2015. Pengaruh Kemudahan Terhadap Kemanfaatan, Minat dan Penggunaan E-Commerce (Studi Kasus pada Penggunaan Situs Olx.co.id), Universitas Brawijaya, Malang

[5] Velmurugan, Manivannan Senthil. 2009. Security And Trust in E-Business: Problems And Prospects, Multimedia University, Malaysia.

[6] Andriana, Dian. 2003. Analisa dan perancangan prototipe aplikasi E-Commerce. Pusat Penelitian Informatika

[7] Andriana, Henry Rossi, Putra, Erwansyah. Implementasi aplikasi e-commerce dengan menggunakan protokol HTTPS sebagai pendukung kemanan jaringan (Studi kasus di PD. Kharima Jaya Cimahi, Bandung). Telkom Polytechnic, Bandung

[8] Tumanggor, Frederic Hamonangan. 2012. Analisa Yuridis Tentang Hukum Asuransi Dalam Transaksi Electronic Commerce Melalui Perspektif Kitab Undang-Undang Hukum Dagang. Universitas Brawijaya, Malang

[9] Tegar, Samuel dan Ardini, Lilis. 2013. Pengaruh Keamanan, Regulasi dan Sistem Pembayaran Terhadap Sistem E-Commerce pada PT. WEBA International. STIESIA, Surabaya

[10] Fauziah dan Agustina, Ina. 2009. E-Commerce dengan memanfaatkan Sistem operasi LINUX. Universitas Nasional, Jakarta Selatan

[11] Damanik, Erikson. 2012. Perancangan Sistem Informasi Pembayaran Online Menggunakan Payment Gateway. STMIK Mikroskil, Medan

[12] Al-Slamy, Nada. M. A. 2008. E-commerce Security. Alzaytoonah University. Jordan

[13] Dharma, Fitra. 2006. Pengaruh Structural Assurance dan Perceived Reputation Terhadap Trust Pengguna Internet di Sistem E-Commerce. Universitas Lampung, Lampung

[14] Christianto, P.A. 2009. E-Gold Sebagai Alternatif Alat Pembayaran pada E-Commerce. Universitas AKI, Semarang

[15] Manik, Tumpal. 2012. Analisa Penerapan Sistem Informasi Akuntansi dan Audit Electronic Data Processing Melalui Electronic Commerce dalam Mengendalikan Transaksi Pembayaran Online. JEMI

[16] Syaifudin, Muhammad. Analisa Pengaruh Privasi, Keamanan, dan Kepercayaan Terhadap Niat Untuk bertransaksi secara Online di OLX.co.id. Universitas Brawijaya, Malang

[17] Pratama, Eva Argarini. 2013. Optimalisasi Cyberlaw Untuk Penanganan Cybercrime pada E-Commerce. AMIK Bina Sarana Informatika, Purwekerto

[18] Dewi, Adityas Widayani. 2011. Kejahatan Teknologi Hacking Paypal. Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM, Yogyakarta.

[19] Cahyadi, Adi. 2004. Mengamankan Transaksi di Internet : Suatu Tinjauan Terhadap Justifikasi dan Metode. Journal The Winners. Jakarta

[20] Palar, Roland Tumbelaka, Priyopradono, Bentar, Wellem, Theopillus J.H. 2012. Model Identifikasi Perencanaan Keamanan Pada E-Business. Universitas Kristen Satya Wacana, Salatiga.

[21] Abdullah, Dahlan dan Erliana, Cut Ita. 2012. Bisnis Rental Mobil Melalui Internetx (E-Commerce) Menggunakan

Algoritma SHA-1 (Secure Hash Algorithm). Universitas Malikussaleh, Aceh.

[22] Ranjan, S , Swaminathan, R, Uysal, M, and Knightly, E. 2006. DDoS – Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection. Rice University, Houston.

[23] Kang, Jian. 2005. Protect E-Commerce Against DDoS attacks with improved D-WARD Detection System. Changchun University, China.

[24] A. Ginanjar, N. Widiyasono, and R. Gunawan. 2019. Analisis Serangan Web Phishing Pada Layanan E-Commerce Dengan Metode Network Forensic Process. JUTEI. vol. 2,no. 2, pp. 147-157.

[25] Geis, Christoph, Pausch, Ebenhard dan Soysal, Thomas. 2003. Method and Apparatus for Recognizing and Reacting to denial of Service attacks on a Computerized Network . USPTO, United State

[26] Smith, Sean W, Palmer, Elaine. R and Weingart, Steve. 2006. Using a High-Performance, Programmable Secure Coprocessor. Lecturer Notes in Computer Science pp 73 – 89.

[27] Wang, Yuanzhou, Lin, Chuang, and Meng, Kun. 2009. Analysis of Attack Actions for E-Commerce Based on Stochastic Game Nets Model. Tsinghua University, Beijing

[28] Harliana, Putri, Perdana, Adidtya, dan Prasetyo, Raden MK. 2017. Sniffing dan Spoofing Pada Aspek Keamanan Komputer. Fakultas Ilmu Komputer dan Teknologi Informasi. Universitas Sumatera Utara.