Turnitin Originality Report

Processed on: 10-Sep-2020 9:13 AM WIB
ID: 1383312745
Word Count: 1955
Submitted: 1

Similarity Index	Similarity by Source	
17%	Internet Sources:	17%
	Publications:	1%
	Student Papers:	1%

Meningkatkan Keamanan Jaringan dengan Menggunakan Model Proses Forensik By Patmi Kasih

13% match (Internet from 24-Jan-2018)
https://media.neliti.com/media/publications/224411-analisis-log-snort-menggunakan-network-f-d0404fb0.pdf

1% match (Internet from 08-Apr-2019)
http://eprints.umm.ac.id/45732/3/jiptummpp-gdl-lukikoriis-43408-3-babii.pdf

1% match ()
http://repository.wima.ac.id/8253/7/LAMPIRAN.pdf

1% match (Internet from 30-May-2020)
http://sinta3.ristekdikti.go.id/authors/detail?id=5975399&page=2&view=documentsgs

< 1% match (Internet from 19-Aug-2020)
https://mafiadoc.com/high-speed-and-spectrally-efficient-optical-_5ba7ec70097c473b148b4699.html

< 1% match (publications)
Lucky Lhaura Van FC. "Rancang Bangun E-Commerce Untuk Meningkatkan Penjualan Petani Ikan Menggunakan Algoritma RSA (Studi Kasus : Desa Koto Tibun)", INOVTEK Polbeng - Seri Informatika, 2018

Meningkatkan Keamanan Jaringan dengan Menggunakan Model Proses Forensik 1Ervin Kusuma Dewi, 2Patmi Kasih 1Sistem Informasi, Fakultas Teknik, Universitas Nusantara PGRI Kediri 2Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri 1ervin@unpkediri.ac.id , 2fatkasih@gmail.com ABSTRAK Penggunaan mobile phone yang semakin meningkat dari tahun ke tahun, yang didukung dengan kecepatan data yang terus meningkat membuat teknologi internet terus berkembang. Dampak dari perkembangan technologi internet yaitu penyerangan dan pemerasan seperti yang terjadi pada tahun 2017, yaitu serangan ransomware yang bernama "WannaCry". Serangan "WannaCry" merupakan jenis serangan phishing, yaitu serangan yang memperoleh informasi user, password atau data-data lainya dengan menggunakan website palsu yang menyerupai aslinya. Sebagai pengelola jaringan tentunya harus meningkatkan keamanan jaringan, seringkali yang terjadi ketika terjadi serangan baru melakukan perbaikan, dan tentunya dapat menambah biaya perbaikan. Oleh karena itu, perlunya sebuah metode yang mampu

menganalisis ketika terjadi serangan, serta dapat menyimpan mencatat serangan, dan catatan tersebut dapat digunakan sebagai pelaporan. Salah satu metode yang support adalah Model Proses Forensik. Hasil dari penelitan adalah dengan menggunakan menggunakan Model Proses Forensik dapat menganalisis serangan pada log SNORT, data analisis tersebut bisa dijadikan salah satu pembuktian terjadinya serangan, selain itu bisa digunakan sebagai bahan untuk pelaporan kepada pihak berwajib (jika diperlukan). Dari hasil 5 serangan dapat dilakukan analisis, yaitu pukul berapa terjadi serangan, jenis serangan, serta total packet. Kata Kunci: Model Proses Forensik, Intrusion Detection System (IDS), SNORT. 1. Pendahuluan Penggunaan mobile phone yang semakin meningkat dari tahun ke tahun, yang didukung dengan kecepatan data yang terus meningkat membuat teknologi internet terus berkembang. Dengan semakin berkembangnya internet tentu memiliki dampak yang luar biasa, salah satunya adalah dimudahkanya dalam berkomunikasi. Namun di lain sisi juga memiliki kelemahan, seperti pada penyerangan dan pemerasan seperti yang terjadi pada tahun 2017, yaitu serangan ransomware yang bernama "WannaCry" yang menyerang 99 negara. Di Indonesia serangan "WannaCry" dilaporkan mulai menginfeksi system computer di beberapa rumah sakit. Semua data terkunci oleh wannacry dan jika mengingnkan data kembali, pihak rumah sakti harus mengirimkan uang tebusan (Kompas, 2017). Ransomware mengandalkan teknik phishing dimana calon korban diminta untuk klik sebuah link atau tautan untuk mengunduh ransomware, missal email atau link yang muncul di sebuah browser. Serangan phishing merupakan serangan yang memperoleh informasi user, password atau data-data lainya dengan menggunakan website palsu yang menyerupai aslinya. Sebagai pengelola jaringan tentunya harus meningkatkan keamanan jaringan, seringkali yang terjadi ketika terjadi baru melakukan perbaikan, yang tentunya dapat menambah biaya perbaikan. Oleh karena itu, perlunya sebuah metode yang mampu menganalisis ketika terjadi serangan, serta dapat menyimpan mencatat serangan, dan catatan tersebut dapat digunakan sebagai pelaporan. Salah satu metode yang support dengan hal teresebut adalah metode Network Forensic. Network Forensic fokus pada monitoring dan analisis pada trafik jaringan local maupun WAN/nternet untuk pengumpulan informasi, pengumpulan bukti, atau Instruction Detection (Mate & Kapse, 2015). Forensik memiliki dua kegunaan, pertama megidentifikasi dengan keamanan, termasuk memeriksa system dan mengenali interupsi atau alert. Kedua, mengidentifikasi hasil serangan yang tersimpan dalam log. Penelitian yang memanfaatkan honeypot yaitu Misra dan Dhir (2012) tentang Network Forensic yaitu dengan menggunakan Honeypots untuk memikat dan menyerang dengan menggunakan jaringan tipuan. Dengan membuat kerentanan keamanan yang kamlufase, selain itu juga menggunakan NFATs untuk pengumpulan data. Tujuan membangun sistem adalah untuk mengumpulkan data jaringan yang berbahaya dan digunakan untuk penyelidikan lebih lanjut untuk mendapatkan informasi tentang penyerang sebagai bukti Network Forensic. Selain itu penelitian yang menggunakan honeypot sebagai salah satu cara yang dapat digunakan sebagai jebakan dalam keamanan jaringan (Nugraha dkk, 2013). Hasil penelitan Misra dan Dhir menunjukkan bahwa teknologi Honeypot mudah digunakan, konfigurasi lebih flexible, tidak membutuhkan resource yang besar. Dewi (2016) membuat rancangan keamanan jaringan dengan menggunakan pendekatan model proses jaringan, penelitian Dewi berupa konsep dan studi literature untuk meningkatkan keamaan jaringan, sehingga penelitian ini belum di implementasikan. Perbandingan penelitian

penulis dengan penelitian sebelumnya adalah tools yang digunakan, jika penelitian sebelumnya menggunakan honeypot, pada penelitian penulis menggunakan Snort dan Base untuk menganalisis jaringan serta pada pencatatan serangan, Penelitian penulis diharapkan mampu melakukan pencatatan serangan dalam jaringan. Penelitian ini mengembangkan dari penelitian Dewi (2016). 2. Metode Penelitian Penelitian ini menggunakan pedekatan kuantitatif. Penelitian kuantitatif menurut pendekatan-pendekatan terhadap kajian empiris untuk mengumpulkan, menganalisa, dan menampikan data dalam bentuk numerik. Riset kuantitatif mencoba melakukan pengukuran yang akurat terhadap sesuatu. Lokasi penelitian pada Biro Sistem Informasi (BSI) Kampus Universitas Nusantara PGRI Kediri. Tahapan Penelitian seperti Gambar 1 Gambar 1. Tahapan Penelitian Tabel 1 merupakan kebutuhan sitem yang digunakan untuk membangun system. Untuk system operasi server menggunakan Ubuntu versi 16.04, sedangkan System Operasi client menggunakan windows 7. Setelah system operasi server terinstall, selanjutnya yaitu melakukan instalasi software yang dibutuhkan salah satunya yaitu SNORT IDS sebagai forensik jaringan. Tabel 1. Kebutuhan sistem Kebutuhan Keterangan Software System Operasi Server Ubuntu versi 16.04 System Operasi Client Windows 7 Intrusion Detection System SNORT IDS Version 2.9.9.0 Tools analysis Wiresharks Hardware 1 Buah PC Sebagai server IDS SNORT Min. 10 PC Sebagai simualsi serangan Kabel UTP Sebagai kabel jaringan 1 Buat Switch Menghubungkan antara komputer 3. Hasil dan Pembahasan 1. Instalasi SNORT Setelah selesai melakukan instalasi Linux Ubuntu 16.04, langkah selanjutnya yaitu instalasi SNORT. Instalasi sesuai dengan petunjuk pada website SNORT https://www.snort.org/. Gambar 2 merupakan hasil instalasi SNORT. Versi yang berhasil di install yaitu version 2.9.9.0 Gambar 2.Versi SNORT 2. Setting dan Konfigurasi SNORT Tahapan setelah melakukan instalasi SNORT adalah melakukan setting IP. Sebagian dari variable yang digunakan oleh SNORT rules untuk mendeterminasi fungsi system dan lokasi. Log pada SNORT dapat memberikan pilihan kondisi tentang event pada alert. Dari event tersebut kita dapat melihat IP address atau TCP port dari penyerang. Spesifik dari setting IP address pada SNORT seperti Gambar 3. Gambar 3. Setting IP Snort Ipvar HOME_NET merupakan IP dari PC yang akan kita lindungi. Pada kasus ini yang akan di lindungi adalah server dari universitas Nusantara PGRI Kediri. Namun pada kasus ini sebelum SNORT di fungsikan atau masih dalam uji coba, masih menggunakan Ipvar HOME_NET 192.168.173.1/24. Setelah melewati pengujian, maka untuk Ipvar HOME_NET akan di set IP Server. Gambar 4. Setting rules snort Rules digunakan untuk mendeteksi serangan. Rules yang di set memberikan knowledge pada saat proteksi, sehingga proses inverstigasi sangat tergantung dari knowledge rule. Gambar 4 merupakan konfigurasi dari penyimpanan rules, ketika terdapat serangan pada server maka log dari serangan tersebut akan tersimpan pada rule. Gambar 5 merupakan rules yang diterapkan yaitu: 1. Ping of death. SNORT melakukan pencatatan untuk semua paket ICMP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan “ping of death”. 2. Ketika terjadi serangan pada FTP maka akan muncul notifikasi “FTP connection attempt”. Gambar 5. Rules snort 3. Analisis Log SNORT Implementasi dilakukan pada server SNORT, log yang tersimpan akan di analisis mengikuti alur model proses forensik. Log akan di parsing untuk melihat isi dari SNORT log, apakah serangan itu bentuk berbahaya atau tidak. Log SNORT merupakan hasil dari Log yang diambil menggunakan opsi biner, TCPDump, atau Ethereal. Salah satu cara untuk membuka Log SNORT dengan menggunakan fungsi -r<filename> baik dari SNORT,

TCPDump, Ethereal atau program lain yang membuat file format libpcap. Gambar 6 merupakan perintah untuk membaca Log SNORT. Snort -dvr snort.log 1494909748 Gambar 6. Membuka Log Arti dari perintah Gambar 6 yaitu: d : untuk melihat isi dari paket. v : untuk melihat header TCP/IP. r : digunakan untuk membaca file log. Log yang dapat dibaca adalah Log yang tersimpan dalam bentuk libpcap format. SNORT dapat membaca selama yang disimpan dalam Log ada binary format dari sniffer SNORT. Setelah file Log tersebut berhasil diparsing, maka selanjutnya adalah melakukan analisis. Dari hasil uji coba terdapat 5 serangan yang tercapture pada SNORT Log, berikut ini adalah hasil inversitasi 5 serangan tersebut: 1) log.1494909748 Gambar 7 adalah hasil dari SNORT ditemukan serangan pada pukul 11:42:28 WIB, IP penyerang adalah 192.168.173.10, jenis serangan ICMP dengan Time to Live 128, ID 928, Seq 12545 dan packet 456 pkts/sec. Gambar 7. Isi dari log. 1494909748 Sedangkan runtime untuk proses packet adalah 0. 53779 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 8 merupakan detil dari penggunaan memory serta rincian packet yang diterima. Gambar 8. Total packet log.1494909748 2) log.1494910751 Gambar 9 adalah hasil dari SNORT ditemukan serangan pada pukul 16:10:29 WIB, IP penyerang adalah 192.168.0.70, jenis serangan ICMP dengan Time to Live 128, ID 384, Seq 27905 dan packet 78 pkts/sec. Gambar 9. Isi dari log. 1494910751 Sedangkan runtime untuk proses packet adalah 0. 38063 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 10 merupakan detil dari penggunaan memory serta rincian packet yang diterima. Gambar 10. Total packet log. 1494910751 3) log.1501040067 Gambar 11 adalah hasil dari SNORT ditemukan serangan pada pukul 16:10:00 WIB, IP penyerang adalah 192.168.0. 72, jenis serangan ICMP dengan Time to Live 128, ID 512, Seq 62976 dan packet 655 pkts/sec. Gambar 11. Isi dari log.1501040067 Sedangkan runtime untuk proses packet adalah 0. 91552 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 12 merupakan detil dari penggunaan memory serta rincian packet yang diterima. Gambar 12. Total packet log.1501040067 4) log.1503910699 Gambar 13 adalah hasil dari SNORT ditemukan serangan pada pukul 15:58:20 WIB, IP penyerang adalah 192.168.0. 96, jenis serangan ICMP dengan Time to Live 128, ID 369, Seq 4096 dan packet 19 pkts/sec. Gambar 13. Isi dari log.1503910699 Sedangkan runtime untuk proses packet adalah 0. 490 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 14 merupakan detil dari penggunaan memory serta rincian packet yang diterima. Gambar 14. Total packet log.1503910699 5) log.1503911199 Gambar 15 adalah hasil dari SNORT ditemukan serangan pada pukul 16:07:09 WIB, IP penyerang adalah 192.168.0.70, jenis serangan ICMP dengan Time to Live 128, ID 182, Seq 42496 dan packet 992 pkts/sec. Gambar 15. Isi dari log.1503910699 Sedangkan runtime untuk proses packet adalah 0.102570 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 16 merupakan detil dari penggunaan memory serta rincian packet yang diterima. 3) Dari hasil 5 serangan dapat dilakukan analisis, yaitu pukul berapa terjadi serangan, jenis serangan, serta total packet. 5. Referensi [1] Kompas., 2017., "Jangan Remehkan Ransomware Wannacry". http://tekno.kompas.com/read/2017/0 Gambar 16. Total packet log.1503910699 5/15/05310067/jangan.remehkan.rans omware.wannacry. 4. Kesimpulan [2] Mate, H.M., Kapse R.S., 2015, "Network Forensic Tool- Concept and Berdasarkan dari metode Model Architecture". Fifth International Proses Forensik dan implementasi dengan Conference on Communication System and Network Technologies. menggunakan tools

keamanan jaringan [3] Misra, R dan Dhir, R., 2012, SNORT maka dapat disimpulkan sebagai Cyber Crime Ivestigation and Network Forensic System Using berikut: Honeypot, International Journal of 1) Server SNORT yang dibangun Latest Trends in Engineering and Technology (IJLTET).ISSN : 2278- dapat memantau lalu lintas packet 621X di dalam jaringan serta mampu [4] Nugraha, S, G., Djanali, S., Pratomo, B, A., 2013, Sistem mendeteksi serangan berdasarkan Pendeteksi dan Pencegahan Serangan rule yang diset, sehingga serangan SQL Injection dengan Penghapusan Nilai Atribut Query SQL dan jaringan komputer tersebut dapat Honeypot, Jurnal Teknik Poimits Vol. segera ditangani. 2, No. 1, ISSN 2337-3539 [5] Dewi, E,K., 2016, Rancangan 2) Menggunakan Model Proses Keamanan Jaringan Dengan Forensik dapat menganalisis Menggunakan Model Proses Forensik, Jurnal Maklumatika, Vol. 2, serangan pada log SNORT, data No. 2, Januari 2016. ISSN 2407-5043. analisis tersebut bisa dijadikan [6] Snort. https://www.snort.org/. salah satu pembuktian terjadinya serangan, selain itu bisa digunakan sebagai bahan untuk pelaporan kepada pihak berwajib (jika diperlukan.) SNATIKA 2017, ISSN 2089-1083, page |30 SNATIKA 2017, ISSN 2089-1083, page |31 SNATIKA 2017, ISSN 2089-1083, page |32 SNATIKA 2017, ISSN 2089-1083, page |33 SNATIKA 2017, ISSN 2089-1083, page |34 SNATIKA 2017, ISSN 2089-1083, page |35 SNATIKA 2017, ISSN 2089-1083, page |36 SNATIKA 2017, ISSN 2089-1083, page |37