JIMP - Jurnal Informatika Merdeka Pasuruan
Vol 3 No 3 Desember 2018
ISSN 2503-1945

Peningkatan Keamanan Jaringan Pada EndPoint Menggunakan Metode Host Instrusion Detection And Prevention System Dengan Centralized Patch Vulnerability

Andri Fauzan [1], Iskandar Fitri [2], Novi Dian Nathasia [3]
Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
e-mail : **andrifauzan93@gmail.com** [1], iskandar.fitri@civitas.unas.ac.id [2], novidian@civitas.unas.ac.id [3]

Abstract

A system and a method enhance endpoint security of a computer network. The system and method generate security assessments of hosts on quarantined and non-quarantined networks. Based on the generated security assessments, secure hosts are connected to the non-quarantined network and non-secure or vulnerable hosts are connected to the quarantined network. Endpoint Security assists with fixing vulnerabilities of the hosts on the quarantined network. Endpoint security agents, security scanners, and remediation engines that carry out the foregoing functions reside on each of the quarantined and non-quarantined networks on hosts that are different from the target hosts. Under such an architecture, the endpoint security system can advantageously be operating system agnostic and can provide complete and powerful endpoint security complete with HIPS/HIDS for every endpoint.

***Keyword** : Endpoint Security, HIPS, HIDS*

Abstrak

Sebuah sistem dan metode meningkatkan keamanan endpoint dari jaringan komputer. Sistem dan metode menghasilkan keamanan endpoint pada jaringan yang dikarantina dan tidak dikarantina. Berdasarkan penilaian keamanan yang dihasilkan, endpoint yang aman terhubung ke jaringan yang tidak dikarantina dan endpoint yang tidak aman atau rentan terhubung ke jaringan yang dikarantina. Endpoint Security membantu memperbaiki kerentanan endpoint pada jaringan yang dikarantina. Agen keamanan Endpoint, pemindai keamanan, dan mesin remediasi yang menjalankan fungsi di atas berada pada masing-masing jaringan yang dikarantina dan tidak dikarantina pada endpoint yang berbeda. Dengan arsitektur seperti itu, sistem keamanan endpoint secara menguntungkan dapat menjadi sistem operasi agnostik dan dapat memberikan keamanan endpoint yang lengkap dan kuat dengan HIPS/HIDS, untuk setiap endpoint.

Kata Kunci : Endpoint Security, HIPS, HIDS

I. PENDAHULUAN

Sistem yang mendeteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem juga tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis. Selain itu sistem pertahanan terhadap aktivitas gangguan saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespons gangguan. Apabila terjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara *remote* sehingga tidak akan dapat melakukan pemulihan sistem dengan cepat. Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara otomatis sehingga memungkinkan administrator mengakses sistem walaupun terjadi malfungsi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Keamanan komputer atau dalam Bahasa Inggris computer *security* atau dikenal

juga dengan sebutan *cybersecurity* atau *IT security* adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. *Computer security* atau keamanan komputer bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi, teknologi yang dikenal dan dikembangkan dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian, pemalsuan data pada server dan keamanan data.

Sistem keamanan komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja dan proses komputer. Penerapan computer *security* dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi, interupsi, diganggu oleh orang yang tidak berwenang dan bertangung jawab. Keamanan bisa diindentifikasikan dalam masalah teknis, manajerial, legalitas. Computer *security* akan membahas 2 hal penting yaitu Ancaman/*Threats* dan Kelemahan sistem/*vulnerabillity*. Keamanan komputer adalah suatu sistem yang memberi persyaratan khusus, pembatasan terhadap komputer yang berbeda untuk Saling terkorelasi / berhubungan. Dilihat dari meluasnya dan perkembangan teknologi yang pesat maka berkembanglah juga sistem pengamanannya.

Penggunaan computer yang terkoneksi dengan jaringan baik intranet maupun internet tidak luput dari yang namanya serangan pada sistem komputer. Serangan tersebut tentunya sangat merugikan user apabila serangan tersebut mengambil, memodifikasi data penting dan merusak sistem atau melumpuhkan sistem yang sudah dimasukinya. Hingga saat ini, pendekatan yang dilakukan oleh administrator sistem adalah bagaimana caranya supaya para penyusup (krecker dan hecker) tidak dapat memasuki server dan mengambil atau merubah data.Namun, ternyata ada cara yang dapat digunakan untuk menanggulangi serangan hacker dengan membangun sistem computer yang memang sengaja dirancang untuk diserang oleh penyusup (krecker dan hacker).Keamanan sistem komputer adalah untuk menjamin sumber daya sistem tidak digunakan / dimodifikasi, diinterupsi dan diganggu oleh orang yang tidak diotorisasi.

1.1 Tujuan

a. Membangun system endpoint security yang tercentralized management.
b. Meningkatkan keamanan jaringan pada endpoint melalui patching vulnerability.

1.2 Batasan Masalah

a. Pengujian endpoint menggunakan salah satu tool aplikasi security.
b. Pengujian data hanya dilukan menggunakan file virus dan exploit system

II. METODE PENELITIAN

2.1 Host-based Intrusion Prevention Sistem (HIPS)

HIPS diinstall secara langsung di sistem yang diproteksi untuk dimonitor aktifitas sistem internalnya. HIPS digabungkan dengan setiap *endpoint security*. Sehingga HIPS bisa memantau dan menghadang sistem yang dicurigai dalam rangka mencegah terjadinya intrusi terhadap *endpoint*. HIPS juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu. Sebagai contoh HIPS untuk mencegah intrusion pada sql server mail server misalnya. Dari sisi *security* mungkin solusi HIPS bisa mencegah datangnya ancaman terhadap host. Tetapi dari sisi performance, harus diperhatikan apakah HIPS memberikan dampak negatif terhadap performance host. Karena menginstall dan bdigabungkan HIPS pada sistem *endpoint security* mengakibatkan penggunaan resource *endpoint* menjadi semakin besar.

2.2 HIDS (Host Intrusion *Detection* Sistem)

IDS jenis ini berjalan pada *endpoint* atau perlengkapan dalam sebuah jaringan. Sebuah HIDS melakukan pengecekan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada user atau administrator sistem jaringan akan adanya kegiatan-kegiatan yang mencurigakan yang terdeteksi oleh HIDS.

2.3 *Endpoint*

Merupakan titik akhir dari sebuah device yang digunakan oleh setiap user ataupun client dalam sebuah network. Baik berupa computer, lasptop, ataupun *mobile device.*

2.4 *Endpoint Security*

Perlindungan sistem *endpoint* dari penggunaan, akses, dan / atau kontrol yang tidak sah dan / atau tidak sah. Contoh sistem untuk perlindungan *endpoint* termasuk, tanpa batasan, sistem anti-malware, sistem otentikasi pengguna, sistem enkripsi, sistem privasi, layanan penyaringan spam, dan sejenisnya.

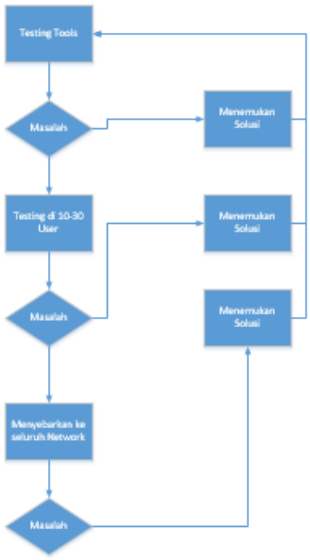
Pada penelitian sebelumnya yang dilakukan oleh: FadlinArsin, MuhYamin,"Implementasi sistem *Security* menggunakan metode IDPS (intrusion, *detection*, and, prevention sistem)" Universitas Halu Oleo 2017. Hanya sebatas layanan realtime notification yang mengahasilkan pengujian terhadap waktu dan penggunaan CPU.
Yang bisa dilihat pada gambar:

Gambar 1. Pengujian Fadlin Arsin Terhadap waktu

Untuk pembaruan yang peneliti lakukan pada pengujian ini menambahkan salah satu layanan yang bisa lebih meningkatkan kemanan jaringan dengan menggunakan *patch vulnerability* pada *endpoint*.

2.5 Perancangan

Langkah awal dalam perancangan sistem ini adalah pembuatan sistem flowchart. Flowchart ini merupakan gambaran awal dari sistem pada *endpoint* ini secara umum, yang menggambarkan sistem beserta hubungannya dengan lingkungan luar dan bagaimana sistem ini berinteraksi. Penjelasan sistem yang lebih rinci dapat dilihat pada Data Flow. Dari sini bisa didapatkan gambaran secara lebih jelas lagi tentang sistem yang akan dibangun.

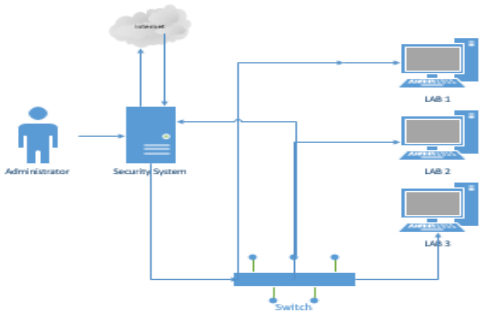


Gambar 2. Mengorganisir Proses

Gambar 3. *Endpoint* Flow

2.6 Tahap Konfigurasi Desain

Konfigurasi desain setiap *tools* untuk metode yang akan diterapkan pada security jaringan endpoint.



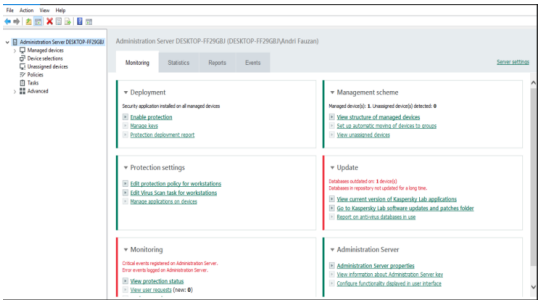
Gambar 4, Step Topology *tools* X

III. HASIL DAN PEMBAHASAN

3.1 Impelementasi

Impelementasi tools yang akan digunakan sebagai *system protection endpoint security* sebagai *console management.*

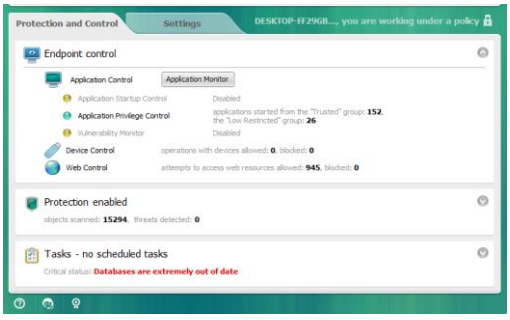
A. Management Console



Gambar 5. Dashboard Monitoring

Melalui dashaboard akan diketahui menegenai status setiap endpoint protection yang ada di setiap client.

B. Endpoint Protection

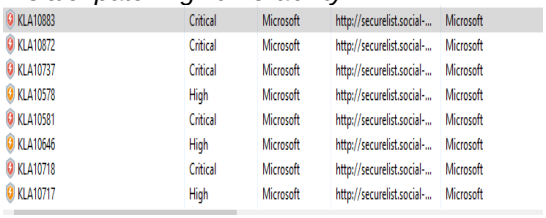


Gambar 6. Dashboard Monitoring

Endpoint Security akan diinstall pada setiap client yang akan di proteksi menggunakan security endpoint.

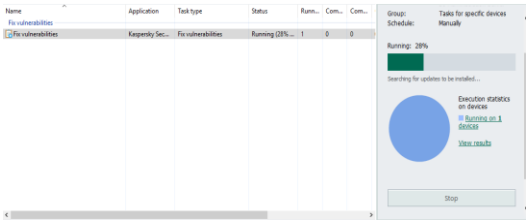
C. *Patching Vulnerability*

Vulnerability merupakan celah keamanan yang dimiliki oleh system operasi, yang merupakan pintu masuk dari hacker/cracker untuk merusak system ataupun mencuri data yang dimiliki. Pada system *endpoint* yang telah dibangun mempunyai salah satu fitur untuk mengatasi celah keamanan *vulnerability* melalui *patching vulnerability*.



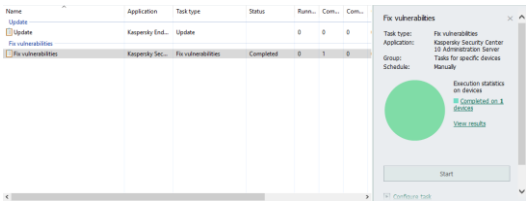
Gambar 7. *Patching Vulnerability*

Pada Gambar *patching vulnerability* akan diketahui informasi mengenai update system dari system operasi yang digunakan, melalui informasi yang didapatkan administrator akan lebih mudah untuk menjalankan task untuk memperbaiki *vulnerability* pada system operasi pada setiap *endpoint* yang terhubung di *network*.



Gambar 8. *Running Patch vulnerability*

Melalui *tasking fix vulenrabilty* akan dilakukan patching terhadap hole vulnerability yang ada disetiap endpoint.



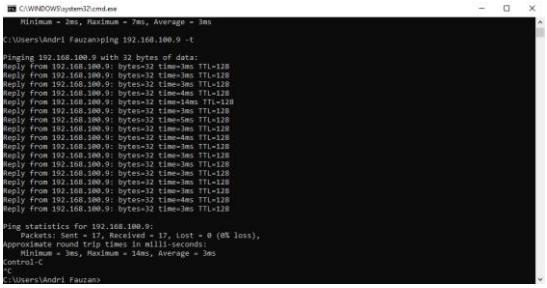
Gambar 9. tasking patching vulenerability complete

3.2 Uji Coba Sistem

Uji coba sistem yang akan dilakukan berikut ini merupakan proses pembuktian bahwa aplikasi ini telah sesuai dengan rancangan awal dari sistem yang telah dirancang pada bab sebelumnya dengan menggunakan metode Host Intrusion Detection and Prevention System dan dilakukan dengan menguji File Antivirus,Exploit. Pengujian dilakukan 2 kondisi pada saat tidak terlindungi dan terlindungi.

A. Pengujian Ping

Saat keadaan server tidak mengaktifkan sistem HIDPS/HIPS, PC penyerang mampu melakukan PING ke IP Address server seperti yang ditunjukkan oleh Gambar



Gambar 10. Pengujian Ping Sebelum di Blocked

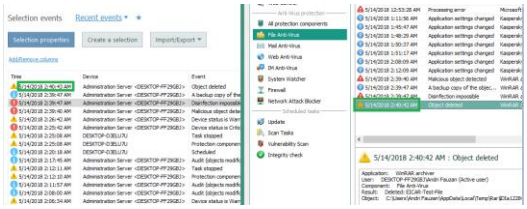
Setelah sistem keamanan HIDS/HIPS diterapkan blocked, maka setiap akses PING yang ditujukan ke server akan di blokir pada saat yang sama ditunjukkan oleh Gambar

Gambar 11, Pengujian Ping saat di Blocked

B. *Hasil Pengujian File Virus*

Hasil pengujian ini di dapat dengan cara memasukan virus eicar ke dalam komputer yang sudah terproteksi oleh *endpoint security*, virus eicar yang mencoba melakukan serangan ke dalam sistem telah dilakukan *blocked* oleh *endpoint security* dengan type virus.

Gambar 12. Grafik Pengamatan Virus Eicar *tools* X



Gambar 13. Waktu syhncronized Server

Pada Tabel dapat dilihat hasil deteksi pada pengujian File Virus

Tabel 1. Hasil Pengujian Virus Eicar

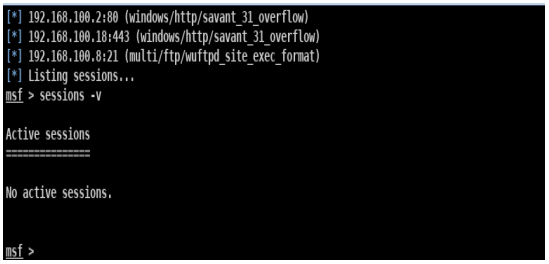
Exploit	IP Victim	Exploit	Blocked
Eicar Test File	192.168.100.8	100	100
Eicar Test File	192.168.100.1	100	100
Eicar Test File	192.168.100.2	100	100
Eicar Test File	192.168.100.18	100	100
Eicar Test File	192.168.100.17	100	100
Eicar Test File	192.168.100.4	100	100
Eicar Test File	192.168.100.7	100	100

Pada uji coba file antivirus dapat di check bahwa malware yang digunakan mampu di blocked oleh endpoint security yang interval synchronized action pada server mempunyai delay 1 second untuk melakukan deleted pada malware yang di uji coba.

C. Hasil Pengujian Exploit

Metode pengujian merupakan pembuktian *endpoint* setiap *tools* terhadap Host *Intrusion Detection Sistem and* Host Instrusion *Prevention Sistem* dengan menggunakan metode *exploit*. Dengan menggunakan linux kali untuk membuat *exploit* melalui network ke setiap *endpoint*:

Gambar 14. *Exploit* Melalui Linux Kali"Metasploit"



Gambar 15. Hasil *Exploit* Melalui Linux Kali"Metasploit"

Tabel 2. Hasil Pengujian Metasploit

Exploit	IP Attacker	IP Victim	Exploit	Blocked
Metasploit	192.168.100.28	192.168.100.8	815	815
Metasploit	192.168.100.28	192.168.100.1	383	383
Metasploit	192.168.100.28	192.168.100.2	408	408
Metasploit	192.168.100.28	192.168.100.18	408	408
Metasploit	192.168.100.28	192.168.100.17	28	28
Metasploit	192.168.100.28	192.168.100.4	25	25
Metasploit	192.168.100.28	192.168.100.7	25	25

Pengujian yang dilakukan melalui *exploit* terhadap jaringan dan *endpoint* menggunakan metasploit terhadap setiap sistem yang dirancang, Memperlihatkan hasil blocked yang 100% mampu melakukan blocked terhadap exploit yang dikirimkan ke setiap endpoint tanda adanya active session pada akhir exploit.

IV. KESIMPULAN

Berdarkan penelitian yang telah dilakukan selama perancangan sampai implementasi dan pengujian terhadap endpoint yang digunakan melalui metode Host Intrusion *Detection* dan Host Instrusion Prevention Sistem,maka dapat diambil kesimpulan bahwa pada penelitian ini:

1. Berhasil dibangun sistem peningkatan keamanan jaringan menggunakan *centralized management* yang mampu mendeteksi terhadap serangan malware, *exploit*pada system operasi yang digunakan yang akan mengurangi dampak dari serangan *malware* dan *network attack*.
2. Berhasilnya patching vulenerability secara centralized management pada endpoint untuk menutup hole vulnerability pada system operasi yang digunakan.

DAFTAR PUSTAKA

[1] Marshall A. Beddoe, Laguna Niguel, "*Sistem and method of network endpoint security*," United Stated Patent Badoe at all 2003

[2] D.Waltermire,D.Harrington, "*Endpoint Security* Posture Assessment," IETF 2015

[3] Matthew Palmer, Menlo Park, "*LOCAL CACHING OF ENDPOINT SECURITY INFORMATION*," Office Action from US. Appl. No. 11/236,987, dated Sep. 25, 2009.

[4] FadlinArsin, MuhYamin,"Implementasi sistem *Security* menggunakan metode IDPS (intrusion,*detection*,and, prevention sistem)" Universitas Halu Oleo 2017

[5] Yan Chen,Philip, "Sistem and Method for Providing *Endpoint* Management for *Security* Threat in Network Environment"Cisco Techonology 2010

[6] Michael Xie,Robert A.May Jinhai Yang,Marwah,,"Automated configuration of *endpoint security* management"Fortinet,Inc 2016

[7] Harald Schitz, Linz (AT); Andrew J. Thomas, Oxfordshire (GB); Kenneth D. Ray, Seattle, WA (US); Dan Schiappa, Bedford, NH (US) "KEY MANAGEMENT FOR COMPROMISED ENTERPRISE,*ENDPOINTS*"Sophos Limited 2016

[8] Kenneth D. Ray, Seattle, WA (US); Dan Schiappa, Bedford, NH (US); Simon Neil Reed, Wokingham (GB); Mark D. Harris, Oxon (GB); Neil Robert Tyndale Watkiss, Oxford (GB); Andrew J. Thomas, Oxfordshire (GB); Robert W. Cook, North Vancouver (CA); Harald Schitz, Linz (AT); John Edward Tyrone Shaw, Oxford (GB); Anthony John Merry, Kessel-lo (BE) "LABELING OBJECTS ON AN

ENDPOINT FOR ENCRYPTION MANAGEMENT" Sophos Limited 2016

[9] Jeffrey,CraigSchlauder, "MANAGING *SECURITY* OF *ENDPOINT*S OF A NETWORK" Jeffrey Craig Schlauder 2016

[10] Fandi,AdityaPutra,Joko Purwanto"PERANCANGAN PENGAMANAN JARINGAN PADA PERGURUAN TINGGI XYZ" Sekolah Tinggi Sandi Negara 2015

[11] Anthony Joseph Vargas,Christoper Robert Sharpe, Hollis Ann Jhonson"Sistem and Methods for providing *security* to an *endpoint* device" *Security* Together Corporation 2018

[12] Kevin Alejandro Roundy,"Sistem and Method For Classifying *Security* Event as Targeted *Attack*" Symantec Corporation 2016.

[13] Priti,More,Pune(in);KevinAgarwal"Siste m and Methods for Otaining information about *security* threats on *endpoint*-device"Syamantec Corporation 2017

[14] Walter Bogorad"Sistem and Methods For secure hybrid third-party data storage"Symantec corporation 2015.

[15] P.Du, A. Nakao,"DDoS Defense as NetworkService", *Network Operations and Management Symp. (NOMS 10)*, IEEE CS, pp.894-897, 2010.