ANALISIS PERBANDINGAN IMPLEMENTASI IPS MENGGUNAKAN FORTIGATE DAN UNTANGLE PADA PT. XYZ

TUGAS AKHIR

Gabriel Alexandro Hunam

41515120082

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2019

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM : 415151200082

Nama : Gabriel Alexandro Hunam

Judul Tugas Akhir : Analisis Perbandingan Implementasi IPS menggunakan Fortigate dan Untangle pada PT. XYZ

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 23 Januari 2020

Gabriel Alexandro Hunam

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Gabriel Alexandro Hunam
NIM	:	41515120082
Judul Tugas Akhir	:	Analisis Perbandingan Implementasi IPS menggunakan Fortigate dan Untangle pada PT.XYZ

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 23 Januari 2020

Gabriel Alexandro Hunam

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Gabriel Alexandro Hunam
NIM	:	41515120082
Judul Tugas Akhir	:	Analisis Perbandingan Implementasi IPS menggunakan Fortigate dan Untangle pada PT.XYZ

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis			Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi			Diajukan	✓
		Jurnal Nasional Terakreditasi	✓			
		Jurnal International Tidak Bereputasi			Diterima	
		Jurnal International Bereputasi				
	Disubmit/dipublikasikan di :	Nama Jurnal	: Rekayasa Sistem dan Teknologi Informasi (RESTI)			
		ISSN	: 2580-0760			
2	Kertas Kerja, Merupakan material haasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review				[✓]
		Hasil analisa & perancangan aplikasi				[✓]
		Source code				[✓]
		Data set				[✓]
		Tahapan eksperimen				[✓]
		Hasil eksperimen seluruhnya				[✓]
		....				
3	HAKI Disubmit / Terdaftar	HKI			Diajukan	
		Paten			Tercatat	
		No & Tanggal Permohonan	:			
		No & Tanggal Pencatatan	:			

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 23 Januari 2020

Gabriel [illegible]nam

LEMBAR PERSETUJUAN

Nama Mahasiswa	:	Gabriel Alexandro Hunam
NIM	:	41515120082
Judul Tugas Akhir	:	Analisis Perbandingan Implementasi IPS menggunakan Fortigate dan Untangle pada PT.XYZ

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 23 Januari 2020

Menyetujui,

(Raka Yusuf , S.T., MTI)

Dosen Pembimbing

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41515120082
Nama	:	Gabriel Alexandro Hunam
Judul Tugas Akhir	:	Analisis Perbandingan Implementasi IPS menggunakan Fortigate dan Untangle pada PT.XYZ

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 11 Februari 2020

(Desi Ramayanti, S.Kom, MT)
Ketua Penguji

(Diky Firdaus, S.Kom, MM)
Anggota Penguji 1

(Herry Derajad Wijaya, S.Kom. MM)
Anggota Penguji 2

LEMBAR PENGESAHAN

NIM	:	41515120082
Nama	:	Gabriel Alexandro Hunam
Judul Tugas Akhir	:	Analisis Perbandingan Implementasi IPS Menggunakan Fortigate Dan Untangle Pada PT. XYZ

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 11 Februari 2020

Menyetujui,

(Raka Yusuf, S.T., MTI)
Dosen Pembimbing

Mengetahui,

(Diky Firdaus, S.Kom, MM)
Koord. Tugas Akhir Teknik Informatika

(Desi Ramayanti, S.Kom, MT)
Ka. Prodi Teknik Informatika

KATA PENGANTAR

Puji syukur kita panjatkan Allah Subhanahu Wa Ta'ala yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Analisis Perbandingan Implementasi IPS menggunakan Fortigate dan Untangle pada PT.XYZ" tepat pada waktunya. Tugas akhir ini disusun untuk memenuhi salah satu syarat memperoleh gelar sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Penulis menyadari bahwa tanpa bantuan dan bimbingan yang melibatkan banyak pihak, penelitian ini tidak akan terlaksana dengan baik. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Raka Yusuf , S.T., MTI , selaku dosen pembimbing tugas akhir yang telah meluangkan waktunya untuk memberikan bimbingan serta arahan dalam penyusunan tugas akhir ini hingga selesai.
2. Ibu Desi Ramayanti, S.Kom., MT, selaku Kepala Prodi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.
3. Bapak Diky Firdaus, S.Kom., MM, selaku Koordinator Tugas Akhir Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana tahun ajaran 2019/2020.
4. Bapak Diky Firdaus, S.Kom., MM, selaku Dosen Pembimbing Akademik Universitas Mercu Buana.
5. Kedua Orang tua yang senantiasa memberikan doa dan dukungan kepada penulis.
6. Semua pihak yang telah banyak membantu dalam penyusunan tugas akhir ini yang tidak dapat penulis sebutkan satu persatu

Akhir kata, penulis berharap tugas akhir ini dapat bermanfaat bagi pembaca guna menambah pengetahuan dan wawasan.

Jakarta, 23 Januari 2020

Gabriel Alexandro Hunam

DAFTAR ISI

Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. x No. x (20xx) xx - xx ISSN Media Elektronik: 2580-0760

Analisis Perbandingan Implementasi Ips Fortigate Dan Untangle pada PT. XYZ

Abstact

Server security is necessary to avoid all attack that will happen. IPS (Intrusion Prevention System is an example of solution for the security system. IPS can prevent an attack by using the IDS (Intrusion Detection System) features and firewall features to block access of a connection.

In this research, IPS (Fortigate and Untangle) on the server tested with some attack include DOS (Denial of Service) and FTP brute force with two different topologies. These attack will conclude security metric analysis using VEA-bility metric which the value of that metric will determine how secure a system owned by a range of value from 0 to 10 based on calculation involving the value of vulnerability dimension, exploitability dimension and attackability dimension. In this experiment we got 3.07 score from non-firewall topology and 6.81 score from server with firewall topology. Meanwhile we got 1.83 score for DOS attack and 4.27 for FTP brute force attack for CVSS.

Keywords: Intrusion Prevention System (IPS), Fortigate, Untangle, VEA-bility metric.

Abstrak

Keamanan server sangat diperlukan untuk menghindari serangan yang akan terjadi. IPS (Intrusion Prevention System) merupakan salah satu contoh solusi yang tepat untuk pengamanan suatu sistem. IPS dapat mencegah suatu serangan dengan memanftaatkan fitur dari IDS (Intrusion Detection System) dan fitur firewall yang mampu menolak akses dari suatu koneksi.

Pada tugas akhir ini, dilakukan implementasi IPS (Fortigate dan Untangle) pada server yang kemudian diuji dengan serangan yang meliputi DOS (Denial of Service) dan FTP brute force dengan dua topologi yang berbeda. Dari serangan tersebut, dilakukan analisa security metric dengan metode VEA-bility metric dimana hasil dari VEA-bility yang berupa nilai akan menentukan seberapa aman suatu sistem yang dimiliki dengan rentang nilai dari 0 hingga 10 yang didapatkan berdasarkan perhitungan yang melibatkan nilai vulnerability dimension, exploitability dimension dan attackability dimension. Dari hasil pengujian, didapatkan nilai 3.07 untuk topologi tanpa firewall an 6.81 untuk topologi server dengan firewall Sementara itu didapatkan nilai CVSS untuk masing – masing serangan yaitu 1.83 untuk DOS dan 4.27 untuk FTP brute force.

Kata kunci: Intrusion Prevention System (IPS), Fortigate, Untangle, VEA-bility metric.

1. Pendahuluan

Jaringan internet merupakan hal yang umum ditemui saat ini. Bagi orang yang bergelut di bidang teknologi dan informasi, jaringan internet merupakan perantara yang diperlukan untuk melakukan pekerjaannya. Selain pekerjaan, internet juga dapat diakses oleh semua orang untuk media hiburan dengan menghubungkan pengguna ke suatu penyedia layanan seperti website. Setiap penyedia layanan tentunya memiliki media penyimpanan yang berukuran besar yang mampu menyimpan data yang dapat diakses oleh pengguna atau sering disebut dengan *server*. Banyak tidaknya pengguna yang akan mengakses layanan, tentunya harus sebanding dengan kemampuan *hardware* yang memadai agar layanan tersebut dapat dinikmati.

Namun, tidak jarang ada pengguna yang melakukan penyerangan terhadap *server* dari suatu layanan. Dari pengguna yang hanya mencoba menyerang, hingga serius menyerang untuk memperoleh tujuan tertentu. Selain berdampak pada *server*, penyerangan suatu layanan tak jarang akan menganggu pengguna lain juga. Misalnya penyerangan DOS yang akan membuat *traffic* padat sehingga *server* menjadi *down* dan pengguna lainnya tidak dapat mengakses layanan tersebut. Contoh lain misalnya adanya sniffing yang membuat *password* terekam oleh pengguna yang melakukan *sniffing*.

Diterima Redaksi : xx-xx-20xx | Selesai Revisi : xx-xx-20xx | Diterbitkan Online : xx-xx-20xx

Tentunya hal ini membuat rugi dari sisi pengguna dan penyedia layanan.

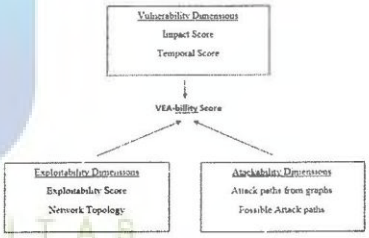
Oleh karena itu, diperlukan sebuah sistem keamanan yang dapat diimplementasikan di server sehingga pengguna akan merasa aman pada saat mengakses suatu layanan yaitu IPS. IPS (*intrusion prevention system*) merupakan suatu system keamanan jaringan yang dapat memantau aktifitas jaringan yang mencurigakan. Fungsi utama dari IPS adalah mengidentifikasi, mencatat, hingga menghentikan aktivitas yang mencurigakan pada suatu jaringan. IPS merupakan gabungan Antara IDS (*intrusion detection system)* yang berguna untuk mengidentifikasi atau mendeteksi suatu aktifitas yang mencurigakan pada jaringan dan *firewall* yang berfungsi untuk memblokir lalu lintas data pada suatu jaringan. **[1]**

Banyaknya IPS yang ada membuat pemilik suatu sistem harus benar – benar memilih dari segala sisi. Ada 2 IPS yang pada tugas akhir ini akan dilakukan untuk melakukan tindakan perlindungan dan pencegahan yaitu IPS dari Fortigate dan IPS dari Untangle. Fortigate adalah sebuah sistem keamanan dari segmen produk jaringan yang dikhususkan untuk menangani fungsi keamanan jaringan secara terpadu yang dikeluarkan oleh perusahaan Fortinet yang mana merupakan pemimpin pasar untuk *unified threat management.* Fortigate memiliki fitur – fitur unggulan seperti *firewall, antivirus, web filtering,* dan pada penelitian kali ini fitur *intrusion prevention system* nya lah yang akan digunakan. **[2]** Fortigate ini nantinya akan dibandingkan dengan Untangle, suatu aplikasi yang digunakan pada perangkat jaringan computer untuk menangani serangan – serangan seperti *spam filter, spyware blocker, virus, adware,* dan lain – lain. Aplikasi ini merupakan turunan dari Debian dan terdiri atas dua jenis yaitu versi gratis dan versi berlangganan. **[3]**

Kedua IPS ini akan diuji secara terpisah untuk melakukan simulasi pertahanan dari serangan – serangan yang pada tugas akhir ini adalah DDOS (*Distributed Denial of Service Attack)* suatu jenis serangan melumpuhkan sebuah layanan dengan cara menghabiskan sumber daya yang diperlukan system komputer untuk melakukan kegiatan normalnya. Serangan ini awalnya melakukan *scanning* terhadap celah yang ada. Setelah mendapatkan celah keamanan, maka serangan akan dilakukan. Beberapa cara melakukan penyerangan diantaranya *traffic flooding* yaitu membanjiri lalu lintas data, *request flooding* yaitu membanjiri dengan banyak *request,* dan melakukan perubahan system terhadap konfigurasi yang sudah disediakan. Contoh jenis serangan DDOS pada penelitian kali ini adalah SYN Flood yang dilakukan dengan cara memanfaatkan kelemahan protocol pada saat terjadinya proses *handshake.* **[4]** Serangan yang akan disimulasikan selanjutnya adalah seperti FTP *brute force* suatu metode yang bertujuan untuk mendapatkan password pada layanan FTP. Serangan ini dilakukan pada *port* 21 dan mencoba semua kemungkinan *password* yang ada secara paksa hingga mendapatkan *password* yang diinginkan. Semakin panjang dan unik karakter dari *password,* waktu yang dibutuhkan untuk mendapatkan *password* dari metode ini semakin lama. **[5]**

Tujuan dari penelitian adalah untuk melihat hasil perbandingan performa dari kedua IPS ini dalam melakukan pencegahan dengan mengukur tingkat keamanan system dengan CVSS (*Common Vulnerability Scoring System)* untuk menilai kerentanan suatu system keamanan dari skor 0.0 – 10.0 yang dimana terbagi menjadi 4 aspek, yakni Low (0.0 – 3.9), Medium (4.0 – 6.9), High (7.0 – 8.9), dan Critical(9.0 – 10.0). **[6]**

Setelah penilaian dari suatu system oleh CVSS perbandingan akan dilakukan melalui pendekatan metode *security metric* yaitu VEA-*bility. VEA-bility* merupakan suatu metric yang dapat menunjukkan seberapa aman system yang diuji dengan memberikan nilai dari 0 hingga 10. Metode ini sendiri dipecah menjadi tiga dimensi yaitu V (*vulnerability),* E *(exploitability)* dan A *(attackbility)* data yang digunakan untuk mengolah metric ini didapat dari topologi jaringan (*network topology), attack graph,* dan nilai yang ditetapkan oleh Common Vulnerability Scoring System (CVSS). [7]



Gambar 1. Dimensi VEA-bility metric

Gambar 1. Merupakan dimensi untuk VEA-bility *metric.* Dari gambar, dapat dilihat bahwa nilai VEA-bility dipengaruhi oleh *Vulnerability Dimension* didapat dari *impact score* dan *temporal score, Exploitability Dimension* didapat dari *exploitability score* dan *network topology,* dan *Attackbility Dimension* yang didapat dari *attack path* dan *possible attack path.* Untuk suatu jaringan N, dapat dibagi V(*host*), E(*host*), dan A (*host)* sebagai skor untuk setiap dimensi.

Untuk menghitung *Network Vulnerability Dimension* dapat dilihat pada Gambar 2.

Network Vulnerability dimension

$$V(host) = \min(10, \ln \Sigma e^{S(v)})$$

$$S(v) = \frac{Impact\ Score(v) + Temporal\ Score(v)}{2}$$

Keterangan :
V (*host*) = Nilai *vulnerability* pada *host*
Min = Fungsi minimum (mengambil nilai terendah)
Ln = Logaritma natural
Σ = Fungsi *sigma* yaitu operator penjumlahan
e = Eksponensial, merupakan bilangan natural dengan nilai 2.71828183
S(v) = Nilai *severity* dari *vulnerability*
Impact score (v) = Nilai *impact* yang didapat dari perhitungan CVSS
Temporal score (v) = Nilai temporal yang didapat dari perhitungan CVSS

Gambar 2. Network Vulnerability Dimension

Untuk menghitung *Network Exploitability Dimension* dapat dilihat pada Gambar 3.

Network Exploitability Dimension

$$E(host) = \frac{(\min(10, \ln \Sigma e^{Exploitability\ score(v)})(\#service\ on\ host)}{(\#network\ services)}$$

Keterangan :
E (*host*) = Nilai *exploitability* pada *host*
Min = Fungsi *minimum* (mengambil nilai terendah)
ln = Logaritma natural
Σ = Fungsi *sigma* yaitu operator
e = Eksponensial, merupakan bilangan natural dengan nilai 2.71828183
#service on host = Jumlah *service* yang dapat diakses *host*
#network services = Jumlah *service* yang tersedia pada jaringan

Gambar 3. Network Exploitaility Dimension

Untuk menghitung *Network Exploitability Dimension* dapat dilihat pada Gambar 4.

***Network Attackability dimension*:**

$$A(host) = \frac{(10)(\#attackpaths)}{(\#network\ paths)}$$

Keterangan :
A (*host*) = Nilai *attackability* pada *host*
#attack path = Jumlah jalur untuk melakukan serangan
#network path = Jumlah jalur yang tersedia untuk mengakses layanan

Gambar 4. Network Attackability Dimension

Analisa dari segi *security metric* dilakukan untuk mengetahui IPS mana yang lebih aman untuk diimplementasikan ke suatu sistem akan diambil kesimpulan berdasarkan hasil akhir dalam penilaian *VEA-bility.*

Perhitungan VEA-bility:

$$VEA - bility = 10 - \frac{(10)(\#attack\ paths)}{(\#network\ paths)}$$

Keterangan :
VEA-bility = Nilai VEA-bility pada sistem
V = Nilai *vulnerability*
E = Nilai *exploitability*
A = Nilai *attackability*

Gambar 5. Perhitungan VEA-bility

2. Metode Penelitian

Intrusion Prevention System bisa dikatakan adalah sebuah sistem keamanan jaringan komputer yang perlu dikonfigurasi agar dapat secara otomatis melakukan perlindungan dari serangan – serangan yang berusaha untuk menghancurkan atau mencuri data dan informasi yang kita miliki. Namun saat ini banyak sekali produk dan juga aplikasi IPS yang tersedia mulai dari yang versi gratis hingga berbayar. Oleh karena itu, dibutuhkan teori dan metode pendukung untuk membandingkan kinerja dari IPS agar dapat diambil kesimpulan performa IPS mana yang lebih baik.

2.1. Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah dengan cara studi pustaka dan observasi. Metode studi pustaka digunakan mengetahui teori dan praktik yang berhubungan dengan penelitian yang dilakukan oleh penulis. Selain melakukan studi pustaka, penulis juga melakukan observasi objek penelitian. Objek penelitian yang dilakukan penulis adalah di PT. Artha Mulia Trijaya untuk menentukan perangkat jaringan yang menjadi bahan untuk diteliti, mulai dari jumlah perangkat, tipe perangkat, desain topologi jaringan dan konfigurasi dari perangkat jaringan. Untuk alat observasi yang digunakan adalah berupa buku catatan untuk mencatat informasi penting dari hasil kegiatan oservasi dan desain topologi jaringan PT. Artha Mulia Trijaya.

Dari hasil observasi yang dilakukan didapati informasi bahwa jaringan yang tersedia saat ini hanya menggunakan router dari provider sebagai yang menjembatani Antara server dengan internet. Ada beberapa masalah dengan topologi yang ada saat ini seperti menurut informasi dari IT support setempat server pernah diserang beberapa kali dengan DDOS dan dengan *brute force.* Dikarenakan tidak adanya perlindungan yang mampu menangani serangan ini maka solusi sementaranya adalah memutuskan koneksi server dengan internet.

Gambar 6. Topologi tanpa firewall

2.2. Analisis Data

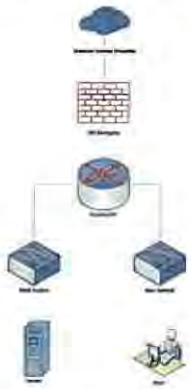
Dengan permasalahan yang ada maka usulan metode yang dilakukan ialah melakukan implementasi dengan menggunakan IPS untuk melindungi server dari serangan – serangan yang sebelumnya tidak dapat diatasi oleh router dari provider.

Gambar 7. Topologi server dengan firewall

Dengan topologi yang direkomendasikan seperti ini, maka tindakan pencegahan terhadap serangan – serangan terhadap server internal dapat dilakukan karena setiap *traffic* dari luar yang masuk menuju server akan dilakukan *filtering* oleh IPS untuk dapat dipantau keamanan dari *traffic* tersebut. Jika *traffic* yang masuk setelah di periksa oleh IPS didapati mengandung data yang berbahaya dan dapat mengancam keamanan dari server maka dengan otomatis IPS akan melakukan pemblokiran terhadap *traffic* tersebut.

2.3. Metode Pengujian

Metode pengujian tugas akhir ini adalah dengan mengimplementasikan IPS Fortigate dan Untangle. Penyerang akan melakukan serangan seperti DDOS dan *brute force* menuju server dan akan dilindungi oleh IPS yang telah diimplementasikan. Maka dari itu pengujian akan dilakukan dengan 2 topologi yang berbeda yang mana topologi pertama IPS yang akan diimplementasikan adalah IPS Fortigate.



Gambar 8. Implementasi IPS Fortigate

Sementara untuk topologi yang kedua, IPS yang akan diimplementasikan adalah IPS dari Untangle.

Gambar 9. Implementasi IPS Untangle

2.4. Kebutuhan Perangkat

Untuk membangun dan mengimplementasikan IPS dibutuhkan perangkat pendukung mulai dari yang sudah ada maupun yang akan diimplementasikan dalam berupa *software* dan *hardware*. Berikut tabel dari kebutuhan perangkat pendukungnya :

Tabel 1 Kebutuhan software

Nama	Versi	Fungsi
Windows OS	7 Ultimate	FTP Server
Kali Linux OS	5.2.9	Attacker

Tabel 2 Kebutuhan *hardware*

Nama	Versi	Fungsi
Mikrotik	v6.44.6	Router ISP
HP	v12.57	Switch
Fortigate	v5.6	IPS
Untangle	v14.2	IPS

Untuk spesifikasi FTP Server yang dibutuhkan untuk dijalankan meliputi 2GB RAM, 500 HDD, Processor Intel i5 dan OS yang digunakan adalah Windows 7 Ultimate.

3. Hasil dan Pembahasan

3.1. Pemilihan poin pada metric

VEA-bility metric dipengaruhi oleh tiga metric yaitu Vulnerability, Exploitability, dan Attackability. Untuk mendapatkan nilai Vulnerabilit, dan Exploitability, diperlukan perhitungan metric dari CVSS. Langkah pertama untuk mencari nilai tersebut adalah memilih poin yang mempengaruhi nilai base metric dan temporal metric untuk setiap serangan yang diuji pada masing – masing IPS. Tabel pemilihan metric CVSS terdapat pada lampiran.

Tabel 3. Pemilihan poin Base metric pada Fortigate

Serangan	Base Metric					
	Attack Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability
DOS	Local	Low	None	None	None	Partial
FTP Brute Force	Local	Medium	None	Partial	Complete	None

Tabel 4. Pemilihan poin Temporal Metric pada Fortigate

Serangan	Temporal Metric		
	Exploitability	Remediation Level	Report Confidence
DOS	Functional exploit exists	Official fix	Unconfirmed
FTP Brute Force	Functional exploit exists	Official fix	Unconfirmed

Tabel 5. Pemilihan poin Base Metric pada Untangle

Serangan	Base Metric					
	Attack Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability
DOS	Local	Low	None	None	None	Partial
FTP Brute Force	Local	Medium	None	Partial	Complete	None

Tabel 6. Pemilihan poin Temporal Metric pada Untangle.

Serangan	Temporal Metric		
	Exploitability	Remediation Level	Report Confidence
DOS	Functional exploit exists	Official fix	Uncorroborated
FTP Brute Force	Functional exploit exists	Official fix	Uncorroborated

Pada Tabel 3 menunjukkan pemilihan base metric pada Fortigate, dan Tabel 5 menunjukkan pemilihan base metric pada Untangle. Base metric dipengaruhi oleh attack vector, access complexity, authentication, confidentiality, integrity, dan availability. Pada serangan kedua serangan yang diuji, dipilih "local" pada attack vector karena serangan pada percobaan ini dilakukan dengan media kabel (wireline). Access complexity pada serangan DOS dipilih "low" karena serangan dapat dilakukan secara manual dan tidak memerlukan informasi tambahan, sedangkan pada serangan FTP Brute force dipilih "medium" karena untuk melakukan serangan, diperlukan informasi tambahan seperti nama username dan akun FTP. Pada authentication, ketiga serangan dipilih "none" karena untuk melakukan serangan tidak diperlukan adanya authentikasi. Pada confidentiality untuk serangan DOS dipilih "low" karena serangan tersebut tidak akan berdampak pada ke kerahasiaan (confidential) dari system yang diserang, sementara itu untuk serangan FTP brute force dipilih "partial" karena serangan ini akan berdampak pada ke kerahasiaan (confidential) dari system yang diserang, sementara itu untuk serangan FTP Brute Force dipilih "partial" karena serangan ini akan berdampak ke kerahasiaan suatu system seperti memberikan informasi apa yang ada dalam server FTP. Pada Integrity, serangan DOS dipilih "none" karena serangan tersebut tidak mempengaruhi integritas system, sedangkan pada serangan FTP brute force dipilih "complete" karena serangan ini dapat mempengaruhi integritas system yaitu dengan cara memodifikasi file pada system. Pada availability, serangan DOS dipilih "complete" karena serangan ini dapat mempengaruhi availability system atau dapat membuat server menjadi tidak dapat diakses, sementara itu serangan FTP brute force dipilih "none karena tidak mempengaruhi availability dari system.

Pada Tabel 4 menunjukan pemilihan temporal metric pada Fortigate dan Tabel 6 menunjukkan pemilihan temporal metric pada Untangle. Temporal metric dipengaruhi oleh exploitability, remediation level dan report confidence. Pada kedua serangan exploitability dipilih "functional exploit exist" karena serangan tersebut memiliki source code dan dapat bekerja dalam situasi apapun. Pada remediation level, dipilih "official fix" karena baik fortigate maupun untangle memiliki signature yang resmi dan dapat di update.

Pemilihan base metric pada kedua IPS sama karena serangan mengakibatkan pengaruh yang sama. Sedangkan pada temporal metric yaitu Report Confidence berbeda. Report Confidence merupakan suatu laporan mengenai kerentanan (vulnerability) dari IPS yang digunakan. Pada Fortigate dipilih "unconfirmed" karena laporan vulnerability tidak ada pada situs resminya namun ada sedikit daftar vulnerability yang dapat dilihat pada situs cvedetails. Sedangkan pada untangle dipilih "uncorroborated" karena laporan vulnerability tidak tersedia pada situs resminya namun terdapat banyak daftar vulnerability dibandingkan Fortigate yang dapat dilihat pada situs cvedetails.

3.2. Perhitungan base dan temporal metric pada setiap serangan

Langkah selanjutnya setelah pemilihan poin serangan adalah menghitung nilai dari poin yang telah ditentukan. Berikut merupakan table hasil perhitungan base dan temporal metric berdasarkan perhitungan CVSS.

Tabel 7. Nilai base dan temporal score pada Fortigate

Serangan	Base Score			Temporal Score
	Base	Impact	Exploitability	
DOS	2.1	2.9	3.9	1.6
FTP BRUTE FORCE	5.4	7.8	3.4	4

Tabel 8. Nilai base dan temporal metric pada Untangle

Serangan	Base Score			Temporal Score
	Base	Impact	Exploitability	
DOS	2.1	2.9	3.9	1.6
FTP BRUTE FORCE	5.4	7.8	3.4	4

Tabel 7 menunjukkan nilai base dan temporal pada Fortigate. Pada table dapat dilihat bahwa nilai base, impact dan temporal berbeda – beda untuk setiap serangan. Sedangkan untuk exploitability hanya berbeda untuk serangan FTP brute force, Misalnya untuk serangan DOS, didapatkan nilai 2.1 untuk base, 2.9 untuk impact, 3.9 untuk exploitability dan 1.6 untuk temporal. Hal ini didapat dari pemilihan poin metric pada Tabel 3.1 dan Tabel 3.2.

Tabel 8 menunjukkan nilai base dan temporal untuk Untangle. Pada table dapat dilihat bahwa nilai base, impact dan temporal berbeda beda untuk serangan FTP brute force.

Tabel 8 menunjukkan nilai base dan temporal untuk Untangle. Pada table dapat dilihat bahwa nilai base, impact dan temporal berbeda beda untuk serangan FTP brute force. Hal ini didapat dari pemilihan point metric pada Tabel 5 dan Tabel 6. Perhitungan tersebut didapat dengan perhitungan CVSS.

Berikut merupakan contoh perhitungan base score dan temporal score pada serangan DOS.

a. Perhitungan base score. Nilai pada setiap poin didapat dari CVSS.

Diketahui:
Attack vector = local = 0.395
Attack Complexity = low = 0.71
Authentication = none = 0.704
Conf Impact = none = 0
Integ Impact = none = 0
Avail Impact = partial = 0.275

Keterangan :
I = Impact
E = Exploitability
C = Conf Impact
Ig = IntegImpact
A = AvailImpact
R = round_to_1_decimal
Av = Attack Vector
Ac = AttackComplexity
Au = Authentication

$$\text{Base Score} = R\left(((0.6 * I) + (0.4 * E) - 1.5) * f(I)\right) \quad (3.1)$$

$$f(I) \{ 0, I = 0 \} \quad (3.2)$$

$$f(I) \{ 1.176, I \neq 0 \quad (3.2)$$

$$I = 10.41 * (1 - (1 - C) * (1 - Ig) * (1 - A)) \quad (3.3)$$

$$E = 20 * Av * Ac * Au \quad (3.4)$$

Keterangan :
Round_to_1_decimal = pembulatan keatas yang menghasilkan satu angka decimal.
R = Round_to_1_decimal

Perhitungan :
Impact = 10.41 * (1 – (1-0) * (1 – 0) * (1 – 0.275))
= 10.41 * (1 – 0.725)
= 2.86275
Exploitability = 20 * 0.395 * 0.71 * 0.704
= 3.948736
Base Score = R (0.6*2.86275) + (0.4 * 3.948736) – 1.5) * 1.176
= R ((1.71765 + 1.5794944 – 1.5) * 1.176)

= R (2.1134418144)
= **2.1**

b. Perhitungan temporal score. Nilai pada setiap poin didapat dari CVSS.

Berikut merupakan perhitungan nilai temporal pada Fortigate.

Diketahui :
Exploitability = functional = 0.95
Remediation Level = official fix = 0.87
Report Confidence = unconfirmed = 0.9

Keterangan :
T = TemporalScore
R = Round_to_1_decimal
Bs = Base Score
E = Exploitability
Rm = RemediationLevel
Rc = ReportConf

$$T = R (Bs * E * Rm * Rc) \quad (3.5)$$

Keterangan :
Round_to_1_decimal = Pembulatan keatas yang menghasilkan satu angka decimal.
BaseScore = nilai base yang didapat dari persamaan (3.1)

Perhitungan :
TemporalScore = R (2.1*0.95*0.87*0.9)
= R (1.562085)
= **1.6**

Nilai base dan temporal pada Bro dan Snort sama walaupun terdapat perbedaan pemilihan poin pada report confidence. Hal ini dikarenakan pada selisih score pada poin unconfirmed dan uncorroborated hanya 0.05 dan pada perhitungannya terdapat pembulatan sehinga nilai yang dihasilkan sama.

3.3. Perhitungan nilai VEA setiap topologi

Setelah mendapatkan nilaibase dan temporal, langkah selanjutnya adalah menghitung nilai VEA pada setiap serangan yang ada di topologi yang berbeda. Seperti yang sudah dijelaskan pada persamaan (2.2) nilai V dipengaruhi oleh nilai base dan temporal, sedangkan nilai E dipengaruhi oleh nilai Exploitability (Persamaan (2.3)). Berikut merupakan nilai VEA untuk setiap topologi :

a. Topologi tanpa firewall

Tabel 9. Nilai VEA pada topologi tanpa firewall

Serangan	VEA-bility tiap serangan				VEA Score
	V	E	A	Nilai VEA	
DOS	2.25	3.9	10	4.61666667	3.07121811
FTP Brute Force	5.9	3.4	10	3.56666667	

Tabel 9 menunjukkan nilai VEA-bility pada topologi tanpa firewall. Perhitungan ini, didapatkan dari persamaan (2.1), nilai E didapat dari persamaan (2.2), dan nilai A menjadi 10 karena seperti yang bisa dilihat pada gambar 3.2, Server tidak memiliki perlindungan sama sekali dari serangan yang dilakukan. Sehingga A = 10 * (4/4) = 10 sesuai dengan persamaan (2.3). Tabel 4.7 menunjukkan nilai VEA untuk topologi tanpa firewall adalah 3.07. Nilai ini didapat dari persamaan (2.5).

b. Topologi server dengan firewall

Tabel 10. Nilai VEA pada topologi server dengan firewall

Serangan	VEA-bility tiap serangan				VEA Score
	V	E	A	Nilai VEA	
DOS	2.25	2.925	0	8.275	6.809386448
FTP Brute Force	5.9	2.55	0	7.18333	

Tabel 10 menunjukkan nilai VEA-bility pada topologi server dengan firewall. Perhitungan ini, didapatkan dari perhitungan pada persamaan (2.5). Pada topologi ini, nilai V didapat dari persamaan (2.1), nilai E didapat dari persamaan (2.2), dan nilai A dibuat menjadi 0 karena pada topologi ini (Gambar 2.4) dapat dilihat bahwa terdapat firewall yang terimplementasi. Hal ini berarti penyerang tidak memiliki jalur untuk menyerang (attack path) sehingga A = 10 * (0/4) = 0 sesuai dengan persamaan (2.3). Tabel 3.8 menunjukkan nilai VEA untuk topologi server dengan firewall adalah 6.80. Nilai ini didapat dari persamaan (2.5).

Terdapat perbedaan nilai A pada setiap topologi. Hal ini terjadi karena nilai A dipengaruhi oleh attack path dan network path (persamaan (2.4)). Nilai A menjadi 0 ketika pada suatu topologi memiliki firewall. Sehingga kedua tabel diatas dapat dibuat sebuah diagram perbandingan nilai VEA setiap topologi.

Gambar 10. Grafik perbandingan jenis topologi terhadap nilai VEA

Gambar 10 menunjukkan grafik perbandingan nilai VEA-bility untuk topologi yang berbeda. Pada topologi tanpa firewall didapati 3.071, dan 6.809 untuk topologi server dengan firewall. Nilai VEA-bility untuk Fortigate dan Untangle sama pada setiap topologi. Hal ini dikarenakan nilai yang didapat dari base dan temporal score sama.

Berikut merupakan contoh perhitungan VEA pada topologi tanpa firewall :

a. VEA untuk serangan DOS untuk topologi tanpa firewall.

Nilai VEA didapatkan dari persamaan (2.5). Berikut merupakan perhitungannya.

Diketahui :
ImpactScore = 2.9
TemporalScore = 1.6
ExploitabilityScore = 3.9
#service on host = 4
#network services = 4
#attack path = 4
#network path = 4

Perhitungan :
V = $\min(10, \ln \sum e^{S(v)})$
Diketahui S(v)=(2.9 + 1.6) / 2 = 2.25, sehingga
= $\min(10, \ln \sum e^{2.25})$
= min(10, 2.25)
= **2.25**
E = $\min(10, \ln \sum e^{3.9})$ * 4/4
= min(10,3.9)
= **3.9**
A = (10*4) / 4
= **10**
VEA = 10 – ((2.25 + 3.9 + 10(/ 3)
= 10 – 5.38333333
= **4.616666667**

b. VEA untuk topologi tanpa firewall.

Diketahui :
S(v) DOS – 2.25
S(v) scan = 0
S (v) FTP brute force = 5.9
Exploitability DOS = 3.9
Exploitability FTP brute force = 3.4
#service on host = 4
#network services = 4
#attack path = 4
#network path = 4

Perhitungan :
V = $\min(10, \ln \sum e^{S(v)})$
= $\min(10, \ln (e^{2.25} + e^{0} + e^{5.9}))$
= min(10, ln (9.487735836 + 1 + 365.0374679)
= min (10, ln(375.5252037))
= min (10.5.928325589)
= **5.928325589**
E = $\min(10, \ln \sum e^{\text{ExploitabilityScore}(v)})$ * #service on host / #network services
= $\min(10, \ln (e^{3.9} + e^{3.9} + e^{3.4}))$ * 4/4
= min(10, ln (49.40244911 + 49.40244911 + 29.96410005))
= min(10, ln(128.7689983))
= **4.858020088**
A = (10*4) / 4
= **10**
VEA = 10 – ((5.928325589 + 4858020088 + 10) / 3)
= 10 – 6928781892
= **3.071218108**

3.4 Perbandingan nilai VEA-bility dengan CVSS

Perbedaan mendasar Antara perhitungan nilai VEA dengan CVSS adalah adanya nilai environmental. Untuk mendapatkan niai VEA tidak diperlukan nilai environmental, sedangkan untuk mendapatkan nilai CVSS diperlukan nilai environmental. Nilai tersebut didapat dari pemilihan poin pada metric Environmental yang terdapat pada tabel pemilihan metric CVSS. Berikut merupakan poin – poin yang mempengaruhi nilai environmental pada setiap serangan.

Tabel 11. Pemilihan poin Environmental Metric pada setiap serangan

Serangan	Environmental Metric				
	Collateral Damage Potential	Target Distribution	Confidentiality Requirement	Integrity Requirement	Availability Requirement
DOS	Low	Medium	Not Defined	Not Defined	Medium
FTP BRUTE FORCE	Low	Medium	Medium	Medium	Not Defined

Tabel 11 menunjukkan pemilihan poin pada environment metric untuk masing – masing serangan. Environmental metric dipengaruhi oleh collateral damage potential, target distribution, confidentiality requirement, integrity requirement, dan availability requirement. Pada collateral damage potential, kedua serangan dipilih "low" karena serangan tersebut hanya mempengaruhi sedikit kerusakan secara fisik maupun

kerusakan produktifitas pada suatu system. Pada target distribution, untuk kedua serangan dipilih "medium" karena target berada pada lingkungan (environment) dengan skala 26% hingga 75%. Pada confidentiality requirement dan integrity requirement, untuk serangan DOS dipilih "not defined" karena serangan tersebut tidak mempengaruhi kerahasiaan maupun integritas dari system. Sedangkan untuk serangan FTP brute force dipilih "medium" karena serangan tersebut berdampak ke kerahasiaan dan integritas dari suatu system. Pada availability requirement, untuk serangan DOS dipilih "medium" karena serangan ini dapat membuat peningkatan pada CPU Usage, sedangkan untuk FTP Brute force dipilih "not defined" karena serangan tersebut tidak berpengaruh ke availability dari sistem.

Dari tabel 11 akan didapatkan nilai environmental dan dari nilai tersebut dana dihitung nilai CVSS di setiap serangan.

Tabel 12. Nilai environmental dan CVSS pada Fortigate

Serangan	Base	Temporal	Environmental	Nilai CVSS
DOS	2.1	1.6	1.8	1.83333333
FTP BRUTE FORCE	5.4	4	3.4	4.26666667

Tabel 12 menunjukkan niain environmental dan CVSS pada Fortigate untuk masing – masing serangan. Perhitungan base dan temporal didapat dari persamaan (3.1) dan (3.5), sedangkan untuk nilai environmental didapat dari persamaan (3.6). Dari tabel diatas didapat nilai environmental sebesar 1.8 untuk serangan DOS dan 3.4 untuk FTP brute force. Sementara itu, untuk nilai CVSS didapatkan 1.83 untuk serangan DOS, dan 4.267 untuk FTP brute force.

Tabel 13. Nilai environmental dan CVSS pada Untangle

Serangan	Base	Temporal	Environmental	Nilai CVSS
DOS	2.1	1.6	1.9	1.86666667
FTP BRUTE FORCE	5.4	4	3.6	4.33333333

Tabel 13 menunjukkan nilai environmental dan nilai CVSS pada IPS Fortigate untuk masing – masing serangan. Dari tabel, didapat nilai environment untuk serangan DOS sebesar 1.9 dan 3.6 untuk FTP brute force. Sementara itu untuk nilai CVSS didapat 1.87 untuk serangan DOS dan 4.333 untuk serangan FTP brute force.

Berikut merupakan contoh perhitungan nilai environmental dan CVSS pada Fortigate:

a. Perhitungan nilai environmental pada serangan DOS. Nilai pada setiap poin didapat dari CVSS.

Diketahui :
Impact = 2.9
Exploitability = 3.9
CollateralDamagePotential = low = 0.1
TargetDistribution = medium = 0.75
ConfReq = not defined = 1
IntegReq = not defined = 1
AvailReq = medium = 1
ConfImpact = 0
AvailImpact = 0.275

Keterangan :
Ev = Environment Score
R = Round_1_to_decimal
I = Impact
At = Adjusted Temporal
Co = Colateral Damage Potential
T = TargetDistribution
Ai = AdjustedImpact
C = ConfImpact
Cr = ConfReq
Ig = IntegImpact
Ir = IntegReq
A = AvailImpact
Ar = AvailReq

Ev = R ((At + (10 – At) * C) * T) (3.6)

At = R (((0.6 * I) + (0.4 * Ai) – 1.5) * f (I) (3.7)

At = min(10,10.41 * (1 – (1 – C * Cr) * (1 – Ii * Ir) * (1 – A * Ar))) (3.8)

Perhitungan :

Ai = min (10,10.41 * (1 – (1 –0 * 1) * (10 * 1) * (10.275 * 1)))
= min(10,10.41*(10(1 * 1 * 0.725)))
= min(10,2.86275)
= 2.86275

At = R (((0.6 * 2.9)+(0.4*2.86275) – 1.5)*1.176
= R ((1.74 + 1.1451 – 1.5) * 1.176
= R (1.6288776)
= 1.6

Ev = R ((1.6+(10 – 1.6) * 0.1) * 0.75)
= R (1.6+8.4 * 0.1) * 0.75)
= R (1.83)
= 1.8

b. Perhitungan CVSS pada serangan DOS.

Diketahui :
Base = 2.1
Temporal = 1.6
Exploitability = 1.8
CVSS didapat dari rata – rata ketiga metic tersebut sehingga
CVSS = (2.1 + 1.6 + 1.8) / 3
= **1.83333**

Dari Tabel 12 dan 13 dapat dibuat grafik perbandingan nilai CVSS antar IPS.

Gambar 11. Grafik perbandingan jenis serangan terhadap nilai CVSS pada Fortigate dan Untangle

Gambar 11 menunjukkan grafik perbandingan jenis serangan terhadap nilai CVSS untuk IPS Fortigate dan Untangle. Dari gambar didapatkan selisih nilai CVSS pada serangan DOS sebesar 0.179 untuk kedua IPS dan selisih serangan FTP brute force sebesar 0.066 untuk kedua IPS. Nilai VEA-bility menunjukkan rentang nilai 0 hingga 10, dimana semakin tinggi nilai, system tersebut dianggap aman. Sedangkan nilai CVSS menunjukkan nilai kerentanan (Vulnerability) dari suatu sistem terhadap suatu serangan. Semakin besar nilainya, semakin besar tingkat kerentanan sistem tersebut. Pada tabel 13 nilai CVSS pada Untangle lebih besar dibandingkan Fortigate, hal ini didapat karena pada poin report confidence yang terdapat pada temporal metric memiliki nilai uncorroborated yaitu pada Untangle memiliki banyak laporan vulnerability pada situs cvedetails. Hal ini dapat diartikan bahwa Untangle lebih rentan terhadap serangan jika dibandingkan dengan Fortigate.

4. Kesimpulan

Dari hasil percobaan dan analisa yang telah dibuat, dapat disimpulkan bahwa :

1. IPS Fortigate dan Untangle berhasil diimplementasikan pada topologi yang direkomendasikan.
2. Nilai VEA-bility dipengaruhi oleh tiga metric yaitu Vulnerability, Exploitability, dan Attackability.
3. Nilai VEA-bility didapat dari perhitungan yang dilakukan dengan pemilihan poin – poin setiap metric yang telah disediakan oleh CVSS.
4. Dari hasil analisa analisa, didapatkan nilai VEA-bility yang sama untuk Fortigate dan Untangle pada kedua topologi yang diujikan. Nilai VEA-bility dari masing – masing topologi tersebut adalah : tanpa firewall = 3.071218108, dan topologi server dengan firewall = 6.809386448.
5. Nilai CVSS pada Untangle (DOS = 1.867 dan FTP brute force=4.33) lebih tinggi dibandingkan pada Fortigate (DOS = 1.833 dan FTP brute force 4.267) yang berarti Untangle lebih rentan terhadap serangan. Hal ini dikarenakan adanya perbedaan pada poin report confidence pada temporal metric.

Ucapan Terimakasih

Terima kasih penulis sampaikan kepada PT XYZ, khususnya *Manager* unit kerja *Operation & Maintenance Network & Device* yang memberikan izin kepada penulis dalam melakukan penelitian dan dapat mengimplementasikan hasil penelitian ini.

Daftar Rujukan

[1] Piper, S., 2011., Intrusion Prevention Systems for Dummies., Wiley Publishing, Inc.,
[2] Kenneth Tam., K., 2012. UTM Security with Fortinet: Mastering FortiOS. Newnes: Elsevier
[3] El-Bawab., E., 2014. Untangle Network Security. Packt Publishing Ltd,
[4] EC-Council., 2014. CEHv9 Module 09 Denial of Service. EC-Council
[5] EC-Council., 2014. CEHv9 Module 05 System Hacking. EC-Council
[6] Mell, P., 2007. A Complete Guide to the Common Vulnerability Scoring System version 2.0. Natl. Inst. Stand. Technol.
[7] Tupper, M., 2007. VEA-bility Security Metric: A Network Security Analysis Tool.
[8] D. E. Prayogo, "Uji Keamanan Jaringan Dengan Metode Intrusion Detection System (Studi Kasus: LAB FASILKOM Mercu Buana)," p. 50, 2015
[9] A. Huda, "Sistem Penanganan Serangan (Ips-Intrusion Prevention System) Berbasis Ossim (Open Source Security Information Management)," 2015.
[10] Muh. Arsyi Azimin, "Implementasi Intrusion Prevention System (Ips) Menggunakan Untangle," 2015.
[11] S. Pakpahan, "Implementasi Firewall Dan Intrusion Prevention System (Ips) Dengan Sistem Operasi Ipfire," 2015.
[12] Hanif Pradivta Gartiwa, "Perancangan Dan Implementasi Intrusion Prevention System (IPS) Menggunakan SNORT Di PT. Insan Teknologi Semesta," 2015.
[13] Raka Yusuf, *Analysis of Snort Rules to Prevent Synflood Attacks on Network Security. J. Tek Inform.*, 2015.

KERTAS KERJA

Ringkasan

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Saat ini begitu banyak cara untuk melakukan serangan terhadap suatu sistem jaringan. Cara-cara ini terus berkembang dari zaman dahulu sampai sekarang. Dahulu untuk melakukan suatu serangan membutuhkan pengetahuan dan pemahaman teknis IT yang tinggi, akan tetapi saat ini sangat mudah untuk melakukan serangan bukan hanya orang yang mempunyai keahlian yang tinggi. Metode dan alat-alat yang dipakai semakin banyak dan mudah digunakan, bahkan terhadap sistem keamanan jaringan. Contoh serangan yang sering dilakukan seperti *DDoS Attack*, *Port Scanning*, *Sniffing*, *FTP brute force, SQL Injection*, *Malware*, *Phishing*, *Exploit*, dll.

Oleh karena itu diperlukan solusi untuk menangani serangan yang semakin berkembang. Intrusion Prevention System (IPS) merupakan solusi untuk menangani serangan-serangan tersebut. Dikarenakan banyaknya tools IPS yang tersedia saat ini, pengguna diharuskan dapat memilih tools IPS yang terbaik, Pada penelitian ini akan membandingkan tools IPS yakni Fortigate dan Untangled. Untuk mengetahui tools IPS terbaik maka dilakukan analisis performansi dan tingkat keamanan sistem dari tools IPS tersebut. Analisis tingkat keamanan menggunakan *security metric* dengan metode VEA-bility. Metode VEA-bility akan menghasilkan nilai dengan skala 0 hingga 10. Penelitian ini diharapkan dapat membantu pengguna dalam memilih tools IPS terbaik guna memperketat keamanan jaringan, pengawasan jaringan komputer dan mengurangi serangan dari pihak yang tidak bertanggung jawab.

1. Metode penelitian yang dilakukan yaitu dengan melakukan 7 langkah sebagai berikut : Pengumpulan Data
   Penulis melakukan observasi dan dokumentasi pada jaringan yang sudah ada di Perusahaan tersebut untuk mengumpulkan data.

2. Studi Literatur

   Studi Literatur adalah proses pencarian segala informasi dan referensi dari buku, jurnal, artikel, maupun internet yang berkaitan dengan topik *Intrusion Prevention System* (IPS).

3. Analisa Kebutuhan Perangkat Lunak

   Penulis mempersiapkan Perangkat Luna kapa saja yang dibutuhkan sebelum merancang topologi baru demi melakukan pengujian dan implementasi

4. Perancangan Sistem

   Penulis melakukan perancangan pada topologi dimana semua kebutuhan sudah terpenuhi dan terpasang sehingga pengujian dapat segera dilakukan.

5. Pengujian dan Implementasi

   Penulis melakukan implementasi serta pengujian pada dua sistem yang berbeda. Penulis mengeluarkan dan memisahkan data dari hasil uji dengan sistem yang pertama dengan yang kedua.

6. Analisa dan Perbandingan

   Penulis melakukan analisa dari hasil pengujian dari dua sistem yang berbeda untuk dilakukan perbandingan sistem mana yang memiliki performa lebih baik.

7. Hasil dan Penarikan Kesimpulan

   Penulis dapat menunjukkan hasil perbandingan kepada pelanggan serta dapat menarik kesimpulan mengenai kinerja sistem yang terbaik berdasarkan data pengujian dan implementasi yang dilakukan.