Implementasi *Network Intrusion Detection System* Dan *Intrusion Prevention System* Pada Jaringan LAN Berbasis *Threats* Dan *Vulnerabilities Assessment* Di Universitas Muhammadiyah Cirebon

Khairul Anwarudin[1], Arief Zulianto[2], Yucki Prihadi[3]
Prodi Magister Teknik Informatika, Pascasarjana, Universitas Langlangbuana [1,2,3]
khairuddin25@gmail.com[1]
madzul@gmail.com[2]
yuckiprihadi@gmail.com[3]

Abstrak— Keamananan jaringan merupakan suatu hal yang penting di Server Universitas Muhammadiyah Cirebon. Tujuan dari penelitian ini ialah untuk mengetahui dampak *vulnerabilities* pada jaringan lokal, dan melakukan implementasi dari keamanan berupa *NIDS, NIPS, S*NORT, *Suricata* dan *Pfense* untuk menjaga kerahasiaan data, keaslian data dan ketersediaan data.

Metode *OWASP Top* 10 dengan pengumpulan data *Prepare, Plan, Design, Implementation, Operation, Optimization.* Hasil dari penelitian menunjukkan *vurnerability assessment* memiliki nilai yang berbeda dari tingkat sukar dengan nilai 1 sampai mudah dengan nilai 3 pada serangan jaringan melalui *OWASP Top* 10, serta dengan adanya implementasi *NIDN, NIPS, S*NORT, *Suricata* dan *Pfense* dapat mendeteksi dan memberikan perlindungan, pertahanan dari *Attacker Ddos, Sniffing Attack* dan *Scanner Attack* pada jaringan LAN Universitas Muhammadiyah Cirebon. Berdasarkan hasil yang telah diperoleh pada penelitian ini, dapat ditarik kesimpulan bahwa implementasi *NIDN, NIPS, S*NORT, *Suricata* dan *Pfense* sangat efektik menahan serta melakukan perlawanan terhadap *attacker* di jaringan Universitas Muhammadiyah Cirebon.

***Keywords*— NIDN, NIPS, Network Security**

I. PENDAHULUAN

Teknologi jaringan komputer selalu berkembang, dengan adanya perkembangan teknologi jaringan komputer maupun data maka informasi dapat di akses dengan cepat, mudah dan akurat sehingga keamanan dari jaringan komputer ialah suatu hal yang harus diperhatikan. Jaringan komputer dapat didefinisikan sebagai suatu himpunan interkoneksi sejumlah komputer yang mana jaringan komputer merupakan sebuah kumpulan beberapa komputer yang terhubung satu sama lain yang menggunakan sebuah media perantara sebagai penghubungnya. Keamanan jaringan (*network security*) terdiri dari kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan maupun penolakan yang terjadi pada sebuah jaringan komputer. Beberapa akses informasi baik publik maupun pribadi yang biasa digunakan dalam pekerjaan sehari – hari diantaranya; melakukan transaksi dan komunikasi diantara bisnis, instansi pemerintah dan individu. Setiap jaringan tersebut pasti melibatkan *Network Security* pada penggunaanya. Seperti pada Universitas Muhammadiyah Cirebon yang menggunakan mikrotik *router* untuk pengamanan jaringan. Dimana mikrotik *router* merupakan alat perangkat keras yang menjembatani dua jaringan yang berfungsi mengatur kegiatan keluar masuk yang ada di jaringan Universitas Muhammadiyah Cirebon, serta memberikan kemudahan dalam pembagian *Internet Protocol* (*IP*) baik jaringan *wireless* maupun jaringan *Local Area Network* (LAN). Dengan adanya *router* tersebut maka alamat *Internet Protocol* dibagi berdasarkan kebutuhan dan dijadikan setiap blok *Internet Protocol* yang berbeda agar dapat dengan mudah dipantau atau dimonitor.

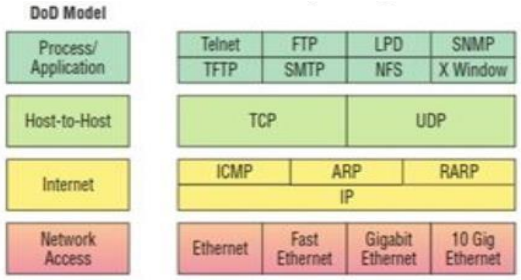
Pemberian alamat IP pada karyawan, mahasiswa dan bagian lainnya di Universitas Muhammadiyah Cirebon akan berbeda. Dengan adanya perbedaan tersebut kegiatan akses dalam pertukaran data dapat dimonitor dan terkendali begitu juga dengan alamat *Server* Universitas Muhammadiyah Cirebon, dengan adanya perbedaan tersebut setiap *client* memiliki batasan dalam mengakses server Universitas Muhammadiyah Cirebon. Berdasaran informasi yang diperoleh dari karyawan di Universita Muhammadiyah Cirebon, terdapat beberapa oknum yang melakukan kegiatan pembobolan password wifi dan melakukan akses internet secara illegal pada jaringan Universitas Muhammadiyah Cirebon, diperoleh juga laporan dari luar kampus bahwa ada beberapa mahasiswa yang berhasil masuk kedalam sistem akademik dan melakukan kegiatan menangkap password pada salah satu aplikasi yang ada di server Universitas Muhammadiyah Cirebon. Banyak mahasiswa yang dapat meretas dengan menggunakan *tools* meskipun sudah menggunakan system keamanan jaringan yaitu mikrotik router. Namun dari kegiatan meretas tersebut belum bisa mendeteksi serangan dari luar jaringan dan dari dalam jaringan. Selain terjadi tindakan pertasan password dan peretasan oleh hacker dengan tools juga terjadi peretasan wifi internet dan penangkapan user id beserta password yang membanjiri sistem yang ada adi server Universitas Muhammadiyah Cirebon. Hal tersebut terjadi dikarenakan jaringan menggunakan mikrotik router masih memiliki kekurangan dalam keamanan jaringan di Universitas Muhammadiyah Cirebon.

Maka dari itu, penulis melakukan penelitian tentang Implentasi *Network Security Intrusion Detection System* dan *Intrusion Prevention System* Pada Jaringan LAN Berbasis *Threats* dan *Vulnerabilities Assessment* di Universitas Muhammadiyah Cirebon.

II. LANDASAN TEORI

A. TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) dibuat oleh DoD (*Department of Defense*) untuk memastikan dan menjaga integritas data sama seperti halnya menjaga komunikasi dalam situasi kekacauan perang.



Gambar 1 *TCP/IP Layer dan Protokol*

B. Konsep Keamanan Jaringan

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, pastikan bahwa user dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang dibuat. Jika tidak memahami hal tersebut, maka akan menciptakan lubang (*hole*) keamanan pada jaringan.

Ada dua elemen utama pembentuk keamanan jaringan :

1. Tembok pengamanan, baik secara fisik maupun maya, yang ditaruh diantara piranti dan layanan jaringan yang digunakan dan orang-orang yang akan berbuat jahat.

2. Rencana pengamanan, yang akan diimplementasikan bersama dengan user lainnya, untuk menjaga agar sistem tidak bisa ditembus dari luar.

C. *Intruction Detection Sistem (IDS)*

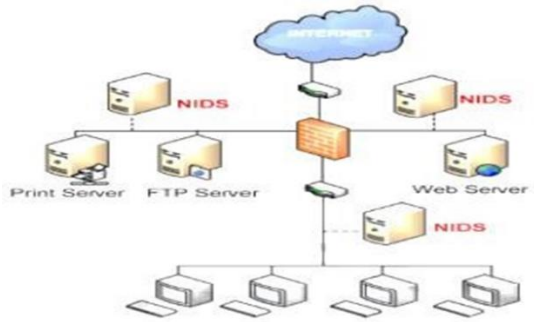
IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah system atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah system atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusion (penyusupan).

Kebanyakan produk IDS merupakan sistem yang bersifat pasif, mengingat tugasnya hanyalah mendeteksi penyusupan yang terjadi dan memberikan peringatan kepada administrator jaringan bahwa mungkin ada serangan atau gangguan terhadap jaringan. Akhir-akhir ini, beberapa vendor juga mengembangkan IDS yang bersifat aktif yang dapat melakukan beberapa tugas untuk melindungi host atau jaringan dari serangan ketika terdeteksi, seperti halnya menutup beberapa port atau memblokir beberapa alamat IP. Produk seperti ini umumnya disebut sebagai *Intrusion Prevention System* (IPS). Beberapa produk IDS juga menggabungkan kemampuan yang dimiliki oleh HIDS dan NIDS, yang kemudian disebut sebagai system hybrid (hybrid intrusion detection system). Ada dua jenis IDS yaitu :

1. *Network Based Intrusion Detection System* (NIDS)
2. *Host Based Intrusion Detection System* (HIDS)

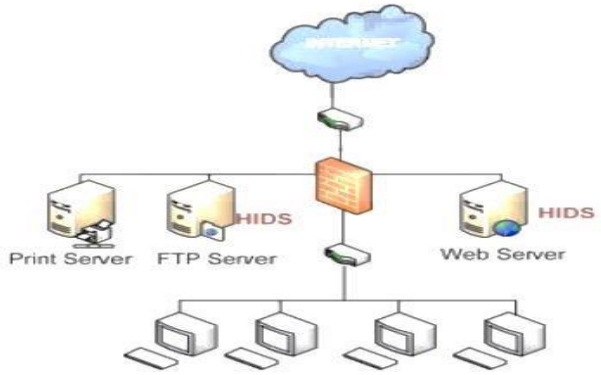
Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada “pintu masuk” jaringan. Kelemahan NIDS adalah agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.

Network-based Intrusion Detection Sistem (NIDS) Tipe IDS ini bekerja dengan cara melakukan analisis langsung dalam traffic sebuah jaringan apakah ditemukan sebuah percobaan penetrasi terhadap server jika ada maka IDS akan memberikan peringatan. NIDS ini biasanya diletakan dalam segmen jaringan yang cenderung credential di mana server berada tepat pada "pintu masuk" jaringan tersebut, untuk memudahkannya bisa dilihat dalam topologi gambar 2 berikut ini :



Gambar 2 *Basic Concept Netwok based intrusion Detection System*

Dan untuk topologi HIDS dapat dilihat pada gambar berikut:



Gambar 3 *Basic Concept Host-based Intrusion Detection System*

D. *Intrusion Prevention System (IPS)*

Intrusion Prevention System merupakan kombinasi antara fasilitas blocking capabilities dari Firewall dan kedalaman inspeksi paket data dari *Intrusion Detection System* (IDS).

IPS diciptakan pada awal tahun 1990-an untuk memecahkan masalah serangan yang selalu melanda jaringan komputer. IPS membuat akses kontrol dengan cara melihat konten aplikasi, dari pada melihat IP address atau ports, yang biasanya dilakukan oleh firewall. IPS komersil pertama dinamakan *BlackIce* diproduksi oleh perusahaan *NetworkIce*, hingga kemudian berubah namanya menjadi ISS(Internet Security System). Sistem setup IPS sama dengan sistem setup IDS. IPS mampu mencegah serangan yang datang dengan bantuan administrator secara minimal atau bahkan tidak sama sekali. Secara logic IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, selain itu IPS membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga bisa menginterupsi sistem call.

Jenis-jenis Intrusion Prevention System (IPS) sebagai berikut :

1. *Host-based Intrusion Prevention System*
2. *Network Intrusion Prevention System*

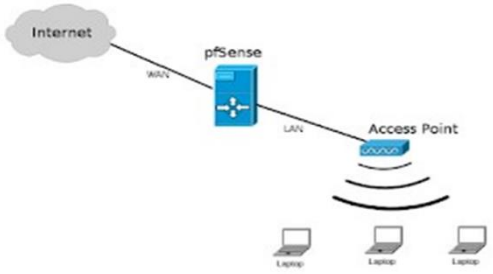
E. *Snort*

Snort merupakan tool atau aplikasi open source dari *Intrusion Detection System* (IDS). Snort dirancang untuk beroperasi pada command line dan telah diintegrasikan ke beberapa aplikasi pihak ketiga serta mendukung cross platform. Snort menganalisis semua lalu lintas jaringan untuk melakukan sniffing dan mencari beberapa jenis penyusupan maupun serangan dalam sebuah jaringan.

F. *PFSENSE*

Pfsense merupakan distro linux turunan free bsd akan tetapi disesuaikan untuk digunakan sebagai firewall dan router. Selain menjadi, platform yang kuat fleksibel firewall dan routing, itu termasuk daftar panjang fitur terkait dan sistem paket yang memungkinkan upgrade lebih lanjut tanpa menambahkan dan kerentanan keamanan potensial untuk distribusi dasar. pfSense adalah proyek populer dengan lebih dari 1 juta download sejak awal, dan terbukti dalam instalasi yang tak terhitung jumlahnya mulai dari jaringan rumah kecil melindungi PC dan Xbox untuk perusahaan besar, universitas dan organisasi lainnya melindungi ribuan perangkat jaringan."

PfSense adalah distribusi perangkat lunak komputer firewall / router open source berbasis FreeBSD. Ini diinstal pada komputer fisik atau mesin virtual untuk membuat firewall / router khusus untuk jaringan. Ini dapat dikonfigurasi dan ditingkatkan melalui antarmuka berbasis web, dan tidak memerlukan pengetahuan tentang sistem FreeBSD yang mendasarinya untuk dikelola.



Gambar 4 *Pfsense Snort*

Dari Gambar 4 Pfsense Snort diatas, bahwa Pfsense merupakan sejenis firewall untuk melindungi jaringan LAN serta isi dari jaringan lokal tersebut, sehingga dengan adanya penyasangan sesuai gambar tersebut kondisi jaringan LAN dapat terpantau oleh administrator jaringan.

G. *Suricata*

Suricata merupakan suatu software open source yang dapat digunakan untuk mendeteksi dan mencegah ancaman terhadap lalu lintas jaringan. Suricata dikembangkan oleh OISF dan vendor pendukungnya [Kuswanto 2014].

H. *Threats* Dan *Vulnerabilities Assessment* pada keamanan jaringan LAN (Local Area Network)

Tabel 1 Teknik Serangan pada Jaringan LAN

Kategori Serangan	**Teknik Serangan**
Deniel Of Service	*DdoS Attack*
Session Hijacking	*Snifing Attack*
Website Attack	*Scanning Attack*

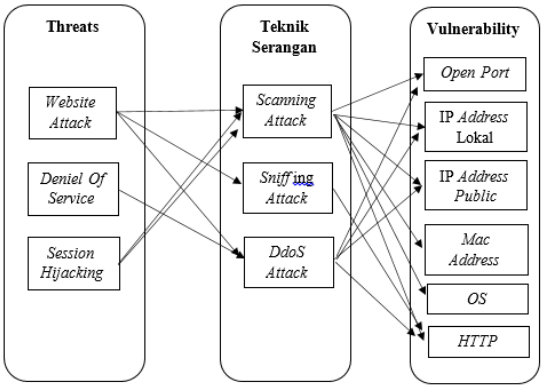
Saat jenis threat sudah dapat terkumpul disertai teknik serangan pada jaringan LAN maka dapat dicari kerentanan penilaian. Menurut Sergio Marphy Junan Lawalata (2020) *Vulnerability assessment* (penilaian kerentanan) adalah proses mengidentifikasi, mengukur, dan memprioritaskan (atau memberi peringkat) kerentanan dalam suatu sistem. *Vulnerability Assessment* dapat digunakan oleh Attacker untuk dapat mengetahui kelemahan sistem. Sehingga perlu dilakukan adanya alur serangan supaya dapat menemukan celah hingga penyerangan sistem dianggap berhasil. Berikut ini tabel tentang adanya hubungan teknik serangan dengan *Vulnerability* pada jaringan LAN :

Tabel 2 *Vulnerability* pada jaringan LAN

Teknik Serangan	***Vulnerability***
Scanning Attack	*Open Port* IP *Address* Lokal IP *Address Public* *Mac Address* *OS* *HTTP*
Sniffing Attack	*HTTP*
DdoS Attack	*Open Port* *IP Address* Lokal IP *Address Public* *Mac Address*

	OS *HTTP*

Berdasarkan tabel 2 diatas tentang vulnerability terdapat adanya beberapa teknik serangan yaitu Scanning Attack, Sniffing Attack, DdoS Attack. Akan tetapi dari serangan tersebut yang paling banyak mengancam keamanan pada jaringan LAN yaitu tidak terpasang sistem pendeteksian dari serangan, maka berbagai jenis serangan dapat berhasil dilakukan oleh attacker terhadap jaringan LAN. Dari komponen adanya threats, teknik serangan, dan *vulnerabilities* digambarkan pada gambar 2.5 Berikut :



Gambar 5 Peta Threats, Attack Techniques, dan Vulnerabities pada Jaringan LAN

I. *Vulnerabilities Assessment Open Web Application Security Project (OWASP)*

Vulnerabilities adalah lubang atau kelemahan dalam aplikasi, yang dapat berupa cacat desain atau bug implementasi, yang memungkinkan penyerang menyebabkan kerugian bagi pemangku kepentingan aplikasi. Pemangku kepentingan termasuk pemilik aplikasi, pengguna aplikasi, dan entitas lain yang mengandalkan aplikasi tersebut. Dari penilaian kerentanan ditemukan dapat dijelaskan sebagai berikut (Dwivedi, 2016):

1. *High severity risk* merupakan kemungkinan bagi seorang peretas dapat mengakses *root*, super user dan berdampak langsung pada operasi sistem. Jenis yang termasuk pada *high severity risk* yaitu *SQL injection* dan *cross-site scripting*.
2. Medium *severity risk* yang dapat menimbulkan gangguan keamanan dan memperoleh akses terbatas pada pengguna. Jenis yang termasuk dalam medium *severity risk* yaitu *application error message* dan *slow http denial of service attack*
3. *Low severity risk* yaitu sangat sedikit kemungkinan atau peluang bagi seorang peretas dapat mendapatkan akses data. Jenis yang termasuk pada *low severity risk* yaitu *autocomplete enabled dan version disclosure*.

Open Web Application Security Project (OWASP) adalah komunitas terbuka yang didedikasikan untuk memungkinkan organisasi mengembangkan, membeli, dan memelihara aplikasi yang dapat dipercaya.

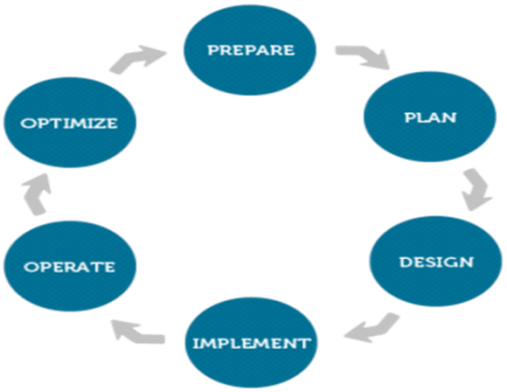
III. METODE DAN DESAIN PENELITIAN

A. Metode Penelitian

Metode penelitian menggunakan kuantitatif dengan penetration testing untuk dijadikan acuan dan dasar sistem keamanan pada jaringan LAN menggunakan analisa *security assessment* dalam hal ini menggunakan beberapa tahapan yaitu dengan penilaian kerentanan dengan standarisasi OWASP Top 10 yang akan dijadikan sebagian dari penilaian terhadap aplikasi yang ada di jaringan server Universitas Muhammadiyah Cirebon.

B. Pengumpulan Data

- Metode pengumpulan data yang digunakan pada penelitian ini menggunakan *Prepare*, *Plan*, *Design*, *Implementation*, *Operation*, *Optimization*. Menurut K. Mindo, dkk (2017) beberapa penelitian sebelumnya menunjukkan bahwa metode tersebut dapat digunakan untuk merancang infrastruktur jaringan dan dapat melakukan urutan untuk optimalisasi sesuai dengan penilitian berdasarkan objek yang diteliti baik secara data maupun sebuah informasi yang ada di lapangan.
- Berikut langkah-langkah penelitian :

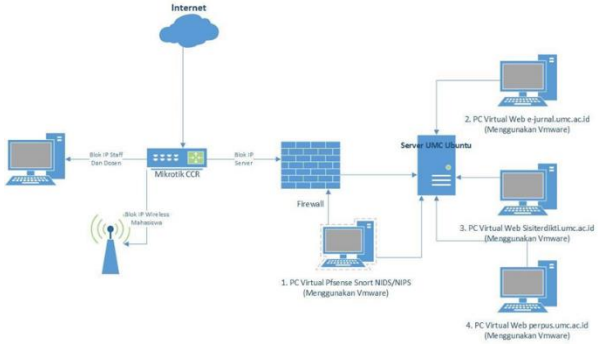


Gambar 6 Diagram Alir Penelitian

Pada penelitian ini dilakukan dengan menggunakan metode PPDIOO yang pertama adalah prepare dengan cara kerja menyusun waktu dan tempat penelitian hingga melakukan studi literature terhadap keamanan di dalam jaringan LAN kemudian tahap perencanaan sesuai permasalahan sehingga mendesaign dari perencanaan yang akan diimplementasikan sesuai dengan kebutuhan penelitian yaitu implementasi NIDS dan NIPS selanjutnya akan dioperasikan oleh administrator jaringan yaitu bertujuan memfilter dan menganalisis hasil dari jaringan melalui alat pendeteksian, kemudian yang terakhir mengoptimalkan hasil dari implementasi NIDS dan NIPS pada jaringan Local Area Netwok di Universitas Muhammadiyah Cirebon.

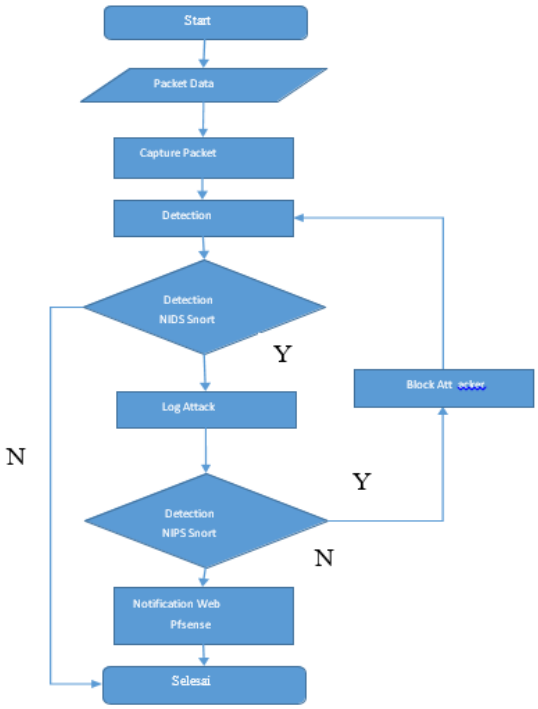
Berikut merupakan topologi dari *NIDS* dan *NIPS* yang diterapkan pada jaringan LAN Universitas Muhammadiyah Cirebon yang akan dirancang sesuai kebutuhan serta memberikan sebuah service yang menjadikan jaringan Universitas Muhammadiyah menjadi aman serta terkontrol salah satunya akan mendesain serta mengimplementasikan sebuah firewall yang hasil dari log tersebut berupa aplikasi website yaitu *pfsense*, dan Perancangan perangkat NIDS dan NIPS membutuhkan beberapa komponen hardware dan

software yang dapat memenuhi kriteria untuk dapat diterapkan pada jaringan LAN.



Gambar 7 Topologi Penerapan NIDS, NIPS *Snort pfSense*

Adapun *flowchart* deteksi serangan pada gambar dibawah ini:



Gambar 8 Flowchart Deteksi Serangan

Gambar 8 merupakan *flowchart* pola pendeteksian NIDS dan NIPS snort dan *Pfsense* bahwa mulainya proses transfer data packet akan diseleksi isi data tersebut, apakah data tersebut aman diteruskan atau yang berisi virus atau lainnya dan apabila tidak ada suatu hal yang mencurigakan maka paket akan diteruskan sampai selesai. Begitupun sebaliknya, apabila data tersebut mengandung sebuah virus atau serangan yang menggunakan tools maka akan diselesaikan menggunakan NIPS yang akan melakukan eksekusi terhadap *attacker*.

IV. HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil

Setelah mengetahui hasil-hasil kerentanan pada aset dan kondisi infrastruktur jaringan LAN, maka langkah selanjutnya membuat *Vulnerability Assessment* yang digunakan untuk menganalisa dan menilai tingkat resiko kerentanan pada sistem dan infrastruktur jaringan terhadap keamanan jaringan yang nantinya akan direkomendasikan untuk dilakukan perbaikan pada sistem jaringan LAN. Berikut tahap pengujian kerentanan menggunakan tools *owasp* zap 2.10.0 sebagai berikut :

Tabel 3 *Vulnerability Assessment* Hasil Uji Sebelum Implementasi NIDS dan NIPS

IP/Domain	***Tools Alert***	***Vulnerability Assessment***				***Description***
		Critical	*High*	*Medium*	*Low*	
Simaku. Universitas Muhammadiyah Cirebon. ac.id	*SQL Injection*		1			*Risk*
	X-Frame-Options header Not Set			5		*Risk*
	Absence of Anti-CSRF Token				3	*Risk*
	Cross-Domain JavaScript Source File Inclusion				8	*Risk*
	Incomplete or No Cache-Control And Pragma HTTP Header Set				3	*Risk*
	X-Content-Type-Option Header Missing				11	*Risk*
Sisterdikti.Universitas Muhammadiyah Cirebon. ac.id	*Cros Domain Misconfiguration*			12		*Risk*
	Vulnerable JS Library			2		*Risk*
	X-Frame-Options header Not Set			5		*Risk*
	Absence of Anti-CSRF Token				4	*Risk*
	Cookie No HttpOnly Flag				2	*Risk*

	Cookie Without SameSite Attribute				2	*Risk*
	X-Content-Type-Option Header Missing				23	*Risk*
	SQL Injection	-	-	-	-	-
feeder.Universitas Muhammadiyah Cirebon.ac.id	*SQL Injection*					-
	Cros Domain Misconfiguration			12		*Risk*
	X-Frame-Options header Not Set			9		*Risk*
	Absence of Anti-CSRF Token				6	*Risk*
	Cookie No HttpOnly Flag				2	*Risk*
	Cookie Without SameSite Attribute				2	*Risk*
	Server Leaks Information via "X-Powered-By" Http Response Header Field				13	*Risk*
	X-Content-Type-Option Header Missing				18	*Risk*

Setelah diperolah hasil seperti tabel 3, selanjutnya dilakukan pengujian kembali dengan mengimplementasi NIDS dan NIPS yang hasilnya dapat dilihat pada tabel berikut :

Tabel 4 *Vulnerability Assessment* Hasil Uji Sesudah Implementasi NIDS dan NIPS

IP/Domain	***Tools Alert***	**Vulnerability Assessment**				***Description***
		Critical	*High*	*Medium*	*Low*	
Simaku.Universitas Muhammadiyah Cirebon.ac.id	*SQL Injection*					
	X-Frame-Options header Not Set			4		*Risk*
	Absence of Anti-CSRF Token				3	*Risk*
	Cross-Domain JavaScript Source File Inclusion				8	*Risk*
	Incomplete or No Cache-Control And Pragma HTTP Header Set				3	*Risk*
	X-Content-Type-Option Header Missing				10	*Risk*
Sisterdikti.Universitas Muhammadiyah Cirebon.ac.id	*Cros Domain Misconfiguration*			13		*Risk*
	Vulnerable JS Library			2		*Risk*
	X-Frame-Options header Not Set			5		*Risk*
	Absence of Anti-CSRF Token				4	*Risk*
	Cookie No HttpOnly Flag				2	*Risk*
	Cookie Without SameSite Attribute				2	*Risk*
	X-Content-Type-Option Header Missing				25	*Risk*
feeder.Universitas Muha	*Vulnerable JS Library*			2		*Risk*
	Cros Domain Misconfiguration			13		*Risk*
	X-Frame-Options header Not Set			5		*Risk*

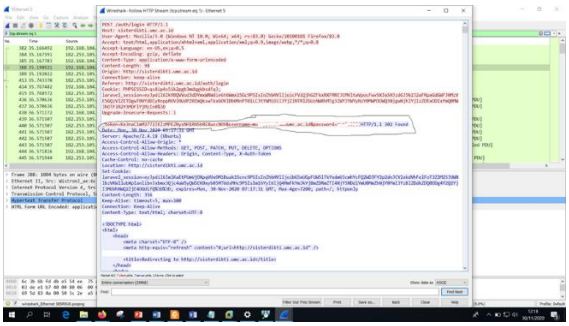
mmadiyah Cirebon.ac.id	*Absence of Anti-CSRF Token*				4	*Risk*
	Cookie No HttpOnly Flag				2	*Risk*
	Cookie Without SameSite Attribute				2	*Risk*
	X-Content-Type-Option Header Missing				25	*Risk*

Dari tabel 4 diatas menunjukan nilai kerentanan dari aplikasi yang berdomain *simaku.Universitas Muhammadiyah Cirebon.ac.id, sisterdikti.Universitas Muhammadiyah Cirebon.ac.id* dan *feeder.Universitas Muhammadiyah Cirebon.ac.id* tersebut diuji menggunakan tools owasp zap antara lain dari nilai kerentanan terendah sampai nilai kerentanan tertinggi. Dari aplikasi scanner setelah dilakukan uji tahap implementasi NIDS dan NIPS tersebut menunjukkan nilai kerentanan yang rendah disebabkan oleh adanya perlawanan dari *snort* atau *suricata* dan *Pfsense*. Sehingga dari implementasi tersebut dapat menjaga kerahasiaan data dan menjaga adanya penyerangan berupa *port scanning*, *sniffing* dan *Ddos*.

B. Pembahasan

1. Pengujian Menggunakan *Wireshark*

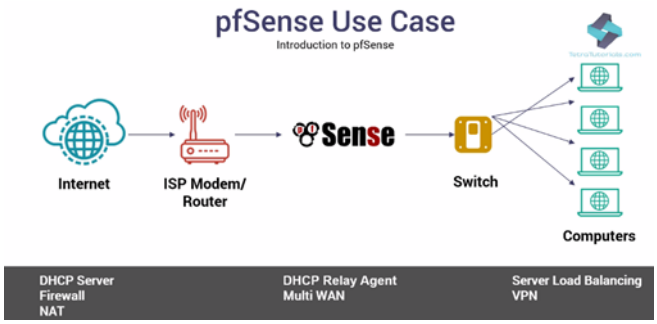
Vulnerability yang memiliki tingkat kerentanan paling besar terkait dampak yang diakibatkan dari serangan pada jaringan LAN Universitas Muhammadiyah Cirebon karena dapat mengetahui kerahasiaan data. Barikut ini hasil uji kerentanan menggunakan tools *Wireshark* :



Gambar 9 *Sniffing Wireshark*

2. Implementasi *NIDS* dan *Network Prevention System* dengan *Snort* dan *Suricata* pada *Pfsense*

Berikut proses tahapan implementasi *Network Intrusion Detection System and Network Prevention System menggunakan Snort, Suricata* dan *Pfsense* :

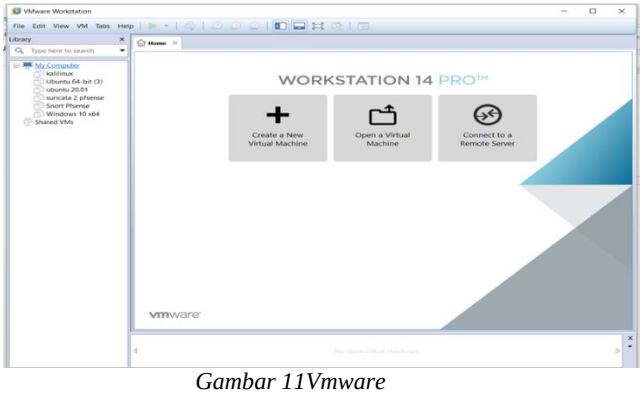


Gambar 10 pfSense Use case

Untuk melakukan persiapan implementasi, penulis mempersiapkan proses *software*. Berikut tahap persiapannya:

a. *Vmware*

Vmware adalah *software* yang bertujuan untuk menjalankan sistem operasi *Free BSD* yang akan menghasilkan web browser *pfsense*, berikut pada gambar dibawah ini :

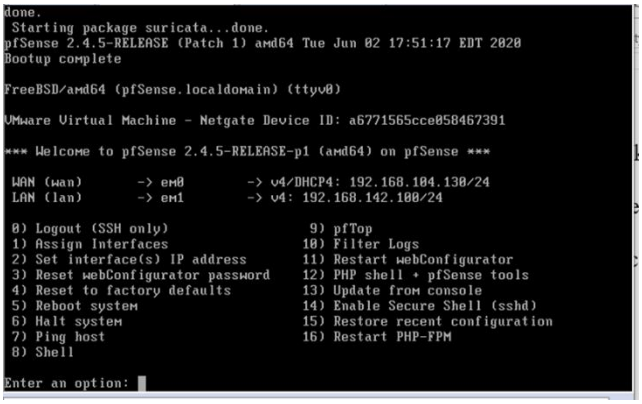


Gambar 11Vmware

Pada gambar 4.3. Vmware adalah aplikasi virtual untuk menjalankan sistem operasi windows, Ubuntu, *FreeBSD* dll yang berjalan diatas fisik komputer sehingga dalam satu komputer bisa terdapat lebih dari satu sistem operasi yang dijalankan dalam satu komputer fisik.

b. Persiapan *OS Free BSD*

Aplikasi program *Snort* dan *pfsense* yang terdapat aplikasi iso yaitu *FreeBSD* yang akan diinstal didalam aplikasi virtual yaitu *vmware*, yang kemudian setelah diinstal sistem operasi *FreeBSD* dan di konfigurasi sesuai kebutuhan yang akan diterapkan di jaringan LAN, setelah diinstal lalu jalankan *pfsensenya* seperti gambar berikut:

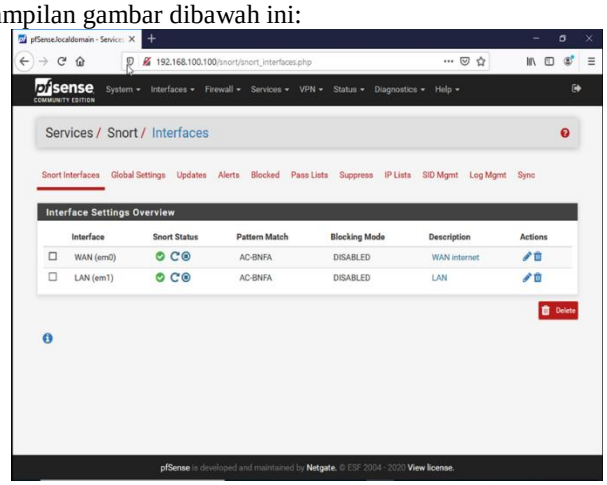


Gambar 12 Running FreeBSD pfsense

3. Konfigurasi *Pfsense Snort* dan *Suricata*

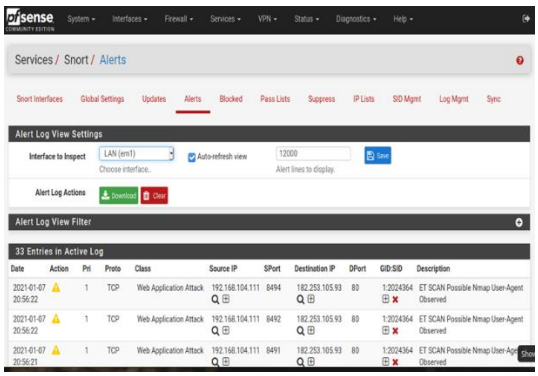
Konfigurasi pfsense snort dan suricata diakses melalui browser yang menggunakan localhost yang kemudian dikonfigurasi secara manual dan berdasarkan kebutuhan dari hasil akses website yaitu halaman *login pfsense*, yang kemudian melakukan *login*. Dengan melakukan *login password* dan *username* masih secara *default* yaitu *user admin* dan *password*-nya adalah *pfsense* setelah itu *login*. Dari proses tersebut maka akan dihasilkan berupa configurasi selanjutnya untuk melakukan implementasi *pfsense*.

Pada menu *system* terdapat *packet manager* seperti tampilan gambar dibawah ini:



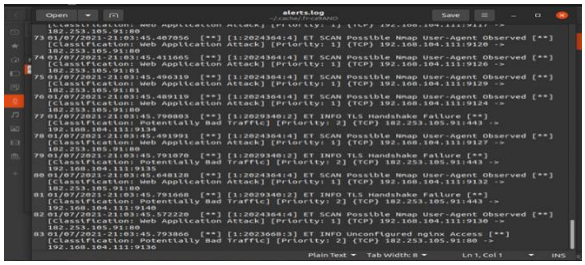
Gambar 13 Konfigurasi Rule LAN dan WAN

Dari gambar 13 menjelaskan didalam *interface settings overview* tersebut adanya WAN dan LAN. Untuk Menyiapkan paket *Snort* atau *suricata* pertama kalinya Klik tab Pengaturan *Global* dan aktifkan unduhan kumpulan aturan untuk digunakan. Beberapa contoh serangan yang terdeteksi setelah dilakukannya impelementasi dapat dilihat sebagai berikut:



Gambar 14 NIDS,NIPS *Snort* dan *pfsense* www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id Jalur LAN

Dari Gambar 14 diatas, hasil dari pengujian pada jalur LAN dengan alamat web yaitu www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id melalui pengujian *scanner attack* menggunakan NIDS dan NIPS dengan *tools Snort* dan *Pfsense* total pendeteksian berjumlah 33 TCP. Hasil deteksi menggunakan *snort* dan *pfsense*, tahapan pengujian tersebut melalui hasil pengujian dari jalur LAN, sedangkan dari pendeteksian dari jalur WAN tidak terdeteksi. Selanjutnya hasil dari pengujian pada jalur *web* dengan alamat *web* yaitu www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id dari salah satu teknik penyerangan yaitu menggunakan *scanning attack* pada *suricata* dan *pfsense*. Berikut gambar hasil *suricata* dibawah ini :



Gambar 15 NIDS,NIPS Suricata dan pfsense www.feeder.Universitas Muhammadiyah Cirebon.ac.id jalur LAN

Dari Gambar 15 diatas bahwa hasil dari pengujian pada jalur *web* dengan alamat *web www.feeder.Universitas Muhammadiyah Cirebon.ac.id* melalui pengujian *scanner attack* menggunakan NIDS dan NIPS dengan *tools Suricata* dan *Pfsense*, total pendeteksian berjumlah 83 TCP. Tahapan pengujian tersebut melalui hasil pengujian dari jalur LAN, sedangkan dari pendeteksian dari jalur WAN dengan menggunakan suricata dan pfsense terdeteksi UDP.

Berikut merupakan table rangkuman dari pengujian deteksi NIDS, NIPS, Snort dan Suricata pada LAN dan WAN:

Tabel 5 Vulnerability Assessment Hasil Uji Sesudah Implementasi NIDS dan NIPS

Alamat *Web*	***TCP Snort* Pada LAN**	***UDP Snort* pada WAN**	**Keterangan**
www.simaku.Universitas Muhamma	73	0	Terdeteksi berjumlah 73 tcp dan

diyah Cirebon.ac.id			UDP tidak terdeteksi
Alamat *Web*	***TCP Suricata* Pada LAN**	***UDP Suricata* pada WAN**	**Keterangan**
www.simaku.Universitas Muhammadiyah Cirebon.ac.id	79	1	Terdeteksi berjumlah 79 tcp dan UDP terdeteksi berjumlah 1
Alamat *Web*	***TCP Snort* Pada LAN**	***UDP Snort* pada WAN**	**Keterangan**
www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id	33	0	Terdeteksi berjumlah 33 tcp dan UDP tidak terdeteksi
Alamat *Web*	***TCP Suricata* Pada LAN**	***UDP Suricata* pada WAN**	**Keterangan**
www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id	35	3	Terdeteksi berjumlah 35 tcp dan UDP terdeteksi berjumlah 3
Alamat *Web*	***TCP Snort* Pada LAN**	***UDP Snort* pada WAN**	**Keterangan**
www.feeder.Universitas Muhammadiyah Cirebon.ac.id	78	0	Terdeteksi berjumlah 78 tcp dan UDP tidak terdeteksi
Alamat *Web*	***TCP Suricata* Pada LAN**	***UDP Suricata* pada WAN**	**Keterangan**
www.simaku.Universitas Muhammadiyah Cirebon.ac.id	83	69	Terdeteksi berjumlah 83 tcp dan UDP terdeteksi berjumlah 69

Dari data tabel 5 diatas, hasil dari pengujian NIDS dan NIPS menggunakan *tools Snort Pfsense* dengan alamat website www.simaku.Universitas Muhammadiyah Cirebon.ac.id pada data TCP berjumlah 73 NIDS dan NIPS sehingga UDP tidak terdeteksi, kemudian dari alamat *website* www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id dengan data TCP berjumlah 33 NIDS dan NIPS sehingga UDP tidak terdeteksi, kemudian dari alamat website www.feeder.Universitas Muhammadiyah Cirebon.ac.id dengan data TCP berjumlah 78 NIDS dan NIPS sehingga UDP tidak terdeteksi.

Hasil dari pengujian NIDS dan NIPS menggunakan *tools Suricata Pfsense* dengan alamat *website* www.simaku.Universitas Muhammadiyah Cirebon.ac.id pada data TCP berjumlah 79 NIDS dan NIPS sehingga UDP terdeteksi 1, kemudian dari alamat website www.sisterdikti.Universitas Muhammadiyah Cirebon.ac.id dengan data TCP berjumlah 35 NIDS dan NIPS sehingga UDP terdeteksi 3, kemudian dari alamat website www.feeder .Universitas Muhammadiyah Cirebon.ac.id dengan data TCP berjumlah 83 NIDS dan NIPS sehingga UDP terdeteksi 69.

Pada tabel 4 tampak bahwa perbandingan NIDS dan NIPS menggunakan *Snort Pfsense*, NIDS dan NIPS menggunakan *suricata pfsense* menunjukkan hasil pendeteksian melalui jalur LAN dan WAN memiliki hasil yang berbeda karena pendeteksian lebih unggul serta lebih responsive menggunakan NIDS dan NIPS dengan tools *suricata* dan *Pfsense* daripada dengan tools *snort* dan *PfSense*.

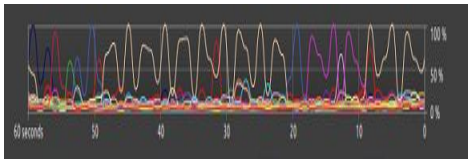
V. KESIMPULAN DAN SARAN

A. Kesimpulan

Beberapa kesimpulan yang dapat diambil tentang implementasi *network intrusion detection system* dan *Network intrusion prevention syste*m pada jaringan LAN berbasis *threats* dan *vulnerabilities assessment* di Universitas Muhammadiyah Cirebon, salah satunya adalah standar keamanan dan otentikasi yang dikembangkan oleh peneliti mengenai perlindungan jaringan LAN yang ada di Jaringan Universitas Muhammadiyah Cirebon perlu ditingkatkan. Seiring dengan perkembangan serangan dari waktu ke waktu *vulnerability* pada jaringan LAN memiliki nilai masing – masing diantaranya pada sisterdikti memiliki kerentanan mendium, simaku memiliki kerentanan *high* dan feeder memiliki kerentanan medium.

Berdasarkan penelitian dengan menggunakan OWASP Top 10 dalam vulnerabilities Assesment dapat mengetahui suatu nilai kerentanan tersebut dalam jaringan LAN dari tingkat high sampai *low*. Dampak yang ditimbulkan dari serangan tersebut dapat merugikan pengguna yaitu sistem *simaku, feeder, sisterdikti*, sehingga dari dampak tersebut maka jaringan LAN perlu terpasang NIDS dan NIPS menggunakan *Suricata* dan *Pfsense* karena *tools suricata* lebih responsive dan lebih unggul dalam pendeteksian serangan daripada *tools snort* dan *Pfsense*.

Adapun suatu *traffic* dalam mendeteksi adanya serangan dan bisa melakukan pertahanan serta untuk memblokir akses penyerang pada gambar dibawah ini :



Gambar 16 *Traffic* Normal Akses

NIDS dan NIPS berkolaborasi melengkapi dalam mempertahankan adanya serangan, hanya saja dari kedua aplikasi tersebut memiliki *traffic* normal terhadap menahan serta melakukan perlawan terhadap *attacker* pada jaringan LAN UNIVERSITAS MUHAMMADIYAH CIREBON.

B. Saran

Saran dan penelitian lebih lanjut, yang dapat dilakukan adalah menambahkan serangan-serangan sebuah tools untuk meningkatkan kekuatan dari NIDS dan NIPS menggunakan tools lainnya dan penambahan HIDS dan NIPS untuk mendeteksi serangan dari luar jaringan LAN dan berfungsi sebagai pertahanan pada area *host.*

DAFTAR PUSTAKA

[1] A. Kurniawan, I. R.-J. of T. &, and undefined 2017, "Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack Using Open Web Application Security Project (Owasp), (Online)" Search.Ebscohost.Com, vol. 95, no. 6, pp. 1363–1371, diakses pada jam 13.00 WIB Tanggal 24 Desember 2020.

[2] Amarudin, Faruk Ulum. 2018. "Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking". Jurnal Teknoinfo, Vol 12 (2), 72-75.

[3] Alamsyah. 2011. "Implementasi Keamanan Instrusion Detection System (IDS)

[4] Dan Instrusion Prevention System (IPS) Menggunakan Clearos". Jurnal SMarTek. Vol 9 (3), 223 – 229.

[5] A. Yasin and I. Mohidin. 2018. "Dampak Serangan DDoS pada Software Based Openfow Switch di Perangkat HG553," Jurnal Technopreneur. Vol. 6 (2), 01-72.

[6] Benny Sugiarto, 2018. "Konsep Dan Mekanisme Threat. (Online)". Tersedia: https://slideplayer.info/slide/13129122/. Diakses pada jam 11.00 WIB Tanggal 28 Oktober 2020.

[7] BeyonSecurity, 2020. "CVSS Explained.https://beyondsecurity.com/vulnerability assessment-requirements-cvss-explained", diakses jam 11.30 WIB Tanggal 28 Oktober 2020.

[8] Emir Risyad, Mahendra Data, Eko Sakti Pramukantoro. 2018. "Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood". Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol 2 (9), 2615-2624.

[9] Fadlin Arsin, Muh. Yamin, La Surimi. 2017. "Implementasi Security System Menggunakan Metode Idps (Intrusion Detection And Prevention System) Dengan Layanan Realtime Notification". Jurnal Semantik. Vol 3 (2), 39-48.

[10] F. B. Perdana, I. R. Munadi, and A. I. Irawan. 2019. Implementasi Sistem Keamanan Jaringan Menggunakan Suricata Dan Ntopng. e-Jurnal Proceeding of Engineering.Vol.6(2), 4076-4083.

[11] F. Arsin, M. Yamin, and L. Surimi. 2017. "Implementasi Security System Menggunakan Metode Idps (Intrusion Detection And Prevention System) Dengan Layanan Realtime Notification". Jurnal. Vol. 3(2), 39– 48.

[12] Hendri Alamsyah, Riska, Abdussalam Al Akbar. 2020. "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention Sistem". Jurnal Jointecs, Vol 5 (1), 17-24

[13] Jo˜ ao M. Ceron, Christian Scholten, Aiko Pras, Jair Santanna. 2018. "MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification". Jurnal IEEE Explore.1-9.

[14] Mamay Syani, Ali Muhammad Ropi. 2018. "Analisis Dan Implementasi Network Security System Menggunakan Teknik Host-Based Intrusion Detection System (Hids) Berbasis Cloud Computing". Proceeding Seminar Nasional Telekomunikasi Dan Informatika Selisik. 158-160.

[15] Maria Ulfa. 2013. "Implementasi Intrusion Detection System (IDS). Jurnal Ilmiah Matrik". Vol.15 (2), 105 – 118.

[16] Mohamad Nurul Huda Monoarfa, Xaverius B.N. Najoan, ST.,MT., Alicia A.E. Sinsuw, ST., MT. 2016. "Analisa dan Implementasi Network Intrusion Prevention System Jaringan". Jurnal Teknik Elektro dan Komputer Vol. 5(4), 34-45.

[17] Muhammad Anif, Sindung HWS & Mokhamad Daman Huri. 2015. "Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang". Jurnal Tel, 13(1), 25-30.

[18] Muqorobin1, Zul Hisyam1, Moch. Mashuri1, Hanafi1, Yudhi Setiyantara. 2017. "Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing. Jurnal Majalah Ilmiah Bahari", Vol 17(2),1-9

[19] N. Fahriani, P. A. R. Devi, and D. Aditama. 2017. "Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer," Proceeding. Semin. Nas. Teknol. dan Rekayasa Inf.19–24.

[20] Okasha Eldow,Prashant Chauhan,Punit Lalwani,M.B.Potdar. 2016. Computer Network security ids tools and techniques (snort/suricata). Jurnal International Journal of Scientific and Research Publications, Vol 6 (1), 593-597.

[21] Parningotan Panggabean. 2018. "Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (IDS)". Jurnal Jursima, Vol 6 (1), 112.

[22] P. Johnson, R. Lagerström, M. Ekstedt, and U. Franke, "Can the Common Vulnerability Scoring System be Trusted? A Bayesian Analysis," IEEE Transactions on Dependable and Secure Computing, vol. 15(6), 1002–1015.

[23] Rifkie Primartha. 2017. "Security Jaringan Komputer Berbasis CEH". Informatika,ISBN : 602-6232-57-1.

[24] Sergio Marphy Junan Lawalata. 2020. "Perancangan Wireless Intrusion DetectionSystem Pada Jaringan WI-FI Berbasis Threats Dan Vulnerabilities Assessment", Tesis. Teknik. Teknik Elektro. Institut Teknologi Bandung.

[25] Sofana Iwan, dkk. 2019. "Network Security dan Cyber Security". Bandung : Informatika Bandung.

[26] Sutarti, Adi Putranto Pancaro, Fembi Isnanto Saputra. 2018. "Implementasi Ids (Intrusion Detection System) Pada Sistem Keamanan Jaringan". Jurnal Prosisko. Vol. 5 (1), 1-8.

[27] Y. Ariyanto and B. Harijanto. 2017. "Implementasi Suricata Pada Server CLOUD PROXMOX VE Sebagai Intrusion Detection System (IDS) Dalam Pengamanan Jaringan". Jurnal . Vol. 3 (1), 78–189.

[28] Yusuf, F. 2017, "Mengenal Berbagai Jenis Serangan pada Jaringan Komputer". (Online). Tersedia : http://netsec.id/jenis-serangan-jaringan-komputer/. Diakses pada jam 11.45 WIB tanggal 28 Oktober 2020.