ANALISIS SISTEM KEAMANAN JARINGANMENGGUNAKAN FRAMEWORK NIST

M. Zen Andriyansa[1], Febriyanti Panjaitan[2]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email:m.zen.andriyansa@gmail.com[1], febriyanti_panjaitan@gmail.com[2]

ABSTRAK

Keamananjaringan merupakan aspek yang sangat penting bagi sebuah jaringan komputer. Jaringan komputer memiliki kelemahan-kelemahan yang jika tidak dilindungi dan dijaga dengan baik maka akan menyebabkan kerugian. Maka sudah sepatutnya keamanan jaringan harus lebih diperhatikan untuk mencegah ancaman menyerang sistem, terlebih lagi saat jaringan LAN sudah tersambung ke internet maka ancaman keamanan jaringan akan semakin signifikan. Universitas Sjakhyakirti merupakan universitas yang terletak di kota Palembang yang juga berpartisipasi dalam menyelenggarakan sistem keamanan tersebut. Pentingnya penelitian ini yaitu agar dapat mengurangi adanya ancaman yang berdampak negatif terhadap sistem keamanan informasi, sehingga mengurangi dampak insiden sistem informasi dan meminimalisir resiko-resiko yang mungkin akan terjadi. Selanjutnya dilakukan analisa sistem keamanan jaringan dengan FrameworkNIST*(National Institute Standard Technology)*, framework yang dirancang untuk sesuatu perhitungan kualitatif yang didasarkan pada analisis sistem keamanan.

Kata kunci: Analisis, Keamanan, Jaringan, *Framework NIST*

ABSTRACT

Network security is a very important aspect for a computer network. Computer networks have weaknesses which, if not protected and protected properly, will cause harm. So it is needed by network security to be have more concern to prevent possible threats of system, especially when a LAN network is connected to the internet, network security threats will be increasingly significant. Sjakhyakirti University is a university located in the city of Palembang which also participated in organizing the security system. The importance of this research is to reduce threats that have a negative impact on information security systems, thereby reducing the impact of information system incidents and minimizing the risks that might occur. The network security system analysis is then performed with the NIST Framework (National Institute of Standard Technology) which is a framework designed to be something of a qualitative calculation and based on an analysis of security systems.

Keywords: *Analysis, Network, Security, NIST Framework*

1. PENDAHULUAN

Penggunaan Teknologi saat ini telah berkembang pesat, salah satunya dalam bidang jaringan komputer. Keamanan Jaringan merupakan aspek yang sangat penting bagi sebuah jaringan komputer.

Universitas Sjakhyakirti merupakan universitas yang terletak di kota Palembang yang juga berpartisipasi dalam menyelenggarakan sistem keamanan tersebut. Universitas Sjakhyakirti perlu menyediakan perlindungan jaringan untuk mendukung dan memastikan lancarnya kegiatan yang ada di universitas. Jaringan komputer Universitas Sjakhyakirti menjadi jembatan antara mahasiswa, dosen, dan pihak civitas akademik.

Framework NIST(*National Institute Standard Technology*) adalah framework yang dirancang untuk menjadi sesuatu perhitungan kualitatif dan didasarkan pada analisis sistem keamanan yang cukup sesuai dengan keinginan pengguna dan ahli teknik untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola resiko dalam sistem teknologi informasi. NIST memiliki 9 tahapan, yaitu *System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations* dan *Results Documentation.*

2. METODOLOGI PENELITIAN

Tahapan penilaian risiko berdasarkan NIST (*National Institute Standard Technology*) 800-30 yaitu sebagai berikut:

1) *System Characterization*
2) *Threat Identification*
3) *Vulnerability Identification*
4) *Control Analysis*
5) *Likelihood Determination*
6) *Impact Analysis*
7) *Risk Determination*
8) *Control Recommendations*
9) *Results Documentation*

2.1 Metode Pengumpulan Data

Metode Pengumpulan Data adalah langkah yang strategis dalam penelitian, karena tujuan utama penelitian yaitu untuk mendapatkan data (Sugiyono, 2010).Metode Pengumpulan Data yang digunakan dalam penelitian ini yaitu:

1) Studi *Literature*
   Studi *literature* merupakan penelitian yang dilakukan untuk mendapatkan bahan rujukan berupa referensi yang bersifat teoristis dari buku-buku dan sumber bacaan lain yang dapat mendukung topik.
2) Persiapan *Sofware*
   Pada tahapan ini dilakukan persiapan *software* yang mendukung untuk menganalisa sistem jaringan.
3) Keamanan Jaringan
   Mengidentifikasi sistem keamanan jaringan Universitas Sjakhyakirti yang berupa spesifikasi perangkat keras *(hardware)* dan perangkat lunak *(software)*, dan mengenali ancaman *(threat)* dan kerentanan *(vulnerability)* sistem keamanan jaringan pada Universitas Sjakhyakirti.
4) Analisa Resiko
   Tahapan ini merupakan tahapan analisa resiko sistem keamanan jaringan dengan Framework NIST.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Pada tahap awal penelitian terdapat 9 tahapan yang digunakan pada framework NIST. Namun penelitian ini akan menggunakan 4 tahap awal sebagai berikut:

1) *System Characterization*

   Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.Hasil yang didapat dari tahapan ini yaitu karakteristik sistem yang berupa spesifikasi perangkat keras dan perangkat lunak pada jaringan serta batasan penggunaan masing-masing perangkat.

2) *Threat Identification*

   Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada. Hasil yang didapat dari tahapan ini yaitu identifikasi adanya segala bentuk ancaman baik fisik maupun logik yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan.

3) *Vulnerability Identification*

   Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya. Identifikasi dilakukan terhadap kerawanan atau vulnerability yang berkaitan dengan sistem komputer yang memungkinkan seseorang mengoperasikan atau menjalankannya dengan benar, dan memungkinkan pihak tak berwenang *(hacker)* mengambil alih.

4) *Control Analysis*

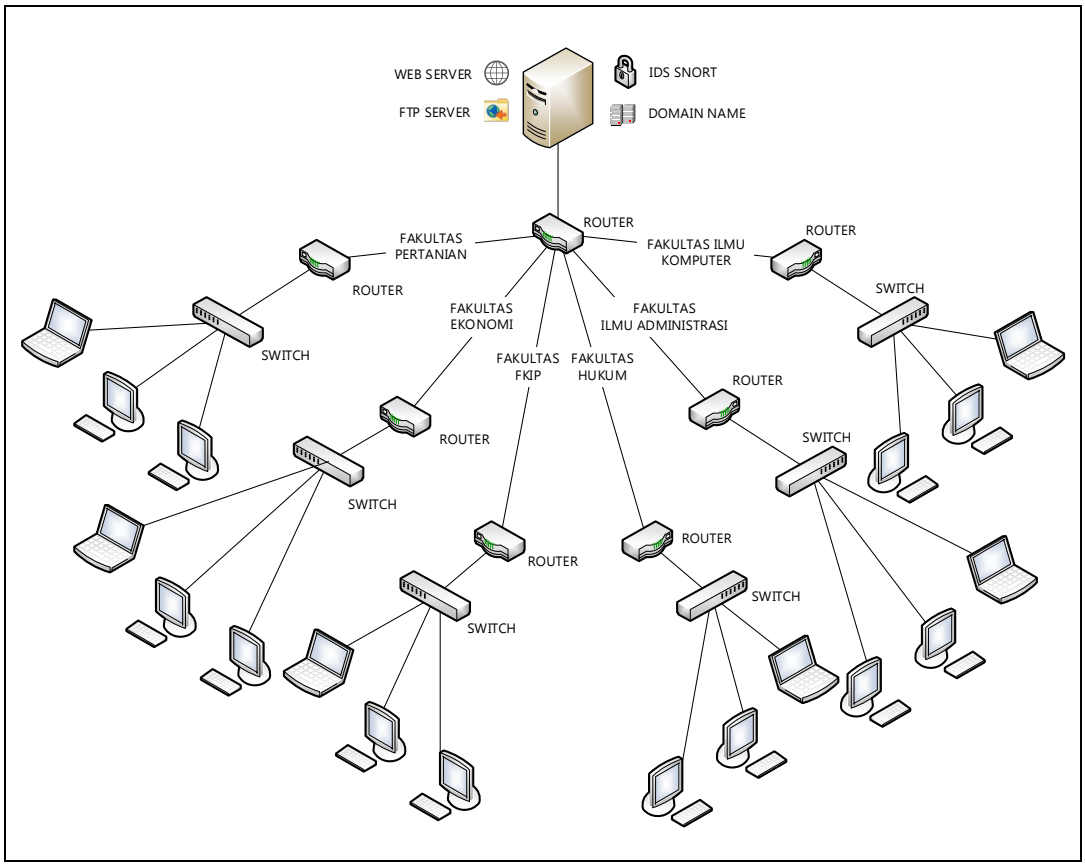
   Analisis terhadap kontrol yang telah dilaksanakan dan direncanakan untuk implementasi oleh organisasi untuk meminimalisir atau menghilangkan kemungkinan-kemungkinan pengembangan dari ancaman. Tahapan ini diperlukan agar tahu apa yang harus dilakukan saat adanya ancanan. Akan berbahaya jika tidak nengetahui langkah selanjutnya setekah ditemukan kerentanan di dalam jaringan.

3.2 Pembahasan

3.2.1 *System Characterization*

Pada tahapan ini, peneliti mencoba mengenali karakteristik sistem jaringan Universitas Sjakhyakirti. Maka yang pertama kali dilakukan yaitu mengetahui bagaimana jaringan bekerja melalui topologinya. Jaringan Universitas Sjakhyakirti terdapat server yang mencakup enam jurusan. Masing masing jurusan memiliki routernya tersendiri yang terhubung ke router server. Kemudian, di setiap router terdapat switch yang mencakup beberapa komputer dan laptop. Sebagai peladen utama pada jaringan, peladen (Server) jaringan Universitas Syakhyakirti memiliki beberapa fasilitas yaitu sebagai Web Server dengan perangkat lunak Apache, kemudian FTP Server dengan perangkat lunak Filezilla, IDS *(Intrusion Detection System)* dengan perangkat lunak Snort, dan Domain Name Server yang menggunakan perangkat lunak BIND9. Dengan begitu, dapat disimpulkan bahwa setiap perangkat host dalam jaringan Universitas Sjakhyakirti sudah terlindung dalam sistem keamanan jaringan.

Berikut adalah hasil karakterisasi sistem melalui topologi yaitu sebagai berikut :



Gambar 1.*Karakterisasi Sistem Melalui Topologi*

Selain dari segi topologi, peneliti juga akan mengenali karakterisasi sistem melalui penggunaan perangkat keras *(hardware)* yang ada. Hasil karakterisasi sistem melalui perangkat keras pada jaringan Universitas Sjakhyakirti adalah sebagai berikut:

1) Mikrotik RB 750

   Router yang dapat digunakan untuk menjadikan komputer biasa menjadi router yang handal, mempunyai banyak fitur yang mencakup untuk IP Network dan Jaringan wireless. Mikrotik RB 750 dipilih karena memiliki sistem konfigurasi jaringan yang baik.

2) Switch D-Link DES-10160 dengan 24 Port

   Switch dengan fitur auto switch membuat instalasi cepat dan bebas kerumitan. Juga terdapat auto-negosiasi pada setiap port yang mendeteksi kecepatan link dari perangkat jaringan serta dengan cerdas menyesuaikan kompatibilitas dan kinerja yang optimal.

3) Kabel UTP Cat6e

   Digunakan sebagai penghubung suatu jaringan dan juga power untuk koneksi AP ke POE dan Router. Dengan merk AMP original agar bisa digunakan dalam jangka waktu yang lama dan untuk mengurangi masalah yang terdapat pada koneksi kabel.

4) Port Jaringan RJ45

   Konektor atau penghubung kabel *ethernet* yang biasanya dipakai untuk jaringan. Konektor ini juga bisa dipakai pada topologi jaringan komputer LAN *(Local Area Network).*

3.2.2. *Threat Identification*

Pada tahapan ini, peneliti mencoba mengidentifikasi ancaman *(threat)* pada sistem keamanan jaringan Universitas Sjakhyakirti. Seperti yang kita ketahui jaringan rentan terkena serangan, maka perlu diketahui terlebih dahulu ancaman serangan seperti apa saja yang mungkin membahayakan sistem. Berikut adalah hasil pendataan ancaman sistem yaitu sebagai berikut:

1) *DDoS*
   Jenis serangan DOS yang menggunakan banyak host dan untuk menyerang satu server sehingga mengakibatkan server tidak dapat berfungsi bagi klien. Dengan penggunaan host sekaligus dalam DOS maka jaringan akan lebih cepat mengalami down dan menolak memberikan pelayanan karena server yang sudah tidak dapat berfungsi.
2) *Packet Snifing*
   Teknik yang digunakan yaitu dengan melakukan pencurian data, cara kerjanya yaitu dengan memonitoring dan menganalisis setiap paket data yang ditransmisikan dari klien ke server.
3) *Ransomware*
   Jenis malware yang dirancang untuk menghalangi akses kepada sistem komputer atau data hingga tebusan dibayar.
4) *Spoofing*
   Teknik yang digunakan yaitu dengan cara memalsukan data sehingga penyerang *(attacker)* dapat mengakses sistem seperti host yang bisa dipercaya

3.2.3. *Vulnerability Identification*

Pada tahapan ini, peneliti mencoba mengidentifikasi kerentanan *(vulnerability)* pada sistem keamanan jaringan Universitas Sjakhyakirti. Seperti yang kita ketahui jaringan rentan terkena serangan, maka perlu diketahui terlebih dahulu celah yang dapat dimanfaatkan penyerang untuk melancarkan serangannyadan membahayakan sistem. Berikut adalah hasil pendataan *vulnerability* sistem yaitu sebagai berikut:

1) *Miskonfigurasi*
   Kesalahan konfigurasi pada *server* dan perangkat keras (*hardware*) sangat sering membuat para penyusup dapat masuk ke dalam suatu sistem dengan mudah. Konfigurasi yang tidak hati-hati dapat menyebabkan usaha penyusupan menjadi jauh lebih mudah terlebih jika ada pilihan lain yang dapat diambil oleh para penyusup.
2) *Backdoor*
   Yaitu langkah memasuki sistem selain akses login utana admin. Biasanya backdoor tersembunyi dan menggunakan jalur autentikasi berbeda dari jalur utama.
3) *Rootkit*
   Merupakan alat yang digunakan untuk menyembunyikan jejak apabila telah melakukan penyusupan. *Rootkit* menggunakan beberapa *tool* yang dipakai oleh sistem yang sudah dimodifikasi sehinggadapat menyembunyikan jejak.
4) *Control Analysis*
   Pada tahapan ini, peneliti akan menjabarkan analisa kendali *(control analysis)* untuk meminimalisir atau menghilangkan bahaya yang dapat menyerang sistem keamanan jaringan Universitas Sjakhyakirti. Tahapan ini diperlukan agar tahu apa yang harus dilakukan saat adanya ancanan *(threat)* atau kerentanan *(vulnerability).*

Tabel 1. Hasil Penentuan Kendali *(Control)*

No	Identifikasi	Jenis	Kendali
1	Ancaman	*DDoS*	1. Mengatur sistem pembatasan bandwith upload maupun download pada RouterOS Mikrotik. 2. Memasang perangkat lunak yang akan segera memotong koneksi jika penggunaan bandwith mulai membajiri trafik atau bahkan memberi tantangan keamanan seperti Captcha
2	Ancaman	*Packet Sniffing*	1. Mulai menggunakan enkripsi yang secure seperti WPA-PSK2 dilengkapi dengan SSH 2. Mulai menerapkan akses SSL serta Always HTTPS dan enkripsi bertingkat.
3	Ancaman	*Ransomware*	1. Membatasi pembagian akses sumber daya file agar tidak terlalu bebas 2. Menerapkan antivirus guna mendeteksi bahaya terhadap setiap software pada jaringan.
4.	Ancaman	*Spoofing*	3. Menerapkan sistem whitelist (daftar putih) yang hanya mengizinkan pengguna tertentu untuk mengakses seluruh fitur dan fasilitas jaringan. 4. Mulai menggunakan sistem identifikasi host yang lengkap yang semestinya menggunakan IP, DNS, MAC Address, hostname, dan autorisasi handshake.
5.	*Vulnerability*	*Miskonfigurasi*	Pastikan konfigurasi port-port akses sistem agar tidak digunakan penyerang, misalnya port 43 telnet, port 20 FTP, dan sebagainya.
6.	*Vulnerability*	*Backdoo*r	1. Mulai menutup setiap backdoor, seperti ditutupnya akses WPS (WiFi Pin Setup) yang hanya memiliki pola 8 digit. 2. Men-scan sistem dari adanya penanaman shell sebagai remote backdoor.
7.	*Vulnerability*	*Rootkit*	Menerapkan antivirus guna mendeteksi adanya rootkit dalam sistem operasi jaringan.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari evaluasi sistem jaringan ini adalah:

1) Penelitian berhasilmenjawab apakah sistem keamanan jaringan di Universitas Sjakhyakirti Palembang dapat dianalisa dengan frameworkNIST.
2) Setelah diteliti, ditemukan bahwa sistem keamanan jaringan Universitas Sjakhyakirti memiliki celah terhadap ancaman DDoS, Packet Sniffing, Ransomware, dan Spoofing. Selain itu, sistem keamanan jaringan Universitas Sjakhyakirti juga memiliki kerentanan dari sisi miskonfigurasi, backdoor, dan rootkit.
3) Dengan adanya penelitian ini, berhasil menerapkan tujuannya untuk menganalisis sistem keamanan jaringan komputer menggunakan metode framework NISTpada Universitas Sjakhyakirti.
4) Penerapan Framework NIST pada penelitian ini menguntungkan Universitas Sjakhyakirti karena dapat membantu menganalisa kekurangan yang ada pada jaringan. Jika tidak diterapkan, maka

Universitas Sjakhyakirti tidak akan mengetahui kelemahan jaringan dan tidak dapat mengantisipasi adanya ancaman dan kerentanan pada jaringan. Ancaman tersebut antara lain DDoS, packet sniffing, ransomware, dan spoofing, kerentanan tersebut antara lain miskonfigurasi, backdoor, dan rootkit.

5. DAFTAR PUSTAKA

[1] Melwin, S. (2005). Pengantar Jaringan Komputer. Yogyakarta: CV. Andi Offset.

[2] Hendrawan1, Parman Sukarno2, Muhammad Arief Nugroho. "Analisis Perbandingan Quality of Service (Qos) Penerapan Snort Ids Dan Bro IdsDalam Arsitektur Software Define Network (Sdn)." (2018).

[3] Ma'sum, Muhammad Suyuti. "Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort Dan Netfilter. Pontianak: Universitas Tanjungpura." (2017).

[4] Shah Khadafi, Budanis Dwi Meilani, Samsul Arifin. "Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System) ". (2017).

[5] Sugiyono. "Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada Pt Guna Indonesia. Jakarta: Stikom Cipta Karya Informatika." (2016).

[6] S Triyono. "Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali. " (2013).