BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi saat ini telah berkembang pesat, salah satunya dalam bidang jaringan komputer. Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node, maupun teknologi yang digunakan, oleh sebab itu diperlukan pengelolaan jaringan yang baik. Sehingga untuk ketersediaan jaringan selalu ada, namun demikian dalam pengelolaan jaringan memiliki banyak permasalahan diantaranya yang berhubungan dengan keamanan jaringan.

Keamanan jaringan 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 berupa resiko data loss, kerusakan sistem server, tidak maksimal service nya dan kehilangan objek vital instansi baik perusahaan, organisasi maupun akademisi. (Ikhwan, 2014).

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. Misalnya DDoS attack dan sebagainya, juga serangan peretas, virus, trojan, malware dan sebagainya yang semuanya merupakan ancaman yang tidak bisa diabaikan.

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.

Dari pengamatan dan interview awal yang dilakukan peneliti. Jaringan komputer Universitas Sjakhyakirti telah dilengkapi dengan sistem keamanan. Namun sejauh ini belum ada tolak ukur untuk menguji apakah jaringan komputer telah mampu mendeteksi semua serangan, maka diperlukan analisa pada sistem keamanan untuk mengidentifikasi, mengevaluasi dan mengelola resiko jaringan ditembus yaitu dengan metode Framework NIST.

Jaringan komputer yaitu himpunan “interkoneksi” antara 2 komputer autonomous atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel *(wireless)*. Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan autonomous (tidak melakukan kontrol terhadap komputer lain dengan akses penuh).

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. Penelitian ini diadakan pada Universitas Sjakhyakirti

karena mempertimbangkan belum adanya analisa sistem keamanan jaringan komputer pada Universitas Sjakhyakirti.

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*.

Tahapan yang akan dipakai pada penelitian ini adalah *System Characterization* yaitu karakteristik sistem yang berupa spesifikasi perangkat keras dan perangkat lunak pada jaringan serta batasan penggunaan masing-masing perangkat, *Threat Identification* pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada. *Vulnerability Identification,* yaitu Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya. Terakhir, *Control Analysis* yaitu analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinan-kemungkinan pengembangan dari ancaman.

Berdasarkan uraian latar belakang diatas penulis akan melakukan penelitian yang berjudul “ANALISIS SISTEM KEAMANAN JARINGAN MENGGUNAKAN FRAMEWORK NIST”. Penelitian ini diharapkan untuk

mempermudah administrator jaringan dengan adanya analisa keamanan jaringan pada Universitas Sjakhyakirti sehingga akan banyak pengembangan kedepannya.

1.2 Rumusan Masalah

Pada latar belakang yang telah diuraikan, maka untuk perumusan masalah didapatkan yaitu “Bagaimana menganalisa sistem keamanan jaringan komputer dengan metode Framework NIST (*National Institute Standard Technology*)?”.

1.3 Batasan Masalah

Untuk lebih mengarahkan masalah yang ada serta agar tidak terlalu menyimpang dari permasalahan yang akan dilakukan penulis, maka penulis ingin membatasi permasalahan.

1. Menganalisa sistem keamanan jaringan komputer.
2. Framework yang digunakan dengan metode Framework NIST (*National Institute Standard Technology*).
3. Penelitian diadakan pada Universitas Sjakhyakirti.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan

Tujuan dari penelian ini yaitu untuk menganalisis sistem keamanan jaringan komputer menggunakan metode Framework NIST pada Universitas Sjakhyakirti.

1.4.2 Manfaat Penelitian

Adapun manfaat dari "Analisis Sistem Keamanan Jaringan Menggunakan Framework NIST" ini adalah :

1. Menganalisa sistem keamanan jaringan komputer di Universitas Sjakyahkirti.
2. Untuk mendata serangan-serangan ke sistem keamanan jaringan Universitas Sjakyahkirti dari pihak yang tidak bertanggung jawab.
3. Dapat digunakan sebagai acuan peningkatan sistem keamanan jaringan pada Universitas Sjakhyakirti.

1.5 Metodologi Penelitian

1.5.1 Waktu dan Tempat

Waktu penelitian dilakukan pada bulan November 2019 sampai dengan bulan Maret 2020 di Jl. Sultan Muhammad Mansyur Kb Gede 32 Ilir, Ilir Barat II, 32 Ilir, Ilir Bar. II, Kota Palembang, Sumatera Selatan 30145.

1.5.2 Alat

Alat yang digunakan dalam penelitian ini terbagi menjadi perangkat keras *(hardware)* dan perangkat lunak *(software)*, sebagai berikut:

a. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan adalah sebagai berikut :

1. Laptop Lenovo G40
2. Processor Intel Celeron N8240
3. RAM 2 GB
4. Harddisk 500 GB

5. Printer Epson L120
6. Flashdisk 8 GB

b. Perangkat Lunak (*Software)*

a . *Windows10 Enterprise* sebagai *operating system*

b. *Microsoft Word 2010* untuk penulisan laporan tugas akhir ini

c. *Software* pendukung yaitu *browser* menggunakan Google Chrome.

1.5.3 Bahan

Bahan yang digunakan dalam penelitian ini yaitu:

a. Data jaringan komputer pada Universitas Sjakhyakirti.
b. Jurnal penelitian yaitu jurnal-jurnal yang telah diteliti sebelumnya berkaitan dengan metode penelitian yang digunakan sebagai referensi penulis dalam penelitianya.

1.5.4 Metode Penelitian

Dikarenakan penelitian ini lebih menitikberatkan pada penelitian analisis, maka penelitian menggunakan metode NIST (*National Institute Standard Technology*) untuk analisa. NIST 800-30 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Technology* yang mana merupakan kelanjutan dari tanggung jawab hukum di bawah undang-undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko.

Tahapan penilaian risiko berdasarkan NIST 800-30 yaitu menurut (Syalim, Hori, dan Sakurai, 2009) dalam penelitian :

1. *System Characterization*

   Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.

2. *Threat Identification*

   Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada.

3. *Vulnerability Identification*

   Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya.

4. *Control Analysis*

   Analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinan-kemungkinan pengembangan dari ancaman.

5. *Likelihood Determination*

   Proses rangking terhadap potensi dari kerawanandapat dilaksanakan dalam lingkungan dari kerawanan tersebut. Faktor yang menjadi pertimbangan adalah ancaman (sumber dan kemampuan), sifat dari kerawanan serta keberadaan dan efektifitas kontrol jika diterapkan.

6. *Impact Analysis*

   Tahapan ini digunakan untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan.

7. *Risk Determination*

   Penilaian tingkat risiko pada sistem IT dilakukan pada langkah ini.

8. *Control Recommendations*

Tahapan ini menilai kontrol yang mana dapat mengurangi atau menghilangkan risiko yang telah teridentifikasi. kontrol yang direkomendasikan sebaiknya harus dapat mengurangi tingkat risiko pada sistem IT dan data, kepada tingkat risiko yang dapat diterima.

9. *Results Documentation*

Pada tahap ini, dilakukan pengembangan laporan hasil penilaian risiko (sumber ancaman, kerawanan, risiko yang dinilai dan kontrol yang direkomendasikan).

1.5.5 Metode Pengumpulan Data

Metode pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data.(Sugiyono, 2010)

Metode Pengumpulan Data yang digunakan dalam penelitian ini adalah :

a. Studi *Literature*

Studi *literature* adalah penelitian yang dilakukan untuk mendapatkan bahan rujukan berupa referensi yang bersifat teoristis dari buku-buku dan sumber bacaan lain yang dapat mendukung topik.

b. Persiapan *Software*

Tahapan ini dilakukan persiapan *software* yang mendukung dalam analisa sistem jaringan.

c. 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.

d. Analisa Resiko

Tahapan ini merupakan tahapan analisa resiko sistem keamanan jaringan dengan Framework NIST.

1.6 Sistematika Penulisan

Adapun, sistematika penulisan yang digunakan pada penelitian ini yaitu:

BAB I PENDAHULUAN

Pada Bab ini menjelaskan tentang uraian Latar Belakang, Identifikasi Masalah, Batasan Masalah, Perumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bab ini akan menjelaskan hasil-hasil penelitian sejenis terdahulu yang menginspirasi atau melandasi pelaksanaan penelitian ini dan juga mengulas landasan teoritik yang berhubungan dengan penelitian yang akan dilakukan, seperti landasan teori dan penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan metodologi dalam penelitian yang meliputi penentuan teknik atau metode dalam menganalisa sistem keamanan jaringan Universitas Sjakhyakirti.

BAB IV HASIL DAN ANALISIS

Dalam bab ini menjelaskan tentang hasil dan analisis dari sistem keamanan jaringan yang dilakukan dalam penelitian Universitas Sjakhyakirti.

BAB V KESIMPULAN DAN SARAN

Bab ini menjelaskan tentang uraian kesimpulan dari keseluruhan bab yang telah dibuat serta mencoba memberikan saran-saran yang mungkin berguna untuk mengatasi masalah yang dihadapi.