Bab I Pendahuluan

I.1 Latar Belakang

Aktivitas *security auditing* kerentanan sistem operasi sangat penting untuk mencegah serta mengurangi dampak kerusakan karena akibat adanya serangan dari pihak yang tidak bertanggung jawab. Hal ini menjadi dasar untuk meningkatkan kesadaran dan melakukan langkah awal untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem operasi. Faktor-faktor internal dan eksternal yang menjadi kelemahan tersebut adalah kurangnya kesadaran pemilik sistem operasi dan kurangnya *maintenance* serta pembaruan untuk sistem operasi tersebut. Menurut HP *Cyber Risk Report*, tahun 2015 terjadi beberapa kasus yang disebabkan karena kerentanan perangkat lunak. Kerentanan tersebut sudah terjadi dari tahun-tahun sebelumnya bahkan sampai dekade-dekade sebelumnya.

Berdasarkan kasus tersebut maka sangat penting untuk menerapkan uji kerentanan yang dilakukan dengan menggunakan *vulnerability scanner* seperti OpenVAS, serta menggunakan aplikasi IDS (*Intrusion Detection System*) untuk membantu mendeteksi ujicoba serangan yang dilakukan terhadap OS (*Operating System*) serta mengelompokkan jenis-jenis serangan yang dilakukan. Didalam penelitian ini, OS yang digunakan adalah Typhoon OS karena Typhoon OS memiliki *repository* sehingga bisa untuk meng-*install* aplikasi yang diperlukan didalam penelitian. OpenVAS merupakan alat bantu uji kerentanan dengan sumber kode terbuka yang mampu menjadi salah satu solusi untuk memberikan gambaran dari sebuah penelusuran celah keamanan. Penelitian ini menggunakan OpenVAS karena OpenVAS memiliki *database* kerentanan yang cukup lengkap serta hasil scan mudah untuk dibaca IDS adalah *tool*, metode atau sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan computer. Melakukan uji kerentanan akan mampu membantu proses identifikasi kelemahan dalam sistem sebelum serangan dapat terjadi serta dapat menjadi langkah pencegahan dalam meningkatkan keamanan terhadap sebuah sistem. Menggunakan *vulnerability scanner* memungkinkan untuk pendeteksian dini dan sekaligus dapat dilakukan penanganan yang sudah diketahui

kerentanannya serta mudah untuk mengidentifikasi kerentanan yang ada pada jaringan. Kerentanan tersebut memungkinkan timbulnya resiko yang berpotensi dieksploitasi. Karena itu, diperlukan suatu upaya untuk mengauditing sistem operasi. Salah satu upaya tersebut adalah *security auditing,* terhadap *vulnerable machine*.

Penilitian ini menyajikan tentang pengendalian terhadap ancaman serangan pada sistem dengan memberikan solusi perbaikan untuk menahan resiko melalui *vulnerability assessment.*

I.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan dalam penelitian dirumusukan sebagai berikut :

1. Bagaimana membuat profil resiko berdasarkan analisa kerentanan pada *vulnerable machine?*
2. Bagaimana memodelkan serangan yang akan diuji cobakan pada *vulnerable machine?*
3. Bagaimana NIST *cybersecurity framework* mendasari proses *security auditing?*

I.3 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah sebagai berikut :

1. Menganalisa serta mengestimasi profil resiko pada *vulnerable machine.*
2. Memodelkan serangan dari literatur *walkthrough.*
3. Menganalisa bagaimana NIST *cysbersecurity framework* terlibat dalam mendasari proses *security auditing.*

I.4 Manfaat Penelitian

Manfaat teoritis dari penelitian ini sebagai berikut :

1. Memberikan informasi tentang kerentanan apa saja yang ada didalam *vulnerable machine,* yaitu Typhoon OS.
2. Memberikan informasi tentang pemodelan serangan yang bisa dilakukan terhadap *vulnerable machine,* yaitu Typhoon OS.
3. Memberikan informasi terkait peran NIST *cybersecurity framework* dalam proses *security auditing.*

4. Membantu dalam mengestimasi resiko dari suatu kerentanan pada *vulnerable machine,* yaitu Typhoon OS.
5. Memberikan solusi terhadap kerentanan yang ada didalam *vulnerable machine,* yaitu Typhoon OS.

I.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini sebagai berikut :

1. Sistem keamanan jaringan komputer pada sistem operasi *Linux*.
2. Data *vulnerability* berdasarkan hasil *scanning* OpenVAS.
3. Data *threat* berdasarkan data literatur *walkthrough.*
4. Implementasi penelitian dilakukan sebatas LAN secara virtual.
5. Analisa *vulnerability* dilakukan sebatas pada level sistem.

I.6 Sistematika Penulisan

Penelitian ini memiliki sistematika pelaporan sebagai berikut :

BAB I Pendahuluan

Bab ini berisi penjelasan latar belakang untuk melakukan penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, serta batasan penelitian yang menjadi dasar penulis untuk melakukan penelitian.

BAB II Tinjauan Pustaka

Bab ini memuat teori yang relevan dengan judul penelitian serta uraian penelitian sebelumnya.

BAB III Metodologi Penelitian

Bab ini mendefinisikan langkah-langkah penelitian, diantaranya pembangunan model konseptual dari *security auditing* serta merancang sistematika pemecahan masalah.

BAB IV Analisis dan Perancangan

Bab ini menganalisis semua komponen dari penelitian, mulai dari analisis IDS, analisis *vulnerability scanner*, analisis *framework*,

analisis *vulnerability*, dan analisis serangan, serta melakukan perancangan serangan pada *vulnerable machine.*

BAB V Implementasi dan Pembahasan

Bab ini mengimplementasi dari serangan yang telah dirancang sebelumnya dan membahas hasil *scanning*, hasil serangan, serta solusi dari setiap kerentanan.

BAB VI Kesimpulan dan Saran

Bab ini menjelaskan kesimpulan dari hasil penelitian serta saran yang diperlukan agar penelitian lebih baik.