Bab I Pendahuluan

I.1 Latar Belakang

Proses atau 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 *operating system* 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, sedangkan menurut badan kementrian komunikasi dan informatika atau sering diseabut Kominfo diindonesia sendiri cukup sering terjadi serangan siber seperti yang terjadi pada tahun 2017 yaitu searangan siber berupa *ransomware* dimana serangan siber ini menyerang dan merusak sistem komputer dari jarak jauh, *ransomeware* sendiri memanfaatkan kelemahan sistem keamanan yang terdapat pada sistem operasi yang belum terupdate. Berdasarkan kasus tersebut maka sangat penting untuk menerapkan uji kerentanan yang dilakukan dengan menggunakan *vulnerability scanner* seperti openvas, serta menggunakan aplikasi *Intrusion Detection System* untuk membantu mendeteksi ujicoba serangan yang dilakukan oleh *kali linux* sebagai alat penyerangan, terhadap *Operating System* serta mengelompokkan jenis-jenis serangan yang dilakukan. Didalam penelitian ini, *Operating System* yang digunakan adalah *Typhoon OS* karena *Typhoon* didisain dengan memiliki beberapa kerentanan dan kesalahan konfigurasi. Typhoon dapat digunakan untuk menguji kerentanan dalam layanan jaringan, kesalahan konfigurasi, aplikasi web yang rentan, serangan peretasan kata sandi, serangan eskalasi hak istimewa, langkah pasca eksploitasi, pengumpulan informasi, dan serangan DNS sehingga sangat mendukung dalam penelitian ini.

Openvas merupakan alat bantu uji kerentanan dengan sumber kode terbuka yang mampu menjadi salah satu solusi untuk memberikan gambaran dari sebuah penelusuran celah keamanan. *Intrusion Detection System* 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* berdasarkan National Institute of Standard Technology (NIST), terhadap *vulnerablemachine*. Penelitian ini menyajikan tentang pengendalian terhadap ancaman serangan pada sistem dengan memberikan solusi perbaikan untuk menahan resiko melalui vulnerability assessment.

I.2 Perumusan Masalah

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

1. Bagaimana menganalisa kerentanan dan threat dalam membuat profil resiko berdasarkan pada vulnerable machine?
2. Bagaimana NIST cybersecurity framework mendasari proses security auditing?

I.3 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah sebagai berikut :

1. Menerapkan serta mengestimasi profil resiko pada *vulnerable machine.*
2. Menganalisa bagaimana *security auditing* menangani proses identifikasi dan memberikan solusi terhadap *vulnerable machine.*

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 Ruang Lingkup

Proposal Tugas Akhir ini mempunyai ruang lingkup yang perlu diperhatikan yaitu :

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

BAB I Pendahuluan

Bab ini terdiri dari latar belakang, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika laporan.

BAB II Landasan Teori

Bab ini berisi tentang teori dasar yang digunakan dalam penyelesaian penelitian ini, khususnya mengenai *Security Auditing* Terhadap system *snort* IDS dan penelitian dahulu untuk mendukung serta mendasari penelitian ini.

BAB III Metodologi Penelitian

Bab ini berisi tentang penjelasan metode-metode penyelesaian peneliti berdasarkan hasil berpikir peneliti.

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.