Bab I Pendahuluan

I.1 Latar Belakang

Perkembangan teknologi diikuti oleh pertambahan jumlah ancaman terhadap keamanan jaringan tersebut. Aktivitas- aktivitas illegal yang dikenal dengan *cyber crime* atau kejahatan siber dalam bentuk hacking, virus, spyware, trojan dan lain sebagainya terus tumbuh. Selain bertumbuh dalam jumlah dan jenis, ancaman digital juga bertumbuh di sisi kualitas dan kompleksitas.

Security Auditing dan sistem informasi digunakan untuk menilai efektivitas kontrol TI dalam kehidupan sehari hari . Perlunya menerapkan keamanan informasi dan sistem audit wajib bagi semua organisasi maupun perusahaan. Mengingat pentingnya *privasi* dan keamanan bagi perusahaan dan organisasi, masalah memutuskan kapan harus melakukan audit keamanan dan menjadi bagian penting dari proses kontrol organisasi. Melihat pertimbangan ini, maka dibutuhkan sebuah *framework* yang membahas tentang rangkaian yang menggambarkantahapan serangan *cyber* yang berkaitan dengan keamanan jaringan.

Mengacu dari fakta tersebut, diperlukan solusi keamanan yang efektif dan efisien. Untuk dapat mendapat keamanan jaringan yang optimal maka diperlukan visibilitas terhadap kemungkinan serangan di segala aspek jaringan. Hal ini dapat dipenuhi oleh *Security Auditing* yang dapat melakukan korelasi antara informasi yang dikumpulkan dari berbagai solusi keamanan jaringan yang ada dan melakukan analisa terhadap *security incident* yang terjadi.

Security Auditing merupakann suatu tim yang terorganisir dan mempunyai kemampuan dalam bidang keamanan *cyber* yang bertugas memantau dan meningkatkan postur keamanan organisasi dengan mencegah, mendeteksi, menganalisis, dan menanggapi insiden keamanan *cyber* dengan menggunakan teknologi dan proses yang telah disusun dengan baik.

Cyber Kill Chain merupakan sebuah *framework* yang dimana memposisikan diri sebagai penyerang untuk mengetahui kekurangan dari suatu situs/sistem. Dengan *framework* ini team *Security Auditing* mempermudah melakukan pencarian kekurangan dari objek. *CyberKillChain* ini memiliki 7 tahapan diantaranya;

Reconnaissance, Weaponize, Delivery, Exploitation, Installation, Command Control (C2), Act on Objective. Sehingga akan didapatkan klasifikasi berupa hubungan antara *tools* dan *vulnerability* berdasarkan *framework Cyber Kill Chain.*

I.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian *Security Auditing* dengan *framework Cyber Kill Chain* adalah sebagai berikut :

1. Bagaimanaa analisis kerentanan pada asset IT ?
2. Bagaimanaa merumuskan bentuk *attack model* ?
3. Bagaimanaa hubungan antara kerentanan, *attack* dan profil risiko berdasarkan *framework Cyber Kill Chain* ?
4. Bagaimanaa hubungan dan implementasi VulnOS menggunakan *framework Cyber Kill Chain* dalam analisa *Security Auditing ?*

I.3 Tujuan Penelitian

Adapun tujuan dalam penelitian ini adalah:

1. Dapat menganalisis kerentanan pada VulnOS.
2. Dapat membuat *attack model* berdasarkan hasil analisis.
3. Mengetahui hubungan kerentanan, *attack* dan profil risiko berdasarkan *framework Cyber Kill Chain.*
4. Mampu mengimplementasikan hubungan *Security Auditing* dan *framework Cyber Kill Chain.*

I.4 Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Teoritis

   Dapat memberikan pengetahuan untuk mendapatkan informasi terkait risiko dan kelemahan dari aset IT.

2. Praktis

   Diharapkan mendapatkan pengetahuan terkait sistem *security auditing* menggunakan *software open source*.

I.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah :

1. *Vulnerability* dan *threat* dilakukan pada level sistem *virtual vulnerability machine.*
2. Eksperimen dilakukan secara terbatas pada *local* area *network* secara *virtual*.
3. Menggunakan *software open source* secara terbatas.
4. Melakukan analisis berdasarkan data kuantitatif dan kualitatif berdasarkan data.

I.6 Sistematika Penulisan

Adapun sistematika penulisan dari penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi mengenai uraian latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematikan penelitian.

BAB II KAJIAN TEORI

Berisi tentang penjelasan dan kutipan yang relevan dengan permasalahan yang dihadapi, dan juga teori-teori yang digunakan seperti *Security Auditing, vulnerability, threat, risk, dan control*.

BAB III *FRAMEWORK* PENELITIAN

Berisikan model untuk merumuskan solusi dari permasalahn yang ada seperti pengenalan *framework* yang akan digunakan. Serta penjelasan secara rinci mengenai tahapan-tahapan dari penelitian ini.

BAB IV PERANCANGAN SISTEM DAN SKENARIO PENGUJIAN

Berisikan penjelasan mengenai *software, environment*, dan scenario praktik yang dilakukan saat penelitian.

BAB V PENGUJIAN SISTEM DAN ANALISIS

Berisikan penjelasan menganai setiap hasil dan perbandingan yang diperoleh dari penelitian disertai dengan analisis.

BAB VI KESIMPULAN DAN SARAN

Bab ini menjelasakan tentang kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian selanjutnya tentang topik yang sama.