BAB 1

PENDAHULUAN

1.1 Latar Belakang

Web Server rentan diretas oleh orang yang melakukan pencurian informasi dan data untuk disalahgunakan. Bahkan protokol SSH (*Secure Shell*) yang memiliki keamanan yang kuat dapat diretas. Terdapat sebuah kasus penyerangan terhadap protokol SSH, salah satunya *malware* berjenis *backdoor*. Perusahaan ESET mengidentifikasi *malware* tersebut adalah *Linux/*SSH*Door.A*., yang dirancang untuk mampu mencuri data penting, seperti halnya informasi mengenai *username* dan *password*[1].

Pentingnya suatu keamanan SSH pada *Web Server* yang di dalamnya terdapat suatu data maupun informasi dan tidak disalahgunakan oleh seseorang yang tidak bertanggung jawab, sehingga dapat menghindari dari ancaman peretasan. Salah satu upaya untuk menangani hal ini dibutuhkan keamanan *Honeypot*. *Honeypot* merupakan metode pengalihan dan menjebak ke server palsu. baik itu informasi maupun data yang terdapat di dalam *Web Server*, sehingga serangan yang ditunjukan untuk *Web Server* tersebut bukan data yang sebenarnya. Bahkan data terlindungi dari serangan *hacking*. *Honeytrap* merupakan implementasi dari metode *Honeypot*, dimana peretas dapat di pantau bahkan terdapat fitur *IP Blacklist*. Fitur ini mengizinkan penyerang untuk mengambil data palsu yang telah disiapkan, bahkan dapat menghentikan penyerang dan melihat teknik apa yang digunakan.

Seseorang yang melakukan peretasan dapat dijerat oleh Pasal 30 Ayat 1 UU ITE No.11 Tahun 2008. Pasal 30 Ayat 3 UU ITE No.11 Tahun 2008 disebutkan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dapat dituntut secara hukum pidana[2].

Pada penelitian Proyek Akhir ini dibangun keamanan *Web Server* dari serangan SSH menggunakan implementasi dari keamanan *Honeypot* dengan metode *Honeytrap* yang bertujuan untuk mengalihkan serangan ke dalam server palsu.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diutarakan, maka rumusan masalah dalam Proyek Akhir ini ialah sebagai berikut.

1. Bagaimana mengimplementasikan keamanan *Web Server* dari serangan SSH menggunakan *Honeytrap*?
2. Bagaimana melakukan pengujian keamanan *Web Server* dari serangan SSH menggunakan *Honeytrap*?

1.3 Tujuan

Adapun tujuan masalah dalam penelitian ini adalah sebagai berikut.

1. Memperkuat keamanan *Web Server* dari serangan SSH menggunakan *Honeytrap*.
2. Melakukan pengujian *Honeytrap* dari serangan SSH dan melihat aktifitas yang dilakukan penyerang.

1.4 Batasan Masalah

Agar penelitian ini dapat lebih sempurna, Maka perlu membatasi permasalahan dalam penelitiannya. Permasalahan yang dibatasi adalah sebagai berikut.

1. Pengujian dilakukan dengan serangan Port Scanning, Metasploit, Hydra, dan SSH-Console.
2. Pengamanan *Web Server* dilakukan hanya pada serangan SSH.

1.5 Definisi Operasional

Web Server merupakan suatu sistem yang memiliki tempat penyewaan untuk menampung data-data yang dapat di akses melalui internet dan berupa situs web atau biasa dikenal dengan *hosting,* yang bertujuan untuk menyediakan layanan protokol *Hyper Text Transfer Protokol* (HTTP) atau *Hyper Text Transfer Protokol Secure* (HTTPS). Fungsi utama *Web Server* adalah memberikan layanan informasi dan data, serta media yang menjadi suatu halaman web.

Pada tahun 1990 *Web Server* adalah proyek yang diusulkannya pada atasannya di CERN (Organisasi Riset Nuklir Eropa) bernama CERN httpd yang diusulkan oleh Sir Tim Berners-Lee. *Web server* ini berjalan pada server NeXT. NeXT merupakan perusahaan yang didirikan oleh Steve Jobs setelah keluar dari Apple[3].

Linux merupakan nama dari sebuah sistem operasi komputer bertipe Unix. *Linux* ini salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Pada umumnya, kode sumber *Linux* dapat dimodifikasi kembali secara bebas oleh siapa saja. Nama "*Linux*" berasal dari nama pembuatnya, yang diperkenalkan tahun 1991 oleh *Linux* Torvalds. Biaya operasional pada *Linux* rendah, dan kompatibilitas yang tinggi dibandingkan dengan sistem operasi yang lainnya seperti Microsoft Windows[4].

Golang (atau biasa disebut dengan Go) adalah bahasa pemrograman baru yang dikembangkan di Google oleh Robert Griesemer, Rob Pike, dan Ken Thompson pada tahun 2007 dan mulai diperkenalkan di publik tahun 2009. *Golang* memiliki banyak kelebihan, terbukti dengan banyaknya perusahaan besar yang menggunakan bahasa ini dalam pengembangan produk-produknya, hingga level production tentunya[5].

Honeytrap merupakan *opensource framework* untuk menjalankan, memantau dan mengelola *Honeypot*s. Dengan dukungan untuk berbagai jenis mode, *Honeytrap* dapat digunakan untuk menggunakan arsitektur *Honeypot* yang kompleks atau hanya untuk menggunakan satu server. Bergantung pada mode yang dipilih dan dapat memeriksa semua port untuk mendeteksi ancaman dan mengumpulkan informasi, atau memeriksa port tertentu dan memberikan jawaban yang telah ditentukan. Beberapa sistem operasi didukung, seperti *Linux*, MacOS dan Windows. Beberapa fungsi yang tersedia tergantung pada sistem operasi host-direktur LXC misalnya hanya tersedia di *Linux,* tetapi kebanyakan tersedia untuk setiap OS[6].

Secure Shell adalah protokol jaringan yang berada di lapisan aplikasi pada protokol TCP/IP, memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur klien server dengan menyediakan kerahasiaan dan integritas data melalui teknik enkripsi dan dekripsi yang dilakukan secara otomatis di dalam koneksinya, untuk menggunakan SSH dibutuhkan otentifikasi *user* berupa kunci umum dan *password* yang terenkripsi[7].

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan pada Proyek Akhir ini terdiri dari lima tahap yaitu studi literatur, analisis kebutuhan, perancangan sistem, implementasi dan pengujian serta penyusunan laporan.

1. Studi literatur

   Pada studi literatur kegitan yang dilakukan adalah mengetahui permasalahan yang muncul terhadap keamanan *Web Server* yang rentan diretas oleh pihak yang tidak bertanggungjawab. Oleh karena itu, untuk mencari solusi yang disarankan untuk mengatasi permasalahan tersebut yaitu dengan mengimplementasikan *Honeypot* dengan metode *Honeytrap.*

2. Analisis

   Pada tahap ini dilakukan pengumpulan data penelitian sebelumnya yang berhubungan dengan keamanan jaringan yang membantu keamanan *Web Server*. Setelah itu mengolah data yang telah didapat agar dapat melanjutkan ke proses selanjutnya.

3. Implementasi

   Mengimplementasikan dari berbagai sumber yang membuat suatu sistem keamanan yang baru dengan metode yang beda.

4. Pengujian

   Dalam tahap pengujian diperlukan beberapa *tools* atau program yang mendukung untuk bisa menjalankan *Honeytrap* dan membuat catatan dari segala serangan.

5. Penyusunan Buku Proyek Akhir

   Dalam pelaksanaannya membuat laporan Proyek Akhir mengenai semua informasi yang ingin disampaikan dengan menggunakan metode pengumpulan beberapa data yang valid dari berbagai sumber referensi dan dibuat secara sistematika karya ilmiah.

1.7 Jadwal Pengerjaan

Tabel 1. 1 Jadwal Pengerjaan

Kegiatan	Februari 2019				April 2019				Mei 2019				Februari 2020				Maret 2020	
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
Identifikasi																		
Analisis																		
Implementasi																		
Pengujian																		
Laporan																		

Pada Tabel 1.1 terdapat jadwal pengerjaan Proyek Akhir dalam Implementasi *Honeypot* Dengan Metode *Honeytrap* dengan 5 tahap kegiatan yaitu, studi literatur, analisis, implementasi, pengujian dan analisis, serta penyusunan buku Proyek Akhir yang berlangsung hingga bulan Maret 2020.