BAB I PENDAHULUAN

I.1. Latar Belakang Masalah

Pada era perkembangan digital yang sangat pesat, *Universal Serial Bus* (USB) adalah mekanisme yang saat ini digunakan di mana-mana dengan memungkinkan fungsionalitas *plug and play,* memungkinkan transfer data yang cepat dan mudah dibandingkan dengan perangkat keras lainnya. USB menawarkan fleksibilitas yang dibutuhkan oleh pengguna yang dapat digunakan untuk keperluan sehari-hari. USB juga merupakan mekanisme untuk melakukan eksploitasi yang sangat efisien yang mampu mengirimkan, menginstal dan menjalankan *malware* pada sistem. (Orrey, 2011)

Social Engineering adalah suatu teknik pengambilan data atau informasi penting / rahasia dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial dengan cara mengeksploitasi kelemahan manusia.(Indrajit, 2013). *Social engineering* mengkonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu pengguna. Setiap orang yang mempunyai akses kedalam sistem secara fisik adalah ancaman, bahkan jika orang tersebut tidak termasuk dalam kebijakan kemanan yang telah disusun.

Social Engineering dapat dimanfaatkan sebagai teknik untuk penyerangan yang sangat efektif pada orang yang memiliki hubungan sosial. Dalam kehidupan sosial manusia saling berinteraksi satu dan lainnya seperti meminjam barang pada orang yang baru dikenal. Contoh yang mendukung ialah manusia memiliki USB sebagai kebutuhan pribadi dalam pengiriman *file-file* secara *offline*. Hal itu dapat dimanfaatkan untuk penyerangan melalui USB dengan cara meluncurkan serangan dengan menanamkan *file-file* berbahaya didalamnya, akan tetapi pengguna tidak menyadari bahwa USB tersebut tidak aman sehingga penyerang dapat dengan mudah melakukan serangan ketika USB tersebut disambungkan oleh pengguna, dan juga sudah banyak peringatan untuk tidak menyambungkan USB yang bukan milik

mereka sendiri agar tidak terkena serangan file berbahaya. Sudah banyak orang yang terkena serangan-serangan melalui USB yang dapat berdampak minor hingga fatal.

Salah satu penyerangan *social engineering* menggunakan USB yaitu menanamkan *DNS Spoofing*, dan menjalankan program untuk mencuri data penggunanya. Penanaman *DNS Spoofing* dapat mudah dilakukan pada sistem operasi *Windows*. Sistem operasi desktop yang paling banyak digunakan didunia saat ini dengan pengguna sebanyak 73.6% (W3schools, 2019), dan masih memiliki celah keamanan yang harus dibenahi. Celah yang dimanfaatkan pada penelitian ini adalah mudahnya mengubah *file hosts* oleh pihak yang tidak bertanggung jawab kepada komputer yang bukan miliknya. Hanya membutuhkan hak akses admin pada *command prompt* (CMD) komputer target, penyerang dapat melakukan pengubahan *file hosts* pada komputer target. Metode penyerangan yang digunakan adalah metode *USBdriveby* (Vouteva, 2015).

Pada penelitian ini membahas metode penyerangan menggunakan Mikrokontroler *Arduino* yang akan dijadikan perangkat *USBDriveby*. *USBDriveby* adalah perangkat yang dapat dengan cepat melakukan *DNS Spoofing* pada komputer target melalui USB dalam hitungan detik. Penyerangan menggunakan metode *DNS Spoofing* adalah sebuah metode hacking *Man In The Middle Attack* (MITM) yang dapat memanipulasi paket DNS yang ada dalam jaringan DNS itu sendiri dengan mengubah sebuah alamat domain menjadi palsu. Dan penyerang dapat mencuri data yang diinputkan kedalam website.(Kamkar, 2014) Dengan menggunakan metode ini diharapkan dapat mengetahui dampak dari penyerangan dengan mengubah *file hosts* dan *DNS Spoofing* yang akan dilakukan. *USBDriveby* dikembangkan oleh seorang peneliti keamanan dan privasi yang bernama Samy Kamkar. Dengan adanya penelitian ini diharapkan dapat mengetahui dampak dari penyerangan *USBDriveby* terhadap sistem operasi *Windows*.

I.2. Rumusan Masalah

Dari berbagai uraian yang sudah disebutkan di atas, maka ditarik rumusan masalah:

1. Bagaimana mengimplementasikan *USBdriveby* pada *Arduino Pro Micro*?
2. Bagaimana cara kerja penyerangan *USBDriveby* ?
3. Bagaimana cara mengetahui dampak dari penyerangan pada sistem operasi windows dengan menggunakan *USBDriveby*?
4. Bagaimana cara mencegah penyerangan dari celah keamanaan yang ada?

I.3. Tujuan Penelitian

Adapun tujuan dari pembuatan tugas akhir ini, yaitu:

1. Mengimplementasi *USBdriveby* menggunakan *Arduino Pro Micro*
2. Untuk mengetahui cara kerja *USBdriveby*
3. Mengetahui dampak dari penyerangan terhadap Sistem Operasi *Windows* dengan menggunakan *USBDriveby*.
4. Mengetahui cara mencegah penyerangan dari celah keamanaan yang ada

I.4. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Masyarakat menjadi lebih berhati-hati dalam mengakses sebuah situs website
2. Cara mencegah serangan *DNS Spoofing*

I.5. Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, yaitu :

1. Jenis serangan menggunakan *DNS Spoofing*
2. Hanya melakukan *Spoofing* pada beberapa *Website*
3. Sekali serangan hanya bisa menargetkan 1 website pada jaringan *LAN*
4. *Webserver* menggunakan *Kali Linux* yang diinstal di *VMware*
5. *Web cloning* menggunakan *Social Engeneering Tools* pada *Kali Linux*
6. Penyerangan hanya dilakukan pada user admin pada komputer target
7. Penyerangan hanya dilakukan pada jaringan lokal (LAN)

1.6. Sistematika Laporan

Pada penyusunan laporan Tugas Akhir ini, dibuat sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini mendeskrisikan topik penelitian mulai dari latar belakang, rumusan masalah, tujuan penelitian, Batasan masalah, manfaat penelitian, dan sistematika penulisan penelitian

BAB II LANDASAN TEORI

Bab ini menjelaskan dasar teori yang digunakan dalam penelitian mengenai *USBDriveby.* dalam penelitian ini dengan teori-teori penunjang penelitian yang berkaitan dengan topik yang dibahas.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan pelaksanaan penelitian mulai dari tahapan-tahapan yang dilakukan selama penelitian, pelaksanaan penelitian, dan metode konseptual.

BAB IV PERANCANGAN SISTEM DAN SKENARIO PENYERANGAN

Bab ini menjelaskan dua bagian yaitu perancangan dan Analisa. Bagian Analisa menjelaskan analisa apa saja yang dapat dilakukan oleh *USBDriveby* dan bagian Perancangan akan menjelaskan tentang perancangan *USBDriveby* sendiri.

BAB V PENGUJIAN SISTEM DAN ANALISIS

Bab ini menjelaskan tentang implementasi dari hasil perancangan yang telah dibuat sebelumnya. Implementasi yang dilakukan yaitu membuat *USBDriveby* menggunakan *Arduino*. Setelah itu dilakukan pengujian terhadap *USBDriveby* meliputi unit *testing*, Dampak serangan USB.

BAB VI KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan yang didapatkan dari hasil penelitian yang dibuat serta saran dalam melakukan perbaikan selanjutnya.