BAB I

PENDAHULUAN

1.1 Latar Belakang

Komputasi perangkat telah berubah secara revolusioner dari arsitektur komponen lama atau tua ke perubahan yang lebih baru, lebih kuat dan lebih terjaga keamanannya. Seiring perkembangan zaman, masyarakat menjadi lebih cerdas sehingga sering menemukan kelemahan atau celah keamanan pada teknologi komputer yang telah dibangun. Sistem komputer rentan terhadap banyak kerentanan dimana cacat pada sistem dapat membuka sebuah ancaman serius. Perangkat lunak keamanan, *firewall, antivirus* dan sejenisnya telah diberlakukan untuk melindungi data berharga pada komputer. Tidak ada 100% sistem anti kerentanan yang mengklaim dirinya sebagai sistem komputer paling canggih yang pernah ada. (Wahab & Zain, 2018)

Banyak yang tidak menyadari bahwa serangan komputer dapat dilakukan menggunakan tampilan antar muka yang umum seperti *Universal Serial Bus (USB)* pada *port usb* komputer atau laptop. (Bang & J., 2010)

Masyarakat luas diharuskan berhati-hati dengan serangan komputer seperti serangan *keystoke injection* pada *port usb* komputer atau laptop. *Port usb* pada sistem komputer pada dasarnya adalah sebuah *port* terbuka, sehingga banyak yang menyalahgunakan celah keamanan *usb* pada komputer atau laptop. Dampaknya sangat beresiko ketika komputer telah terkena serangan *keystroke injection usb*, seperti dapat menghapus *file-file* data penting pada *system32* pada *Windows* C. *Port* terbuka pada *usb* ini membuat mesin komputer tidak dapat memindai adanya *virus*

atau *malware*, bahkan *antivirus* tidak dapat mendeteksi atau mempertahankan sistem melawan serangan ini. (Cannols & Ghafarian, 2017)

Sistem operasi pada komputer selalu mempercayai seluruh perangkat *usb* yang dicolok tanpa terkecuali. Sistem operasi *Windows* tidak pernah bertanya meminta persetujuan pengguna untuk menggunakan *keyboard* atau *mouse* yang terhubung ketika pengguna mencolok *keyboard* atau *mouse usb*. *Windows* akan segera mengaktifkannya dan langsung dapat digunakan oleh pengguna, karena sistem pada komputer mempercayai inputan pada manusia.

Keystroke injection tool atau biasa disebut dengan *USB Rubber Ducky* sering diperbincangkan oleh ahli keamanan komputer setelah kemunculan film mr.robot pada tahun 2015 silam. *USB Rubber Ducky* pada awalnya diperkenalkan pada tahun 2010 dan menjadi alat favorit bagi para *hacker*, *penetration testers* dan *IT professional*.

USB Rubber Ducky adalah sebuah perangkat yang berbentuk seperti *flashdisk* atau *flash dive* tetapi terdeteksi layaknya *keyboard* ketika telah dicolok pada *usb* komputer. Jenis serangan ini mengambil keuntungan dari fakta bahwa komputer mempercayai input dari manusia. Jika komputer percaya terhadap inputan manusia, maka komputer juga percaya terhadap *keyboard*. Cara kerjanya adalah cukup dengan memprogram *script auto keyboard* pada *USB Rubber Ducky* untuk mengirim atau mengunduh *backdoor* yang telah dibuat, maka komputer target akan dapat dikontrol penuh oleh penyerang. (Dever, 2015)

Didalam serangan *USB Rubber Ducky*, perlu adanya pembuatan *backdoor* untuk mengontrol akses *root* pengguna. *Backdoor* sendiri merupakan kode berbahaya yang memasang dirinya sendiri ke komputer untuk memungkinkan akses

sistem korban oleh pihak penyerang. *Backdoor* biasanya membiarkan penyerang terhubung ke komputer dengan sedikit atau tidak ada autentikasi dan jalankan perintah di sistem lokal. (Sikorsi & Honig, 2012)

Metasploit framework adalah sebuah *penetration tool* yang cukup *powerfull* untuk melakukan penestrasi kedalam sebuah sistem. *Metasploit* termasuk sebuah *framework* penetrasi jaringan komputer yang *free* dan *open source*, diciptakan oleh H.D. Moore pada tahun 2003 dan kini diakuisisi oleh Rapid7. *Metasploit framework* bisa juga dikatakan sebagai sebuah *platform* pengembangan untuk membuat alat keamanan dan *exploit*. *Metasploit* biasa dikaitkan dengan istilah *remote exploitation*, maksudnya walaupun penyusup sistem berada pada jarak jangkauan yang jauh tetapi dapat mengendalikan komputer korban.

Metasploit Framework adalah alat yang secara kolektif menggabungkan eksploitasi menjadi satu lokasi pusat yang ideal bagi para peneliti keamanan. awalnya dikembangkan menggunakan bahasa scripting Perl Metasploit sekarang saat ini pada reinkarnasinya. Metasploit dianggap multi-platform yang berjalan di sebagian besar variasi Unix dan Windows. (N., S., G., & S., 2016)

Sebuah penemuan baru untuk menggantikan *keystroke injection tool* atau *USB Rubber Ducky* yakni menggunakan *Arduino*. *Arduino* dapat menggantikan *keystroke injection tool* sebagai *keyboard* otomatis yang telah ada pada *library*. Tujuannya adalah untuk mengirim dan mengunduh *backdoor* dari penyerang sehingga penyerang dapat mengontrol dan mengeksploitasi komputer target. Keunggulan Arduino adalah terdeteksi berupa sebuah driver Arduino, bukan sebagai *HID keyboard* maupun *mouse* otomatis.

Pada penelitian ini, penulis ingin mengimplementasikan bagaimana cara

kerja penggunaan alat papan *Arduino* untuk melakukan serangan *remote exploit* menggantikan *keystroke injection tools* dengan bantuan *framework metasploit*.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah di jelaskan di atas maka dapat rumusan masalah sebagai berikut :

1. Bagaimana tahapan serangan *remote exploit* menggunakan papan *Arduino* pada sistem operasi *Windows 10, Linux Ubuntu 18.04 Lts* dan *Mac OS Mojave*?
2. Bagaimana bentuk dari *script* pada program *Arduino*?
3. Bagaimana *payload* untuk sistem operasi *Windows 10*, *Linux Ubuntu* dan *Mac OS Mojave*?
4. Bagaimana mengirim *backdoor* menggunakan papan *Arduino* melalui jaringan yang berbeda?
5. Bagaimana cara membuat *backdoor* secara permanen untuk dapat mengakses setiap saat?

1.3 Batasan Masalah

Adapun yang menjadi batasan-batasan dalam penelitian ini adalah sebagai berikut :

1. Implementasi yang di lakukan adalah *remote exploit* menggunakan papan *Arduino* dan perangkat lunak *Arduino IDE*.
2. Sistem operasi penyerang menggunakan *Kali Linux*.
3. Sistem operasi target yang akan diuji menggunakan *Windows 10, Linux Ubuntu 18.04 Lts* dan *Mac OS Mojave*.

4. *Framework* yang digunakan untuk *remote exploit* menggunakan *framework metasploit*
5. *Payload file* yang digunakan dalam bentuk *format exe* dan *python*.
6. *Internet Protocol* yang digunakan oleh penyerang adalah *IP Local* yang dapat diakses diluar jaringan lokal menggunakan *tunnels* pada *Ngrok.*

1.4 Tujuan Penelitian

Adapun Tujuan dari penelitian yang dilakukan oleh penulis dengan judul "Implementasi Serangan *Remote Exploit* Menggunakan *Arduino Micro* pada Sistem Operasi *Windows, Linux* dan *Mac OS*" antara lain :

1. Memahami cara peretas membuat sebuah *backdoor* dan mendapatkan kontrol penuh pada sistem operasi target.
2. Memahami peretas mengirimkan sebuah *remote exploit* menggunakan *Arduino* melalui *port usb* komputer.
3. Memahami dampak dari sistem operasi target (*Windows 10, Linux Ubuntu* dan *Mac OS Mojave*) setelah terinfeksi *remote exploit* pada *port usb PC*.

1.5 Manfaat Penelitian

Ada pun manfaat dari pengujian serangan *remote exploit* menggunakan *Arduino Micro* pada sistem operasi *Windows, Linux* dan *Mac OS* sebagai berikut:

1. Bagi penulis adalah sebagai sarana untuk mengimplementasikan pengetahuan yang telah didapatkan dalam mata kuliah "Keamanan Jaringan" selama perkuliahan berlangsung, dan dapat memahami berbagai jenis serangan melalui celah keamanan pada sistem komputer.
2. Bagi mahasiswa maupun pembaca sebagai sarana untuk penelitian lebih lanjut tentang keamanan jaringan dalam lingkup serangan *remote exploit*.