**Nama : Juanda Fahrizal**

**NIM : 09011181520006**

# Tugas Trojan

- **Penjelasan Trojan**

Trojan Horse (Kuda Troya), Trojan Horse bukanlah sebuah virus, karena Trojan Horse tidak memiliki kemampuan untuk menggandakan diri. Namun demikian, Trojan Horse tidak kalah berbahaya jika dibandingkan dengan virus. Trojan Horse umumnya dikemas dalam bentuk sebuah software yang menarik. Namun dibalik daya tarik software tersebut, tersembunyi fungsi lain untuk melakukan perusakan. Misalkan saja software Keygen /key generator atau software pencari Serial Number(SN) kunci, nah tentunya kita tertarik bukan untuk menjalankan software tersebut? Karena kadang-kadang software meminta kita melakukan registrasi dengan memasukkan SN utuk menghilangkan masa trialnya. Pengguna komputer yang mendapatkan file yang telah mengandung

Trojan Horse ini umumnya akan terpancing untuk menjalankannya karena daya tarik tadi. Akibatnya tentu fatal, karena dengan demikian pengguna telah meenjalankan rutin-rutin perusak yang siap menebar bencana di komputernya. Trojan bisa berupa program perusak maupun program kendali. Contoh trojan misalnya kaHt, Back Orifice dan Netbus. Apabila korban telah terkena salah satu dari program ini maka apabila korban terhubung ke jaringan atau internet, si pengirim trojan dapat mengendalikan komputer korban dari jauh,karena trojan membuka port-port tertentu agar komputer dapat diremote, bahkan tidak mustahil untuk mematikan atau merusak dari jauh. Itu sama halnya dengan penduduk kota Troy yang terlambat menyadari bahwa kota mereka sudah di masuki oleh tentara musuh.

Trojan tidak mempunyai masa aktif. Maksudnya, Trojan akan ada selamanya (bersarang) dan tidak pernah akan habis.Komputer yang telah terinsfeksi Trojan dapat dikendalikan oleh penyerang melalui versi client-nya.Cara kerja, sifat, dan fungsi Trojan mirip dengan remote administration tool. Trojan masuk ke komputer seseorang melalui dua bagian, yaitu client dan server. Ketika korban (tanpa diketahui) menjalankan komputer,penyerang akan menggunakan client untuk koneksi dengan server dan mulai menggunakan trojan.Trojan dapat bekerja dengan baik pada jenis protokol TCP/IP, tetapi beberapa trojan juga dapat menggunakan protokol TCP/IP, tetapi Beberapa trojan juga dapat menggunakan protokol UDP dengan baik. Ketika server mulai dijalankan , Trojan umumnya mencoba untuk

menyembunyikan diri di suatu tempat dalam sistem komputer tersebut, kemudian mulai "mendegarkan" di beberapa port untuk melakukan koneksi, memodifikasi registry, atau menggunakan metode lain yaitu metode autostarting. Hal penting diketahui oleh penyerang adalah mengetahui IP address korban untuk menghubungkan komputernya ke komputer korban.

- **File Transfer Protocol (FTP) Trojan**

Merupakan troajan yang berfungsi untuk membuka port 21 di komputer korban yang menyebabkan mempermudah seseorang memiliki FTP client untuk memasuki komputer korban tanpa password serta melakukan download atau upload file.

- **Cara kerja FTP Trojan**

Penyerang secara aktif menyerang pengunjung situs web dan begitu pengunjung ini terinfeksi dengan Windows dieksekusi, ia mengambil kredensial FTP dari mesin korban. Akun FTP kemudian digunakan untuk menginfeksi setiap halaman web server. Dengan cara ini sistem menambah jumlah halaman yang terinfeksi, sehingga menyerang semakin banyak komputer. seluruh proses terotomatisasi dan pemilik sistem perlu menyesuaikan sistem dan memperbarui executable.(Mahmood, Takahashi, & Arakawa, 2012).

- **Cara mendeteksi Trojan**

1. **Task List**

Cara pendeteksiannya adalah dengan melihat daftar program yang sedang berjalan dalam task List.Beberapa Trojan tetap mampu meyembunyikan dari Task List.Sehingga untuk mengetahui program yang berjalan secara keseluruhan,perlu di buka System Information Utility(msinfo32.exe) yang berada di **C:\Program files\common files\microsoft shaed\msinfo.**Tools ini dapat melihat semua proses itu sedang berjaln, baik yang tersembunyi dari Task List maupun tidak. Ha-hal yang perlu diperiksa adalah path,nama file, properti file, dan berjalannya file ***.exe** serta file ***.dll.**

2. **Netstat**

Netstat berfungsi membuka koneksi ke dan dari komputer seseorang. Jika perintah ini dijalankan, maka akan menampilkan IP Address dari komputer tersebut dan komputer yang terkoneksi dengannya. Jika ditemukan IP Address yang tidak dikenal, maka perlu diselidiki lebih lanjut.

3. **TCPView**

TCPViev adalah suatu free utility dari sysinternals yang mempunyai kemampuan menampilkan IP Address dan menampilkan program yang digunakan oleh orang lain untuk koneksi dengan komputer pemakai.Dengan menggunaka informasi tersebut, kita dapat mengetahui dan melakukan serangan balik terhadap penyerang.

Mahmood, K., Takahashi, H., & Arakawa, Y. (2012). Gateway access permission technology for high assurance. *Proceedings - 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012*, 375–381. https://doi.org/10.1109/ICDCSW.2012.64