**LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1**

**“Analisis Malware”**

**Pertemuan 3**

**Logo

Description automatically generated**

**Disusun oleh :**

**Nama                  :Nayaka Iman Wiraputra**

**NIM                    : 21/482203/SV/19910**

**Kelas                   : TRI A**

**Hari, Tanggal          : Selasa,  28 Febuary 2022**

**Dosen Pengampu    : Anni Karimatul Fauziyyah, S.Kom., M.Eng.**

**Asisten Dosen         : Gabriella Alvera Chaterine**

**LABORATORIUM KEAMANAN INFORMASI**

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**

**DEPATEMEN TEKNIK ELEKTRO DAN INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS GADJAH MADA**

**YOGYAKARTA**

**2022**

1. TUJUAN

Tujuan dari praktikum pada pertemuan kali ini adalah agar mahasiswa dapat memahami dan mengidentifikasi karakteristik, perilaku, dan fungsi dari suatu malware, hal ini dilakukan unutk beberapa tujuan, analisis malware dapat membantu mendeteksi keberadaaan malware di dalam sistwm computer atau jaringan ehingga dapat segera diambil Tindakan unutk meminimalisir dampak yang di timbbulkan, selain itu kita juga bisa mengidentifikasi sumber asal dari malware seperti apa yang membuat nya, bagaimana cara menyebarny, dan tujuan pembuatan nya, bagaimana malware menyebar, dan tujuan pembuatan nya

1. ALAT DAN BAHAN

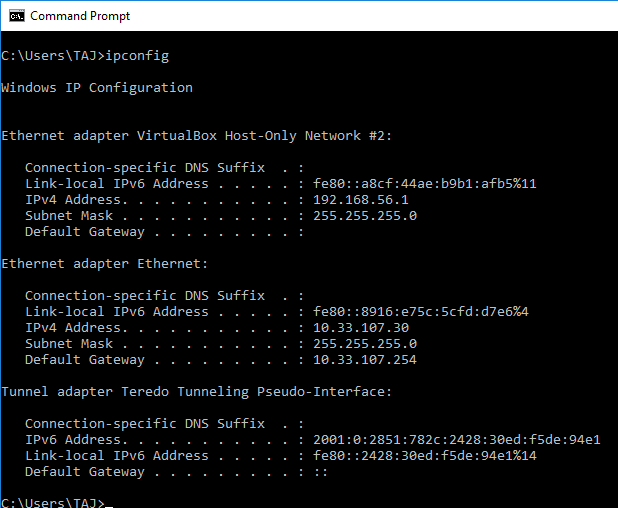
Alat dan bahan yang di gunakan pada praktikum kali ini addalah

1. Koneksi internet
2. Computer
3. Computer client
4. Njrat
5. DASAR TEORI

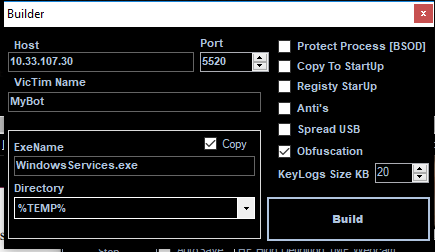
NjRat adalah salah satu jenis perangkat lunak jahat (malware) yang termasuk dalam kategori Remote Access Trojan (RAT). NjRat dirancang untuk memungkinkan pengguna jahat mengambil alih dan mengendalikan komputer target dari jarak jauh, dengan tujuan melakukan berbagai jenis aktivitas yang merugikan pengguna komputer tersebut, seperti mencuri data pribadi, merusak sistem, atau menggunakan komputer untuk melakukan serangan ke jaringan lain.

NjRat dapat menyebar melalui email, situs web yang dirancang untuk mengeksploitasi kerentanan pada sistem, atau melalui download tidak sah dari perangkat lunak atau file. Ketika NjRat terinstal pada sistem target, pengguna jahat dapat memonitor dan mengontrol komputer tersebut dari jarak jauh menggunakan berbagai fitur, seperti mengakses file, menonton aktivitas pengguna, atau bahkan merekam suara dan gambar dari mikrofon dan webcam. NjRat termasuk dalam kategori malware yang sangat berbahaya dan dapat menyebabkan kerusakan serius pada sistem dan privasi pengguna.

1. LANGKAH KERJA
2. Cek ip address kita terlebih dahulu



1. Lalu buka njrat dan buka tab builder



Di bagian host masukan ip address kita

1. Setelah di build maka akan mandapatkan file application



File ini jika di buka tidak akan muncul cover aplikasi nya

1. Setelah file di buka oleh victim (korban) maka akan muncul table seperti

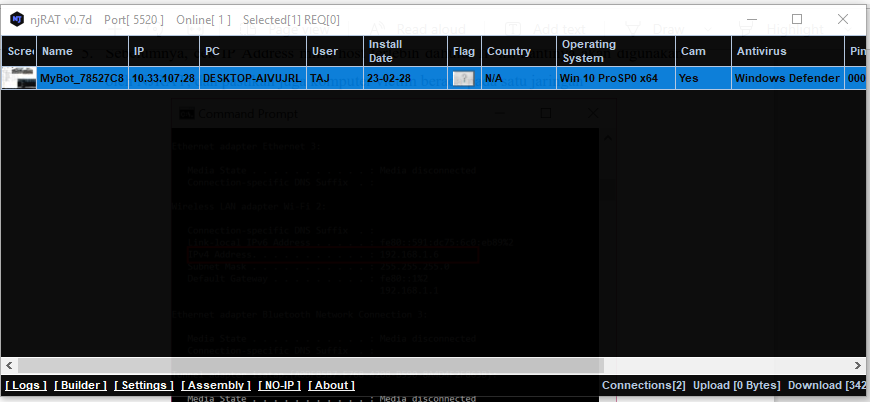


Table tsb terhubung dengan pc victim

1. Setelah terhubung seperti di atas kita bisa membuka kamera bahkan file yang terdapat di pc korban A screenshot of a person

   Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with medium confidence

1. Tidak hanya itu kita ajuga bisa berkomunikasi dengan pc korban

Text

Description automatically generated

Lab berikut nya yaitu mengalanisis malware dengan metode osint

1. Virustotal

Graphical user interface, text, application, email

Description automatically generated

Dari 69 scanner terdapat 47 yang mendateksi bahwa ini adalah malware

1. OPSWAT

Graphical user interface, application

Description automatically generated

Dari 16 scanner, 9 diantara nya mendeteksi adanya anacaman malware

1. VIRSCANA screenshot of a computer

   Description automatically generated with medium confidence

Dari 64 engine yang mendeteksi 16 diantara nya mendeteksi bahwa adanya ancaman malware

1. Jotti

Graphical user interface, text, application, email

Description automatically generated

Dari 14 scanner yang ada terdapat 10 yang terdeteksi bahwa ini adalah malware

1. Bitbaan Malab

Graphical user interface

Description automatically generated with medium confidence

Terdapat error di website Bitbaan malab yang tidak memungkinkan nya pengetesan

1. Polyswarm

Graphical user interface, application

Description automatically generated

Dari 17 engine yang berjalan 10 diantara nya mendeteksi adanya ancaman malware

1. PEMBAHASAN

NJrat (juga dikenal sebagai Bladabindi) adalah salah satu jenis Trojan Remote Access (RAT) yang dirancang untuk memberikan akses jarak jauh ke sistem yang terinfeksi oleh malware. NJrat mampu mengambil alih kendali sistem operasi dan memberikan akses ke file sistem, webcam, mikrofon, keyboard, mouse, dan perangkat keras lainnya yang terhubung ke sistem. Trojan ini dapat mematikan atau mengaktifkan program atau layanan, mengunduh dan mengunggah file

1. KESIMPULAN

Cara kerja malware Njrat sifatnya sangat berbahaya sehingga attacker dapat melakukan hak akses apa saja terhadap PC korban bahkan untuk membobol kamera victim dan mengetauhi isi file korban denga nada nya serangan malware yang terjadi

DAFTAR PUSTAKA

bersama, i. (n.d.). *ilmubersama*. Retrieved from https://ilmubersama.com/2020/02/24/malware-njrat-remote-access-trojan/

karimatul, a. (n.d.). *ELOK*. Retrieved from https://elok.ugm.ac.id/pluginfile.php/2314502/mod\_resource/content/1/pertemuan%203%20KI%201.pdf

Mubarok, H. (2016, Desember). *ResearchGate*. Retrieved from https://www.researchgate.net/publication/318962355\_Investigasi\_Serangan\_Malware\_Njrat\_Pada\_PC

Unknown. (2017, feburary 03). *Xiaozhu*. Retrieved from https://zhuyeo-developer.blogspot.com/2017/02/cara-mudah-menggunakan-njrat.html