LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN KE-3

ANATOMY MALWARE, DEVELOP MALWARE TROJAN DENGAN NJRAT, DAN MALWARE DENGAN METODE OSINT

Di susun oleh :

Nama	:	Natasya Ovelia Zamris
NIM	:	21/475446/SV/19121
Kelas	:	TRI kelas A
Hari, tanggal	:	Selasa, 28 Februari 2023
Dosen pengampu	:	Anni Karimatul Fauziyyah, S.Kom., M.Eng

PROGRAM SARJANA TERAPAN DIPLOMA IV

TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Unit 4

Analisis Anatomy Malware

Develop Malware dengan Metode NjRAT

Analisis Malware dengan Metode OSINT

A. TUJUAN

1. Praktikan dapat meneliti dan menganalisis malware.
2. Praktikan dapat membuat *server* menggunakan njRAT.
3. Praktikan dapat mengakses mesin target dari jarak jauh.

B. LANDASAN TEORI

Malware atau perangkat lunak berbahaya mengacu pada berbagai program perangkat lunak berbahaya yang dapat digunakan untuk menyebabkan kerusakan pada sistem komputer, mencuri data, dan melewati tindakan keamanan. Malware juga dapat menyerang infrastruktur penting, menonaktifkan layanan darurat, menyebabkan jalur perakitan membuat produk yang cacat, menonaktifkan generator listrik, dan mengganggu layanan transportasi. Pakar keamanan memperkirakan bahwa lebih dari satu juta ancaman malware baru dirilis setiap hari. *McAfee Labs Threats Report* 2019 menunjukkan penemuan teknik *ransomware* baru, pengungkapan miliaran akun melalui *dump* data profil tinggi, eksploitasi web HTTP yang signifikan, kerusakan pada *Windows*, *Microsoft Office*, dan Apple iOS, serta serangan lanjutan pada perangkat pribadi IoT.

Malware atau *Malicious Software* merupakan program komputer yang dirancang untuk merusak, mengganggu, atau mengambil alih sistem atau data pengguna tanpa izin atau pengetahuan pemiliknya. Malware dapat menyebar melalui email, *download* ilegal, jaringan komputer, atau media penyimpanan seperti USB Drive. Beberapa malware juga bisa menyebar melalui celah keamanan atau kerentanan dalam sistem operasi atau aplikasi tertentu. Malware dapat menimbulkan kerusakan pada sistem dan data pengguna, termasuk pencurian data pribadi, pencurian informasi keuangan, kerusakan sistem operasi, kehilangan data, dan lain sebagainya.

Jenis-jenis malware, diantaranya yaitu :

- *Ransomware*, merupakan program yang mengenkripsi data pada komputer korban dan meminta uang tebusan untuk mendapatkan kunci dekripsi.
  Contoh : *WannaCry* (2017), *Petya* yang menyerang sistem (2016), *Locky* yang menyebar melalui email (2016).
- *Trojan*, merupakan program yang menyembunyikan fungsi yang sebenarnya dan memungkinkan akses ke komputer korban untuk mengambil alih atau merusak data.

Contoh : Zeus yang mencuri informasi perbankan (2007), *SpyEye* yang mengumpulkan informasi keuangan (2010), *BlackEnergy* yang menyerang sistem industri (2015).

- *Adware*, merupakan program yang memunculkan iklan yang tidak diinginkan di komputer korban.
  Contoh : Genieo yang memunculkan iklan (2015), *CrossRider* yang menyediakan iklan (2013), JollyWallet yang menampilkan iklan (2014).
- *Rootkit*, merupakan program yang menyembunyikan keberadaannya pada sistem operasi korban dan memungkinkan pengendaliannya secara jarak jauh.
  Contoh : Sony BMG *rootkit* yang terinstall pada CD audio (2005), *Rustock rootkit* yang menyerang sistem email (2010), *ZeroAccess rootkit* yang menyerang sistem operasi *Windows* (2011).

Remote Access Trojan merupakan sebuah trojan yang dibuat dan diinfeksikan ke korban, yang mana setelah trojan berjalan, penyerang mempunyai hak akses dan kontrol penuh terhadap komputer infeksi tersebut. *Tools* yang digunakan yaitu njRAT. Dibuat menggunakan bahasa pemrograman berbasis .NET sehingga bagi pengguna *Windows* XP, trojan mempunyai kemungkinan tidak dapat dijalankan karena dibutuhkannya .NET *framework*. Biasanya pengguna njRAT akan menjual akun korban yang terinfeksi trojan hingga menjual generator trojan dan tutorial penggunaannya. njRAT merupakan salah satu *tools hacking* untuk OS *windows* yang digunakan untuk meremote PC satu dengan PC lainnya. RAT (*Remote Administrator Tool*) digunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan seperti :

- *Screen* atau *Camera Capture* atau *Control*,
- *File Management* (*download* / *upload* / *execute*),
- *Shell Control* (CMD *control*),
- *Computer Control* (*power off* / *on* / *log off*),
- *Registry Management* (*query* / *add* / *delete* / *modify*),
- *Password Management*.

OSINT (*Open Source Intelligence*) merupakan alat yang memungkinkan pengumpulan informasi yang tersedia untuk umum atau *open-source*. Ini bertujuan untuk mempelajari lebih lanjut tentang seseorang atau bisnis. OSINT dapat menggabungkan beberapa titik data dan untuk informasi referensi silang untuk mendapatkan sumber kebenaran.

C. ALAT DAN BAHAN

Alat dan bahan yang di butuhkan yaitu :

1. PC *Host* dengan minimal RAM 8GB dan Hardisk 40GB,
2. *Internet access*.
3. Aplikasi njRAT.

D. UNIT 4 – STRUKTUR MALWARE

Langkah Pengerjaannya, yaitu :

1. Melakukan pencarian untuk malware terbaru. Pilih empat contoh malware, masing-masing dari jenis malware yang berbeda, kemudian bahas detail yang dilakukan masing-masing, bagaimana masing-masing ditransmisikan, dan dampak masing-masing penyebabnya.
   Contoh jenis malware antara lain : *Ransomware*, *Trojan*, *Hoax*, *Adware*, Malware, PUP, *Exploit Kit*, dan Kerentanan. Cari malware dengan mengunjungi situs web berikut menggunakan istilah pencarian berikut :
   - Dasbor Lanskap Ancaman Pusat Ancaman McAfee.
   - Pusat Ancaman *Malwarebytes Labs* (10 Malware Teratas).
   - Securityweek.com > Ancaman Virus > Virus-Malware.
   - Technewsworld.com > Keamanan > Malware.

2. Pilih salah satu dari contoh sebelumnya dan buat ringkasan singkat yang menjelaskan apa yang dilakukan malware, cara penularannya, dan dampaknya.

   Trojan

   Contohnya yaitu *Emotet*, jenis malware ini akan memperoleh akses komputer dengan menginfeksi melalui lampiran email. Malware ini dirancang untuk mencuri informasi sensitif, seperti nama pengguna, kata sandi, dan data keuangan. Emotet dapat menjadi ancaman serius bagi individu, bisnis, dan organisasi, karena dapat menyebabkan kerugian finansial dan kehilangan data sensitif.

   Ransomware

   Contohnya yaitu *LockBit*, jenis malware ini bertujuan untuk mengenkripsi *file* pada komputer atau jaringan dan meminta pembayaran uang tebusan agar *file* tersebut dapat dibuka kembali. *LockBit* akan secara otomatis memeriksa target yang berharga, menyebarkan infeksi, dan mengenkripsi semua sistem komputer yang dapat di akses di jaringan. Malware ini dapat menyebabkan kehilangan data yang signifikan.

   Rootkit

   Contohnya yaitu *BlackLotus*, jenis malware yang dirancang untuk menyembunyikan keberadaannya pada sistem dengan mengganti kode *boot* di sistem operasi *windows*. Hal ini memungkinkan penyerang untuk memperoleh akses tidak sah ke sistem dan mengambil kontrol atasnya. *BlackLotus* juga dapat menonaktifkan solusi keamanan, termasuk *Hypervisor-protected Code Integrity* (HVCI), *BitLocker*, dan *Windows Defender*.

Malware Linux

Jenis malware yang menyerang sistem operasi Linux dan dapat menyebar melalui situs web yang tidak aman, aplikasi yang tidak terverifikasi atau celah keamanan pada sistem. Malware ini bertujuan untuk mencuri data, merusak sistem, atau mengambil kendali atas sistem untuk melakukan operasi yang tidak sah.

E. MALWARE NJRAT

Dibawah ini merupakan tampilan njRAT ketika pertama kali diaktifkan :

Langkah pengerjaannya, yaitu :

1. Mematikan semua antivirus dan *firewall* pada kedua PC yang digunakan untuk memakai aplikasi njRAT.

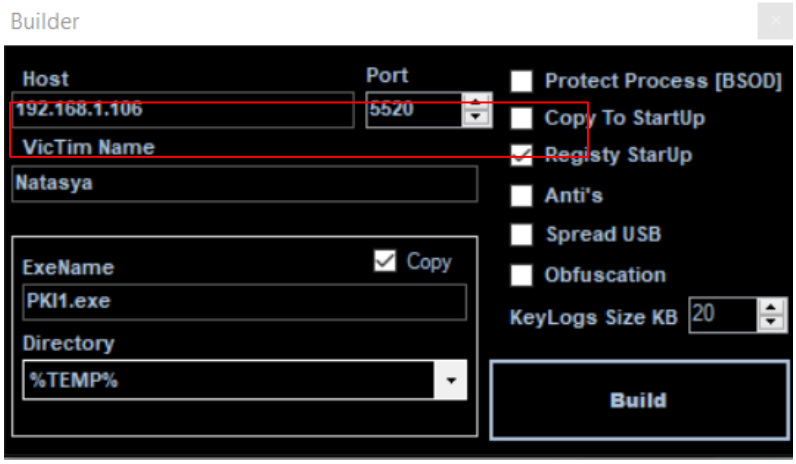
2. Mendownload dan mengekstrak aplikasi njRAT. Kemudian *run* aplikasi njRAT pada PC *host*.

3. Memasukkan port yang ingin digunakan yaitu 5520.

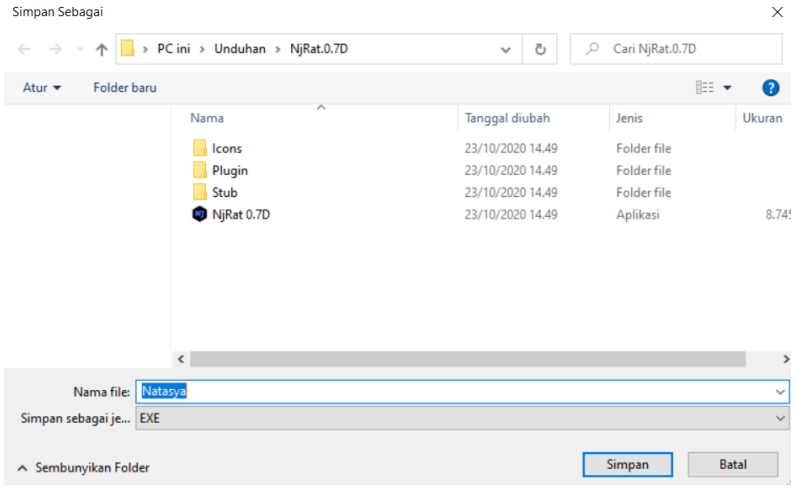
4. Melakukan pengecekan IP *Address* milik *host*. IP ini akan digunakan oleh njRAT. Komputer *host* dan komputer *victim* harus berada pada satu jaringan.

```
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1e4b:46bf:64e1:d78d%16
   IPv4 Address. . . . . . . . . . . : 192.168.70.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ffd6:4e46:b498:aa19%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

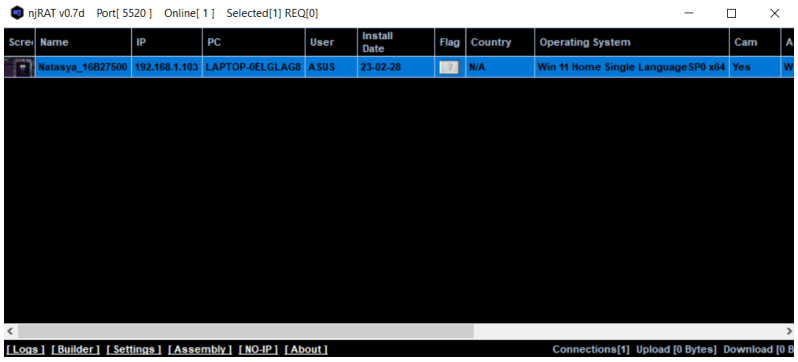
5. Membuat aplikasi yang akan dipasang pada komputer *victim*. Kemudian masukkan IP *Address* milik *host* pada kolom *host* dan port yang sesuai dengan yang ditentukan sebelumnya agar dapat diakses nantinya. Kemudian klik tombol ***build***.



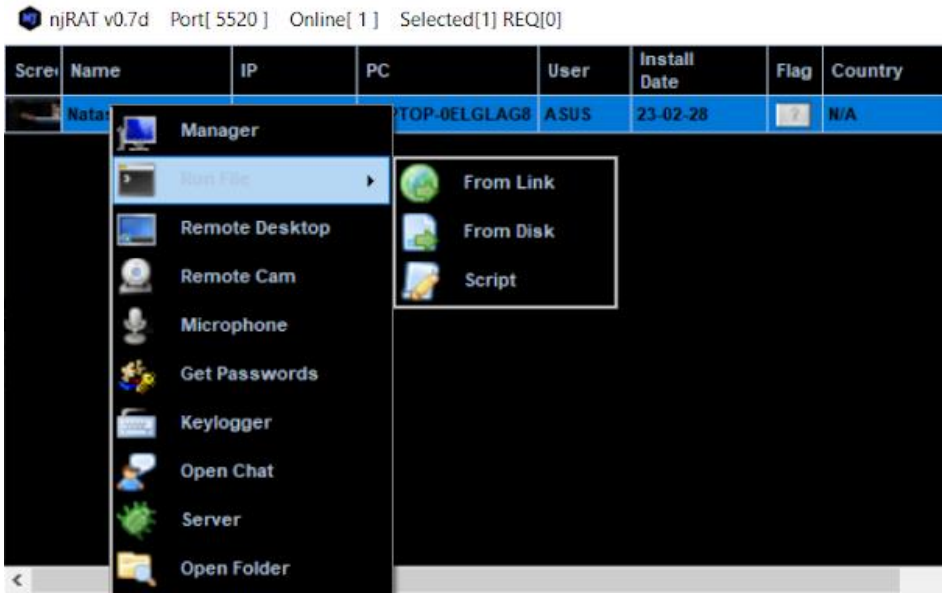
6. Kemudian simpan aplikasi hasil *build*.



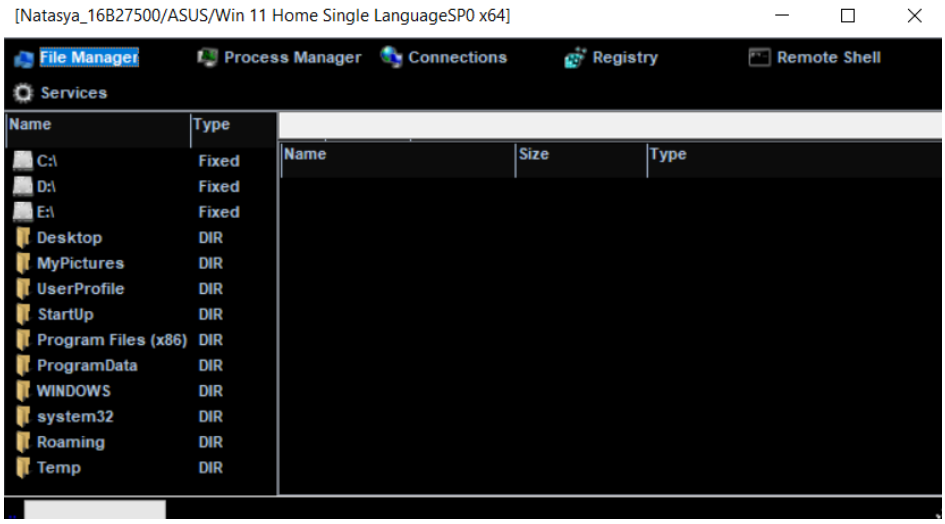
7. Kemudian *copy*-kan aplikasi **natasya.exe** yang telah dibuat sebelumnya ke dalam komputer *victim*. Kemudian, jalankan aplikasi tersebut pada komputer *victim*. Ketika sudah terpasang pada komputer *victim*, njRAT pada *host* akan mendeteksi komputer *victim*.



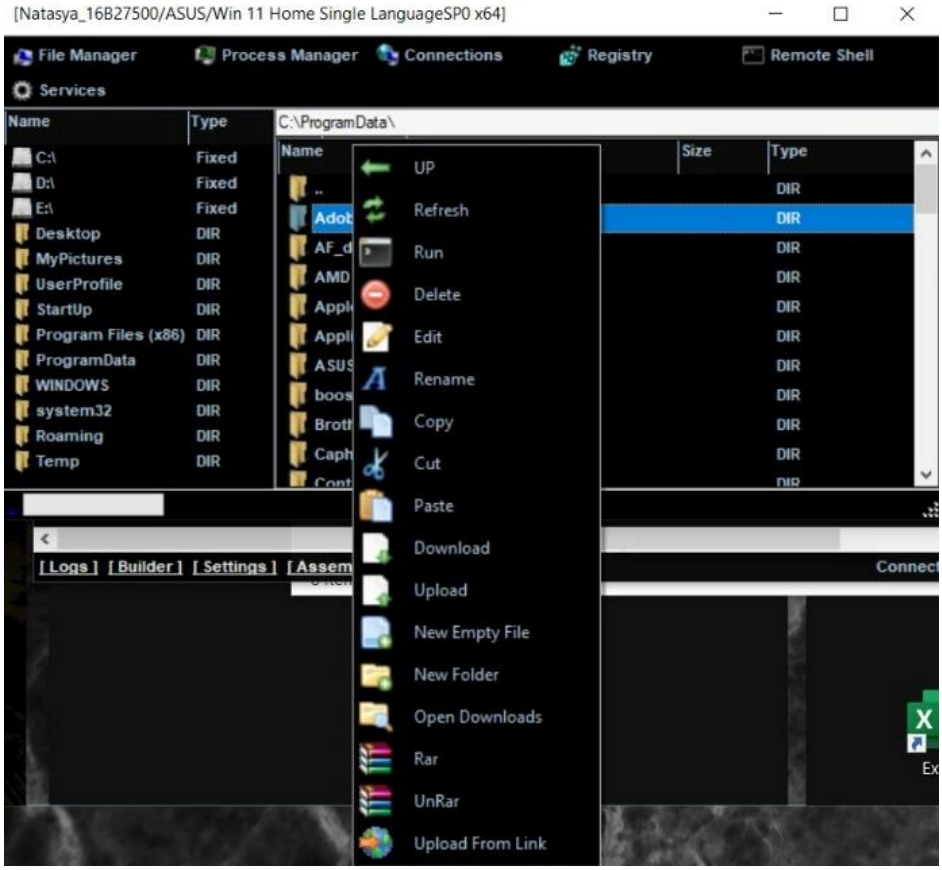
8. Klik kanan pada komputer yang aktif, maka akan muncul beberapa pilihan *menu*.



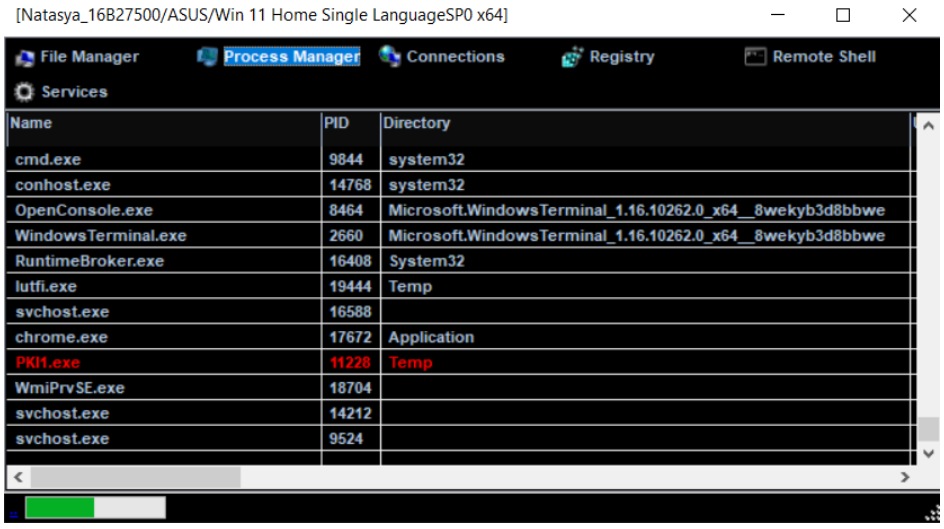
9. Pilih *menu* **manager** agar dapat melihat seluruh isi *file manager* yang ada pada komputer *victim*.



10. Pada *menu* **manager** terdapat **file manager**. Semua *file* atau direktori dapat dilihat pada panel kanan. Klik kanan *file* atau direktori yang dipilih dan kita dapat memanipulasinya menggunakan opsi kontekstual.

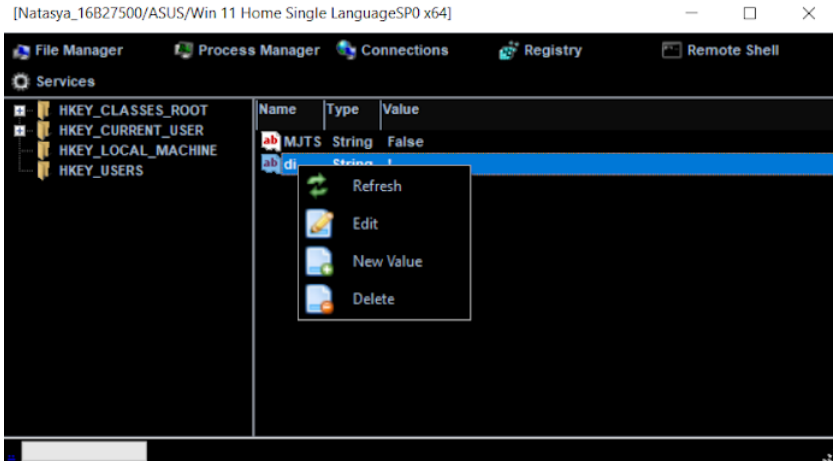


11. Pada *menu* **manager** terdapat **process manager**. Disini kita dapat melakukan tindakan seperti *kill*, *delete*, dan *restart* pada proses yang dipilih.

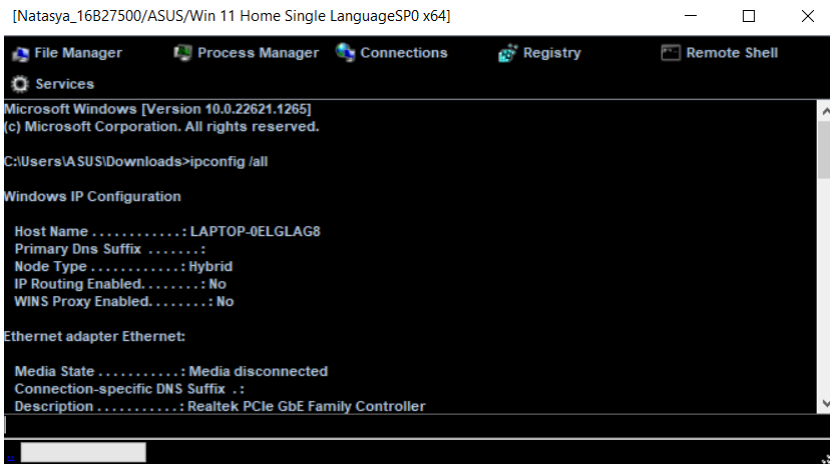


12. Pada *menu* **manager** terdapat **connections**. Disini kita dapat memutuskan koneksi antara dua mesin yang berkomunikasi melalui port tertentu.

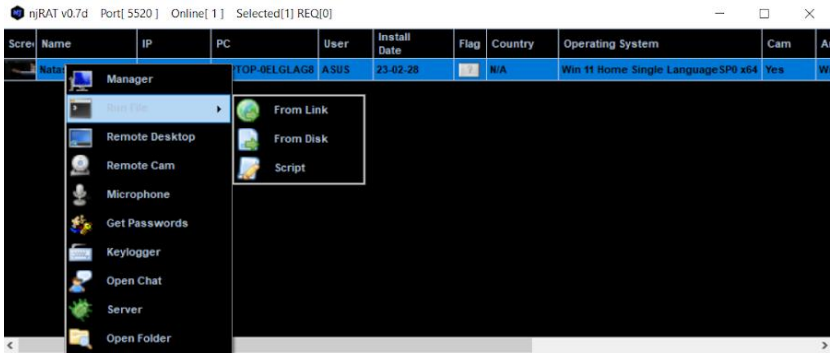
13. Pada *menu* **manager** terdapat **registry**. Disini kita dapat memanipulasi *file* atau direktori yang dipilih.



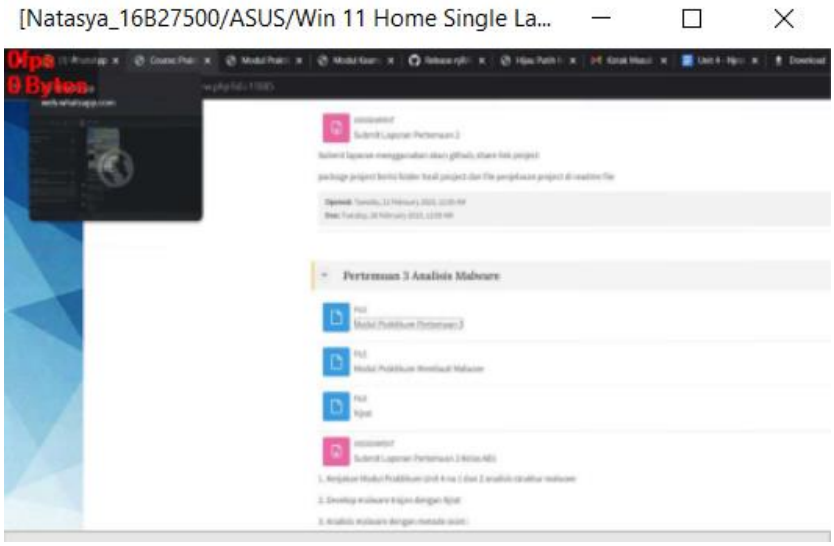
14. Pilih *menu* **manager** terdapat **remote shell**. Disini kita dapat meluncurkan *prompt* perintah jarak jauh dari mesin korban dengan cara ketik perintah **ipconfig /all** kemudian tekan *enter*.



15. Pilih *menu* **run file** agar dapat mengeksekusi skrip atau *file* dari jarak jauh dari mesinnya.

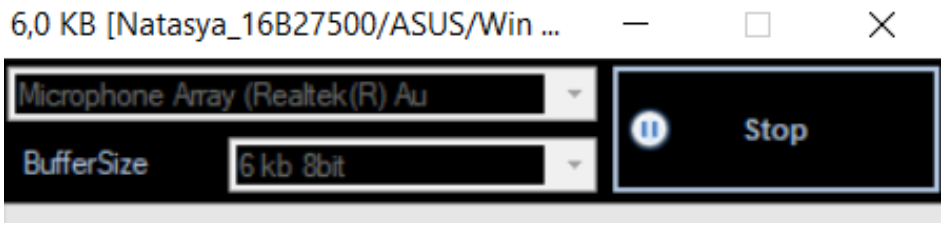


16. Pilih *menu* **remote desktop** agar dapat meluncurkan koneksi dekstop jarak jauh tanpa disadar oleh korban.

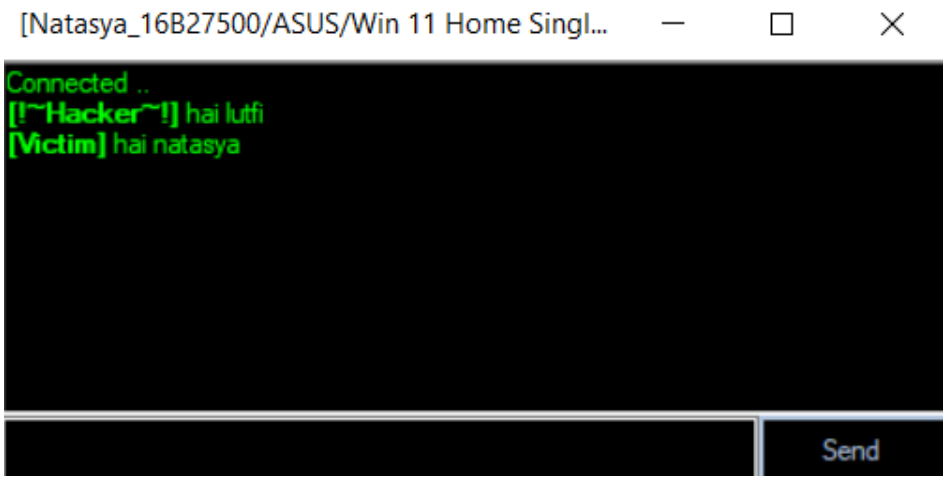


17. Pilih *menu* **remote cam** agar dapat membuka *webcam* yang ada di komputer *victim* dan dapat melihat segala aktivitas yang dilakukan oleh *victim*.

18. Pilih *menu* **microphone** agar dapat memata-matai korban dan melacak percakapan suara.



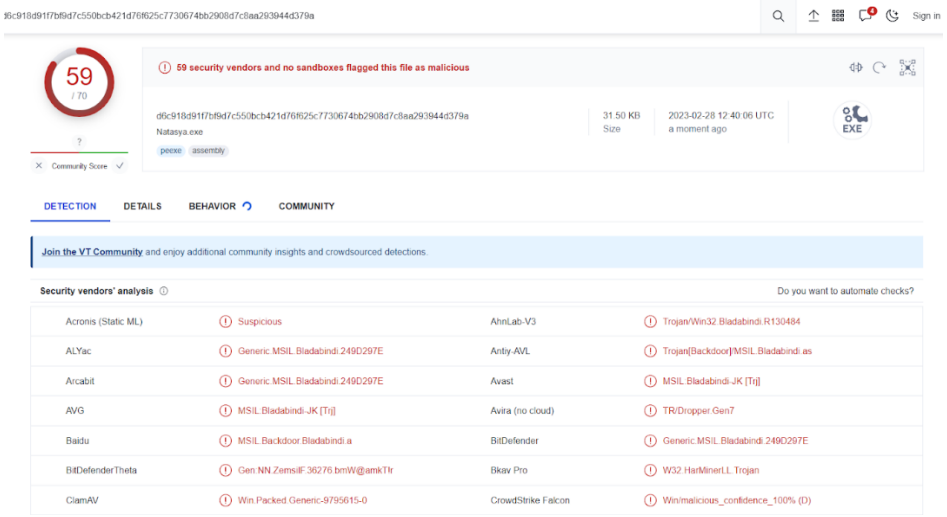
19. Pilih *menu* **open chat** agar dapat mengirimkan pesan ke layar dekstop komputer *victim* dan *user* komputer dapat melakukan balasan tanpa bisa menutup chat.



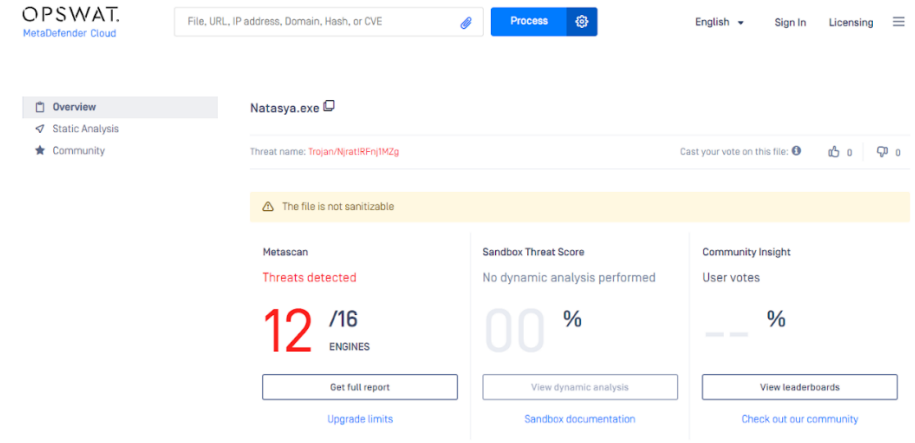
F. METODE OSINT

Beberapa *tools* yang digunakan, diantaranya yaitu :

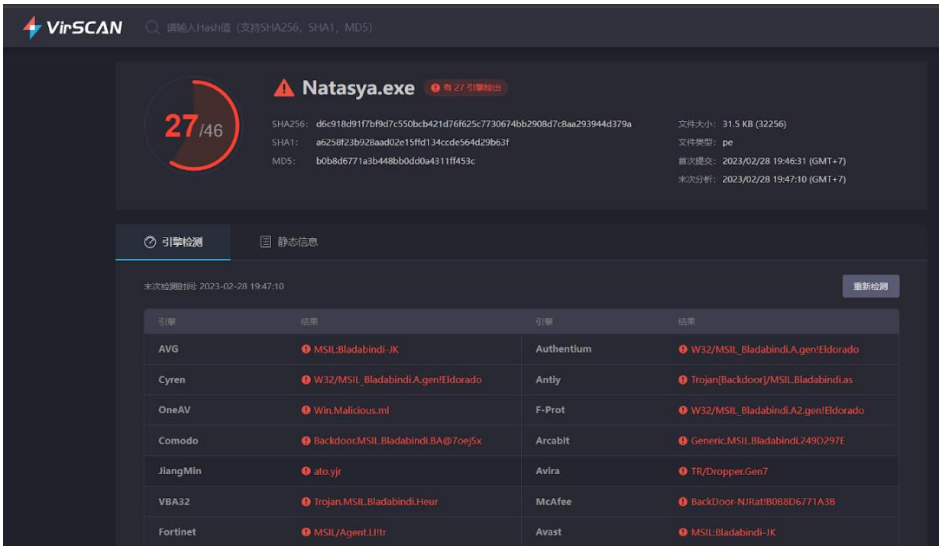
- VirusTotal



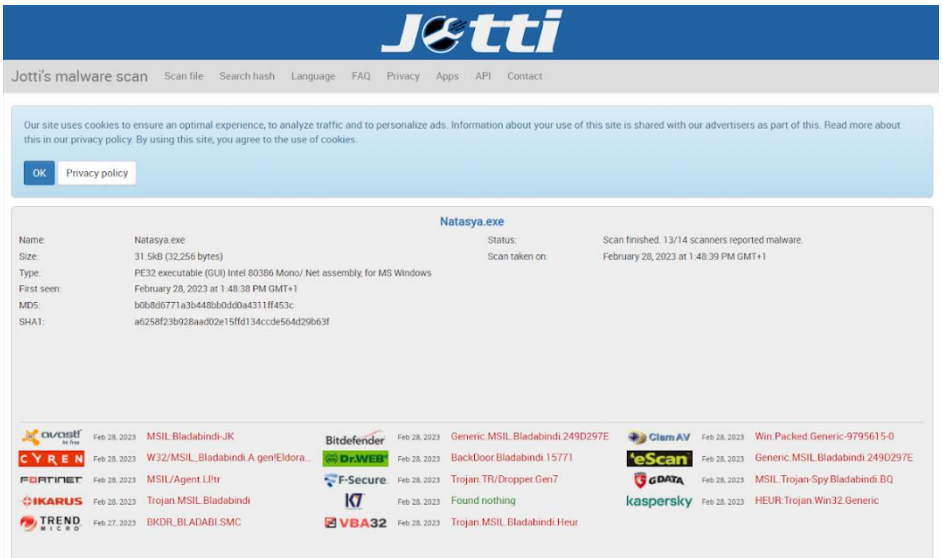
- OPSWAT (Meta Defender)



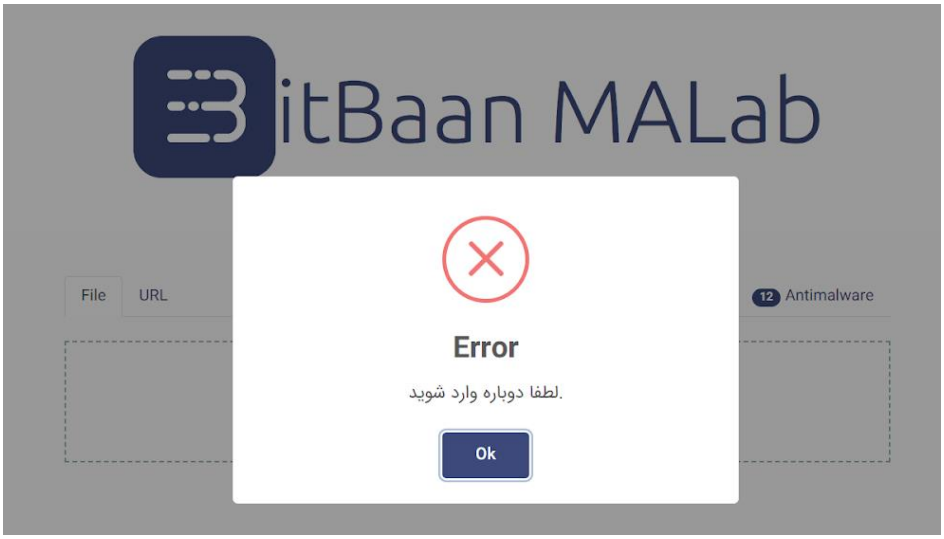
- VirSCAN



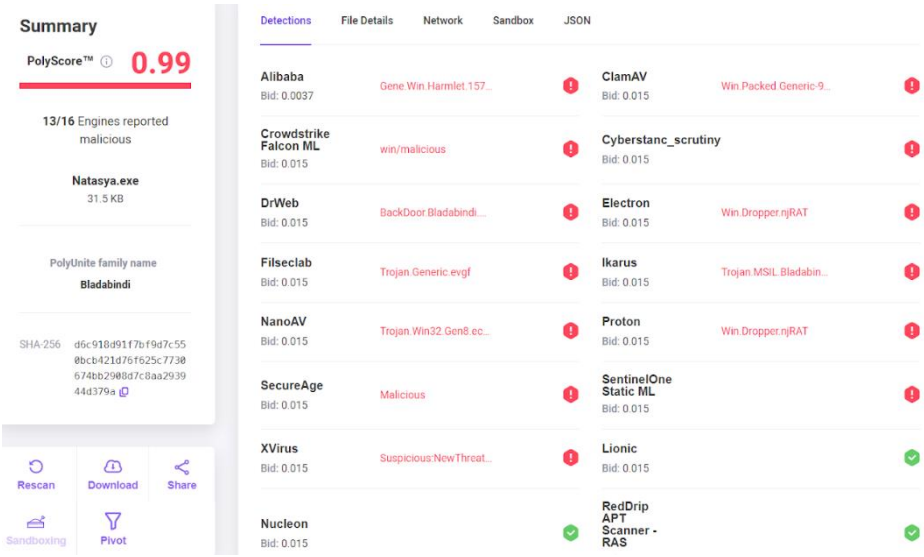
- Jotti



- Bitbaan MaLab



- PolySwarm



G. PEMBAHASAN

Malware (*Malicious Software*) merupakan program komputer yang dirancang untuk merusak, mengganggu, atau mengambil alih sistem atau data pengguna tanpa izin atau pengetahuan pemiliknya. Malware dapat menyebar melalui email, *download* ilegal, jaringan komputer, atau media penyimpanan seperti USB Drive. Beberapa malware juga bisa menyebar melalui celah keamanan atau kerentanan dalam sistem operasi atau aplikasi tertentu.

Terdapat berbagai macam jenis-jenis malware, diantaranya yaitu *Trojan*, *Ransomware*, *Rootkit*, dan Malware Linux. *Trojan* merupakan program yang menyembunyikan fungsi yang sebenarnya dan memungkinkan akses ke komputer korban untuk mengambil alih atau merusak data. Contohnya yaitu Emotet, dimana jenis ini akan memperoleh akses komputer dengan menginfeksi melalui lampiran

email. Malware ini dirancang untuk mencuri informasi sensitif, seperti nama pengguna, kata sandi, dan data keuangan. Malware ini dapat menyebabkan kerugian finansial dan kehilangan data sensitif. Sedangkan *Ransomware* merupakan program yang mengenkripsi data pada komputer korban dan meminta uang tebusan untuk mendapatkan kunci dekripsi. Contohnya yaitu *LockBit*. *LockBit* akan secara otomatis memeriksa target yang berharga, menyebarkan infeksi, dan mengenkripsi semua sistem komputer yang dapat di akses di jaringan. Kemudian *Rootkit* merupakan program yang menyembunyikan keberadaannya pada sistem operasi korban dan memungkinkan pengendaliannya secara jarak jauh. Contohnya yaitu *BlackLotus*, dimana jenis ini dirancang untuk menyembunyikan keberadaannya pada sistem dengan mengganti kode *boot* di sistem operasi *windows*. Hal ini memungkinkan penyerang untuk memperoleh akses tidak sah ke sistem dan mengambil kontrol atasnya. *BlackLotus* juga dapat menonaktifkan solusi keamanan, termasuk *Hypervisor-protected Code Integrity* (HVCI), *BitLocker*, dan *Windows Defender*. Dan yang terakhir yaitu Malware Linux merupakan jenis malware yang menyerang sistem operasi Linux dan dapat menyebar melalui situs *web* yang tidak aman, aplikasi yang tidak terverifikasi atau celah keamanan pada sistem. Malware ini bertujuan untuk mencuri data, merusak sistem, atau mengambil kendali atas sistem untuk melakukan operasi yang tidak sah.

Kemudian, pada praktikum ini praktikan juga membuat *server* menggunakan aplikasi njRAT. RAT (*Remote Administrator Tool*) merupakan sebuah *trojan* yang dibuat dan diinfeksikan ke korban, yang mana setelah *trojan* berjalan, penyerang mempunyai hak akses dan kontrol penuh terhadap komputer infeksi tersebut. RAT digunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan. NjRAT merupakan salah satu malware sejenis *trojan* yang menginfeksi komputer *victim* melalui installasi program. Ketika malware terpasang pada komputer, maka segala bentuk kegiatan komputer *Victim* dapat dimonitoring atau dikendalikan melalui komputer *Host* yang berada pada satu jaringan melalui akses IP dan port yang telah ditentukan diawal.

Sebelum menginstall njRAT, matikan semua antivirus dan *firewall* pada kedua komputer yang akan digunakan karena njRAT terdaftar sebagai *file* yang berbahaya. Setelah itu *run* aplikasi njRAT pada komputer *Host*. Kemudian masukkan port yang ingin digunakan, disini saya menggunakan port 5520. Sebelum lanjut ke aplikasi njRAT, lakukan pengecekan IP *Address* pada komputer *Host* terlebih dahulu. Pastikan komputer *host* dan komputer *Victim* berada pada satu jaringan. Disini IP komputer saya yaitu 192.168.1.1. Kemudian dilanjutkan dengan membuat aplikasi yang akan dipasang pada komputer *Victim* dengan memasukkan IP *Address* yang telah didapat sebelumnya dan sesuaikan port dengan yang sebelumnya telah ditentukan. Kemudian simpan aplikasi tersebut yang berbentuk .exe dan jalankan aplikasi tersebut pada komputer *Victim*.

Ketika sudah terpasang pada komputer *Victim*, njRAT pada komputer *Host* akan mendeteksi komputer *Victim*.

Disini terdapat berbagai macam *menu*, diantaranya yaitu *Manager*, *Run File*, *Remote Desktop*, *Remote Cam*, *Microphone*, *Get Passwords*, *Keylogger*, *Open Chat*, *Server*, dan *Open Folder*. Pada *menu Manager* kita dapat melihat seluruh isi *file manager* yang ada pada komputer *Victim*. Pada *menu Run File* kita dapat mengeksekusi skrip atau *file* dari jarak jauh dari mesinnya. Pada *menu Remote Desktop* kita dapat meluncurkan koneksi dekstop jarak jauh tanpa disadar oleh korban. Pada *menu Remote Cam* kita dapat membuka *webcam* yang ada di komputer *victim* dan dapat melihat segala aktivitas yang dilakukan oleh *victim*. Pada *menu Microphone* kita dapat memata-matai korban dan melacak percakapan suara. Kemudian pada *menu Open Chat* kita dapat mengirimkan pesan ke layar dekstop komputer *victim* dan *user* komputer dapat melakukan balasan tanpa bisa menutup chat.

Tidak hanya itu, pada *menu Manager* juga memiliki berbagai macam pilihan diantaranya yaitu *File Manager*, *Process Manager*, *Connections*, *Registry*, dan *Remote Shell*. Pada *File Manager* kita dapat memanipulasinya menggunakan opsi kontekstual. Pada *Process Manager* kita dapat melakukan tindakan seperti *kill*, *delete*, dan *restart* pada proses yang dipilih. Pada *Connections* kita dapat memutuskan koneksi antara dua mesin yang berkomunikasi melalui port tertentu. Pada *Registry* kita dapat memanipulasi *file* atau direktori yang dipilih. Pada *Remote Shell* kita dapat meluncurkan *prompt* perintah jarak jauh dari mesin korban dengan cara ketik perintah **ipconfig /all**.

Kemudian melakukan analisis terhadap *file* .exe yang telah dibuat sebelumnya dengan menggunakan metode OSINT. OSINT (*Open Source Intelligence*) merupakan alat yang memungkinkan pengumpulan informasi yang tersedia untuk umum atau *open-source*. Ini bertujuan untuk mengumpulkan informasi individu, organisasi, atau kejadian tertentu untuk tujuan analisis atau investigasi. OSINT dapat menggabungkan beberapa titik data dan untuk informasi referensi silang untuk mendapatkan sumber kebenaran. OSINT memanfaatkan sumber informasi yang tersedia secara publik seperti situs *web*, media sosial, basis data publik, dan sumber informasi publik lainnya.

Pada praktikum ini *tools* yang digunakan, diantaranya yaitu VirusTotal, OPSWAT (Meta Defender), VirSCAN, Jotti, Bitbaan MaLab, dan PolySwarm. Hasil yang didapat dari *tools* tersebut pada *file* njRAT .exe yaitu :

No.	OSINT Tools	File .exe
1.	VirusTotal	59 / 70
2.	OPSWAT	12 / 16
3.	VirSCAN	27 / 46
4.	Jotti	13 / 14
5.	Bitbaan MaLab	-
6.	PolySwarm	13 / 16

Dari tabel diatas, dapat disimpulkan bahwa Jotti merupakan *tools* yang paling bagus diantara 5 lainnya karena dari 14 hasil scan terdapat 13 *file* yang terdeteksi berbahaya pada *file* tersebut. Sedangkan VirSCAN merupakan *tools* yang kurang bagus diantara lainnya karena dari 46 hasil scan hanya 27 *file* yang dapat dideteksi berbahaya pada *file* tersebut. Sedangkan Bitbaan MaLab terjadi *error* saat pengecekan status *file* sehingga tidak dapat menemukan hasil scan menggunakan *tools* ini.

H. KESIMPULAN

Adapun kesimpulan dari praktikum ini yaitu :

1. Malware (*Malicious Software*) merupakan program komputer yang dirancang untuk merusak, mengganggu, atau mengambil alih sistem atau data pengguna tanpa izin atau pengetahuan pemiliknya.
2. NjRAT merupakan salah satu malware sejenis *trojan* yang menginfeksi komputer *victim* melalui installasi program. Ketika malware terpasang pada komputer, maka segala bentuk kegiatan komputer *Victim* dapat dimonitoring atau dikendalikan melalui komputer *Host* yang berada pada satu jaringan melalui akses IP dan port yang telah ditentukan diawal.
3. Sebelum menginstall njRAT, matikan semua antivirus dan *firewall* pada kedua komputer yang akan digunakan karena njRAT terdaftar sebagai *file* yang berbahaya.
4. OSINT (*Open Source Intelligence*) merupakan alat yang memungkinkan pengumpulan informasi yang tersedia untuk umum atau *open-source*.
5. Jotti merupakan *tools* yang paling bagus sedangkan VirSCAN merupakan *tools* yang paling kurang bagus diantara *tools* lainnya.

DAFTAR PUSTAKA

Keamanan Siber. 2021, Januari 30. *Awas! Ini Virus Jahat Komputer Paling Berbahaya di Dunia*. Di akses dari, <https://www.keamanansiber.com/2021/01/awas-ini-virus-jahat-komputer-paling.html.>

Arntz, Pieter. 2023, Maret 3. *Ransomware LockBit menuntut $2 juta untuk data Pierce Transit*. Di akses dari <https://www.malwarebytes.com/blog/news/2023/03/public-transportation-service-pierce-transit-struck-by-lockbit-ransomware.>

Kaspersky. *LockBit ransomware – Yang Perlu Anda Ketahui*. Di akses dari <https://www.kaspersky.com/resource-center/threats/lockbit-ransomware.>

Arghire, Lonut. 2023, Maret 2. *BlackLotus Bootkit Dapat Menargetkan Sistem Windows 11 yang Ditambal Sepenuhnya*. Di akses dari <https://www.securityweek.com/blacklotus-bootkit-can-target-fully-patched-windows-11-systems/.>

TedCruz. 2022, Oktober 17. *Rootkit UEFI Black Lotus baru ditawarkan untuk dijual dengan harga $5.000*. Di akses dari <https://malwaretips.com/threads/new-uefi-rootkit-black-lotus-offered-for-sale-at-5-000.117864/.>

Germain, Jack. M. 2023, Januari 23. *Tingkat Malware Linux Naik ke Tingkat Rekor Di Tengah Ketidakkonsistenan Peretas*. Di akses dari <https://www.linuxinsider.com/story/linux-malware-rates-rise-to-record-levels-amid-hacker-inconsistency-176834.html?__hstc=8228397.655a4b98f509a2132bd5eba725626c0a.1678033192947.1678033192947.1678033192947.1&__hssc=8228397.3.1678033192947&__hsfp=1891733359.>