

BAB 4

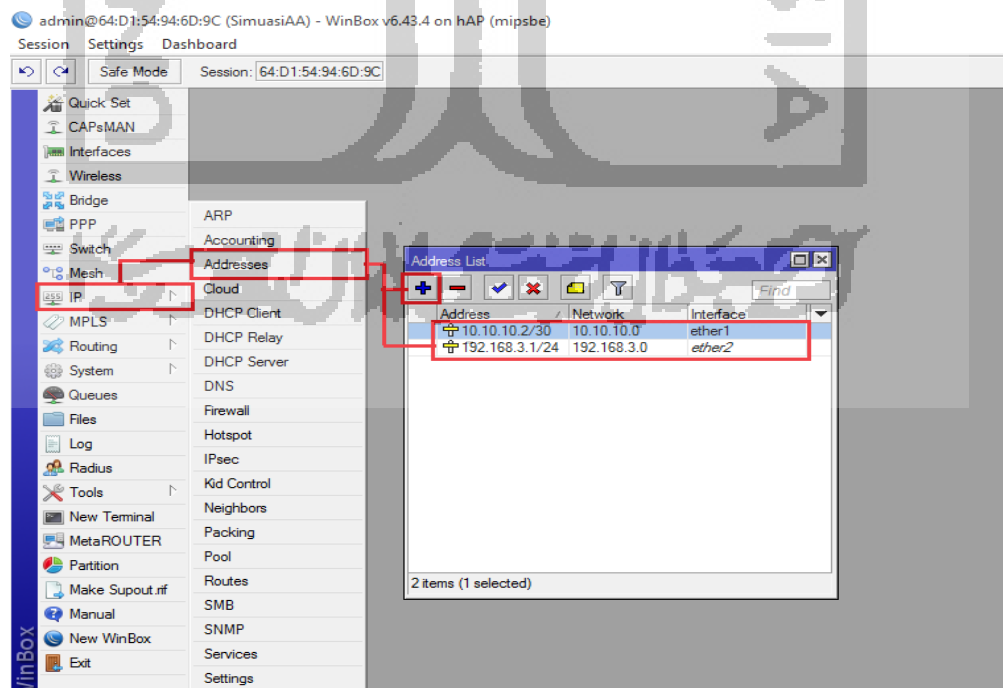
Hasil dan Pembahasan

Bab ini berisikan penjelasan yang diperoleh dari proses penelitian yang telah dilakukan berdasarkan rumusan masalah dan tujuan penelitian yang diajukan sebelumnya, yaitu: 1) Melakukan setting jaringan, 2) Simulasi *Remote Access Trojan (RAT)*, 3) Konfigurasi keamanan data, 4) Hasil pengujian *Remote Access Trojan (RAT)*.

4.1 Settingan Jaringan Router

4.1.1 Melakukan Pengaturan IP Network

Sebelum melakukan konfigurasi ke sistem, terlebih dahulu digunakan aplikasi WinBox versi 3.18. Dalam simulasi ini menggunakan 2 (dua) buah laptop yaitu laptop attacker (penyerang) dan laptop korban, juga menggunakan 2 (dua) buah MikroTik router jenis Router RB931-2nD sebagai Router A untuk laptop attacker dan RB951Ui Versi 6 untuk laptop attacker sebagai Router B untuk laptop korban. Settingan dimulai dengan aplikasi Winbox dengan mengkoneksikan admin user untuk membuat IP Address di laptop attacker dengan alamat IP Address adalah 192.168.3.1 dan IP Address laptop korban adalah 192.168.2.1 dalam gambar berikut :

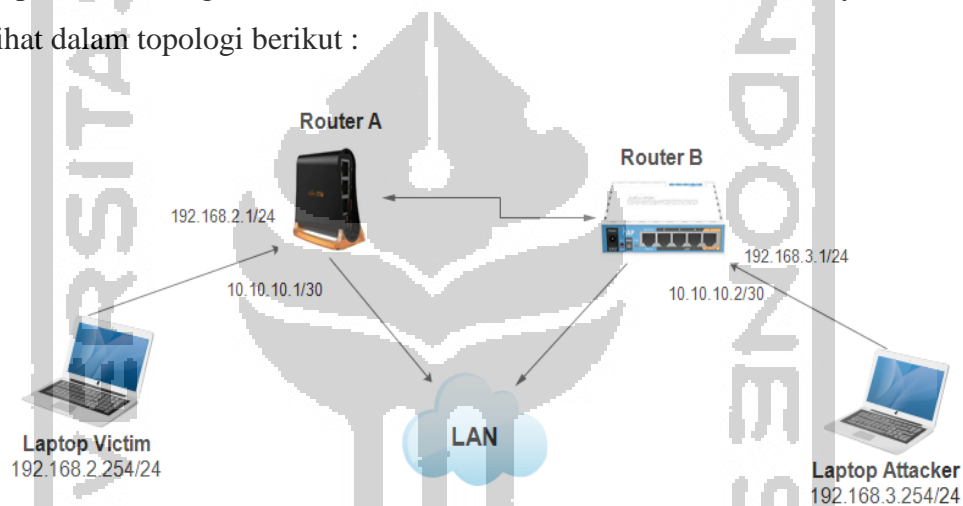


Gambar 4. 1 Setting IP Address Laptop Attacker

Address	Network	Interface
10.10.10.1/30	10.10.10.0	ether1
192.168.2.1/24	192.168.2.0	ether2

Gambar 4. 2 Setting IP Address Laptop Korban

Tahap selanjutnya kita akan menyambungkan ke IP router baik laptop korban dengan Destination-Address 192.168.3.0/24, Gateway 10.10.10.2 dan laptop attacker dengan Destination-Address 192.168.2.0/24, Gateway 10.10.10.1, terlihat dalam topologi berikut :



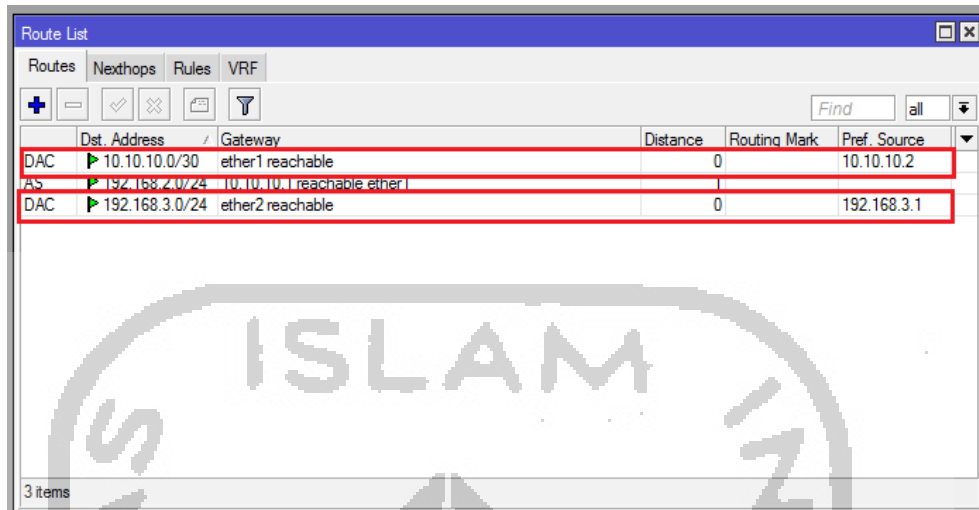
Gambar 4. 3 Topologi Settingan Jaringan

IP Address pada suatu Port Router bisa juga dapat berarti Gateway pada Network. IP Gateway biasa dijadikan sebagai target dari suatu aktivitas serangan pada jaringan lokal sesuai tab informasi IP Address List masing-masing laptop. Setelah pembuatan IP Address tahap selanjutnya membuat IP Routing untuk menghubungkan ke router baik router A dan router B.

4.1.2 Melakukan Settingan Jaringan Router

Tahap berikutnya melakukan settingan jaringan IP Router baik pada Router A dengan IP Route 10.10.10.1/30 sebagai ether1 status DAC (*Dynamic Active Connected*) dan IP Route 192.168.2.1/24 sebagai ether2 status DAC dan Router B dengan IP Route 10.10.10.2/30 sebagai ether1 status DAC (*Dynamic Active Connected*) dan IP Route 192.168.3.1/24 sebagai ether2 status DAC. DAC artinya

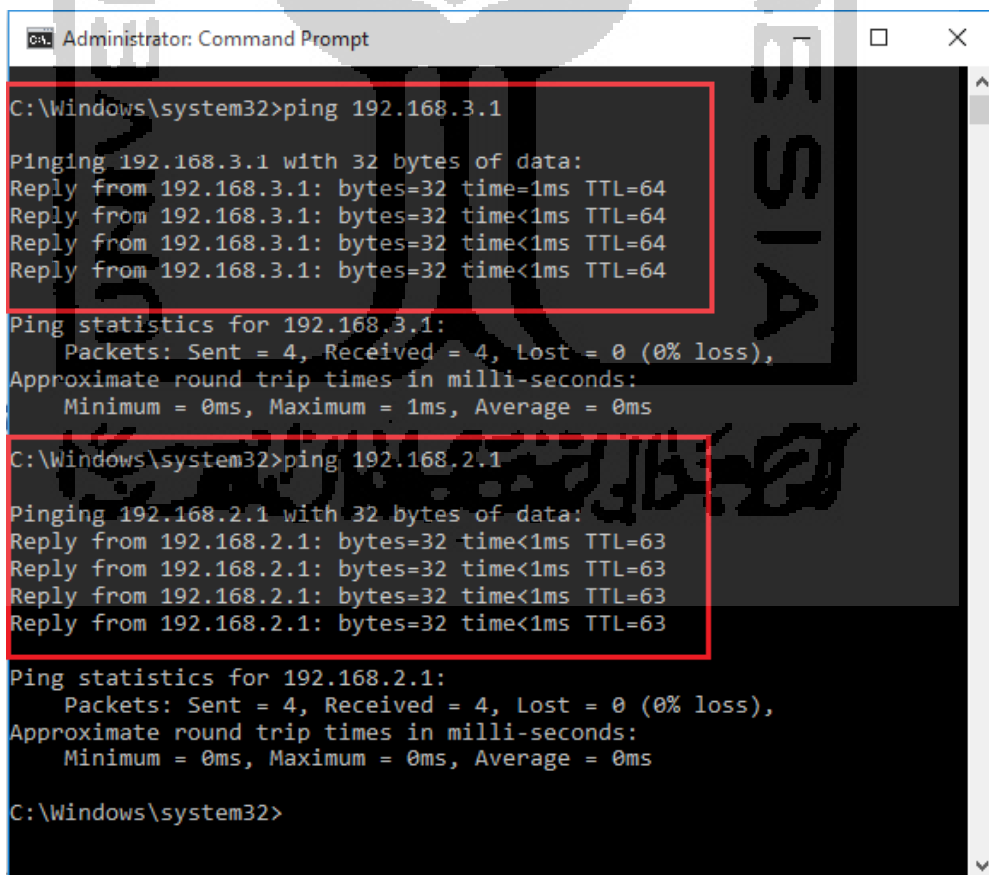
menunjukkan ether yang aktif dan mempunyai IP Route, sedangkan AC (*Active Static*) artinya ada sebuah *route static*.



	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.10.10.0/30	ether1 reachable	0		10.10.10.2
AS	192.168.2.0/24	10.10.10.1 reachable ether1			
DAC	192.168.3.0/24	ether2 reachable	0		192.168.3.1

Gambar 4. 4 Hasil Setting IP Route

Untuk mengetahui setting jaringannya berhasil dilakukan koneksi lokal dengan membuka Command Prompt lalu ping IP laptop baik laptop korban dan laptop attacker. Jika statusnya udah reply berarti settingannya sudah bisa diakses IP Address secara static.



```
Administrator: Command Prompt

C:\Windows\system32>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=1ms TTL=64
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>ping 192.168.2.1

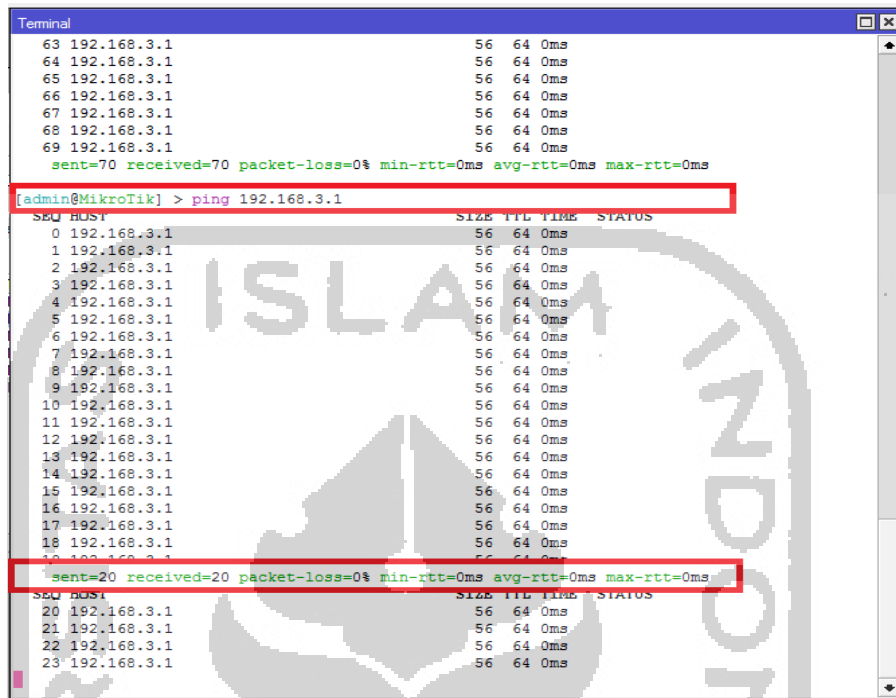
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=63
Reply from 192.168.2.1: bytes=32 time<1ms TTL=63
Reply from 192.168.2.1: bytes=32 time<1ms TTL=63
Reply from 192.168.2.1: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

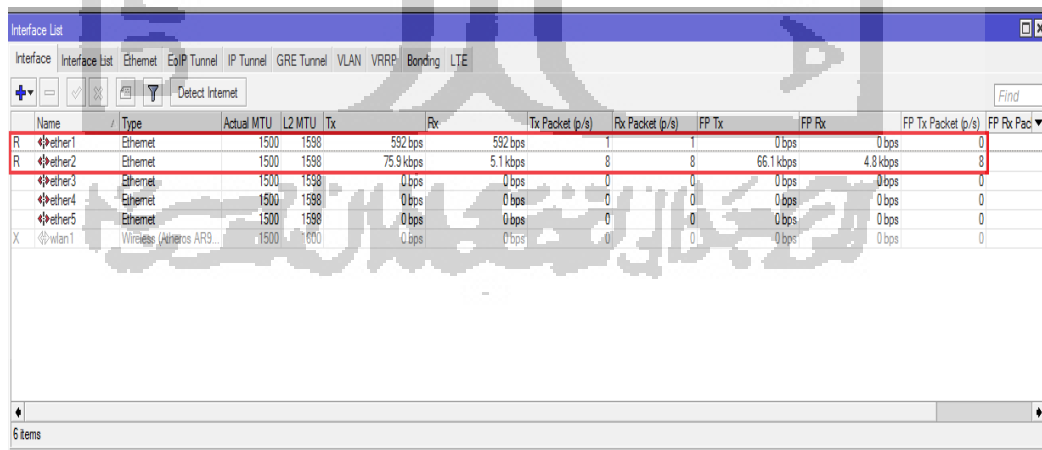
Gambar 4. 5 Setting IP Berhasil Dilakukan

Selanjutnya dilakukan penyesuaian pada terminal di Winbox untuk mengetahui status daripada IP Host setelah dilakukan pembuatan IP Route di Laptop attacker yang terlihat pada gambar berikut :



Gambar 4. 6 Status Terminal Winbox

Untuk mengetahui traffic port masing-masing jaringan dari Router A dan Router B melalui tab Interface List di Winbox, informasinya menunjukkan port di ether1 dan ether2 telah berjalan (Running) yang ditampilkan dalam kecepatan kbps masing-masing port.

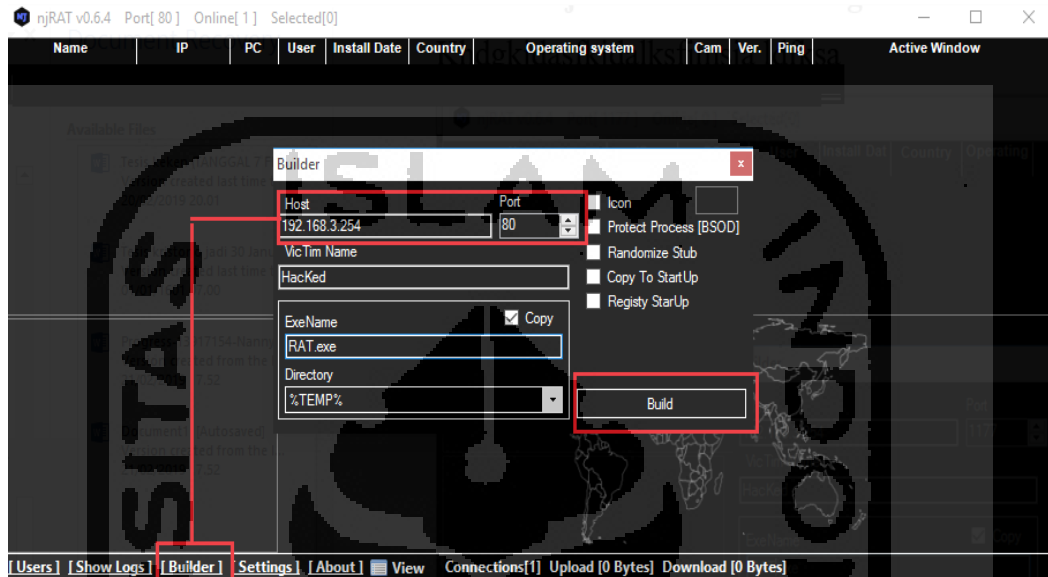


Gambar 4. 7 Hasil Traffic Port Interface List

4.1.3 Simulasi Remote Access Trojan (RAT)

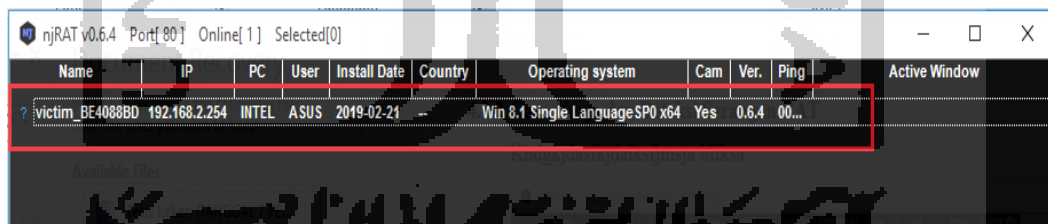
Untuk mengetahui cara kerja dan deteksi serangan RAT dengan melakukan pembuatan *malware* jenis trojan dengan menggunakan tools njRAT v0.6.4,

dimana dalam simulasi ini file njRAT yang digunakan sebagai contoh dalam simulasi ini. Tahap pembuatan *malware* jenis trojan ini dilakukan di laptop attacker dengan menggunakan alamat IP Address Host 192.168.3.254 dengan port 80 dan nama **Victim Hacked** dengan nama file .exe adalah **sss.exe**, seperti gambar berikut :



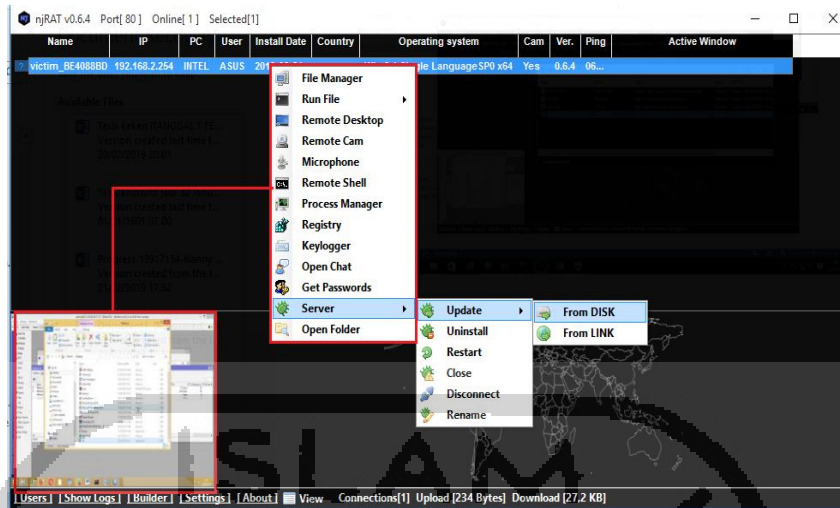
Gambar 4. 8 Hasil Builder RAT

Tahap selanjutnya file **sss.exe** di copy ke laptop korban dengan double klik di desktop korban, maka akan tampil di tools njRAT dengan nama **?victim_BE4088BD**, IP Address 192.168.2.254, jenis PC Intel, User Asus, Tanggal Install tercantum dan informasi Operating System.



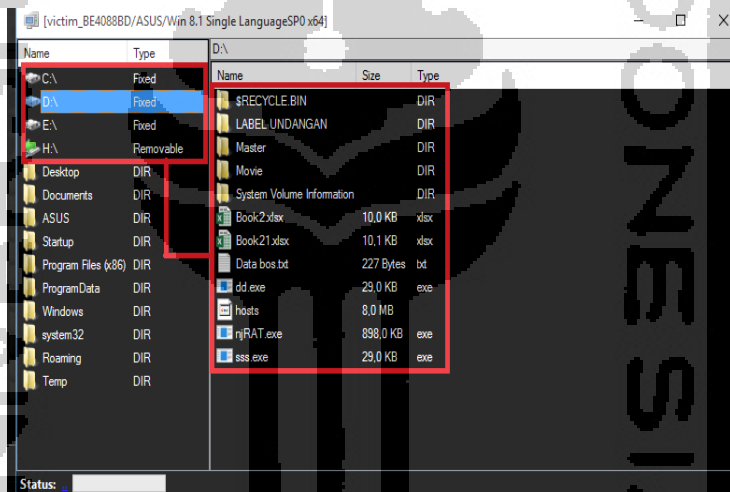
Gambar 4. 9 Proses RAT berhasil di remote

Analisis *Remote Access Trojan* (RAT) dalam hal ini jenis *malware* njRAT pada laptop korban setelah berhasil di ambil alih oleh laptop attacker yang bisa meremote laptop korban, bukti digital yang didapatkan berupa data-data File Manager, Run File, Remote Desktop, Remote Cam, Microphone, Remote Shell, Process Manager, Registry, Keylogger, Open Chat, Get Password, Server (Update, Uninstall, Restart, Close, Disconnect, Rename), dan Open Folder.

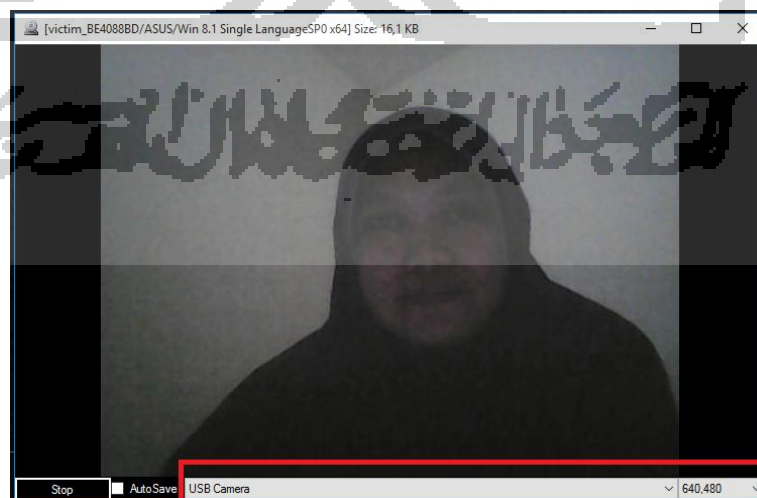


Gambar 4. 10 Hasil Bukti Digital Laptop Korban

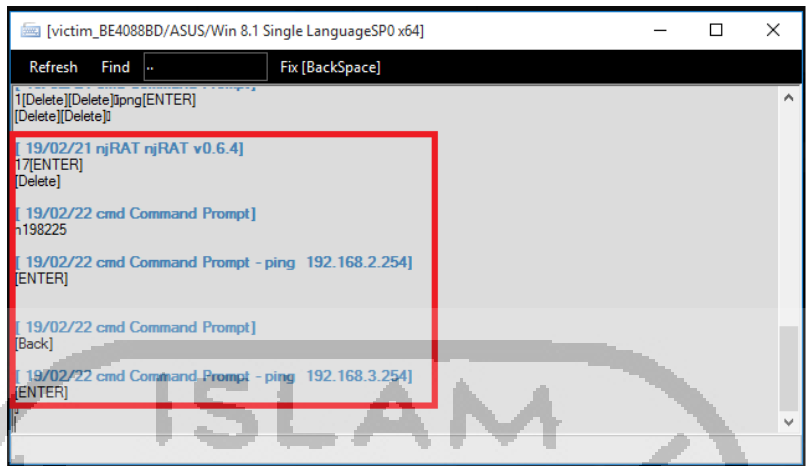
Diantaranya contoh sebahagian dari hasil *Remote Access Trojan* (RAT) digambarkan dalam gambar-gambar dibawah ini :



Gambar 4. 11 Hasil Open Folder



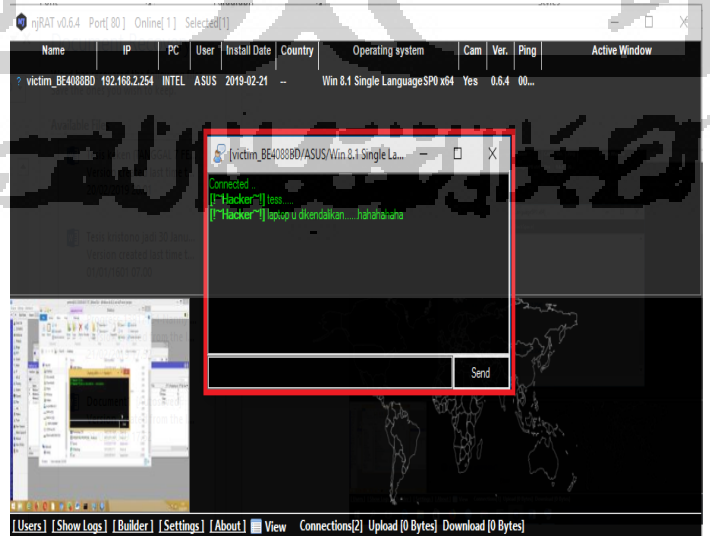
Gambar 4. 12 Hasil Remote Cam



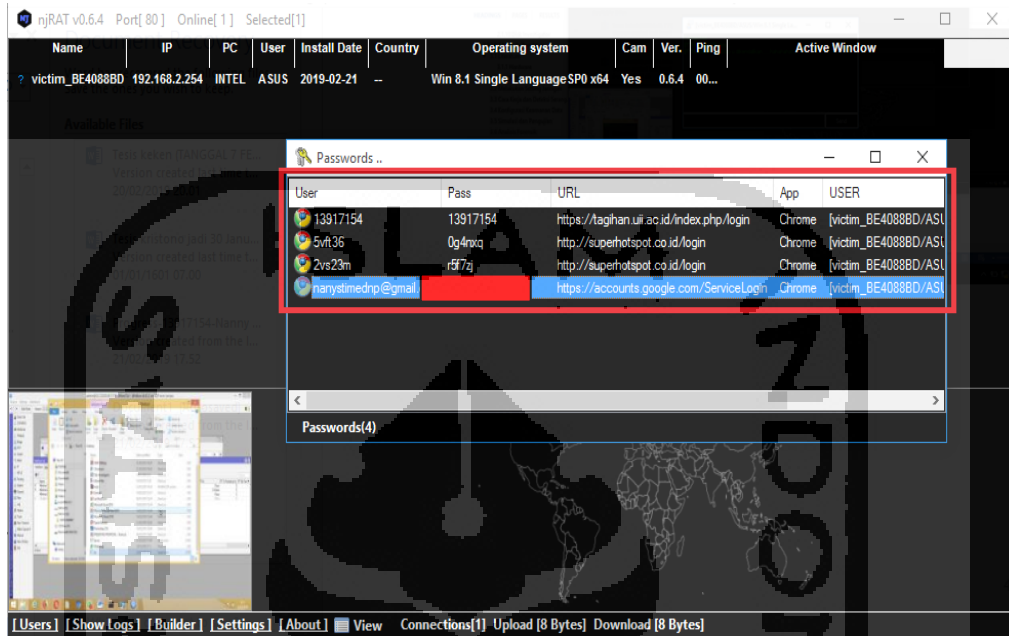
Gambar 4. 13 History Aktivitas Command Prompt

Name	PID	Location	Description
dashhost	1968		
firefox.exe	8072	C:\Program Files (x86)\Mozilla Fir...	Firefox
NVDisplay.Container	5112		
cmd.exe	8656	C:\Windows\system32	Windows Command Processor
spoolsv	1560		
opera	6484		
SearchIndexer.exe	4180	C:\Windows\system32	Microsoft Windows Search Indexer
csrss	568		
csrss	4112		
svchost.exe	1156	C:\Windows\system32	Host Process for Windows Servic...
TunMirror	6276		
KMS Server	8232		
WUDFHost	40492		
splwow64	7176		
firefox.exe	7688	C:\Program Files (x86)\Mozilla Fir...	Firefox
rundll32.exe	2112	C:\Windows\system32	Windows host process (Rundll32)
J6BAMEQBZ	2504		
nvcontainer.exe	4276	C:\Program Files (x86)\NVIDIA Cor...	
svchost.exe	532	C:\Windows\system32	Host Process for Windows Servic...
svchost.exe	4140	C:\Windows\system32	Host Process for Windows Servic...
audiodg	9588		
chrome.exe	3872	C:\Users\ASUS\AppData\Localchr...	Chromium
RuntimeBroker	5280		
chrome.exe	3476	C:\Users\ASUS\AppData\Localchr...	Chromium
vmnat.exe	1896	C:\Windows\system32	VMware NAT Service

Gambar 4. 14 Hasil Analisis System Information yang Tersembunyi



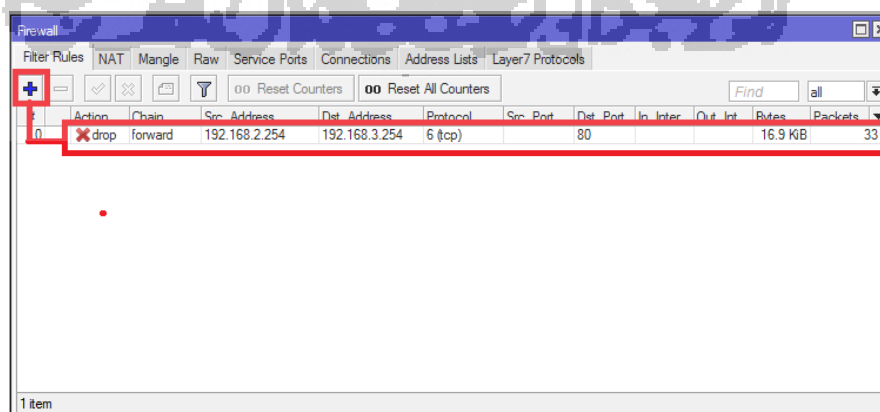
Gambar 4. 15 Hasil Open Chat



Gambar 4. 16 Hasil History Get Password

4.1.4 Konfigurasi Keamanan Data

Melakukan keamanan data daripada laptop korban maka perlu memasang firewall di IP Address laptop korban dengan cara menentukan IP Address di aplikasi Winbox → IP → Firewall dengan IP Address Src Address : 192.168.2.254 adalah IP Address laptop korban, Destination Address 192.168.3.254 adalah IP Address laptop attacker dengan Destination Port 80 berdasarkan lokasi port yang bisa diakses oleh njRAT dan status di tab Action drop, terlihat pada gambar berikut :



Gambar 4. 17 Pembuatan Firewall Traffic

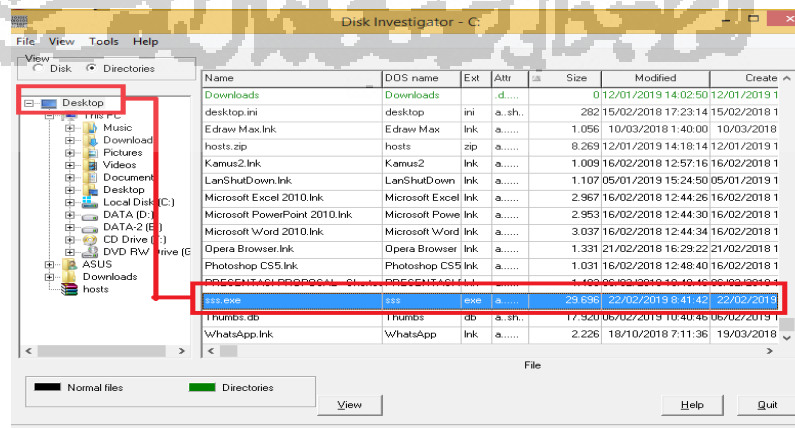
4.1.5 Hasil Pengujian *Remote Access Trojan (RAT)*

Pengujian dilakukan untuk membuktikan bahwa apakah pemblokiran *firewall traffic* berhasil atau tidaknya, maka dilakukan kembali pengujian penyerangan ke laptop korban dengan melakukan penyerangan dari laptop attacker ke laptop korban. Kemudian dilakukan pengecekan ternyata laptop korban sudah tidak bisa deteksi lagi melalui file *malware* jenis njRAT, karena otomatis tidak bisa lagi menarik data-data atau meremote laptop korban dan dibuktikan dalam gambar berikut :

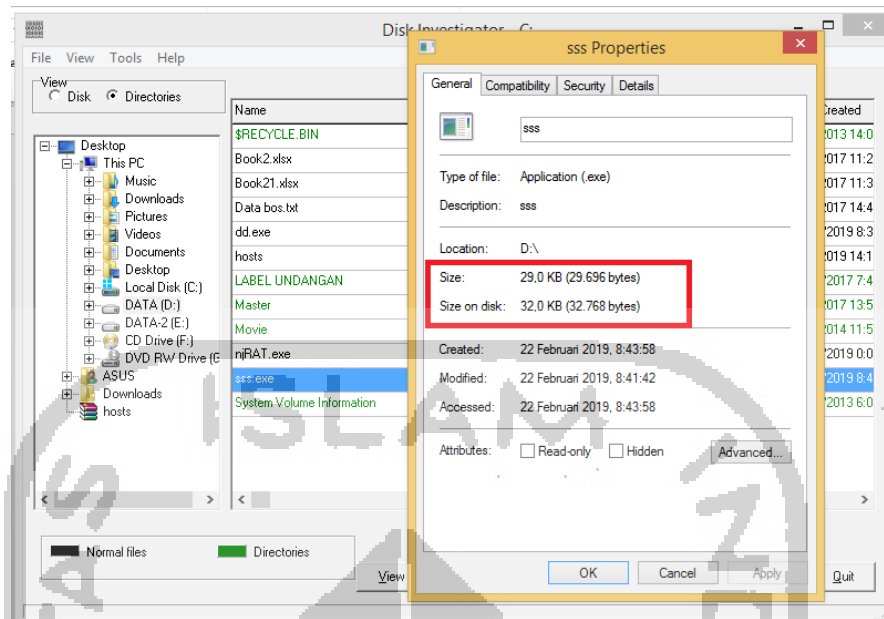


Gambar 4. 18 Hasil Pemblokiran *Firewall Traffic*

Pengujian dilakukan dengan menggunakan beberapa tool forensik diantaranya tools Disk Investigator yang membuktikan bahwa didalam disk terdapat file-file yang merupakan program *malware* jenis berbahaya yang berekstensi .exe. Disk Investigator menunjukkan file mana yang terdapat *malware* dengan memberikan tanda 2 (dua) warna yaitu hijau menunjukkan direktori atau folder dan warna hitam menunjukkan sebuah file. Jenis *malware* yang terjangkit di laptop korban dengan nama file *sss.exe* dengan size **29,696** sector, tanggal dan waktu (*timestamp*) penyerangan terjadi (*Modifed/Create*).

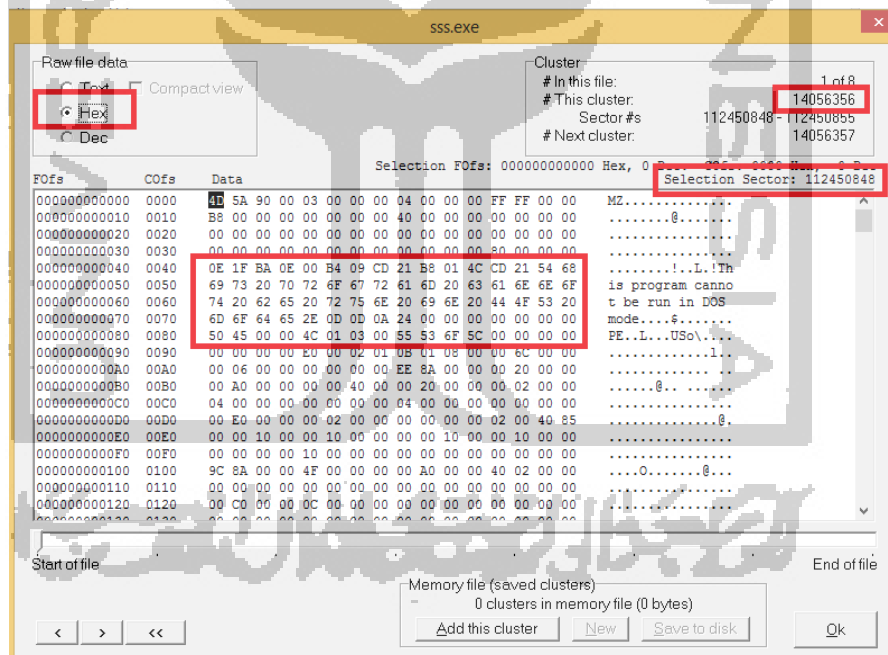


Gambar 4. 19 Analisis Tools Disk Investigator



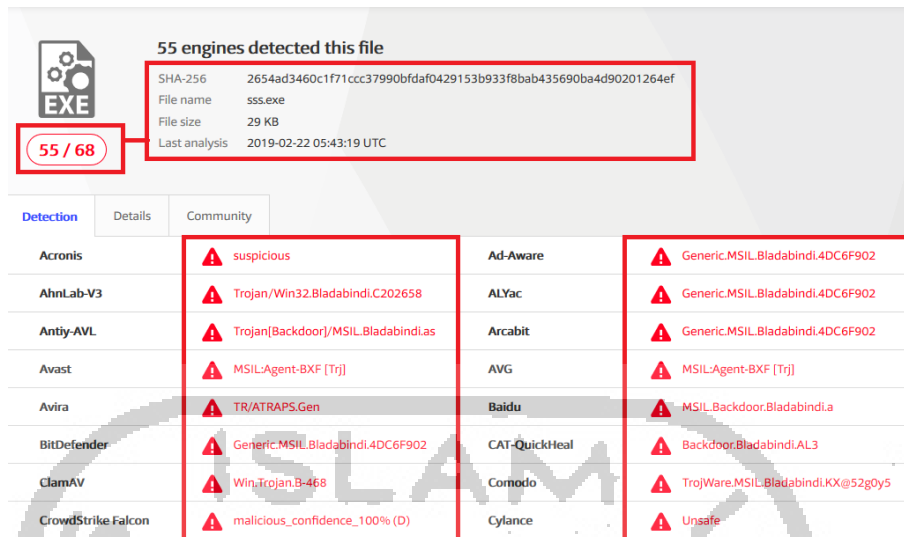
Gambar 4. 20 Hasil Propertis

Hasil propertis menunjukkan dalam bentuk Heksadecimal di Raw file data yang diinformasikan dalam bentuk Cluster disk file *malware* tersebut.



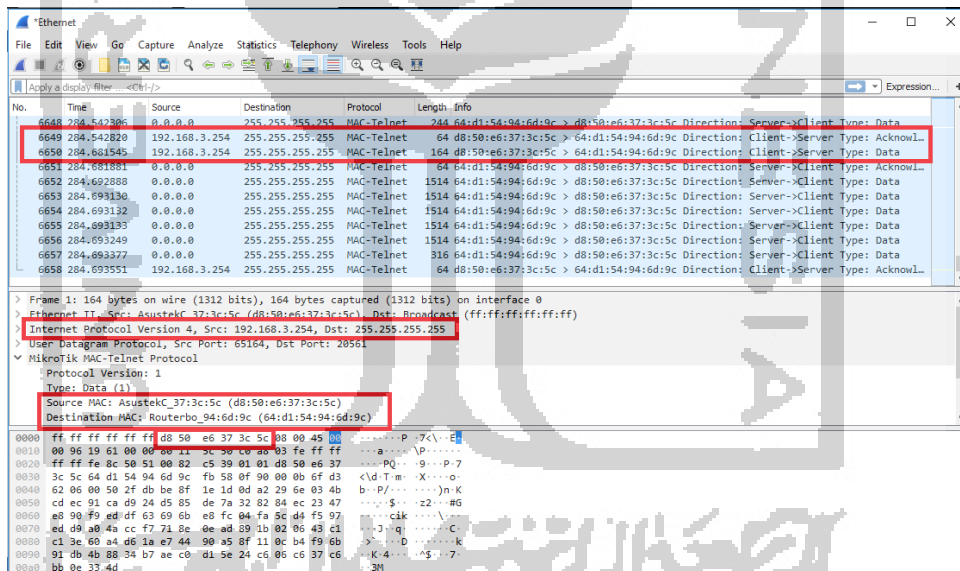
Gambar 4. 21 Analisis Hasil Hexadecimal

Selanjutnya analisis pada tools Virus Total yang membuktikan bahwa terdapat 55 file jenis *malware* yang terdapat dalam file *sss.exe* yang berhasil dideteksi yang diinformasikan dalam gambar berikut :



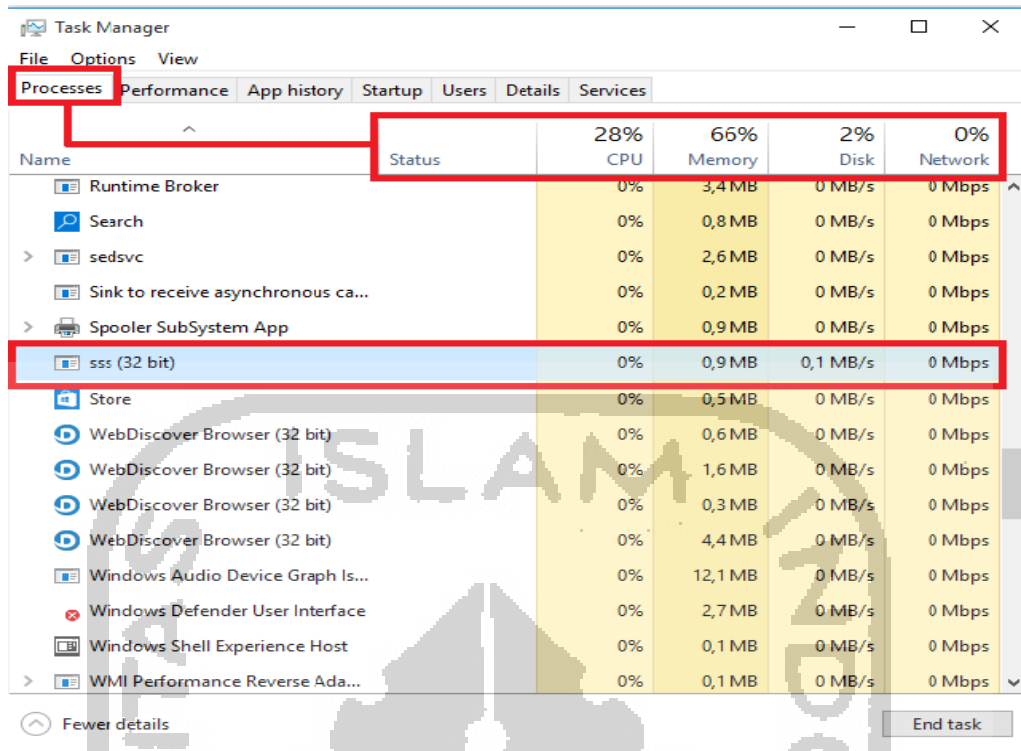
Gambar 4. 22 Hasil Analisis Virus Total

Hasil analisis selanjutnya dengan menggunakan aplikasi Wireshark yang memberikan informasi bagaimana akses penyerangan terjadi. Dalam Wireshark terlihat alamat IP Address yang menyerang laptop korban dengan Mikrotik Router yang tanpa akses internet.



Gambar 4. 23 Hasil Analisis Penyerangan

Hasil pada tahap pengujian mengenai keamanan pemblokiran *firewall traffic* dapat dilihat pada Gambar 4.24.



Gambar 4. 24 Proses Task Manager

Hasil Pengujian pada saat *task manager* berjalan di CPU, *memory*, kecepatan, paket dan status *route*. Dimana kondisi pada saat sebelum diserang, sesudah diserang tanpa dilakukan pengamanan, dan sesudah diserang dengan upaya melakukan peningkatan keamanan yang ditunjukkan pada Tabel 4.1.

Tabel 4. 1 Hasil Pengujian

Task Manager	Sebelum Diserang	Sesudah diserang	Sesudah diserang dengan keamanan
CPU	20 %	28%	20 %
Memory	1,9 GB	0,9 MB	1,9 GB
Kecepatan	1,46 GHz	539.7 kbps	1,46 GHz
Paket	9 Packet	55 Packet	9 Packet
Status Router	Normal	down	Normal

Berdasarkan taha-tahap yang dilakukan diatas, maka cara meningkatkan keamanan data yaitu :

1. Setiap user harus tahu serangan berasal dari mana, jika yang diserang lewat port 80 langkah yang harus dilakukan adalah mengganti port yang digunakan, atau mendisable port atau dimatikan.

2. Memasang firewall traffic pada laptop korban dengan penentuan IP Address, maka akan mencegah terjadinya serangan *malware* jenis njRAT ini.
3. Menggunakan anti virus berbayar yang bisa memblokir setiap program *malware* akan menyerang.

