ANALISIS SERANGAN SIBER DENGAN WIRESHARK UNTUK *NETWORK FORENSIC*

SKRIPSI

Ilham Fadilah

1710511035

PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021

ANALISIS SERANGAN SIBER DENGAN WIRESHARK UNTUK *NETWORK FORENSIC*

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

Ilham Fadilah

1710511035

PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Ilham Fadilah

NIM : 1710511035

Tanggal : 1 Juli 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Garut, 1 Juli 2021
Yang Menyatakan,

(Ilham Fadilah)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Ilham Fadilah
NIM : 1710511035
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti NonEkslusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

Analisis Serangan Siber dengan Wireshark untuk *Network Forensic*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Garut
Pada Tanggal : 1 Juli 2021
Yang Menyatakan,

(Ilham Fadilah)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama	: Ilham Fadilah
NIM	: 1710511035
Program Studi	: Informatika
Judul Skripsi	: Analisis Serangan Siber dengan Wireshark untuk Network Forensic

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Iin Ernawati, S.Kom., M.Si.	**Noor Falih, S.Kom, M.T**
Penguji I	Penguji II
Henki Bayu Seta, S.Kom., MTI.	**I Wayan Widi P, S.Kom., MTI.**
Pembimbing I	Pembimbing II
Dr. Ermatita, M.Kom.	**Yuni Widiastiwi, S.Kom., Msi.**
Dekan	Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Pengesahan : 14 Juli 2021

ANALISIS SERANGAN SIBER DENGAN WIRESHARK UNTUK *NETWORK FORENSIC*

Ilham Fadilah

ABSTRAK

Network Forensic adalah kegiatan menangkap , merekam, dan menganalisis kejadian di dalam jaringan untuk menemukan sumber dan melakukan analisis jenis dari serangan. *Network Forensic* jika dilakukan secara manual akan membutuhkan waktu yang lama dalam mengumpulkan data dan melakukan Analisa jenis serangan dan mencari IP address sumber dari serangan. Maka digunakan *tool* utnuk mengumpulkan log. Emotet adalah Trojan yang terutama disebarkan melalui email spam (malspam). Infeksi mungkin datang melalui skrip berbahaya, file dokumen berkemampuan makro, atau tautan berbahaya. Dengan muncul kembalinya malware tersebut maka diperlu diketahui bagaimana ciri-ciri log koneksi yang terjadi oleh malware tersebut maka dilakukan analisa menggunakan metode *network forensic*, setelah analisa dilakukan ditemukan bahwa malware emotet menggunakan protokol http untuk melakukan pengambilan data dari server *command center*.

Kata Kunci : *Network Forensic*, *Emotet*.

CYBER ATTACK ANALYSIS WITH WIRESHARK FOR NETWORK FORENSIC

Ilham Fadilah

ABSTRACT

Network forensics is the activity of capturing, recording, and analyzing events in the network to find the source and analyze the type of attack. Network forensics if done manually will take a long time to collect data and analyze the type of attack and find the source IP address of the attack. Then used tools to collect logs. Emotet is a Trojan that is mainly spread via spam email (malspam). Infections may come via malicious scripts, macro-enabled document files, or malicious links. With the reappearance of the malware, it is necessary to know how the characteristics of the connection logs that occur by the malware are analyzed using the network forensic method after the analysis, it was found that the emotet malware uses the http protocol to retrieve data from the command center server.

Kata Kunci : *Network Forensic, Emotet*.

KATA PENGANTAR

Penulis ucapkan rasa puji dan syukur kehadirat Allah S.W.T karena atas berkat rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi di pertengahan masa pandemi COVID-19 ini. Adapun judul untuk skripsi ini adalah:

ANALISIS SERANGAN SIBER DENGAN WIRESHARK UNTUK NETWORK FORENSIC

Selanjutnya ucapan terima kasih yang sebesar-besarnya juga ingin penulis berikan kepada pihak-pihak yang selalu sabar untuk menemani, membimbing, serta memberi saran terbaik yang mana tanpa kehadiran mereka, penulisan naskah skrippi ini tidak akan pernah selesai seperti sekarang ini. Adapun pihak terkait antara lain:

1. Kedua orang tua yang telah memberi dukungan dan semangat serta mendoakan penulis agar dapat menyelesaikan naskah skripsi ini tanpa kendala.
2. Bapak Henki Bayu Seta, S.Kom., MTI selaku dosen pembimbing satu yang membimbing penulis dalam menyusun naskah skripsi ini.
3. Bapak I Wayan Widi P., S.Kom., MTI selaku dosen pembimbing dua yang juga telah membimbing dalam penulisan naskah skripsi ini.
4. Bapak Noor Falih, S.Kom., M.T. selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
5. Ibu Iin Ernawati, S.Kom., M.Si selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
6. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta yang telah memberi ilmu yang banyak dan bermanfaat.
7. Teman-teman semua di Tim NaQoS yang telah memberi dukungan moral serta menyediakan waktu untuk melakukan diskusi tentang tugas akhir # Kiryuu-kai FOREVER.

Kemudian penulis juga menyadari bahwa penyusunan skripsi ini masih jauh dari kata sempurna, namun penulis berharap agar pihak yang membaca naskah ini mendapatkan ilmu yang dapat digunakan kelak. Dan penulis juga berharap atas kritik dan saran yang konstruktif dari pembaca.

Akhir kata, semoga Allah S.W.T memberi balasan yang berlipat ganda atas kebaikan dan jasa kepada semua pihak yang turut membantu penyelesaian naskah skripsi ini. Semoga tujuan daripada penulisan skripsi ini dapat tercapai sesuai dengan harapan.

Daftar Isi

PERNYATAAN ORISINALITAS iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS iv
LEMBAR PENGESAHAN v
ABSTRAK vi
ABSTRACT vii
KATA PENGANTAR viii
Daftar Isi ix
Daftar Gambar xi
Daftar Tabel xiii
BAB 1 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Manfaat Penelitian 3
1.5 Batasan Masalah 3
1.6 Luaran Yang Diharapkan 4
1.7 Sistematika Penulisan 4
BAB 2 6
LANDASAN TEORI 6
2.1 *Malware* 6
2.1.1 *Emotet* 6
2.2 *Network Forensic* 7
2.3 Paket Jaringan 9
2.4 Analisis Paket 10
2.5 Packet Sniffer 10
2.5.1 Wireshark 11
2.6 Mesin Virtual 11
2.6.1 VirtualBox 12
2.7 Network Addressing 12
2.7.1 IP Address 12

2.7.2 MAC Address 12
2.8 PENELITIAN SEJENIS 12
BAB 3 METODOLOGI PENELITIAN 15
3.1 Kerangka Pikir 15
3.1.1 Identifikasi Masalah 16
3.1.2 Studi literatur 16
3.1.3 Konfigurasi Sistem 17
3.1.4 Pengujian Sistem 19
3.1.5 Dokumentasi 20
3.2 Alat Bantu Penelitian 20
3.3 Jadwal Penelitian 21
BAB 4 22
Hasil dan pembahasan 22
4.1 Data 22
4.2 Proses Network Forensic 22
4.3. Analisa Data Log 27
4.3.1 Analisa Data Log 2021-01-06-Emotet-Infection.pcap 27
4.3.2 Analisa Data Log 2020-07-17-Emotet-infection-traffic.pcap 31
4.3.3 Analisa Data Log 2021-01-05-Emotet-with-spambot-traffic-part-2.pcap 34
4.3.4 Analisa Data Log 2021-01-05-Emotet-with-spambot-traffic-part-1.pcap 37
4.3.5 Analisa Data Log 2021-01-05-Emotet-Infection-with-Trickbot 40
4.3.6 Analisa Data Log 2020-08-18-Emotet-Infection-with-Qakbot.pcap 43
4.3.7 Analisa Data Log 2020-02-06-Emotet-epoch-2-with-trickbot-gtag-mor92.pcap 46
4.4 Pengujian 49
BAB 5 56
Penutup 56
5.1 Kesimpulan 56
5.2 Saran 56
DAFTAR PUSTAKA 57
RIWAYAT HIDUP 59
LAMPIRAN 60
Lampiran 1 Skor Turnitin 61

Daftar Gambar

Gambar 1. Flowchart Network Forensic *7*
Gambar 2 Flowchart Kerangka Pikir *15*
Gambar 3. Topology Jaringan Awal. *17*
Gambar 4. Topology yang akan digunakan. *18*
Gambar 5. Alur Kerja Konfigurasi *19*
Gambar 6 Konfigurasi Wireshark 1 ..... *22*
Gambar 7 Konfigurarsi Wireshark 2 ..... *23*
Gambar 8 Konfigurasi Wireshark 3 ..... *23*
Gambar 9 Contoh Data Log *24*
Gambar 10 Contoh Follow Stream TCP *25*
Gambar 11 Data Log 1 ..... *27*
Gambar 12 Follow Stream TCP Log 1 ..... *28*
Gambar 13 Export File Data Log 1 ..... *29*
Gambar 14 Virus Total Data Log 1 ..... *30*
Gambar 15 Hasil Cek File Data Log 1 ..... *30*
Gambar 16 Data Log 2 ..... *31*
Gambar 17 Follow Stream TCP Data Log 2 ..... *32*
Gambar 18 Export File Data Log 2 ..... *33*
Gambar 19 Hasil Cek File Data Log 2 ..... *33*
Gambar 20 Data Log 3 ..... *34*
Gambar 21 Follow Stream TCP Data Log 3 ..... *35*
Gambar 22 Hasil Cek File Data Log 3 ..... *36*
Gambar 23 Data Log 4 ..... *37*
Gambar 24 Follow Stream TCP Data Log 4 ..... *38*
Gambar 25 Export File Data Log 4 ..... *39*
Gambar 26 Hasil Cek File Data Log 4 ..... *39*
Gambar 27 Data Log 5 ..... *40*
Gambar 28 Follow Stream TCP Data Log 5 ..... *41*
Gambar 29 Hasil Cek File Data Log 5 ..... *42*
Gambar 30 Data Log 6 ..... *43*
Gambar 31 Follow Stream TCP Data Log 6 ..... *44*
Gambar 32 Hasil Cek File Data Log 6 ..... *45*
Gambar 33 Data Log 7 ..... *46*
Gambar 34 Follow Stream TCP Data Log 7 ..... *47*
Gambar 35 Hasil Cek File Data Log 7 ..... *48*
Gambar 36 Analisis Log Pengujian *49*
Gambar 37 Analisis Log Pengujian 2 ..... *50*
Gambar 38 Filtrasi Http.request *51*
Gambar 39 Analisis Log Pengujian 3 ..... *51*
Gambar 40 Filtrasi IP 91.211.88.52 ..... *52*
Gambar 41 Filtrasi Http.Request or Response *53*
Gambar 43 File export *54*

Gambar 42 Hasil Pengecekan File *54*
Gambar 44 Relasi File *55*

Daftar Tabel

Tabel 1 Penelitian Terkait *14*
Tabel 2 Jadwal Kegiatan Penelitian *21*