VISUALISASI SERANGAN *CYBERWAR* (*PORT SCANNING)* DALAM MENJAGA KEDAULATAN DATA INDONESIA

TUGAS AKHIR

Oleh

Ichwanul Hakim
09011281621047

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

VISUALISASI SERANGAN *CYBERWAR* (*PORT SCANNING)* DALAM MENJAGA KEDAULATAN DATA INDONESIA

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Ssatu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh

Ichwanul Hakim
09011281621047

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

VISUALISASI SERANGAN *CYBERWAR (PORT SCANNING)* DALAM MENJAGA KEDAULATAN DATA INDONESIA

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

ICHWANUL HAKIM

09011281621047

Indralaya, Agustus 2021

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Deris Stiawan, M.T., Ph.D	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 30 Juli 2021

Tim Penguji :

1. **Ketua** : **Huda Ubaya, S.T., M.T.**
2. **Sekretaris** : **Adi Hermansyah, M.T.**
3. **Pembimbing 1** : **Deris Stiawan, M.T., Ph.D**
4. **Pembimbing 2** : **Ahmad Heryanto, S.Kom., M.T.**
5. **Penguji** : **Sarmayanta Sembiring, S.SI., M.T**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Ichwanul Hakim

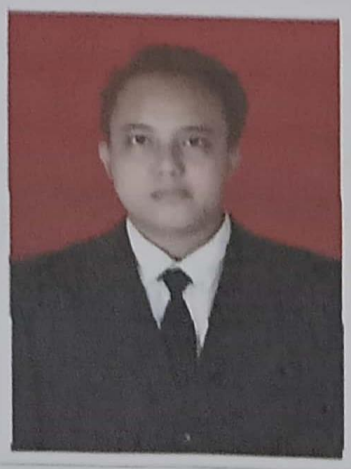
NIM : 09011281621047

Judul : Visualisasi Serangan *Cyberwar (Port Scanning)* Dalam Menjaga Kedaulatan Data Indonesia.

Hasil Penyeccekan *Software iThenticate/Turnitin* : 9 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Indralaya, Agustus 2021

METERAI TEMPEL 10000 9D80AAJX331694274

Ichwanul Hakim
NIM. 09011281621047

HALAMAN PERSEMBAHAN

"Dan Dia memberinya rezeki dari arah yang tidak disangka-sangkanya. Dan barang siapa yang bertawakkal kepada Allah, niscaya Allah akan mencukupkan (keperluan)nya. Sesungguhnya Alaah melaksanakan urusan-Nya. Sungguh, Allah telah mengadakan ketentuan bagi setiap sesuatu."

(QS. Ath-Thalaq : 3)

"Keep Moving Forward !"

Alhamdulillah, dengan izin Allah S.W.T beserta kesungguhan hati, akhirnya penelitian ini mampu diselesaikan, tugas akhir ini penulis persembahkan untuk :

1. Ibu (Netti Herawati) dan Ayah (M. Yanis) tercinta yang berjuang membesarkan, mendidik, dan selalu mengajarkan yang baik dari kecil hingga sekarang serta selalu memberikan do'a setiap saat sehingga penulis mampu menyelesaikan tugas akhir ini.
2. Adik tercinta (Putri Nadhira) yang selalu menjadi salah satu alasan penulis untuk menyelesaikan tugas akhir dan pendidikan sebagai motivasi untuknya.
3. Seluruh keluarga besar yang sudah memberikan bantuan dalam bentuk apapun kepada penulis hingga dapat menyelesaikan tugas akhir ini.
4. Dosen pembimbing terbaik sepanjang masa, Bapak Deris Stiawan, M.T., Ph.D. dan , Bapak Ahmad Heryanto, S.Kom, M.T. yang telah membimbing dan mengarahkan penulis dalam menyelesaikan tugas akhir ini.
5. Seluruh teman-teman seperjuangan terkhusus kepada teman-teman kelas SK16A yang telah membantu penulis dari awal perkuliahan hingga dapat menyelesaikan tugas akhir ini.
6. Teman-teman seperjuangan khususnya Ardin dan Sergio yang sudah membantu dalam riset penelitian ini.
7. Teman-teman LTS Ori yang selalu memberikan dukungan, semangat dan hiburan di kala sulit. Sukses terus untuk LTS Ori.

8. Teman-teman Berenang Family yang menjadi tempat berkeluh kesah dan menjadi keluarga di saat jauh dari rumah. Sungguh bersyukur bisa punya keluarga seperti kalian.
9. Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji dan syukur penulis selalu panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"Visualisasi Serangan *Cyberwar (Port Scanning)* Dalam Menjaga Kedaulatan Data Indonesia"**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad S.A.W beserta keluarga, sahabat dan para pengikutnya yang InshaAllah istiqomah hingga akhir zaman.

Selesainya penyusunan laporan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusun Tugas Akhir ini.
2. Orangtua tercinta, yaitu Ibu Netti Herawati dan Ayah M. Yanis, serta adik penulis, yaitu Putri Nadhira, serta keluarga besar penulis yang tersayang.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M.T., selaku Pembimbing Akademik.
6. Bapak Deris Stiawan, M.T., Ph.D., IPU., selaku Dosen Pembimbing I Tugas Akhir.
7. Bapak Ahmad Heryanto, S.Kom., M.T., selaku Dosen Pembimbing II Tugas Akhir.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Penulis menyadari dalam penyusunan laporan Tugas Akhir ini masih terdapat banyak kekurangan, karenanya penulis mengharapkan kritik dan saran untuk perbaikan. Semoga laporan Tugas Akhir ini dapat bermanfaat bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Indralaya, Agustus 2021

Penulis

Ichwanul Hakim

NIM. 09011281621047

VISUALIZATION OF CYBERWAR ATTACKS (PORT SCANNING) IN MAINTAINING INONESIA DATA SOVEREIGNTY

Ichwanul Hakim (09011281621047)
Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email : hakimichwanul@gmail.com

Abstract

This study focuses on checking the RAMA REPOSITORY pcap file dataset. Aims to see if there are any Port Scanning attack attempts, where Port Scanning generally occurs in the early stages of the attack, namely during the reconnaissance and intrusion processes. The attack pattern was successfully obtained based on the analysis of the pcap file datasaet traffic. There are 2 pcap file datasets that will be checked and analyzed later. The results of this analysis will later be visualized to facilitate further data traffic analysis. The results of Snort's checking of the RAMA REPOSITORY pcap file dataset found that there were a total of 622 alerts in the first pcap file dataset, 484 alerts including Port Scanning attacks. Meanwhile, in the second pcap file dataset, a total of 587 alerts were found, 480 of which were Port Scanning attacks.

Keywords : *Port Scanning, IDS Snort,* RAMA REPOSITORY.

VISUALISASI SERANGAN *CYBERWAR (PORT SCANNING)* DALAM MENJAGA KEDAULATAN DATA INDONESIA

Ichwanul Hakim (09011281621047)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email : hakimichwanul@gmail.com

Abstrak

Penelitian ini berfokus pada melakukan pengecekan terhadap *dataset file pcap* RAMA REPOSITORY. Bertujuan untuk melihat apakah ada upaya serangan *Port Scanning*, dimana *Port Scanning* pada umumnya terjadi di awal tahap penyerangan, yaitu selama proses pengintaian *(Reconnaissance)* dan penyusupan *(Intrusion).* Pola serangan berhasil didapatkan berdasarkan analisa *traffic datasaet file pcap*. Ada 2 *dataset file pcap* yang nantinya akan dicek dan dianalisa. Hasil analisa ini lah yang nantinya akan divisualisasikan agar memudahkan analisa *traffic data* selanjutnya. Hasil pengecekan *Snort* terhadap *dataset file pcap* RAMA REPOSITORY ditemukan terdapat total 622 *alert* pada *dataset file pcap* pertama, 484 *alert* diantaranya seranagan *Port Scanning.* Sedangkan pada *dataset file pcap* kedua ditemukan total 587 *alert*, 480 diantaranya adalah serangan *Port Scanning.*

Kata Kunci : Serangan *Port Scanning*, *IDS Snort*, RAMA REPOSITORY.

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi komputer dan jaringan teknologi telah memberikan kemudahan yang luar biasa bagi masyarakat hidup dalam beberapa tahun terakhir. Dengan meningkatnya kemampuan pemrosesan data komputer dan perkembangan teknologi komunikasi data yang pesat, kebutuhan akan berbagai macam sistem komputasi dan peralatan teknik tidak terbatas pada perluasan fungsi. Tapi juga meningkatnya ancaman serta semakin beragam jenis serangan di bidang *Network Security*.

Network security mencakup banyak teknologi, perangkat dan proses. Dalam istilah yang paling sederahana, ini adalah seperangkat aturan dan konfigurasi yang dirancang untuk melindungi integritas, kerahasiaan dan aksesibiitas jaringan komputer dan data menggunakan teknologi perangkat lunak dan perangkat keras. *Intrusion Detection System (IDS)* adalah suatu perangkat atau aplikasi perangkat lunak yang dapat memantau jaringan dari aktivitas yang riskan atau pengingkaran kebajikan. Degan menggunakan sistem keamanan manajemen informasi dan peristiwa, setiap pelanggaran maupun aktivitas yang mencurigakan pada umumnya dilaporkan dan dikumpulkan secara tersentralisasi [1].

Port Scanning adalah metode untuk menentukan *port* mana pada jaringan yang terbuka dan dapat menerima atau mengirim data. Ini juga merupakan proses untuk mengirim paket ke *port* tertentu pada sebuah *host* dan menganalisis tanggapan untuk mengidentifikasi kerentanan. *Port Scanning* pada umumnya terjadi di awal tahap penyerangan, yaitu selama proses pengintaian (*Reconnaissance)* dan penyusupan (*Intrusion)* [2].

Pada penelitian kali ini penulis akan melakukan ekstraksi file pcap RAMA REPOSITORY dan melakukan pendeteksian apakah ada *serangan Port Scanning* pada file pcap tersebut. Setelah melakukan ekstraksi dan deteksi dari data pcap

tersebut, penulis akan melakukan analisa trafik data hasil dari serangan yang terjadi.

RAMA REPOSITORY ialah repositori nasional milik Indonesia yang bersi laporan hasil penelitian baik berupa skripsi, tugas akhir, proyek mahasiswa (diploma), tesis (S2), disertasi (S3) ataupun laporan penelitian dosen/peneliti yang bukan merupakan publikasi di jurnal, konferensi maupun buku yang diintegrasikan dari Repositori Perguruan Tinggi dan Lembaga Penelitian di Indonesia.

1.2. Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Mengekstraksi data file *pcap* dari *traffic* RAMA REPOSITORY.
2. Mendeteksi adanya serangan *Port Scanning* pada *file pcap* RAMA REPOSITORY.
3. Membuat visualisasi dari hasil serangan *Port Scanning* pada *file pcap* RAMA REPOSITORY.

1.3. Manfaat

Adapun manfaat dari penelitian tugas akhir yang dilakukan ialah :

1. Sebagai gambaran dalam mendata *traffic data* RAMA REPOSITORY.
2. Dapat berkontribusi dalam menghadapi serangan *Port Scanning* lebih awal.
3. Dapat membantu dalam mengklasifikasi serangan pada dataset.

1.4. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, permasalahan utama yang dibahas pada penelitian ini yaitu :

1. Bagaimana menganalisa trafik pengunjung yang tercatat pada file pcap?
2. Bagaimana cara mendeteksi adanya intrusi pada suatu trafik data?
3. Bagaimana cara mendeteksi adanya serangan Port Scanning pada trafik data?

4. Bagaimana cara memvisualisasikan trafik data berdasarkan file pcap yang sudah didapatkan?

1.5. Batasan Masalah

Batasan masalah tugas akhir ini yaitu sebagai berikut :

1. *Dataset file pcap* bersumber dari *website* rama.ristekbrin.go.id.
2. Tidak mengulas tentang tindakan preventif dari serangan yang telah terjadi.
3. Serangan hanya bisa divisualisasikan ketika telah dideteksi sebelumnya.
4. Tidak bisa diujikan jika penyerang melakukan serangan melalui jalur enkripsi

1.6. Sistematika Penulisan

Berikut sistematika penulisan penelitian tugas akhir ini :

BAB I. PENDAHULUAN

Bab ini mencakup uraian dasar seperti latar belakang, tujuan penelitian, manfaat penelitian, perumusan masalah, dan batasan masalah.

BAB II. TINJAUAN PUSTAKA

Bab ini mencakup urain *Intrusion Detection System* (IDS), *Cyberwar*, *Snort*, *Port Scanning*, dan RAMA REPOSITORY.

BAB III. METODOLOGI PENELITIAN

Bab ini mencakup jalannya penelitian. Uraian pada bagian ini menguraikan langkah-langkah dalam merancang dan menerapkan metode penelitian.

BAB IV. HASIL DAN ANALISA

Bab ini akan diuraikan hasil penelitian yang sudah didapatkan dan nantinya akan dianalisa dan divisualisasikan.

BAB V. SIMPULAN

Pada bab ini berisi kesimpulan tentang penelitian yang dilakukan, serta menjawab tujuan yang hendak dicapai pada BAB I (Pendahuluan)

DAFTAR PUSTAKA

[1] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, “Intrusion detection system: A comprehensive review,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[2] J. Gadge and A. A. Patil, “Port Scan Detection,” 2008.

[3] A. S. Ashoor and P. S. Gore, “Intrusion Detection System (IDS) & Intrusion Prevention System (IPS):,” *Springer-Verlag Berlin Heidelb.*, vol. 2, no. 7, pp. 1–3, 2011, [Online]. Available: https://link-springer-com.ezadmin.upm.edu.my/content/pdf/10.1007%2F978-3-642-22540-6_48.pdf.

[4] R. Kaiser, “The birth of cyberwar,” *Polit. Geogr.*, vol. 46, pp. 11–20, 2015, doi: 10.1016/j.polgeo.2014.10.001.

[5] U. Kanlayasiri, “A Rule-based Approach for Port Scanning Detection,” *Proc. 23rd …*, 2000, [Online]. Available: ftp://158.42.249.231/viejo/pub/doc/ids/A_Rule-based_Approach_for_PortScanning_Detection.pdf.

[6] E. V. Ananin, A. V. Nikishova, and I. S. Kozhevnikova, “Port scanning detection based on anomalies,” *11th Int. IEEE Sci. Tech. Conf. "Dynamics Syst. Mech. Mach. Dyn. 2017 - Proc.*, vol. 2017-Novem, pp. 1–5, 2017, doi: 10.1109/Dynamics.2017.8239427.

[7] S. K. Patel and A. Sonker, “Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort,” *Int. J. Futur. Gener. Commun. Netw.*, vol. 9, no. 6, pp. 339–350, 2016, doi: 10.14257/ijfgcn.2016.9.6.32.

[8] S. A. Valianta, T. Salim, and D. Stiawan, “Identifikasi Serangan Port Scanning dengan Metode String Matching,” *Annu. Res. Semin.*, vol. 2, no. Fakultas Ilmu Komputer Unsri, pp. 466–471, 2016.

[9] M. O. F. Engineering, “Deep Packet Inspection using Snort Supervisory Committee Deep Packet Inspection using Snort,” 2016.