p-ISSN
e-ISSN
JURNAL
MEDIA COMPUTER SCIENCE

Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring

Analisa Perbandingan Software Wireshark dan Windump dalam Monitoring Keamanan Jaringan

Julias Sulicdio[1)]; Toibah Umi Kalsum[2)]; Yode Arliando[2)]
[1)]Study Program of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu
[2)] Department of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu
Email: [1)] : juliassulicdio3@gmail.com

How to Cite :
Sulicdio, J., Kalsum, T. U., Arliando, Y. (2022). Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring. Jurnal Media Computer Science, 1(1).

ARTICLE HISTORY
Received [30 Desember 2021]
Revised [02 Januari 2022]
Accepted [22 Januari 2022]

KEYWORDS
Wireshark, Windump, Network Security Monitoring.

ABSTRAK

Keamanan komputer adalah suatu faktor yang penting dalam dunia teknologi informasi. Keamanan jaringan komputer saat ini mulai banyak diminati oleh banyak kalangan. Jika dilihat dari segi negatifnya, maka akan semakin banyak jenis penyusupan ataupun serangan yang dapat dilakukan dalam suatu jaringan. Tujuan yang hendak dicapai dalam penelitian ini adalah perlu adanya monitoring keamanan jaringan untuk mengetahui ganguan atau ancamanan yang terjadi pada sebuah jaringan untuk meminimalisir terjadinya penyusupan. Dan hasil yang didapat dari penelitian ini software wireshark dan windump mampu memonitoring serangan ddidalam jaringan dan software yang mampu menganalisa lebih detail adalah wireshark sedangkan windump untuk menganalisa lebih jauh diperlukan ahli untuk mendapatkan hasil lebih baik

ABSTRACT

Computer security is an important factor in the world of information technology. Computer network security is currently starting to be in great demand by many people. If viewed from the negative side, there will be more types of intrusion or attacks that can be carried out in a network. The aim of this research is the need for network security monitoring to find out disturbances or threats that occur in a network to minimize intrusion. And the results obtained from this research are wireshark and windump software is able to monitoring attacks on a network and software that is able to analyze in more detail is wireshark while windump for further analysis requires experts to get better results..

PENDAHULUAN

Kemajuan teknologi dan akses Internet pada era ini memberikan keuntungan serta kemudahan bagi pengguna komputer dalam berbagi maupun mendapatkan informasi. Kini teknologi menjadi salah satu kebutuhan utama bagi manusia. Di sisi lain, semakin berkembangnya teknologi maka keamanan informasi menjadi salah satu problematika.

Keamanan komputer adalah suatu faktor yang penting dalam dunia teknologi informasi. Keamanan jaringan komputer saat ini mulai banyak diminati oleh banyak kalangan. Jika dilihat dari segi negatifnya, maka akan semakin banyak jenis penyusupan ataupun serangan yang dapat

dilakukan dalam suatu jaringan melihat perkembangan teknologi yang semakin canggih dan moderen.

Modus kejahatan didunia cyber saat ini sangat beragam. Teknik yang digunakan oleh penyerang semakin beragam dan kompleks. Bentuk serangan tersebut dapat dikelompokkan dari hal yang ringan, misalnya hanya mengesalkan sampai dengan yang sangat berbahaya. Ancaman atau serangan banyak sekali seperti Virus, Trojan, Worm, DoS, hacker, cracker, carder, sniffing, defaced, Buffer Overflow, dan sebagainya.

Salah satu bentuk eksploitasi keamanan sistem informasi adalah dengan adanya infeksi digital. Virus, Worm, Trojan Horse adalah bagian dari infeksi digital yang merupakan ancaman bagi pengguna komputer, terutama yang terhubung dengan Internet. Infeksi digital disebabkan oleh suatu perangkat lunak yang dibuat atau ditulis sesorang dengan tujuan untuk menjalankan aksi-aksi yang tidak diinginkan oleh pengguna komputer. Software tersebut sering disebut dengan malicious software atau yang disebut malware yang merupakan suatu program jahat.

Kemampuan untuk melakukan analisa malware bagi investigator menjadi tuntutan dalam setiap melakukan investigasi, hal ini dikarenakan meningkatnya jumlah malware serta evolusi dan mampu beradaptasinya terhadap perangkat analisis yang selama ini digunakan. Tujuan dari analisa malware supaya didapatkan aktivitas, pola serangan dan perilaku malware ketika berada pada jaringan seperti, port yang digunakan dan layanan yang menjadi sasaran malware.

Oleh karena itu, perlu adanya monitoring keamanan jaringan dengan tujuan untuk meminimalisir terjadinya penyusupan. Salah satu software yang paling sering digunakan oleh ahli forensik jaringan dalam melakukan monitoring adalah wireshark dan windump. karna nantinya penulis melakukan pengujian di sistem operasi Windows jadi software yang akan dipakai adalah windump. Windump merupakan versi Windows dari tcpdump. Software wireshark dan windump mempunyai interfaces yang berbeda dimana wireshark berbasis GUI dan windump berbasis Command Line. Karena alasan tersebutlah penulis sangat tertarik untuk melakukan perbandingan pada software tersebut.

LANDASAN TEORI

Pengertian Analisa

Menurut Ahmadi dan Supriyono dalam Wedianto (2016:1) Analisa adalah penelusuran kesempatan atau tantangan atau sumber. Analisa juga melibatkan pemecahan suatu keseluruhan kedalam bagian-bagian untuk mengetahui sifat, fungsi dan saling berhubungan antar bagian tersebut. Analisa sangat diperlukan atau penting karena sifat dari lingkungan sangat dinamis dan berubah dengan cepat.

Menurut Umar dalam Wedianto(2016:2) Analisa Merupakan suatu proses kerja dari rentetan tahapan pekerjaan sebelum riset didokumentasikan melalui tahapan penulisan laporan menguraikan suatu pokok menjadi beberapa bagian dan menelaah bagian itu sendiri serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan.

Menurut Adianso (2015:2) Analisa adalah mengurai suatu pokok menjadi beberapa bagian dan menelaah bagian itu sendiri serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan

Pengertian Monitoring

Menurut Suherman dalam Widiasih (2015:3) monitoring dapat diartikan sebagai suatu kegiatan untuk mengikuti perkembangan suatu program yang dilakukan secara mantap dan teratur serta terus menerus.

Menurut Prijambodo dalam Dave (2019:3) Monitoring (pemantauan) adalah kegiatan untuk mengamati perkembangan pelaksanaan program atau proyek. Dengan monitoring dapat diketahui program atau proyek berjalan sesuai atau kurang sesuai dengan rencana.

Dari uraian diatas maka dapat disimpulkan Perbandingan adalah kegiatan untuk mengamati suatu pelaksaan program atau proyek yang dilakukan secara terus menerus guna memberikan informasi kepada pengelola program apabila terjadi hambatan dan penyimpangan

Jaringan Komputer

Menurut Pratama dalam Susianto (2018:3) Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer(komputer desktop, smartphone, tablet) dan perangkat penghubung (router, switch, modem dan hub).

Menurut Wardhana (2017:2) Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Topologi Jaringan

Menurut Syafrizal (2005 : 39) Topologi jaringan atau arsitektur jaringan adalah gambaran perencanaan hubungan antarkomputer dalam local area network yang umumnya menggunakan kabel (sebagai media transmisi), dengan konektor, ethernet card , dan perangkat pendukung lainnya.

Keamanan Jaringan

Menurut Diansyah (2015:1) Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang berdiri sendiri (standalone). Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi. Namun network security biasanya bertentangan dengan network access semakin mudah, maka network security semakin rawan dan bila network security semakin baik, network access semakin tidak nyaman. Suatu network didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses kesistem komputer, sementara security didesain untuk mengontrol akses. Penyediaan network security adalah sebagai aksi penyeimbang antara open access dengan security.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode eksperimen, yang mana peneliti membuat simulasi mandiri dengan membuat website lokal berbasis media penyimpanan kemudian membuat jaringan LAN dan melakukan pengujian serangan Malware ke web server lokal apache lalu software wireshark dan windump memonitoring keamanan jaringan dari serangan malware, Kemudian penulis langsung melakukan analisa dan membandingkan kedua software tersebut.

HASIL DAN PEMBAHASAN

Analisa Perbandingan Software wireshark dan windump dalam monitoring keamanan jaringan telat selesai dibuat dengan membangun jaringan lokal dan server lokal apache kemudian

sudah dilakukan monitoring dengan pengujian menyerang server dengan menggunakan software prorat. Dan sudah dilakukan analisa lebih lanjut antara kedua Software tersebut,

Didapatkan hasil perbandingan antara kedua software tersebut, dimana dalam segi pengoperasian software tersebut sangat jauh berbeda dikarnakan perbedaan grafis yang mana software wireshark menggunakan Tampilan GUI sedangkan windump menggunakan Command Line.

Wireshark dan windump juga bisa menjadi referensi untuk para administrator dalam pemilihan software mana yang dibutuhkan, karna pada bagian software wireshark para administrator pemula tidak perlu mempunyai keahlian khusus karena sudah didukung oleh fitur grafis dengan antarmuka yang lebih mudah dimengerti, lain halnya dengan software windump para administrator dituntut lebih mendalami syntax atau baris perintah untuk menentukan protokol, port dan interfaces mana yang ingin diicapture bagi pengguna linux itu bukanlah masalah besar.

Tabel 1. Hasil Pengujian Monitoring Wireshark

No	Indikator pengujian	Hasil	Keterangan
1	Pengujian pertama (Penyerang mengirim malware ke web server apache)	1. Protokol keseluruhan yang ditangkap oleh wireshark adalah SSDP, NBNS, HTTP, TCP, IGMP, ICMP, dan MDNS 2. total hasil capture yang ditangkap wireshark adalah 433 capture 3. ukuran file pertama dari wireshark adalah 408 K	Dari segi protokol yang ditangkap wireshark lebih baik dibanding windump, tapi dari total capture dan ukuran file windump lebih baik
2	Pengujian kedua (Penyerang mencoba masuk kedalam sistem server)	1. Protokol keseluruhan yang ditangkap oleh wireshark adalah DHCP dan TCP 2. Total capture yang ditangkap oleh wireshark adalah 19 capture 3. Ukuran file pengujian kedua dari wireshark adalah 3 KB	Dari segi protokol yang ditangkap wireshark lebih baik dibanding windump, tapi dari total capture dan ukuran file windump lebih baik
3	Pengujian ketiga (Penyerang mencuri data pada directory server)	1. Protokol keseluruhan yang ditangkap oleh wireshark adalah TCP 2. Total capture yang ditangkap oleh wireshark adalah 67 Capture 3. Ukuran file pengujian ketiga dari wireshark adalah 25 KB	Terlihat pada segi protokol, total capture dan ukuran file windump lebih mengungguli dari wireshark
4	Pengujian keempat (penyerang menghapus file pada directory server)	1. Protokol keseluruhan yang ditangkap oleh wireshark adalah TCP 2. Total capture yang ditangkap oleh wireshark adalah 54 capture 3. Ukuran file pengujian keempat dari wireshark adalah 7 KB	Terlihat pada segi protokol windump dan wireshark sama, tapi dari total capture dan ukuran file windump lebih mengungguli dari wireshark
5	Pengujian kelima (Penyerang berkomunikasi dengan korban)	1. Protokol keseluruhan yang ditangkap oleh wireshark adalah TCP dan ARP 2. Total capture yang ditangkap oleh wireshark adalah 22 capture 3. Ukuran file pengujian kelima dari wireshark adalah 3 KB	Terlihat pada protokol dan total capture windump lebih mengungguli dari wireshark, tapi dari ukuran file wireshark lebih mengungguli windump

KESIMPULAN DAN SARAN

Kesimpulan

1. Analisa perbandingan software wireshark dan windump dalam monitoring keamanan jaringan telah selesai dilakukan ujicoba dan melakukan analisa perbandingan semoga bisa menjadi

referensi untuk kedepannya dalam melakukan monitoring keamanan jaringan baik itu menggunakan Software Wireshark maupun windump

2. Secara umum hasil dari ujicoba membuat jaringan dan melakukan monitoring mendapatkan hasil dimana masing-masing software wireshark dan windump bisa menangkap dan merekam jejak dari serangan cyber
3. Dan hasil yang didapatkan juga software wireshark dan windump memiliki kelebihan dan keunggulan masing-masing tergantung dari segi pemakaian user tersendiri karna perlu digaris bawahi tidak ada software yang sempurna, melainkan software wireshark dan windump ini bisa bekerja bersama dan bisa saling berkontribusi seperti software windump untuk mencapture dan software wireshark untuk menganalisa hasil dari monitoring itu tersebut

Saran

1. Diharapkan untuk penelitian selanjutnya lebih mendalami keserangan lain seperti serangan DOS, Spoofing, SQL Injection dan lain-lain
2. Melakukan perbandingan software-software lain supaya lebih membuka wawasan tentang sudut pandang serangan hacker dan rekam jejak dari serangan tersebut

DAFTAR PUSTAKA

Ainul Fuad Farhan, 2013, Wireshark, Komunitas E-learning ilmuKomputer.com.

Amat Jaedun, Metodologi Penelitian Eksperimen, Puslit Dikdasmen, Lemlit UNY, 2011.

Andre Wedianto, 2016, Analisa Perbandingan Metode filter Gaussian, Mean, dan Median Terhadap Reduksi Noise. Jurnal INFOTAMA, Vol. 12 No 1 Februari 2016 ISSN 1858-2680.

Anggita Nindya Wisnu Wardhana, 2017, Analisis Quality Of Service (Qos) Jaringan Internet Berbasis Wireless Lan Pada Layanan Indihome. Jurnal semanTIK, Vol.3, No.2, Jul-Des 2017.

Basilius Yance Pramono, 2015, Analisis Serangan Malware Menggunakan Wireshark Pada Simulasi Jaringan Di Mininet. Skripsi Sekolah Tinggi Manajemen Informatika Dan Komputer Amikom Yogyakarta.

Didi Susianto, 2015, Implementasi Dan Analisis Jaringan Menggunakan Wireshark, Cain And Abels, Network Minner. Jurnal CENDIKIA, Vol. XVI Oktober 2018 ISSN 2622-6782.

Eka Widiasih, 2015. Monitoring Dan Evaluasi Program Pelatihan Batik Brebesan. Jurnal Journal of Nonformal Education Vol. 1 No 1, Tahun 2015 ISSN 2442-532X.

Indraswuri Jogiyanto, 2015. Analisa Jaringan Hotspot Area Dengan Metode Reability Maintainabilty Avaibility. Yogyakarta.

Khairil dkk, 2013, membangun web server intranet dengan linux). Jurnal Media Infotama Vol. 9, No. 1, 1 Februari 2013, ISSN : 1858 - 2680.

Melwin Syafrizal, 2005, Pengantar Jaringan Komputer, Andi Offset, Yogyakarta, 241 halaman.

Michael Dave, 2019, Rancang Bangun Prototype Monitoring Kapasitas Air Pada Kolam Ikan Secara Otomatis Dengan Menggunakan Mikrokontroller Arduino. Jurnal IKRA-ITH Informatika Vol 3 No 2 Juli 2019 ISSN 2580-4316.

Muhammad Suyuti Ma'sum, 2017, Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol. 5, No. 1 2017.

Niko Adianson, 2015, Analisa Perbandingan Performansi RSA (Rivest Shamir Adleman) DAN ECC (Elliptic Curve) Pada Protokol Secure Socket Layer (SSL). Jurnal INFOTAMA, Vol. 11 No 1 Februari 2015 ISSN 1858-2680

Rahmat Novrianda, 2014, Analisis Forensik Malware Pada Platform Android. Konferensi Nasional Ilmu Komputer (KONIK), ISSN : 2338-2899.

Resi Utami Putri dan Jazi Eko Istiyanto, 2012, Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. IJCCS , Vol.6, No.2, July 2012, ISSN: 1978-1520

Rika Rosnelly dan Reza Pulungan, 2011, Membandingkan Analisa Trafik Data Pada Jaringan Komputer Antara Wireshark dan Nmap. Konferensi Nasional Sistem Informasi.

Sinuraya dan Heryco Bremana P Tarigan, 2019, Sistem Monitoring Jaringan Wifi Menggunakan Wireshark Pada Stmik Kni Kristen Neuman Indonesia. Jurnal UPPM STMIK Kristen Neuman Indonesia Juli 2019 p-ISSN : 2548-5997, e-ISSN : 2687-1768.

Tabu S.Kondo dan Leonard J.Mselle, 2014, Penetration Testing With Banner Grabbers and Packet Sniffers Jurnal CIS , Vol. 5 No 4 April 2014 ISSN : 2079 -8407.

Tengku Mohd Diansyah, 2015, Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark. Jurnal TIMES , Vol. IV No 2 : 20-23, 2015 ISSN : 2337 -3601.

Virgiawan A. Manoppo, 2020, Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. Jurnal Teknik Elektro dan Komputer Vol.9 No.3 September-Desember 2020, p-ISSN : 2301-8402, e-ISSN : 2685-368X.

Windump, 2021, https://www.winpcap.org/windump/docs/manual.htm. Windump User Guide, diakses tanggal 28 Oktober 2021