Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

ANALISIS KEAMANAN JARINGAN DARI SERANGAN PAKET DATA SNIFFING DI PT RADEN SYAID KANTOR POS PIAYU KOTA BATAM

Angga Novenzo Ihsana[1]
Andi Maslan[2]

[1]Mahasiswa Program Studi Teknik Informatika, Universitas Putera Batam
[2]Dosen Program Studi Teknik Informatika, Universitas Putera Batam
email: pb150210023@upbatam.ac.id

ABSTRACT

Pada era jaman moden ini hapir semua orang menggunakan internet untuk mencari data penting atau kerja, dan lain-lain. Dalam hal ini ke aman jaringan di butuhkan untuk menajaga ke stabilan dalam berinternet atau dalam berbagai transaksi yang terjadi dalam jaringan. Pada kasus ini keaaman jaringan sangat berperan penting untuk mernajaga dan menstabilkan kinerja sistem. Salah satu aplikasi yang di gunakan dalam jurnal ini adalah snort yang di mana dapat melihat paket data yang berjalan pada interface jaringan, Dan snort juga dapat memblok IP atau MAC addres yang di anggap berbahaya. Bukan cuman itu saja di penelitian ini juga menggunakan Wireshark yang di mana bisa melihat aktifitas apa saja yang berjalan pada jaringan terbut. Sehingga untuk keaman jaringan yang lebih baik. Pada peneletian kali ini untuk menguji apakah sebuah sistem telah aman atau tidak menggunakan LOIC ,NMAP, WinArpAttacker. Yang di mana aplikasi tersebut di peruntukan untuk penyerangan.

*Keyword**:** IDS; Keamanan Jaringan; Serangan Jaringan; Sniffing; Snort.*

PENDAHULUAN

Saat ini penggunaan sistem knomputer sudah menjadi kebutuhan bagi setiap individu maupun oraganisasi/perusahaan. Namun dibalik kemudahan sistem yang ada, terdapat ancaman yang dapat menggangu keberadaan sistem sehingga dapat menyebabkan shilang data/informasi, bahkan sampai terganggunya proses bisnis didalam suatu organisasi/perusahaan. Dengan hal tersebut POS atau tempat yang saat ini banyak di gunakan di Indonesia dalam hal jasa pengiriman barang , pengiriman duit secara online, pembayaran listrik, dan masih banyak fitur yang di gunakan secara online. Hal ini bisa di jadi kan niat jahat oleh para hacker yang dengan mudah membajak, merusak, dan mengedit data pada perusahaan.

Saat mengirim data dari klien ke server (atau sebaliknya), di sinilah kemungkinan terjadi tindakan sniffing. Karena itu, ketika Anda mengirim data atau menerima data melalui koneksi Internet, Anda harus selalu waspada, tidak peduli apakah ada proses transmisi, apakah ada sniffer yang mencoba mencuri data. Sulit untuk dapat memeriksa apakah Anda adalah korban

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

sniffer, tidak dapat dideteksi pada awalnya, itu hanya dapat dicegah.

Sniffing adalah bentuk cybercrime dimana pelaku mencuri username dan password orang lain secara sengaja maupun tidak sengaja. Pelaku kemudian dapat memakai akun korban untuk melakukan penupuan atas nama korban aatau meusak/menghapus data milik korban. Sering kali di lakukan dengan program sniffer yang berfungsi sebagai penganalisis jaringan dan berkerja untuk memonitor jaringan computer. Program tersebut mengatur kartu jaringan (LAN Card) untuk memonitor menangkal semua lalu lintas paket data yang melalui jaringan, tanpa mepedulikan kepada siapa paket data yang melalui jaringan, dan tanpa kepada siapa paket data tersebut di kirimkan. (Wardana:2019, 2019)

Pekerjaan mengendus-edus atau menyadap paket data yang melintas dalam sebuah jaringan. Paket data ini bisa berisi informasi mengenai apa saja, baik username atau hal-hal yang di lakukan pengguna melalui jaringan. Bisa juga untuk menganalisis hal yang menyebabkan jaringan macet. Jadi sniffing bukan sekedar untuk kejahatan, karna semuanya tergantung penggunanya. Namun, kebanyak orang yang melakukan sniffing memiliki tujuan buruk untuk mendapatkan ke untungan yang serbesar-besarnya atas data-data tersebut.

Pada dasarnya, ketika data dikirim ke tujuan di beberapa terminal, itu akan diberikan kepada pengguna lain yang tidak bertanggung jawab untuk memotong atau mengubah data atau bahkan mencuri data. Dalam proses pengembangan desainnya, sistem keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan benar agar dapat secara efektif melindungi sumber daya dalam jaringan dan meminimalkan serangan hacker atau cracker.

KAJIAN TEORI

2.1 IDS

Menurut (Adhiatma 2020) IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalarn sebuah sistern atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusion (penyusupan). Kebanyakan produk IDS merupakan sistem yang bersifat pasif, mengingat tugasnya hanyalah mendeteksi penyusupan yang terjadi dan memberikan peringatan kepada administrator Jaringan bahwa mun ada serangan atau gangguan terhadap jaringan. Akhir-akhir ini, beberapa vendor juga mengembangkan IDS yang bersifat aktif yang dapat melakukan beberapa tugas untuk melindungi host atau jaringan dari serangan ketika terdeteksi, seperti halnya menutup beberapa port atau memblokir beberapa alamat IP. Produk seperti ini umumnya disebut sebagai Intrusion Prevention System OPS). Beberapa produk IDS juga menggabungkan kemampuan yang dimiliki oleh HIDS dan NIDS, yang kemudian disebut sebagai sistem hibrid (hybrid intrusion detection system).

2.2 Serangan

Menurut) Serang terhadap security atau security attack merupakan segala bentuk gangguan terhadap keaman sistem informasi. Ada beberapa ke mungkinan serangan terhadap aspek-aspek Serangan:

a. Interruption

   Serangan jenis ini ditujukan terhadap ketersediaan (aspek availability)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

informasi.Sistem dapat dirusak, baik software maupun hardware, sedemikian rupa sehingga informasi tidak dapat diakses lagi.Contoh : penghancuran bagian perangkat keras, seperti hard disk, pemotongan kabel komunikasi.

b. Interception
Serangan jenis ini ditujukan terhadap aspek privacy dan authentication.Pihak yang tidak berwenang dapat mengakses informasi.Contoh dari serangan ini adalah "wiretapping".Contoh :serangan ini pencurian data pengguna kartu kredit.

c. Modification
Serangan jenis ini ditujukan terhadap aspek privacy, authentication, dan integrity.Pihak yang tidak berwenang dapat mengakses dan mengubah informasi.Contoh : mengubah nilai-nilai file data, mengubag program sehingga bertindak secara berbeda, memodifikasi pesan-pesan yang di transmisikan pada jaringan.

d. Fabrication
Serangan jenis ini ditujukan terhadap aspek privacy, authentication, dan integrity.Pihak yang tidak berwenang dapat menyisipkan objek palsu ke dalam sistem seperti jaringan komputer.Contoh :memasukkan pesan-pesan palsu ke jaringan, penambahan record ke file.

2.3 Aplikasi Serangan (Attack) Dan Penyadap

a. Wireshark
Menurut (Radite Bayu Prakoso 2016)Sejak didirikan pada tahun 1997 oleh Gerald Combs untuk memecahkan masalah jaringan di ISP kecil, Wireshark (awalnya disebut Ethereal) kini telah menjadi salah satu alat paling populer yang tersedia untuk analisis tingkat paket jaringan dan aplikasi protokol. Ini sebagian besar karena itu adalah solusi open source, yang membuatnya bebas tersedia untuk setiap profesional teknis, serta berbagai fitur, cakupan lebih dari 1000 protokol, dan dukungan serta peningkatan terus dilakukan mungkin dengan kontribusi dari lebih dari 800 pengembang di seluruh dunia.
Wireshark banyak digunakan untuk memecahkan masalah jaringan, untuk memeriksa keamanan jaringan, men-debug implementasi protokol jaringan dalam perangkat lunak, men-debug implementasi protokol protokol dan pembelajaran. Protokol dan banyak protokol juga digunakan untuk mengendus atau mengendus data pribadi di jaringan. Wireshark disamakan dengan media atau alat yang dapat digunakan pengguna untuk kebaikan dan kejahatan. Ini karena Wireshark dapat digunakan untuk mencari informasi sensitif pada jaringan roaming, seperti kata sandi, cookie, dll.

b. Nmap
Menurut (Brown 2019) Nmap (Network Mapper) merupakan tool opensource untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

c. Loic
Loic (Low Orbit Ion Cannon) merupakan sebuah tool atau aplikasi peretas jaringan atau open source stress testing, loic sering digunakan untuk serangan DDoS. Pada sebelumnya aplikasi loic di namai Ion Cannon dan sekarang berubah nama menjadi Loic. Loic awalnya di kembangkan oleh Praetox Technologies, namun aplikasi ini kemudian di sebar luaskan pada publik domain. Akhir-akhir ini loic menjadi populer semenjak serangan-serangan yang dilakukan hacktivitis Anonymous pada beberapa web besar. Anonymous sendiri sering menggunakan loic dalam operasinya, dan tentu saja ditambah dengan tool-tool lain dan teknik-teknik tersendiri yang hanya mereka sendiri yang tau.

d. WinARPAttacker 3.5.0
Merupakan salah satu networking tool portable yang memiliki banyak fungsi yang dapat digunakan untuk sniffing, spoofing, dan attacking pada jaringan. WinARP Attacker biasanya digunakan untuk mengirimkan suatu data/spam secara terus menerus terhadap suatu komputer (target) sehingga komputer tersebut tidak mampu lagi merespons data (spam) yang dikirimkan dan membuat komputer tersebut terputus koneksinya.

e. Snort
Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas real-time, hal ini dapat mendeteksi berbagai jenis serangan. Snort bukanlah sebatas protocol analisis atau sistem pendeteksi penyusupan (Intrusion Detection System) IDS, melainkan sedikit gabungan diantara keduanya, dan bias sangat berguna dalam merespons insiden-insiden peyerangan terhadap hosthost jaringan. Fitur Snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya.

METODE PENELITIAN

Tahap penelitian ini dilakukan sesuai dengan permasalahan yang ada pada latar belakang dan ketentuan dalam rumusan masalah yaitu bagaimana cara untuk mencegah terjadinya paket data sniffing khususnya di perusahaan PT Raden Syaid POS Batam, penganggulangan bila terjadi penyerangan, serta proses cara kerja penyusupan atau penyerangan. Berikut langkah-langkah desain penelitian yang akan dilakukan penyusun dalam proses penelitian skripsi yang berjudul “Analisis Keamanan Jaringan Dari Serangan Paket Data Sniffing Di PT Raden Syaid Kantor Pos Piayu Kota Batam”

3.1 Analisis Kebutuhan Perangkat

Dalam membangun sistem pendeteksian ini diperlukan beberapa perangkat keras dalam implementasinya.Spesifikasi di bawah ini adalah hasil dari yang di temukan pada PT Raden Syaid POS. Spesifikasi tersebut sudah cukup untuk memenuhi standard untuk pengintalan aplikasi IDS dan untuk pengintalan Aplikasi penyerangan. Berikut adalah spesifikasi yang di miliki:

1 Prosesor :Intel Core i3-4005U CPU
2. Memori :6 GB
3. Ruang : 512 GB
4. OS : Windows 7 64 bit
5. Hardware : Laptop

Selain perangkat keras diatas, agar pengujian sistem pendeteksi serangan

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

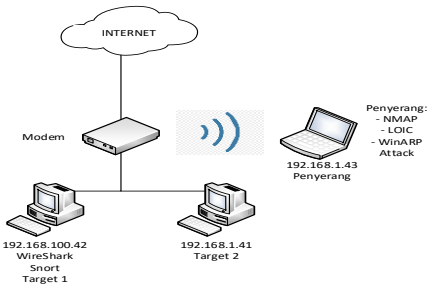
ISSN (Online) 27156265

berjalan, maka dibutuhkan perangkat keras antara lain :

1. Prosesor :Intel(R) Core ™ i5-9400F
2. Memori : 6 GB
3. Ruang : 1024 GB
4. OS : Windows 7 64 bit
5. Hardware: PC (Personal Computer)

3.2 Topologi Jaringan IDS

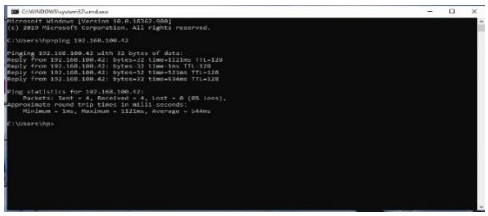
Penyusunan simulasi sistem pendeteksian serangan pada jaringan komputer dengan wireshark menggunakan metode anomally-based memakai 1 (Satu) unit laptop ,2 (dua) Personal Computer dan I (satu) buah modem wireless. Yang dapat dilihat pada gambar dibawah ini:



Gambar 1 TopologiJaringan IDS

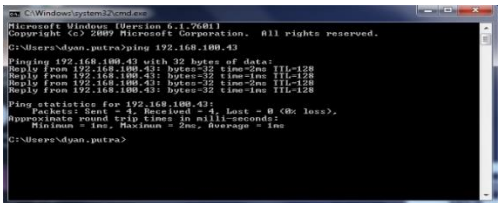
HASIL DAN PEMBAHASAN

Untuk awal akan dilakukan pengujian tanpa menggunakan aplikasi, atau untuk mengetahui apakah kedua perangkat telah terhubung dengan baik atau tidak dengan menggunakan perintah ping. IP yang digunakan pada target 192.168.100.42 dan IP pada penyerang 192.168.100.43, seperti gambar dibawah ini :



Gambar 2 Ping Ke 192.168.100.42

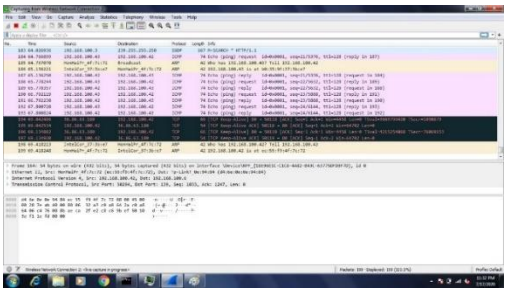
Gambar 2 menunjukkan bahwa ada reply dari IP 192.168.100.42 yang menandakan telah terjadi komunikasi antara komputer target dengan komputer penyerang.



Gambar 3 PingKe IP 192.168.100.43

Dari gambar 3 dapat dilihat juga ada reply dari IP 192.168.100.43 yang menandakan terjadinya komunikasi antara komputer target dengan komputer penyerang.

Pada pengujian ini juga akan dilakukan monitoring oleh wireshark dengan men-capture lalu lintas jaringan dalam keadaan normal atau hanya menunjukkan kegiatan lalu lintas yang biasa atau dalam hal ini hanya melakukan ping diantara kedua komputer. Dapat dilihat pada gambar 4 berikut :

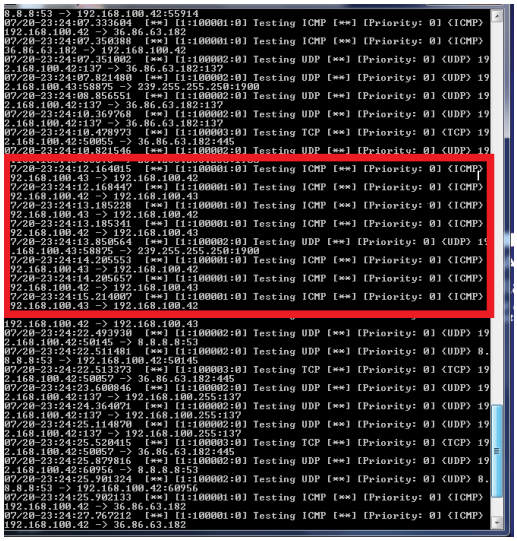


Gambar 4 Keadaan Lalu Lintas Ping

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

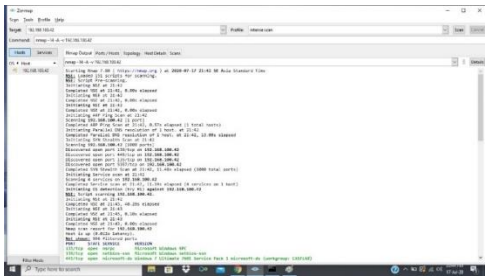


Gambar 5 Snort Mendeteksi

4.3 Pengujian Menggunakan Aplikasi

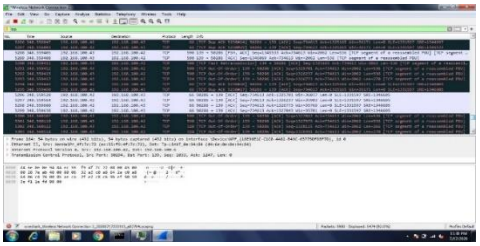
Setelah melakukan pengujian awal, maka untuk selanjutnya akan dilakukan pengujian menggunakan aplikasi, dengan melakukan penyerangan menggunakan aplikasi Nmap, Loic, dan WinARPAttack.

4.3.1 Scanning Port Menggunakan Nmap 7.12



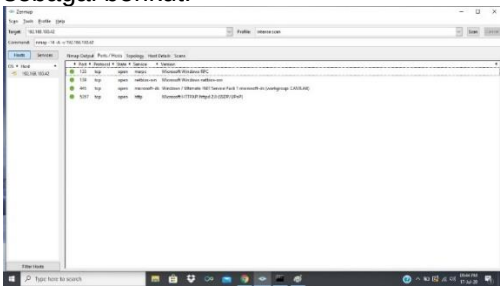
Gambar 6 Serangan Scanning Port Nmap

Nmap telah melakukan penyerangan terhadap komputer target melalui port. Dengan memasukkan IP target dan melakukan scan, maka dapat dilihat port-port yang terbuka dari komputer target.



Gambar 7 Wireshark Mendeteksi Serangan Nmap

Dari gambar 7 dapat dilihat adanya lalu lintas tidak biasa, yang menunjukkan adanya kegiatan penyerangan port scanning, dari kolom source terdapat IP dari komputer penyerang yaitu 192.168.100.43 yang melakukan penyerangan tersebut. Dan pada kolom destination adalah IP 192.168.100.42 yang merupakan komputer target. Protokol yang digunakan adalah TCP dan pada kolom info menyatakan bahwa port dari penyerang sedang melakukan scanning pada semua port komputer target, disitu kita juga dapat melihat pada port 5288 (penyerang) menuju port 348 (target), dan port 348 menuju port 5289, itu artinya bahwa port 348 dalam keadaan terbuka dengan mengirim umpan balik ke komputer penyerang dan telah siap menerima koneksi dari luar. Dari penyerangan NMAP tadi di dapat data sebagai berikut:



Gambar 8 Port/Host Sniffing NMAP

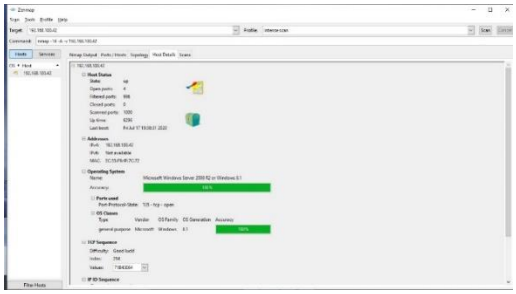
Dari data tersebut kita medapatkan bahwa terdapat 4 port terbuka pada IP 192.168.100.42 yang artinya port tersebut

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

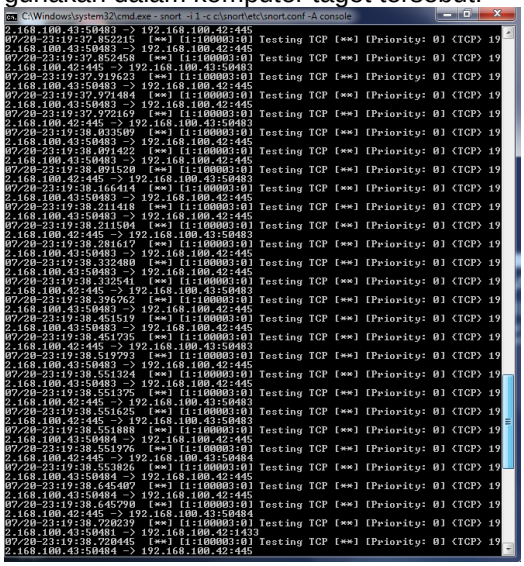
ISSN (Online) 27156265

terbuka dan dapat dengan mudah membedakan mana host dan mana client.



Gambar 9 Host Detail NMAP

Dari data hasil Scan pada IP 192.168.100.42 kita dapat meihat berapa port yang terbuka , menggunakan MAC address berapa, dan kita juga dapat melihat operating system apa yang di gunakan dalam komputer taget tersebut.



Gambar 10 Snort Membaca serangan NMAP

4.3.2 Penyerangan DDoS Menggunakan Aplikasi LOIC 1.04

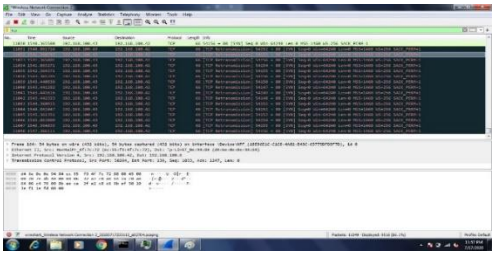
Pada pengujian kedua akan menggunakan aplikasi open sourceloic. Penyerangan menggunakan loic ini akan mengirimkan data terus menerus sehingga komputer target bisa terjadi lumpuh apabila tidak ada pendeteksian.

Gambar 11 Tampilan DDoS Attack Menggunakan LOIC TCP

Tampilan loic dapat dilihat pada gambar 11 melakukan pengiriman data dengan cara mengetikkan IP target 192.168.100.42 selanjutnya memilih port dan protokol yang akan diserang. Selanjutnya klik ready, maka data akan dikirimkan secara terus menerus ke target, hingga komputer target lumpuh.

4.3.2.1 Serangan DDoS TCP

Pada pengujian ini dilakukan penyerangan dengan mengirim data sebanyak mungkin sehingga komputer target akan meningkatnya kinerja CPU bahkan dapat terjadi hang atau bahkan padam pada komputer tersebut. Seperti gambar 12:



Gambar 12 Wireshark Mendeteksi Serangan DDoS TCP

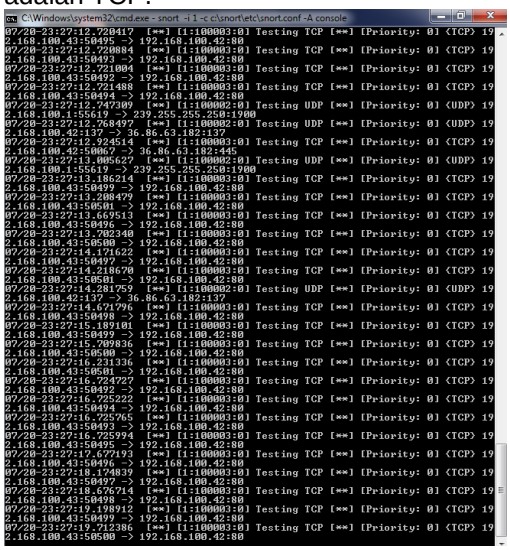
Pada gambar 4.11 adanya lalu lintas tidak biasa yang terdeteksi oleh wireshark, dari kolom source terdapat IP dari komputer penyerang yaitu 192.168.100.43 yang melakukan penyerangan tersebut. Dan pada kolom destination adalah IP 192.168.100.42 yang merupakan komputer target, dapat dilihat pada kolom

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

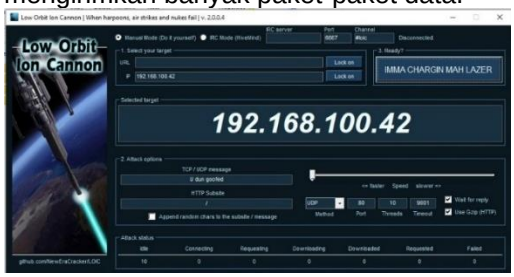
info adanya pengiriman data yang secara terus-menerus dengan inisial paket SYN dari IP 192.168.100.43 melalui banyak port ke satu port yaitu port 80 pada IP destination 192.168.100.42 sebagai target. Dan protokol yang digunakan adalah TCP.



Gambar 13 Snort Mendeteksi LOIC TCP

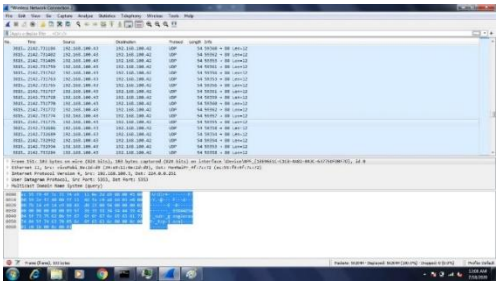
4.3.2.2 Serangan DDoS UDP

Pada pengujian selanjutnya dilakukan penyerangan DDoS juga dengan melalui protokol UDP dengan menentukan port mana yang akan diserang dengan mengirimkan banyak paket-paket data.



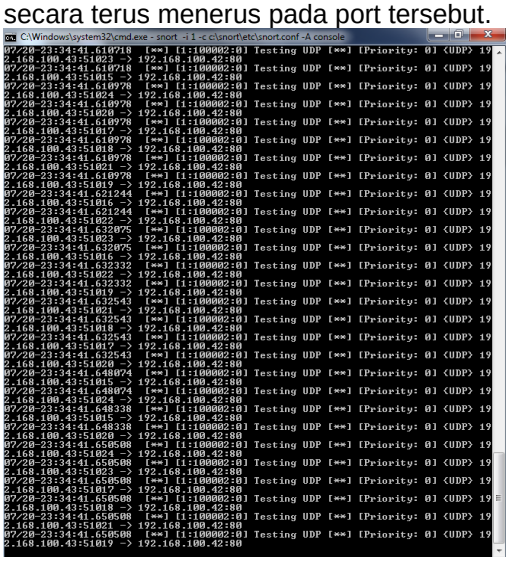
Gambar 14 Tampilan DDoS Attack Menggunakan LOIC UDP

Pada gambar 15 menunjukkan loic akan mengirimkan serangan berupa DDoS dengan mengirimkan data sebanyak-banyaknya melalui port 80, hingga komputer target menjadi lumpuh.



Gambar 15 Wireshark Mendeteksi Serangan DDoS UDP

Untuk serangan menggunakan protokol UDP pada gambar 15, wireshark dapat menunjukkan adanya kegiatan yang tidak normal yang ditandai dengan adanya IP penyerang pada kolom source yang berbeda dengan IP penyerang sebelumnya, dan menggunakan protokol UDP.Dari paket-paket jaringan dapat kita lihat pada kolom info adanya aktivitas mencurigakan yang menuju port 80 secara terus menerus dari IP 192.168.100.43, yang mana terlihat sangat banyaknya pengiriman data secara terus menerus pada port tersebut.



Gambar 16 Snort mendeteksi LOIC UDP

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

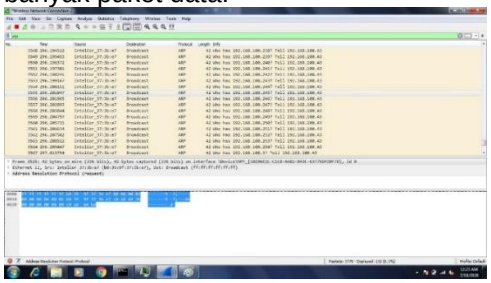
4.3.3 Penyerangan dengan WinARP Attacker 3.5.0

Pada pengujian selanjutnya saya menggunakan aplikasi WinARPattacker.Aplikasi ini memiliki banyak jenis serangan seperti yang saya jelaskan pada bab-bab sebelumnya.

Gambar 17 WinARP Melakukan Penyerangan

4.3.3.1 Serangan Scan

Pada serangan kali ini hampir sama dengan port scanning tapi pada aplikasi ini tidak men-scan port-port pada komputer target melainkan hanya host saja tetapi dengan cara mengirimkan banyak paket data.

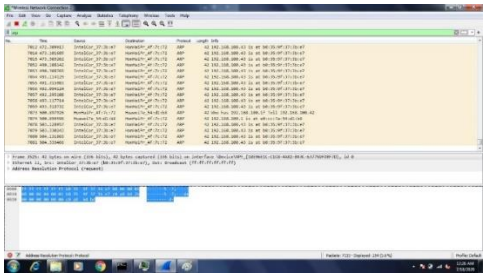


Gambar 18 Wireshark Mendeteksi Adanya Kegiatan Scan

Pada gambar 18 dapat dilihat penyerangan dilakukan dengan cara yang berbeda, dimana kolom source yang kita ketahui adalah sebagai kolom asal paket yang biasanya berisikan alamat IP dari si penyerang, tetapi pada serangan ini wireshark hanya menunjukkan nama perangkat yang digunakan saja. Pada kolom destination hanya menampilkan broadcast, dan juga pada kolom info hanya berisikan IP Who has yang secara berurutan dan tell hanya nol saja. Ini sudah sangat jelas kelihatan sekali adanya kegiatan yang tidak normal pada paket-paket yang terdeteksi yang dapat dicurigai sebagai serangan, adanya kiriman paket- paket data.Dengan menggunakan protokol ARP.

4.3.3.2 Serangan Flood

Pada serangan kali ini juga hampir sama dengan DDoS tapi pada aplikasi ini menggunakan protokol ARP pada komputer target dan juga dengan mengirimkan banyak paket data secara terus menerus.



Gambar 19 Tampilan Deteksi Penyerangan Flood

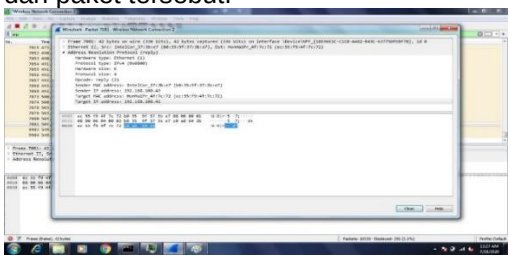
Pada gambar 19 dapat dilihat penyerangan dilakukan dengan cara yang berbeda pula, dimana kolom source yang kita ketahui adalah sebagai kolom asal paket yang biasanya berisikan alamat IP dari si penyerang, tetapi pada serangan ini wireshark hanya menunjukkan private saja bahkan tidak ada nama perangkat. Tetapi pada kolom destinationwireshark dapat menampilkan target dengan menunjukkan nama perangkat juga, dan pada kolom info hanya berisikan bila diartikan kurang lebih “serampangan ARP untuk IP target” dan ada kata Reply. Ini sudah sangat jelas kelihatan sekali adanya kegiatan yang tidak normal pada paket-paket yang terdeteksi yang dapat dicurigai sebagai serangan dan dapat kita lihat data

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

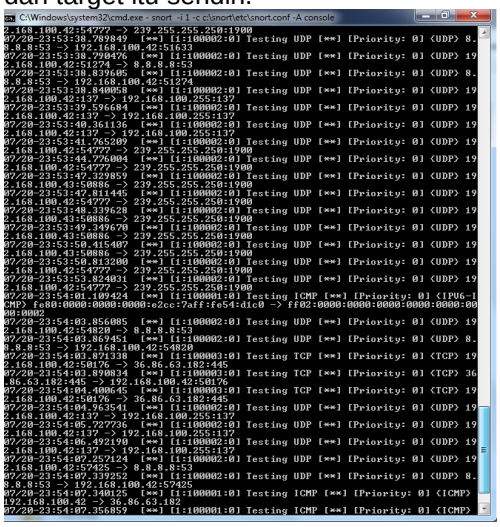
ISSN (Online) 27156265

tersebut dikirim secara terus-menerus. Bila kita double klik salah satu paket data maka akan muncul jendela keterangan dari paket tersebut.



Gambar 20 Tampilan Keterangan Paket

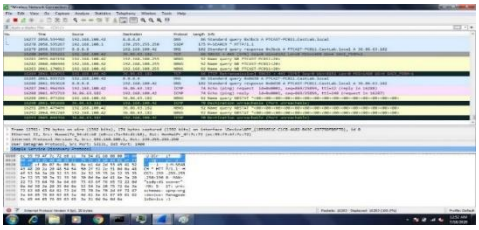
ada identitas dari IP penyerang melainkan hanya 01:01:01 begitu juga dengan MAC-nya. Tetapi yang kita lihat pada sender IP address-nya terdapat IP dari target itu sendiri.



Gambar 21 SNORT menedeteksi WinARP Attacker

4.4 Keadaan Normal

Setelah melakukan beberapa pengujian penyerangan menggunakan tiga aplikasi tersebut diatas. Pada gambar 22 akan menunjukkan bahwa lalu-lintas paket-paket data dalam keadaan normal kembali.



Gambar 22 Lalu Lintas Jaringan Normal Kembali

Dari gambar 22 menunjukkan penyerangan sudah tidak terdeteksi atau jaringan dalam keadaan normal.Dan dapat dilihat pula tidak adanya komunikasi antara IP yang berulang-ulang dalam melakukan penyerangan terhadap IP target. Baik dalam bentuk nama perangkat ataupun alamat IP. Pada paket-paket data yang melintas hanya terlihat kegiatan-kegiatan dari pemakaian untuk browsing, hubungan antar perangkat, dan lain

SIMPULAN

Pada kesimpulan ini di dapat data bahwa dengan menggunakan aplikasi snort sebagai IDS mampu untuk melihat aktifikast serangan yang terjadi pada jaringan di PT Raden Syaid Kator POS Piayu Kota Batam. Dan Wireshark juga dapat membaca serangan yang terjadi pada jaringan tersebut tetapi pada WireArpAttacker tidak bisa membaca serangan yang terjadi di sebabkan aplikasi memblokir atau hiding ip telah terjadi tetapi jika di properties maka akan timbul hasil IP tersbut. Tetapi harus mengecheck kembali atau membuka hiden yang ada di Wireshark.

Dengan aplikasi IDS terbukti bahwa IDS dapat menangkap serang baik itu serangan UDP, TCP , Flooding, dan juga Sniffing. penelitian yang telah dilakukan, rule Snort dapat mendeteksi simulasi serangan yang dilakukan. Namun pada serangan dengan intensitas 10000 paket perdetik, dengan 3 kali pengulangan

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 27156265

skenario, pesan dari telegram bot tidak dapat terkirim. Pada skenario 10000 paket per detikterjadi beban kinerja CPU dari PC (personal komputer) mencapai angka 1.05 dan network throughput dari jaringanmencapai nilai 10.5 MBps, sehingga aplikasi bot tidak mendapatkan resource terutama resource network untuk

DAFTAR PUSTAKA

Adhiatma, Nirwan. 2020. *Master CCNA: Belajar Network Itu Mudah*. nirifa pub. edited by nirifa publisher. Indonesian: nirifa publisher.

Brown, Nicholas. 2019. *Nmap 7: From Beginner to Pro*. United State, America: INDEPENDENTLY PUBLISHED.

Fachri, Barany, and Fadli Hamdi Harahap. 2020. "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan Dan Komputer." *Jurnal Media Informatika Budidarma* 4(2):413.

Parningotan, Pangabean. 2018. "Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (Ids) Untuk Optimasi Keamanan Jaringan Komputer." *JURSIMA Jurnal* 6(1).

Radite Bayu Prakoso. 2016. "Progressive Caching Content-Centric Networking Untuk Streaming Video Content-Centric Networking for Video Streaming." *RADITE BAYU PRAKOSO NRP* 1:73.

Wardana - 2019. 2019. *Belajar Pemrograman Dan Hacking Menggunakan Python*. Elex Media. edited by Elex Media Komputindo. Indonesian:

BIODATA PENULIS

Biodata[I]

PenulisI pertama,Angga Novenzo Ihsana, merupakan mahasiswa Prodi Teknik Informatika Universitas Putera Batam.

Biodata[I]

Penulis kedua, Andi Maslan, S.T., M.SI merupakan Dosen Prodi Teknik Informatika Universitas Putera Batam.