(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407

ANALISA DAN IMPLEMENTASI HONEYPOT HONEYD PADA JARINGAN WIRELESS DI FAKULTAS TEKNIK UNIVERSITAS ISLAM KUANTAN SINGINGI

Kurnia Elviani

Program Studi Teknik Informatika,
Fakultas Teknik,
Universitas Islam Kuantan Singingi, Indonesia
Jl. Gatot Subroto KM. 7 Kebun Nenas, Desa Jake, Kab. Kuantan Singingi
E-mail : kurniaelviani149@gmail.com

ABSTRAK

Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah komputer. Banyak dijumpai komputer tidak mengupdate antivirusnya bahkan ada yang tidak memakai antivirus. Teknik pengamanan jaringan biasanya dengan memblokade serangan menggunakan firewall atau mendeteksi serangan dengan IDS (Intruction Detection System), yang bertugas untuk menjaga dari serangan-serangan yang ada. Namun hanya dengan menggunakan IDS administrator jaringan akan kewalahan memeriksa setiap pemberitahuan yang diberikan oleh IDS. IDS ini bekerja hamper sama seperti antivirus, tidak mampu untuk bekerja dalam lingkungan terenkripsi atau lingkungan IPv6. Hasil penelitian yang telah dilakukan menunjukkan bahwa hasil implementasi honeypot menggunakan honeyd telah berhasil dilakukan implementasi dan konfigurasi. Beberapa jenis serangan yang dilakukan pengujian diantaranya Denial of Service attack, File Transfer Protocol attack, Internet Control Message Protocol dan scan attack. Dari ketiga jenis serangan tersebut dilakukan pengujian dilanjutkan dengan pengamatan. Pengamatan dilihat dari segi waktu yang dibutuhkan oleh honeyd berhasil menampilkan notifikasi di log honeyd ketika serangan masuk.

Kata Kunci : Honeypot Honeyd, DoS attack, Keamanan Jaringan

1. PENDAHULUAN

Teknologi informasi pada jaringan komputer yang semakin maju masih saja mempunyai masalah yang serius, yaitu faktor keamanan. Faktor keamanan begitu penting, dikarenakan tidak semua informasi data bersifat terbuka untuk umum dan tak semua orang berhak mengaksesnya. Salah satu alat bantu keamanan sistem jaringan komputer adalah dengan menggunakan honeypot untuk meningkatkan sistem keamanan. Honeypot merupakan sumber sistem informasi data yang bersifat terbuka, dan dibuat seakan-akan mirip dengan sistem sebenarnya untuk dikorbankan karena memiliki sumber informasi data palsu untuk menjebak penyerang. Dengan adanya honeypot, segala aktivitas ilegal yang dilakukan oleh penyerang dapat digunakan administrator sebagai informasi tentang penyerang untuk menganalisis, serta mempelajari aktivitas-aktivitas yang cenderung membahayakan sistem.

2. METODE PENELITIAN

2.1 Teknik Pengumpulan Data

Adapun teknik untuk pengumpulan data adalah sebagai berikut :

1. Wawancara (Interview)

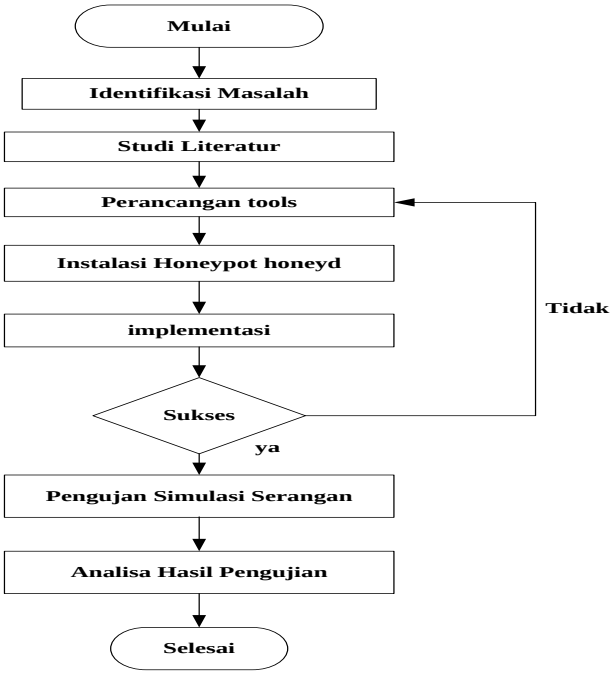
(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407

Merupakan suatu pengumpulan data yang dilakukan dengan cara tanya jawab atau dialog secara langsung dengan pihak-pihak yang terkait dengan penelitian yang dilakukan.Dalam hal ini penulis melakukan tanya jawab kepada pegawai yang ada pada Kantor Polres Kuansing Kabupaten Kuantan Singingi.

2. Pengamatan (Observasi)
   Yaitu metode pengumpulan data dengan cara mengadakan tinjauan secara langsung keobjek yang diteliti. Untuk mendapatkan data yang bersifatnya tadan meyakinkan maka penulis melakukan pengamatan langsung di Kantor Polres Kuansing Kabupaten Kuantan Singingi.
3. StudiPustaka
   Untuk mendapatkan data-data yang bersifat teoritis maka penulis melakukan pengumpulan data dengan cara membaca dan mempelajari buku-buku, makalah atau punreferensi lain yang berhubungan dengan masalah yang dibahas.

2.2 Diagram Alur Penelitian

Diagram alur penelitian yang digunakan dalam penelitian ini adalah sebagai berikut.



Gambar 1. Diagram Alur Peneliti

3. HASIL DAN PEMBAHASAN

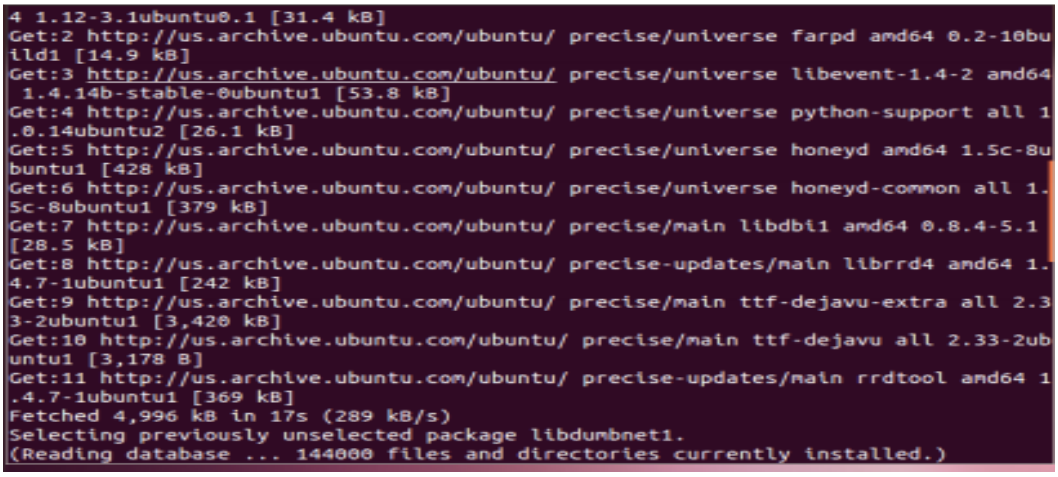
3.1 Analisa

Analisa dilakukan untuk mengetahui bagaiaman penerapan honeypot honeyd di sistem keamanan yang ada di fakultas teknik, analisa penting dilakukan karena merupakan dasar dalam merencanakan dan bagaimana serangan dilakukan untuk mengetahui celah dari sistem keamanan jaringan yang ada, dan mengetahui cara untuk mengantisipasi serangan yang ada.

3.2 Konfigurasi *Honeyd*

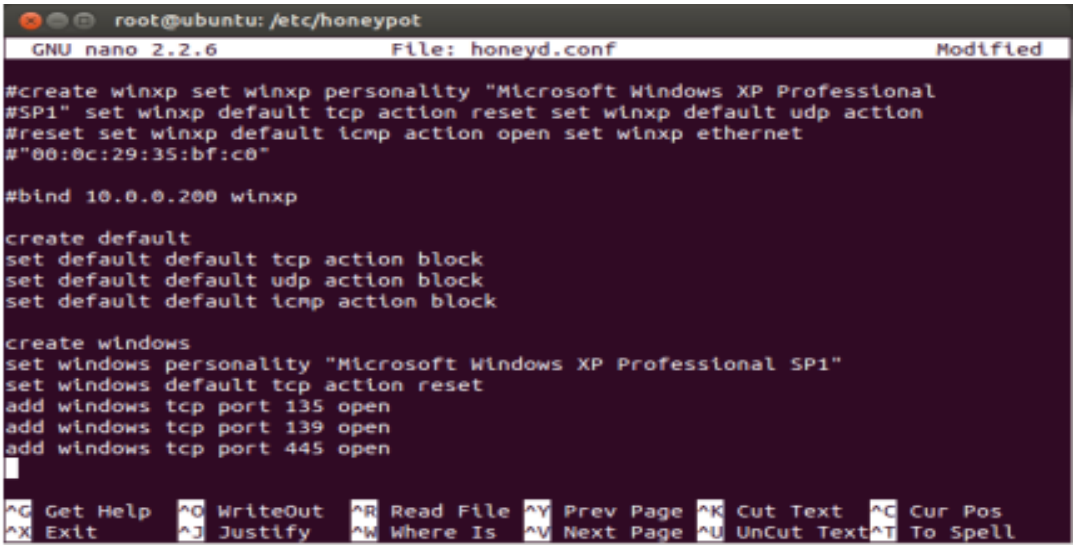
Tahap awal instalasi honeyd di honeypot dengan mengetahui lokasi file honeypot, kemudian proses instalasi dilakukan dengan format **#apt-get install honeyd**. Setalah proses instalasi berhasil maka dilanjutkan dengan proses konfigurasi honeyd.

(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407



Gambar 2. Hasil Instalasi Honeyd

Konfigurasi honeyd akan mendefinisikan beberapa hal, yang pertama adalah personality yang berarti ketika device lain terkoneksi dengan honeypot ini maka honeypot ini akan dikenali sebagai windows XP SP1. Pada template windows ini juga akan dibuka tiga ports yaitu 135,139 dan 445. Ini merupakan ports yang biasa dipakai pada windows system "action resert" adalah akan menghentikan traffic yang tidak termasuk open ports yang didefinisikan pada file konfigurasi "set windows ethernet" akan mengeset MAC address untuk honeypot, hal ini dibutuhkan jika menjalankan honeyot dengan DHCP. Pada penelitian ini,honeypot menjeadi tools utama dalam membangun sistem keamanan jaringan ini.honeypot dipilih karena dapat mengalihakan serangan dari mulanya ditujukan pada server asli ke server palsu yang di buat sendiri saat konfigurasi honeypot. File hoenyd.conf merupakan konfigurasi untuk membuat server palsu agar serangan yang agar serangan yang tertuju pada server asli dapat teralihkan.

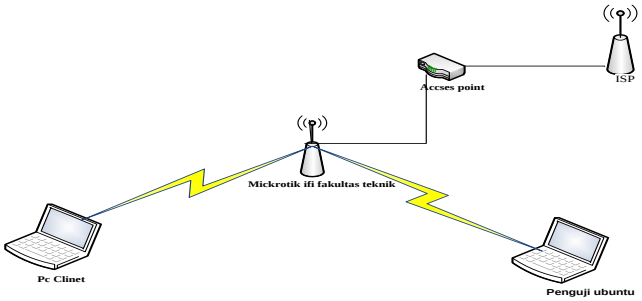


Gambar 3. Hasil konfigurasi Honeyd

3.3 Desain Topologi

Pada simulasi serangan ini menggunakan jaringan local yang terdiri dari 1 *access point* yang terhung ke ISP yang memberi jaringan internet lalu 1 mikrotik sebagai pembagi jaringan dari *access point* dan komputer penguji dan *PC client.*

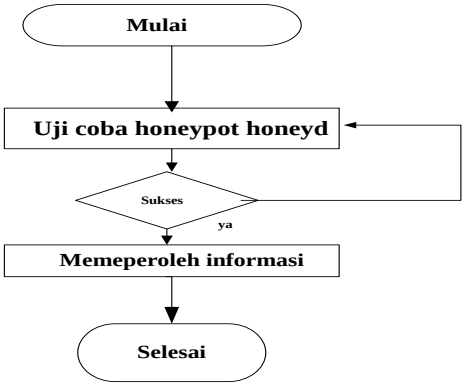
(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407



Gambar 4. Desain topologi

3.4 Flowchart Serangan

Flowchart adalah suatu bagan dengan symbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses(instruksi) dengan proses lainnya dalam suatu program. Berikut adalah flowchart untuk penerapan metode *honeypot honeyd* pada jaringan Fakultas Teknik Universitas Islam Kuantan Singingi.



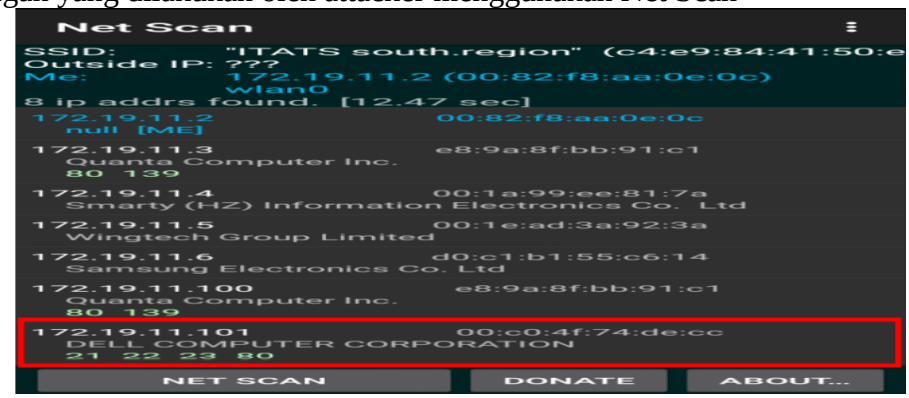
Gambar 5. Flowchart serangan

3.5 Macam –macam serangan

Adapun beberapa serangan yang akan diujikan ke jaringan Fakultas Teknik antara lain :

1. Scanning Host dan Port

Pengujian serangan yang akan dilakukan adalah host scanning dan port scanning yang bertujuan untuk mengetahui host yang sedang aktif. Berikut adalah proses scanning host dan port pada jaringan yang dilakukan oleh attacker menggunakan Net Scan



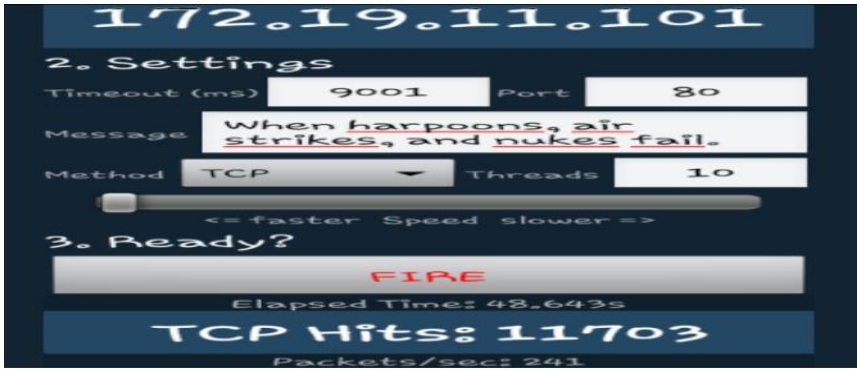
Gambar 6. Proses Scanning Host dan Port

(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407

terlihat bahwa scanning yang dilakukan Netscan dapat mendeteksi dengan baik host yang diciptakan oleh honeyd, pada proses scanning terlihat bahwa beberapa port host honeyd dengan ip 172.19.11.101 dapat terdeteksi dengan baik oleh Netscan yaitu port 21 untuk ftp, port 22 untuk ssh, port 23 untuk telnet dan port 80 untuk http.

2. Serangan Tcp Flood

Berikut adalah proses serangan TCP flood pada host honeyd yang dilakukan oleh attacker menggunakan Loic.

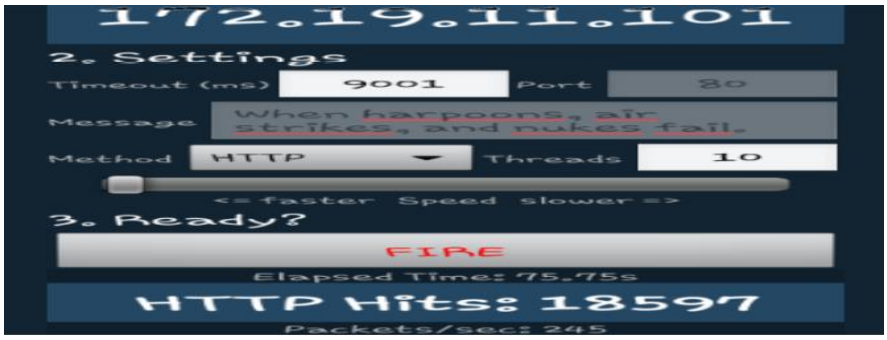


Gambar 7. Proses Serangan Tcp Flood dengan Loic

terdapat ip honeyd yang akan diserang yaitu ip 172.19.11.101, port 80, method yang digunakan adalah TCP, threads yang diisikan 10, serta pengaturan kecepatan penyerangan dengan merubah slider kearah faster.

3. Serangan Http Flood

Berikut adalah proses serangan Http flood pada host honeyd yang dilakukan oleh attacker menggunakan Loic.



Gambar 8. Proses Serangan Http Flood dengan Loic

3.6 Solusi dari serangan

1. Scaning host dan port
   Solusi atau pencegahan untun scaning host dan port ini adalah memastikan kalau port tidak terbuka atau jika sudah terlanjur terbuka bisa diganti dengan port lain seperti port 21 (FTP), 22 (SSH), 23 (telnet), 80 (www/http) dengan tujuan untuk memancing attacker masuk / mengakses port tersebut.
2. ftp flood,http flood,udp flood
   jenis ketiga seranga dia tas merukan bagian dari serangan *Ddos attack* dapat ditarik

(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407

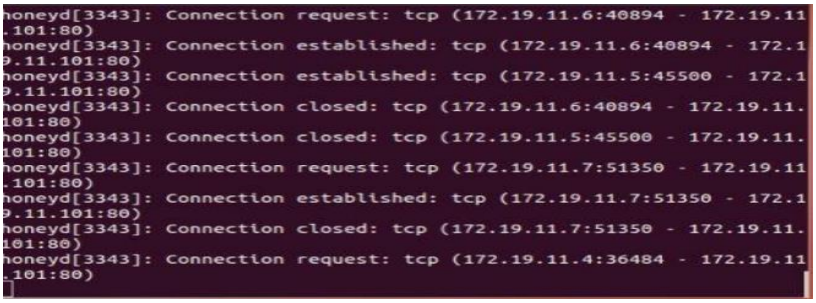
kesimpulan bahwa untuk menghindari banjir flod jaringan terhadap upaya cracking, maka ada beberapa hal yang harus dilakukan, diantaranya :

a. Melakukan Identifikasi Serangan, serangan akan terlihat tanda-tandanya jika mengecek server. Apabila sudah diketahui, alangkah baiknya mempersiapkan penangannya sebelum terjadi serangan yang lebih serius.
b. Syn Flooding, gunakan firewal untuk tidak meneruskan paket data yang tidak diketahui dengan jelas asalnya.
c. Remote Controled Attack, block alamat IP dan portnya.
d. UDP Flooding, Menolak paket trafik yang datang dari luar jaringan dan mematikan semua layanan UDP.
e. Smurf Attack, disable broadcast address pada router atau filtering permintaan ICMP echo request pada firewall atau juga membatasi trafik ICMP.
f. Mempertahankan Parameter Network, salah satunya dengan memperbesar bandwith. Cara ini hanya memberikan waktu supaya sistem tidak down, tetapi cara ini kurang ampuh terhada serangan yang besar.

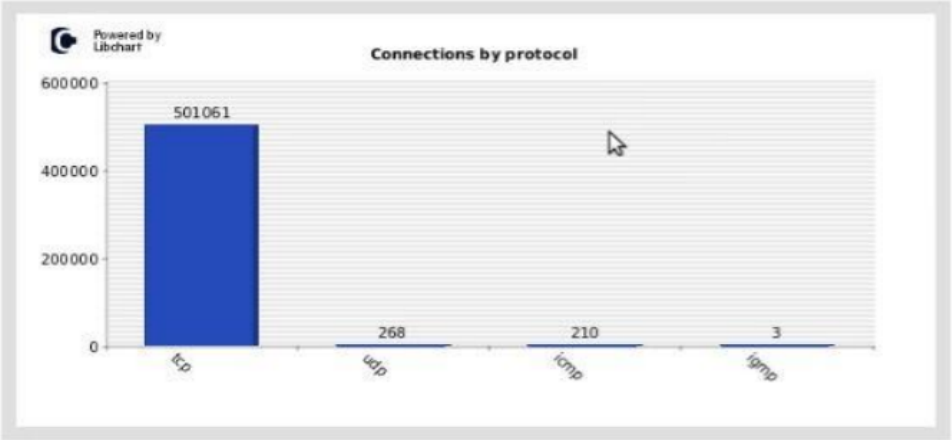
3.7 Hasil Implementasi

1. Tanggapan honeyd dari pengujian tcp flood

Dari gambar di bawah ini menjelasakan bahawa koneksi yang masuk ke honeypot 3343:Id trafik yang berhasil masuk ke dalam sensor *honeypot Honeyd*, connection: status yang di terima Tcp : Protokol yang digunakan, 533371: Waktu masuknya trafik dalam bentuk *timestamp*, 172.19.11.101 : ip target, 139 : Port yang dimasuki, 172.19.11.6: IP penyerang, 80 : Port yang digunakan si penyerang untuk masuk.



Gambar 9 . Proses Honeyd Mendeteksi Serangan Tcp Flood



Gambar 10. Tcp flood Honeyd-viz koneksi dengan protocol

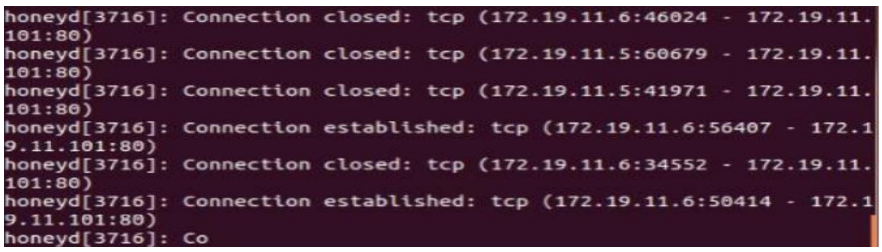
(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407

terlihat bahwa koneksi dengan protocol tcp sebesar 501061, udp sebesar 268, icmp sebesar 210 dan igmp sebesar 3 dan jika tidak ada yang melakukan serangan makan terlihat di protocok koneksi akan kosong tidak ada warna birunya.

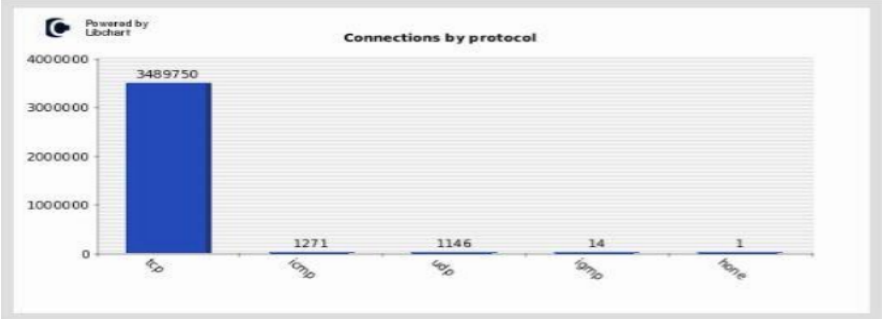
2. Tanggapan honeyd dari pengujian http flood

Untuk melakukan serangan ini, penyerang menggunakan loic, kemudian melakukan seranga ke IP server dengan mengirim paket yang ukurannya besar. Serangan dilakukan dengan cara mengirim paket ICMP yang berlebih secara berturut-turut terhadap server. Tujuan penyerangan ini membuat sistem menjadi crash dan hang. Teknis penyerangan ini adalah ketikkan pada terminal: ping -f -s . Proses penyerangan tersebut penulis uraikan sebagai berikut :

1) Penyerang dengan IP 172.19.11.101 melakukan serangan terhadap laptop
2) target dengan beberapa ip yang berhasil dideteksi oleh honeypot honeyd



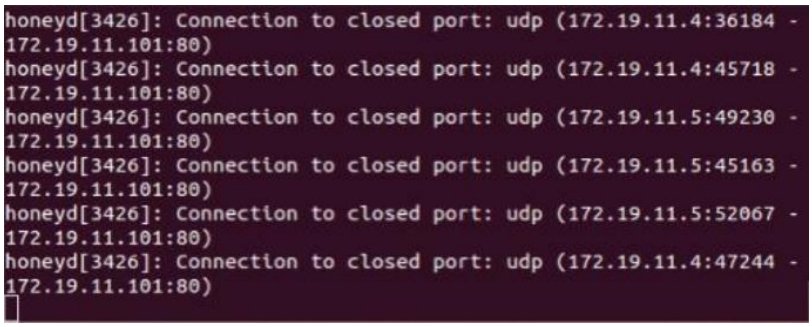
Gambar 11. Proses Honeyd Mendeteksi Serangan Http Flood



Gamba 12 Http flood Honeyd-viz koneksi dengan protokol

terlihat bahwa koneksi dengan protocol tcp sebesar 3489750, icmp sebesar 1271, udp sebesar 1146, igmp sebesar 14.

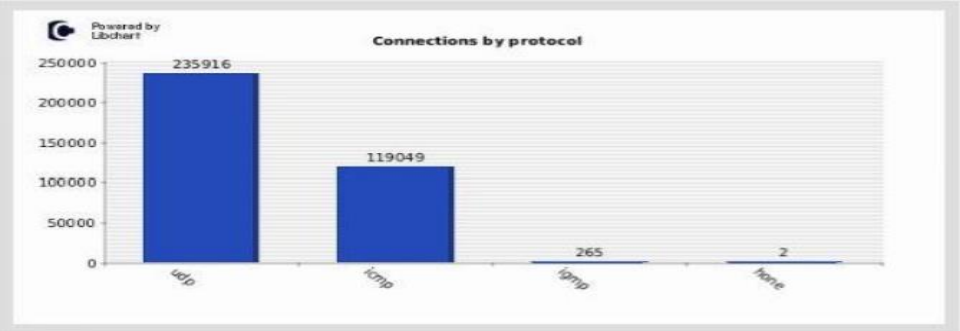
3. Tanggapan honeyd dari pengujian Udp flood



Gambar 13. Proses Honeyd Mendeteksi Serangan Udp Flood

(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407

merupakan proses honeyd dalam mendeteksi serangan yang terjadi. Terlihat beberapa ip yang melakukan akses terhadap honeyd yang mempunyai ip 172.19.11.101 dan port yang dituju adalah port 80 dengan method yang digunakan adalah Udp



Gambar 14. Udp Flood Honeyd-Viz Koneksi Dengan Protokol

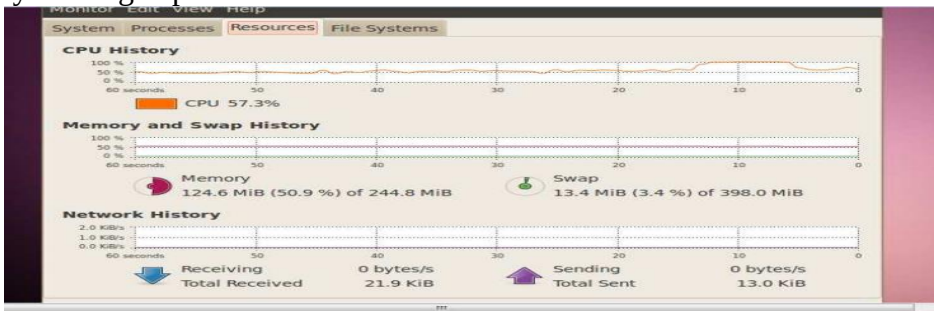
Kesimpulan dari 3 serangan di atas adalah Hasil serangan yang dilakukan melalui PC attacker membuktikan bahwa attacker tidak memperoleh data apapun yang umumnya ditunjukkan adanya packet loss. Sedangkan dari sisi komputer server honeyd akan menampilkan IP penyerang sampai penyerangan pada komputer atau PC attacker berhenti dengan sendirinya tanpa memperoleh apapun. Selanjutnya pada komputer server honeyd dapat dilakukan pengamatan terhadap log yang tersimpan pada file log honeyd yang berisi catatan atau notifikasi dari serangan DoS dimana sebelumnya dilakukan percobaan serangan terhadap komputer server honeyd dan attcaker akan masuk ke server palsu honeypot yang sengaja di buat dan juga Berdasarkan analisis log honeyd di web interface, terdapat informasi aktivitas yang dapat digunakan administrator untuk observasi menentukan kebijakan dalam mengamankan jaringan. Hasil pengujian ini berhasil dilakukan dengan menunjukkan laporan aktivitas serangan yang terjadi dengan tampilan grafik.

3.8 Sebelum dan Sesudah Diterapkannya Honeypot.

Pada PC server honeypot juga dapat melakukan monitoring jaringan untuk mengetahui kondisi sebelum dan sesudah atau saat terjadinya serangan melalui tool sistem monitor.

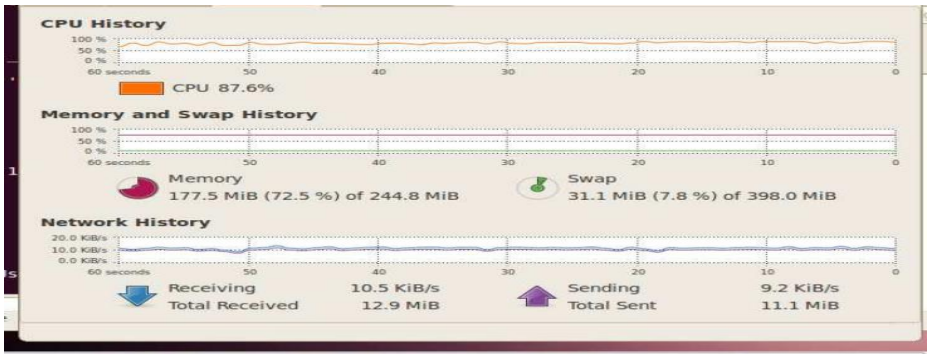
3.9 Kondisi Sebelum Terjadinya Serangan

Berdasarkan hasil pengujian dari serangan yang telah dilakukan pada perancangan sistem keamanan jaringan dalam Tugas Akhir ini terlihat bahwa adanya dampak yang mengganggu sisi performance pada sistem kinerja server dapat dilihat dengan meningginya proses pada memory, processor, swap dan traffic pada jaringan. Gambar 15 memperlihatkan sisi performance pada sistem server ketika dalam keadaan normal yaitu ketika belum terdeteksinya serangan pada server .



Gambar 15. Keadaan Sistem Server Dalam Keadaan Normal

(JuPerSaTeK)
Jurnal Perencanaan, Sains, Teknologi, dan Komputer
Media Cetak : 2622-108X
Media Online : 2622-5980
FAKULTAS TEKNIK (UNIKS)
Vol. 4, No. 2, Desember 2021, Hal : 1398 - 1407



Gambar 16. Keadaan Sistem Server Ketika Setelah Dilakukan Serangan

Sistem monitor ini secara tidak langsung turut membantu mengetahui sebelum dan saat terjadinya serangan pada PC server honeypot, sedangkan file log honeyd memberikaninformasi secara detail bentuk serangan, port dan asal IP attacker berasal dan interface honeyd-viz melengkapi report dalam bentuk grafik

4 PENUTUP

4.1 Kesimpulan

Dari penelitian berupa analisa pada sistem keamanan jaringan yang telah dilakukan maka dapat ditarik kesimpulan bahwa:

1. Implementasi honeypot honeyd pada sistem keamanan jaringan dapat membantu meningkatkan keamanan pada server dan dapat membantu administrator dalam menganalisa, melakukan tindakan pencegahan hingga membuat kebijakan.
2. File log yang ada pada sistem honeyd dapat memberikan informasi detail baik IP address attacker, port dan apa saja yang dilakukan oleh attacker untuk selanjutnya dilakukan analisa.
3. Sistem monitor dan honeyd-viz juga mambantu dalam memberikan informasi dalam bentuk trafik dan gambaran grafis sebagai gambaran sebelum dan saat terjadi serangan.

DAFTAR PUSTAKA

Aminanto, Alja, and Wiwi Sulistyo. "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery." *Jurnal Teknologi Informasi*, Agustus 2019.

Arif Hidayat, Ismail Puji Saputra. "ANALISA DAN PROBLEM SOLVING KEAMANAN ROUTER MIKROTIK RB750RA DAN RB750GR3 DENGAN METODE PENETRATION TESTING." *JURNAL RESISTOR*, 2018.

Bambang Pujiarto, Ema Utami, Sudarmawan. "EVALUASI KEAMANAN WIRELESS LOCAL AREA NETWORK." *JURNAL DASI*, Juni 2013.

Bambang Pujiarto, Ema Utami, Sudarmawan. "Evaluasi Wireless Local Area Network." *JURNAL DASI*, Juni 2013.

Daulay, Muhammad Iqbal. "analisa perbandingan keamanan WEP, WPA, WPA2 pada access point." 2019.

Dermawati, Rosi, and M. Hasim Siregar. "Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik Uniks Menggunakan Dionae Sebagai Keamanan Jaringan." *Jurnal Ilmiah Edutic*, n.d.

firar, Urdirartatmo. *Trik Menjebak Hacker Dengan Honneypot.* yogyakarta: ANDI OFFSET, 2005.

Gilvan Januar Sirait, and Indrastanti R. Widiasari, M.T. "Analisis Keamanan Jaringan Wireless Local Area Network dengan Metode." 2018.

Imam Kreshna Bayu, Muh. Yamin, LM Fid Aksara. "Analisa Keamanan Jaringan Dengan." Juli-Desember 2017: 69-78.

Imam Kreshna Bayu, Muh. Yamin, LM Fid Aksara. "ANALISA KEAMANAN JARINGAN WLAN DENGAN." Juli-Desember 2017: 69-78.

Michael, Ikhwan Ruslianto, and Rahmi Hidayati. "ANALISIS PERBANDINGAN SISTEM KEAMANAN JARINGAN WI-FI." *jurnal komputer dan aplikasi*, 2021.

Muhammad Addy Rahmadani, Mochammad Fahru Rizal , Tedi Gunamawan. "IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN." *e-Proceeding of Applied Science*, Desember 2017: 17-67.