PERBANDINGAN *INTRUSION PREVENTION SYSTEM* (IPS) PADA LINUX UBUNTU DAN LINUX CENTOS

Suryayusra [1)], Dedi Irawan [2)]
[1]Program Studi Teknik Informatika, Universitas Bina Darma, Palembang
[2]Program Studi Sistem Informasi, Universitas Bina Darma, Palembang
e-mail: *[1]suryayusra@binadarma.ac.id, [2]dedi.irawan@binadarma.ac.id

Abstrak

Perkembangan teknologi yang Semakin hari semakin meningkat, kita di tuntut untuk meningkatkan system keamanan jaringan yang kita miliki, karena semakin mudahnya orang bisa mengetahui tentang hacking dan cracking dan juga didukung oleh tools yang mudah didapatkan secara gratis. Dan untuk mencegah hal itu kita harus megamankan jaringan yang kita gunakan, untuk mengamankan jaringan tersebut peneliti menggunakan sebuah metode keamanan yang bernama Intrusion Prevention System (IPS), merupakan media yang banyak digunakan dalam membangun sebuah system keamanan komputer, lalu IPS di gabungkan dengan menggunkan Teknik firewall dan metode Intrusioan Detection System, dalam penelitian ini penulis menggunakan sistem operasi Linux yaitu Ubuntu dan CentOS, karena linux merupakan software yang bersifat free/opensource sehingga untuk memperolehnya dapat diunduh secara gratis. Pada awalnya linux merupakan system operasi yang cocok untuk jaringan tapi sekarang linux sudah berubah menjadi system operasi yang tidak hanya handal dari segi jaringan dan server tapi juga sudah menjelma menjadi sistem operasi yang enak dipakai di lingkungan desktop baik untuk keperluan pribadi atau bahkan untuk perkantoran. Untuk mengamankan jaringan tersebut menggunakan sebuah mtode keamanan yaitu Intrusion Prevention System (IPS), juga dibantu dengan sebuah tools dalam sistem Operasi Linux yang berfungsi sebagai alat untuk melakukan filter (penyaring) terhadap lalulintas data (trafic), yaitu IPTables. Hasil dari penelitian yang dilakukan Linux CentOS lebih aman di bandingkan Linux Ubuntu, dikarnakan juga Linux Ubuntu sering melakukan pembaruan, yang dapat mempengaruhi rules yang telah dibuat.

Kata Kunci : Keamanan Jaringan; Intrusion Prevention System; Linux; Ubuntu; Centos

Abstract

Technological developments are increasing day by day, we are required to improve our network security system, because the easier it is for people to find out about hacking and cracking and it is also supported by tools that are easily available for free. And to prevent that we have to secure the network that we use, to secure the network researchers use a security method called the Intrusion Prevention System (IPS), which is a medium that is widely used in building a computer security system, then IPS is combined with using techniques. firewall and Intrusioan Detection System method, in this study the author uses the Linux operating system, namely Ubuntu and CentOS, because Linux is a free / opensource software so that it can be downloaded for free. Initially, linux was an operating system suitable for networking, but now linux has turned into an operating system that is not only reliable in terms of networks and servers but has also been transformed into an operating system that is comfortable to use in a desktop environment for personal use or even for offices. To secure the network using a security method, namely the Intrusion Prevention System (IPS), it is also assisted by a tool in the Linux operating system which functions as a tool for filtering data traffic, namely IPTables. The results of research conducted on CentOS Linux are safer than Ubuntu Linux, because Ubuntu Linux also frequently updates, which can affect the rules that have been made.

Keywords*: Network Security; Intrusion Prevention System; Linux; Ubuntu; Centos*

I. PENDAHULUAN

Perkembangan teknologi yang sangat pesat menuntut meningkatnya kualitas kemanana jaringan. Terutama dengan semakin terbukanya pengetahuan tentang hacking dan cracking yang didukung tools yang bisa didapatkan secara mudah dan gratis [1]. Banyaknya bermunculan komunitas group *hacking* dan *caracking* yang dibentuk, menjadi suatu ancaman tindak kejahatan terhadap sistem keamanan informasi. Tidak hanya orang-orang yang menguasai Teknologi Informasi (TI) yang mampu melakukan tindak kejahatan *(Cyber Crime)*. karena semakin terbukanya ilmu pengetahuan tentang hacking dan cracking menuntut kita untuk meningkatkan sistem keamanan yang mampu memonitoring lalu lintas jaringan dan mem-block aktivitas-aktivitas yang mecurigakan. Selain itu yang menjadi ancaman keamanan jaringan komputer juga datang dari virus, trojan, DOS, TCP/IP, spoofing, repliying, malicius, spamming, dan lainya. Hal inilah yang mengancam sistem keamanan jaringan dimana data dapat diambil dan dirusak bahkan dihapus oleh attacker. Pada tahun 2018, jumlah kasus pencurian data yang dilakuan oleh hacker sebanyak 945 kasus. Sementara, pada 2017 kasus pencurian data mencapai 1.162 kasus. Gemalto melaporkan, jumlah data yang dibobol oleh hecker per harinya mencapai 6,9 juta data. Hal ini berdasarkan laporan pencurian data sejak 2013 hingga 2018 yang jumlahnya sebanyak 14,6 miliar. Dari sekian banyak, hanya 4 persen dari jumlah tersebut yang dilindungi enkripsi oleh pemiliknya [2].

Oleh karna itu diperlukan sistem keamanan yang bisa mendeteksi dan mengatasi serangan-serangan yang dilakukan attacker (penyerang), dan untuk mengatasi hal tersebut penulis memilih menggunakan system/metode yaitu instruksion Prevention System (IPS) bertindak sebagai Firewall yang akan menerima atau menolak paket yang masuk, dan akan di masukan ke dalam IPTables. IPTables adalah suatu tools dalam sistem Operasi Linux yang berfungsi sebagai alat untuk melakukan filter(penyaring) terhadap lalulintas data (trafic), dan IPTables mampu dijadikan sebagai metodelogi Intrusion Prevention System (IPS) yang memiliki kemampuan memeriksa dan mencatat semua paket data, dan menolak akses yang teridentifikasi yang kemungkinan packet dari seorang attacker salah satunya seperti virus, trojan, DOS, TCP/IP Spoofing Repliying, spaming atau kejahatan lainya. IPTables juga terdapat dibeberapa sistem operasi Linux yaitu Ubuntu, CentOS, Red Hat, Fedora, dan sebagainya.

Dari penelitian sebelumnya berjudul Perbandingan Intrusion Prevention System (IPS) Pada Linux Server dengan Mikrotik RouterBoard. Dalam mengatasi serangan DDoS Linux Server lebih baik dibanding Mikrotik RouterBoard, dari segi deteksi Linux Server dan Mikrotik RouterBoard mempunyai kemampuan yang sama, akan tetapi pada presentase CPU Usage Mikrotik RouterBoard bekerja lebih keras dibanding Linux Server, dan juga pada saat pencatatan Log Mikrotik hanya bertahan 8 Menit, sedangkan pada Linux Server selama 10 menit pengujian Linux Server masih bisa mencatat Log. Mengutip dari hasil penelitian tersebut bahwa Linux server lebih baik dibanding Mikrotik RoauterBord. Maka penulis akan meneliti sistem operasi Linux manakah yang lebih baik dalam mengatasi serangan Brute Force [3].

Dari penjelasan diatas maka penulis akan melakukan analisis "Perbandingan Intrusion Prevention System (IPS) Pada Linux Ubuntu Dan Linux Centos" tujuan dari penelitian ini nanti adalah merancang sistem keamanan jaringan yang lebih aman, dan melakukan perbandingan IPTables yang diimplementasi pada linux Ubuntu dan Linux CentOS.

II. TINJAUAN PUSTAKA

2.1 Analisis Perbandingan

Dalam Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan bahwa perbandingan berasal dari kata banding yang artinya persamaan. Selanjutnya kalimat membandingkan mempunyai arti dua benda untuk mengetahui persamaan atau selisihnya. Tujuan menbandingkan untuk mengetahui kelebihan dan kekurangan masing-masing objek yang dibandingkan. Analisis perbandingan digunakan untuk menguji perbandingan antara dua sampel data atau lebih (k-samples). Pada jenis penelitian komparasi yang dilakukan, peneliti membandingkan dua proses objek atau dua perlakuan pada periode proses yang sama atau tidak [4]. Pada penelitian jenis ini di dapat dibagi menjadi dua jenis proses komparasi (perbandingan) berpasangan dan tidak berpasangan.

2.2 Komparasi berpasangan

Pada penelitian komparasi berpasangan sampel yang digunakan biasanya adalah objek yang sama, yang berbeda adalah perlakuannya. Sebagai contoh : pada judul penelitian "Analisis perbandingan metode mengajar terhadap prestasi mahasiswa SBM-ITB". Yang menjadi subjek penelitian disini adalah mahasiswa yang sama SI SBM ITB. Sedangkan objek (perlakuan) yang dibandingan kan adalah prestasi mahasiswa hasil mengajar dengan metode A dan Metode B [5].

2.3 Komparasi tidak berpasangan

Pada proses penelitian komparasi tidak berpasangan subjek penelitian yang didibandingkan diambil dari sampel yang berbeda. Sebagai contoh pada judul penelitian : "Analisis perbandingan respon karyawan wanita dan pria terhadap kebijakan perusahan". Yang menjadi subjek penelitian ini ada dua kelompok yang berbeda yaitu kelompok karyawan wanita dan pria. Sedangkan yang menjadi objek penelitian (perlakuan) hanya satu yaitu respon atau sikap terhadap kebijakan baru manajeman perusahaan.

2.4 Keamanan Jaringan Komputer

Kebijakan keamana ini dimaksudkan untuk melindungi integrasi jaringan, untuk mengurangi resiko dan kerugian yang terkait dengan ancaman keamana terhadap sumber daya komputasi dan untuk memastikan akses dan kinerja jaringan yang aman dan handal. Dimana sistem kemanan jaringan akan dapat menghentikan ancama memasuki atau menyebar di jaringan, setiap lapisan keamana jaringan menerapkan kebikana dan kontrol. Hanya pengguna yang berwenang mendapatkan akses ke sumber daya jaringan, tetapi pelaku tindak kejahatan di blokir dari melakukan eksplotitasi dan ancaman.

2.5 Jenis-jenis ancaman jaringan komputer

Dalam sistem keamana jaringan komputer terdapat jenis-jenis ancaman yang dapat mengganggu keamana dari sistem itu sendiri, berikut jenis-jenis ancaman pada jaringan komputer [6] :

1. **Spam**
   Ini jenis ancaman yang biasanya sangat terkait dengan e-mail, meskipun tidak selalu.ancaman e-mail adalah spam atau e-mail yang tidak diinginkan oleh penerima. email mulai membanjir masuk ke dalam hard-drive dan mengkonsumsi ruang penyimpanan data. Hal ini akan mengakibatkan respon server menjadi lambat.
2. **Virus dan Worm**
   Ancaman ini tidak hanya dapat menyebar melalui e-mail, tetapi juga melalui software Instant Messaging dan bahkan perangkat mobile.
3. **Packet Snifer**
   Sebuah program yang menangkap / mengcapture data dari paket yang lewat

dijaringan (username, password dan informasi lainya).

4. **Denial of Service (DoS)**
   Serangan Denial of Service (DoS) mencegah pengguna yang sah dari penggunaan layanan ketika pelaku mendapatkan akses tanpa izin ke mesin atau data.
5. **Phising**
   Tindakan pemalsuan terhadap data/identitas resmi yang dilakukan untuk hal yang berkaitan dengan pemanfaatannya. Phishing diawali dengan mencuri informasi personal melalui internet. Phishing telah menjadi aktivitas kriminal yang banyak dilakukan di Internet.
6. **Carding**
   Pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit. Digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.
7. **Deface**
   Perubahan terhadap tampilan suatu website secara illegal.
8. **Probe**
   Probe atau yang biasa disebut Probing adalah usaha untuk mengakses sistem dan mendapatkan informasi tentang sistem.
9. **Hacking**
   Hacking adalah tindakan memperoleh akses kekomputer atau jaringan komputer untuk menapatkan informasi tanpa otorisasi yang sah.
10. **Port Scanning**
    Pada jenis keamanan komputer dengan metode port scanning menurut top1nfo.com pada umumnya sering digunakan penyerang untuk mengetahui port apa saja yang terbuka dalam sebuah sistem jaringan komputer
11. **Brute Force**
    Brute Force adalah serangan yang dilakukan untuk membobol password dengan cara mencoba setiap password sampai akhirnya menemukan password yang tepat. Peretas akan menggunakan algoritma yang menggabungkan huruf, angka dan simbol untuk menghasilkan password untuk serangan tersebut.

2.6 *Intrusion Detection System* (IDS)

IDS (Intrusion Datection System) adalah sebuah aplikasi perangkat atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah Majalah Ilmu Informatika Vol. 3 No.3, sept. 2012 – 40-sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan [7].

2.7 *Intrusion Prevnetion System* (IPS)

IPS (Intrusion Prevnetion System) merupakan sebuah metode yang ada pada software maupun hardware maupun hardware berfungsi memonitoring trafik pada sebuah jaringan dan juga berfungsi mendeteksi aktivitas yang dianggap mencurigakan dan IPS ini juga langsung bisa melakukan block terhadap penyusup. Teknologi ini juga dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan local, dengan sensor saat serangan telah teridentifikasi, IPS disini bertindak sebagai firewall yang bekerja untuk meneyelesaikan seleksi paket yang di izinkan atau tidak [8].

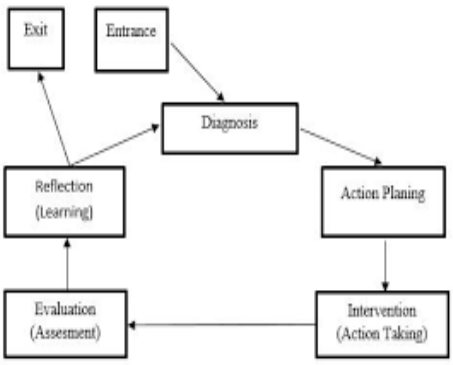
2.8 *Firewall*

Kata firewall jika diterjemahkan menjadi sebuah kata adalah “dinding api”. *Firewall* dimaksudkan untuk melindungi perangkat router dan *client-client* tyang terhubung dengannya. Umumnya firewall dibuat untuk melindungi network internet (LAN) terhadap berbagai gangguan atau serangan yang berasal dari luar (internet). Hal ini adalah wajar, mengingat umumnya “dunia kuar” dan “dunia Bebas”. Sehingga

potensi serangan yang berasal dari luar sangan besar. Sebenernya potensi serangan bisa juga berasal dari LAN. Dan firewall juga bisa dikonfigurasikan untuk melindungi kedua potensi serangan tersebut. Jadi ferewall dibuat agar dapat membuat network lebih secure (aman) [9].

III. METODOLOGI PENELITIAN

Dalam proses penelitian ini menggunakan metode Action Research atau sering kita sebut metode tindakan bertujuan bahwa teori dan proses praktik dapat secara tertutup serta dintegrasikan dengan pembelajaran dari hasil intverentasi yang direncanakan setelah melakukan diagnosis yang rinci terhadap objek permasalahan. Action research adalah salah satu solusi atau proses perbaikan sesuatu cara atau proses perbaikan dimana evalusai pelaksanaanya, perencanaan dan dilakukan secara terstruktur yang mana dalam proses analisis itu sendiri menerapkan tahapan-tahapan yang ada dalam metode ini sendiri agar dapat mendapatkan validasi dan reliabilitasnya untuk mencapai akurasi yang tepat [10].



Gambar 1. Siklus *Action Research*

Berikut penerapan tahapan-tahapan dari metode Action Research:

3.1 Melakukan Diagnosa (*Diagnosing*)

Melakukan identifikasi dan mencari masalah pokok yang ada, untuk mengetahui lebih dalam mengenai objek yang akan di teliti. Keamanan jaringan (network security) adalah bagian yang sangat penting bagi sebuah jaringan komputer untuk mencegah dan mengatasi terjadinya sebuah tindak kejahatan seperti hacking, cracking dan tindak kejahatan lainnya yang dapat merugikan orang lain. Oleh karna itulah dibutuhkan sebuah sistem keamanan jaringan dalam bentuk software maupun hardware dengan kemampuan yang dimiliki masing-masing sistem keamanan, maka dibutuhkan sebuah sistem keamanan yang mampu memonitoring lalu lintas jaringan, mencatat log semua paket dan memblock aktivitas-aktivitas mencurigakan, maka hal tersebut dapat dilakuan dengan menggunakan metode Intrusion Prevention System (IPS).IPTables yang diimplementasi pada linux Ubuntu dan CentOS dan dapat melakukan metode Intrusion Prevention System (IPS). Maka akan dirancang sebuah system keamanan dan dilakukan perbandingan system keamanan dari IPTables di Linux Ubuntu dan CentOS, yang akan di uji coba dengan melakukan serangan dengan menggunakan dan Brute Force.Dalam proses penelitian ini peran perangkat keras (hardware) sangat vital dalam proses analisis, Berikut perangkat keras (hardware) yang digunakan ada 2 yaitu Server dan PC/laptop *attacker* sebagai sarana alat bantu ujicoba :

Gambar 2. Server

Dari gambar 2 komputer akan dijadikan server dengan menggunakan system operasi Linux Ubuntu dan Linux CentOS , dan akan di implementasi aplikasi

IPTables dan fail2ban yang akan diuji seranagan dan Brute Force. Komputer server yang digunkan dalam penelitian ini menggunakan merek Lenovo, Berikut spesifikasi dari server:

Tabel 1. Spesifikasi perangkat

Nama perangkat	Spesifikasi
Platform	Personal Computer
Processor	*CORE i3*
Grapich	*Intel HD Grapich*
Memori	*4 GB*
Hard Drive	*500 GB*
Optical Drive	*DVD RW*
Operating System	*Ubuntu server / CentOS*

Gambar 3. Pc/laptop attacker

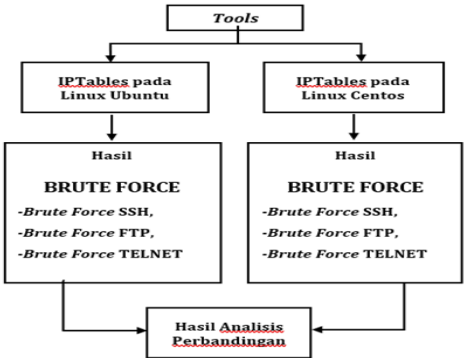
laptop Attacker menggunakan Sistem Operasi Windows 10, berfungsi sebagai komputer utama untuk melakukan serangan dan Packet Sniffing. komputer Attacker dalam penelitian ini adalah merek asus. Berikut spesifikasinya :

Tabel 2. Spesifikasi perangkat

Nama perangkat	Spesifikasi
Platform	Laptop
Processor	*CORE i3*
Grapich	*Nvidia GEFORCE*
Memori	*4 GB*
Hard Drive	*500 GB*
Optical Drive	*DVD RW*
Operating System	*Windows 10*

3.2 Membuat rencana tindakan (Actin planning)

Pada tahapan rencana tindakan (Action planning), dalam tahapan ini peneliti mencoba memahami inti poin-poin dari permasalahan dimana dari pointersebut bertujuan untuk memahami pokok permasalahan yang ada dan menyusun sebuah rancangan menggunakan tindakan yang tepat dalam menyelesaikannya. Untuk melakukan analisa sistem keamanan jaringan yang lebih aman, maka dalam proses implementasi perbandingan sistem pada linux ubuntu dan linux CentOs dirancang lah skema kerangka berfikir dan topologi jaringan untuk memgambarkan alur yang nantinya akan di implementasikan,yang telah direncanakan sebagai berikut :



Gambar 4. Skema kerangka berfikir

Dan pada proses rancang tindakan (action pllaning) sudah di gambar kan melalui skema topologi perbandingan sistem pada linux ubuntu dan linux CentOs yang telah dirancang sebagai berikut :

Gambar 5. Skema linux Ubuntu dan CentOs

Topologi yang digunakan pada penelitian ini adalah topologi peer to peer. Berikut Ip address masing-masing perangkat yang akan di ujicoba kan pada proses implementasi perbandingan sistem pada linux ubuntu dan linux CentOs :

Tabel 3. IP Adress perangkat

Nama perangkat	IP *Address*	Subnetmask
server	192.168.10.2	255.255.255.0
attacker	192.168.10.5 192.168.10.20	255.255.255.0

3.3 Melakukan tindakan (Action taking)

Pada tahapan melakukan tindakan (Action Taking) adalah proses penginstallan pada masing-masing sistem operasi linux Ubuntu di install pada perangkat keras (hardware) server dan Linuk CentOs di install pada PC/Laptop Attecker.

IV. HASIL DAN PEMBAHASAN

4.1 Hasil

Dalam penelitian ini kita siapkan dau komputer atau leptop yang nantinya akan dijadikan sebuah Server dan Clien sekaligus sebagai Attacker, dan sebuah kabel LAN untuk menghubungkan server dan cliean/attacker, sebelum membangun system keamanan dengan menggunkan metode Intrusion Prevention System (IPS) penulias akan menginstal system operasi yang akan di uji yaitu Linux Ubuntu Server 16.04 dan Linux CentOS 7, kemudian setelah diuji kedua system operasi akan dibandingkan system keamananya dengan cara melakukan serangan Brute Force.

Untuk melakukan uji serangannya peneliti menggunakan Linux Backtrack 5 sebagai system operasi attacker dan dengan menggunakan tools medusa yang ada pada linux Backtrack dan file wordlist sebagai kamus username dan password. Kemudian pada server penulis terapkan metode (IPS) yaitu dengan cara mengaktifkan iptables sebagai firewall dan fail2ban sebagai pembuat rules dan pencatat log pada Ubuntu dan Centos . jika sudah siap maka uji coba serangan bisa dilakukan.

Pertama kita hubungkan dulu server dan attacker dengan menggunakan kabel LAN dan kita buat IP Address pada Komputer Server 192.168.10.2 dan pada komputer attacker 192.168.10.5, setelah itu tes ping antara server dan attacker, jika terhubung maka kita bisa memulai serangan dengan membuka terminal pada komputer attacker dan untuk serangan penulis menggunakan Brute Force melaui servie SSH, FTP dan TELNET. Serangan petama melalui SSH dengan cara mengetikan pada terminal "medusa -h 192.168.10.2 -n 22 -U root/wl.lst -P root/wl.lst -M ssh" dan untuk FTP ketikan "medusa -h 192.168.10.2 -n 21 -U root/wl.lst -P root/wl.lst untuk TELNET ketikan "./patator.py telnet_login host=192.168.10.2.inputs='FILE0\FILE1'0= /root/wl.lst 1=/root/wl.lst". berikut adalah hasil dari serangan yg masuk ke Server.

1. Hasil pengujian serangan Brute Force pada Ubuntu server

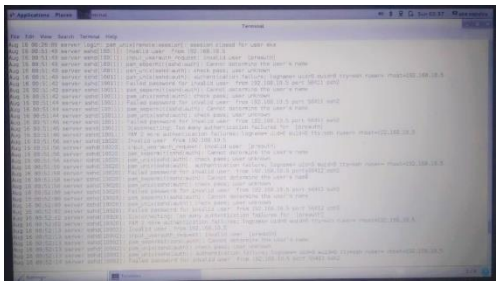
Hasil yang didapat dari pengujian serangan Brute Force yang di lakukan pada linux Ubuntu Server yaitu, terdapat ip address dari penyerang, logname, port dan waktu kapan terjadinya penyerangan yang dilakukan, untuk melihat log serangan ketik perintah : /var/log/auth.log.

Gambar 6. Log Linux Ubuntu

2. Hasil pengujian serangan Brute Force Linux CentOS

Hasil yang didapat dari pengujian serangan Brute Force pada Linux CentOS yaitu sama dengan yang di Uuntu Server, terdapat ip address dari penyerang,

logname,potr dan waktu kapan terjadinya penyerangan yang dilakukan, untuk melihat log serangan ketikan perintah "tail cat/var/log/secure" hal ini dapat dilihat dari log linux Ubuntu server pada gambar berikut.



Gambar 7. Log Linux CentOS

4.2 Pembahsan

Dalam penerapan Intrusion Prevention System peneliti menggunkan dau toolls yaitu mengkombinasikan IPTables yang berfungsi untuk mencatat log dari setiap aktivitas serangan yang dilakukan attacker, dan Fail2ban yang berfungsi sebagai wadah untuk membuat rules atau aturan yang akan di konfigurasi sesuai kebutuhan penelitian..

Setelah diuji serangan pada Ubuntu dan Centos yang telah di terapkan Intrusion Prevention System kita bisa bandingkan IPS yang ada pada Ubuntu dan Centos dengan cara melihat kriteria yang telah tentukan :

1. Serangan yang di terima : yaitu Serangan apa saja yang terdeteksi oleh IPTables.
2. Pembuatan Rules : yaitu dalam pembuatan rules manakah yang lebih rumit atau lebih mudah.
3. Log Serangan : yaitu apakah setiap serangan tercatat di log IPTables
4. Proses : yaitu pada ssat dilakukan serangan apa yang terjadi pada Ubuntu maupun Centos.
5. Kegiatan Sistem : yaitu pada saat serangan telah tercatat di log apa yang dilakukan system di Ubuntu maupun Centos.
6. Memblock Seragnan : yaitu searangan apa saja yang deblock oleh IPTables.
7. Kesimpulan : yaitu kesimpulan yang diperolah oleh penliti.

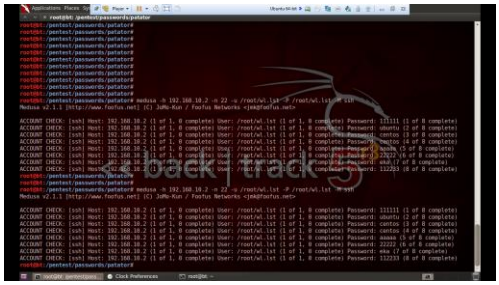
4.3 Uji serangan Brute Force di Linux Ubuntu

Pengujian terhadap Ubuntu Server ini dilakukan dengan beberapa jenis serangan pada beberapa service yang berbeda, antara lain, SSH, FTP, Telnet, dan akan di lakukan pengujian dengan metode *Brute Force*, serangan ini menggunakan medusa versi Open Source yang ada pada Linux BackTrack yang akan diarahkan ke IP Address Server dengan menggunakan wordlist untuk username yaitu 'username.lst' dan untuk password yaitu 'pass.lst'.

Sebelum melakukan pengujian pastikan komputer clien/attacker terhubung dengan server agar pengujian dapat dilakukan. Berikut ini pengujian serangan *brute force* pada Linux Ubuntu Server.

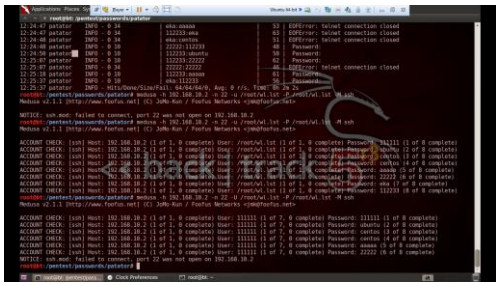
1. Serangan Brute Force Secure Shell (SSH).

Pertama buka buka Linux BackTrack pada komputer clien/attacker kemudian buka terminal lalu ketikan perintah "medusa -h 192.168.10.2 -n 22 -U root/wl.lst -P root/wl.lst -M ssh" dimana ip address tersebut merupakan ip address komputer server, sebelum dilakukan penerapan Intrusioan Prevention System (IPS), Ubuntu server masih bisa di tembus oleh attacker, Dapat dilihat pada gambar gambar 4.3, pada wordlist ke 1 sampai 8 complete, itu tandanya serangan bruteforce berhasil. dan tercatat di log pada gambar 8.



Gambar 8. serangan SSH sebelum diterapkan IPS pada Ubuntu Server.

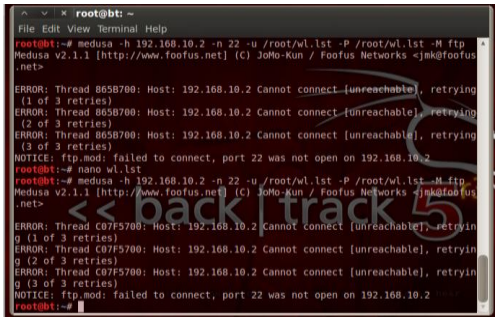
Kemudian kita bandingkan dengan Ubuntu server yang telah diterapkan Intrusioan Prevention System (IPS), dengan menggunkan tools fail2ban yang membantu iptables mecatat log dan memblock otomatis ip address yang mencurigakan. Setelah fail2ban dan iptables telah di aktifkan atau di jalankan maka hasilnya attacker tidak bisa lagi menembus username dan password dari komputer server, terlihat pada gambar gambar 4.4, pada wordlist ke 1 sampai 8 complete, terhenti di wordlist ke 6, karna pada rules yang di buat pada fail2ban maxretri /percobaan = 6, dan otomatis koneksi ke server diputus karena terdeteksi oleh IPS ada ujicoba login terus menerus ke port 22 dengan rentan waktu yang berdekatan. Sehingga IPS mendeteksi serangan tersebut adalah bruteforce SSH.dab serangan bruteforce gagal. terlihat pada gambar 9.



Gambar 9. Serangan Menggunakan SSH Gagal Karna Suda Diterapkan IPS Pada Ubuntu.

2. Serangan Brute Force File Transfer Protocol (FTP).

Serangan Brute Force File dari Transfer Protocol (FTP), ketikan perintah "medusa -h 192.168.10.2 -n 21 -U root/wl.lst -P root/wl.lst -M ftp" pada terminal. Hasilnya tidak bisa ditembus karna sudah diterapkan Intrusioan Prevention System (IPS), dan ip address dari attacker otomatis terblock oleh iptables maka hasilnya attacker tidak bisa menembus username dan password dari komputer server, seperti pada gambar 10.



Gambar 10. Serangan Menggunakan FTP Gagal Karna Suda Diterapkan IPS Pada Ubuntu.

3. Serangan Brute Force Telnet

Serangan Brute Force dari Telnet, ketikan perintah "./patator.py telnet_login host=192.168.10.2.inputs='FILE0\FILE1' 0=/root/wl.lst 1=/root/wl.lst" pada terminal. Hasilnya juga tidak bisa ditembus karna sudah diterapkan Intrusioan Prevention System (IPS), dan ip address dari attacker otomatis terblock oleh iptables maka hasilnya attacker tidak bisa menembus username dan password dari komputer server, seperti gambar 11.

Gambar 11. Serangan Menggunakan Telnet Gagal Karna Suda Diterapkan IPS Pada Ubuntu.

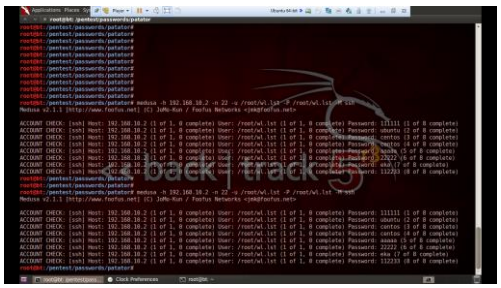
4.4 Uji serangan Brute Force di Linux CentOS

Pengujian terhadap Linux CentOS sama dengan yang ada pala Ubuntu Server, dilakukan dengan beberapa jenis serangan pada beberapa service yang berbeda, antara lain, SSH, FTP, Telnet, dan akan di lakukan pengujian dengan metode Brute Force, serangan ini menggunakan medusa versi Open Source yang ada pada Linux BackTrack yang akan diarahkan ke IP

Address Server dengan menggunakan wordlist untuk username yaitu ‘username.lst’ dan untuk password yaitu ‘pass.lst’.Sebelum melakukan pengujian pastikan komputer clien/attacker terhubung dengan server agar pengujian dapat dilakukan. Berikut ini pengujian serangan brute force pada Linux Ubuntu Server.

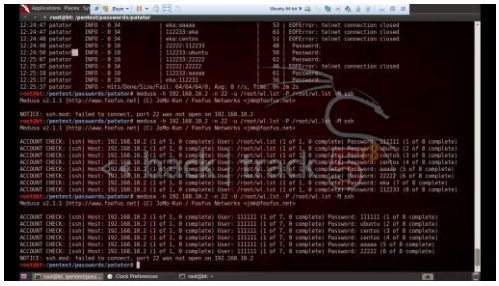
1. Serangan Brute Force Secure Shell (SSH).

Sama seperti pada linux Ubuntu Server pertama buka buka Linux BackTrack pada komputer clien/attacker kemudian buka terminal lalu ketikan perintah “medusa -h 192.168.10.2 -n 22 -U root/wl.lst -P root/wl.lst -M ssh” dimana ip address tersebut merupakan ip address komputer server, sebelum dilakukan penerapan Intrusioan Prevention System (IPS), Ubuntu server masih bisa di tembus oleh attacker, Dapat dilihat pada gambar gambar 4.7, pada wordlist ke 1 sampai 8 complete, itu tandanya serangan bruteforce berhasil. dan tercatat di log pada gambar 12.



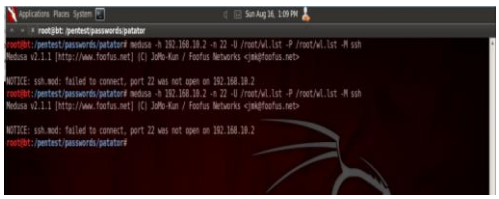
Gambar 12. serangan SSH sebelum diterapkan IPS pada CentOS

Kemudian kita bandingkan dengan Ubuntu server yang telah diterapkan Intrusioan Prevention System (IPS), dengan menggunkan tools fail2ban yang membantu iptables mecatat log dan memblock otomatis ip address yang mencurigakan. Setelah fail2ban dan iptables telah di aktifkan atau di jalankan maka hasilnya attacker tidak bisa lagi menembus username dan password dari komputer server, terlihat pada gambar gambar 4.4, pada wordlist ke 1 sampai 8 complete, terhenti di wordlist ke 6, karna pada rules yang di buat pada fail2ban maxretri /percobaan = 6, dan otomatis koneksi ke server diputus karena terdeteksi oleh IPS ada ujicoba login terus menerus ke port 22 dengan rentan waktu yang berdekatan. Sehingga IPS mendeteksi serangan tersebut adalah bruteforce SSH.dab serangan bruteforce gagal. terlihat pada gambar 13.



Gambar 13. serangan menggunakan SSH gagal karna suda diterapkan IPS pada CentOS.

Setelah di coba lagi tidak bisa jalan karna ipaddress attacker sudah di block otomatis oleh iptables,

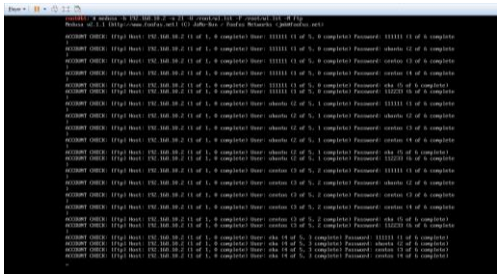


Gambar 14. Serangan Kedua Menggunakan SSH Gagal Karna Suda Diterapkan IPS Pada Centos.

2. Serangan Brute Force File Transfer Protocol (FTP).

Serangan Brute Force File dari Transfer Protocol (FTP), ketikan perintah “medusa -h 192.168.10.2 -n 218iii- 9-U root/wl.lst -P root/wl.lst -M ftp” pada terminal. Hasilnya tidak bisa ditembus karna sudah diterapkan Intrusioan Prevention System (IPS), dan ip address dari attacker otomatis terblock oleh iptables maka hasilnya attacker tidak bisa menembus username dan password dari komputer server, seperti pada gambar 15.

Gambar 15. Serangan Menggunakan FTP gagal karna suda diterapkan IPS pada CentOS.

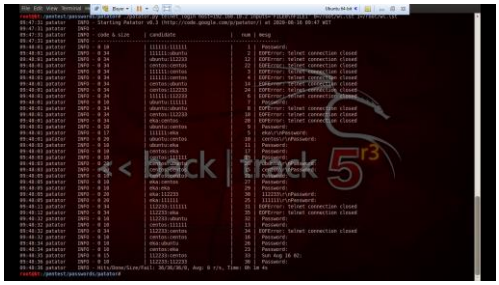


Gambar 16. Serangan Menggunakan FTP berhasil sebelum diterapkan IPS pada CentOS.

3. Serangan Brute Force Telnet

Serangan Brute Force dari Telnet, ketikan perintah "./patator.py telnet_login host=192.168.10.2.inputs='FILE0\FILE1' 0=/root/wl.lst 1=/root/wl.lst" pada terminal. Hasilnya juga tidak bisa ditembus karna sudah diterapkan Intrusioan Prevention System (IPS), dan ip address dari attacker otomatis terblock oleh iptables maka hasilnya attacker tidak bisa menembus username dan password dari komputer server, seperti gambar 12.

Gambar 17. Serangan Menggunakan TELNET gagal karna suda diterapkan IPS pada CentOS.



Gambar 18. Serangan Menggunakan TELNET berhasil sebelum diterapkan IPS pada CentOS.

4.5 Analisis Perbandingan

Dalam mengatasi serangan Brute Force, Linux Ubuntu dan Linux CentOS 141omput sama, tetapi saat pengujian Linux Centos lebih cepat saat melakukan block pada ip address, dan pada saat pembuatan aturan atau rules Ubuntu lebih unggul karana implementasinya lebih mudah dan perintah lebih banyak yang 141omp digunakan. Kemudian dalam pencatatan log, Centos lebih stabil, untuk selebihnya sama kuat untuk mengatasi serangan, hanya saja tergantung pada spesifikasi 141omputer server dan waktu saat pengujian. Kesimpulannya menurut peneliti adalah Linux CentOS lebih aman di bandingkan Linux Ubuntu, dikarnakan juga Linux Ubuntu sering melakukan pembaruan.

Tabel 4. Perbandingan Intrusian Prevention System.

No	PERBEDAAN	LINUX UBUNTU	LINUX CENTOS
1	**Serangan Brute Force melalui SSH**		
	Durasi Pengujian	30 menit	30 menit
	deteksi	IP Address	IP Address
		- 192.168.10.5	- 192.168.10.5
		PORT	PORT
		-64891 SSH2	-56412 SSH2
		WAKTU	WAKTU

		Agustus 12,2020 01:20	Agustus 16,2020 00:52
2	**Serangan Brute Force melalui FTP**		
	Durasi Pengujian	20 menit	20 menit
	deteksi	IP Address	IP Address
		- 192.168.10.5	- 192.168.10.5
		PORT	PORT
		-64891 FTP	-56412 FTP
		WAKTU	WAKTU
		Agustus 12,2020 01:50	Agustus 16,2020 01:20
3	**Serangan Brute Force melalui TELNET**		
	Durasi Pengujian	20 menit	20 menit
	deteksi	IP Address	IP Address
		- 192.168.10.5	- 192.168.10.5
		PORT	PORT
		-64891 TELNET	-56412 TELNET
		WAKTU	WAKTU
		Agustus 12,2020 02:20	Agustus 16,2020 01:50

4.6 Hasil Perbandingan Linux Ubuntu Dan Linux CentOS

Menurut kriteria perbandingan yang ada pada 4.2 maka hasil perbandingannya adalah sebagai berikut :

Tabel 5. Hasil Perbandingan Intrusian Prevention System

NO	KRITERIA PERBANDINGAN	LINUX UBUNTU	LINUX CENTOS	KETERANGAN
1	Serangan yang di terima	(Brute Force) SSH, FTP,TELNET	(Brute Force) SSH, FTP,TELNET	Pada saat pengujian serangan dilakukan menggunakan Brute Force
2	Pembuatan Rules	menggunkana iptabless dan fail2ban	menggunkana iptabless dan fail2ban	Dalam pembuatan rules ubuntu lebih mudah karna lebih banyak perintah yang bisa dipakai dan untuk contoh rules ubuntu lebih banyak di temui
3	Log Serangan	Setiap serangaan tercatat semua di log	Setiap serangaan tercatat semua di log	Saat pencatatan log serangan linux centos lebih stabil
4	Proses	Pada saat serangan di terima ubuntu langsung mendeteksi serangan tersebut	Pada saat serangan di terima centos langsung mendeteksi serangan tersebut	Proses saat terjadi serangan ubuntu dan centos sama cepat
5	Kegiatan Sistem	Pada saat serangan telah terdeteksi Ubuntu langsung memblock ipaddress dari komputer penyerang	Pada saat serangan telah terdeteksi Centos langsung memblock ipaddress dari komputer penyerang	Pada saat memblock ubuntu dan centos sama cepat karna rules yang diterapkan pada masing-masing linux sama

6	Memblock Serangan	Brute Force SSH, Brute Force FTP Brute Force TELNET	Brute Force SSH, Brute Force FTP Brute Force TELNET	Serangan yang diblock pada Ubuntu dan Centos.
7	Kesimpulan	Linux CentOS lebih aman di bandingkan Linux Ubuntu, dikarnakan juga Linux Ubuntu sering melakukan pembaruan, yang dapat mempengaruhi rules yang telah dibuat.		

V. KESIMPULAN

Ada pun kesimpulan dari penelitian perbandingan Intrusion Prevention System pada Linux Ubuntu dan Linux Centos.

1. Pengujian Serangan Brute Force dengan menggunakan medusa versi Open Source yang ada pada Linux BackTrack, Linux Ubuntu dan Linux mampu mencatat ip address dari penyerang, logname, port dan waktu kapan terjadinya penyerangan, dan deblock oleh Linux Ubuntu sehingga komputer penyerang tidak dapat menembus komputer server karena lilimit sudah di batasi.
2. Pengujian Serangan Brute Force dengan menggunakan medusa versi Open Source yang ada pada Linux BackTrack, Linux Centos dan Linux mampu mencatat ip address dari penyerang, logname, port dan waktu kapan terjadinya penyerangan, dan deblock oleh Linux Ubuntu sehingga komputer penyerang tidak dapat menembus komputer server karena lilimit sudah di batasi.
3. Dalam pengujian serangan pada service ssh, ftp dan telnet pada Linux Ubuntu dan Linux Centos, sebelum diterapkan IPS serangan tersebut berhasil dilakuan namun setelah IPS diterapkan maka serangan tersebut gagal.
4. Untuk keamanan dalam mengatasi serangan Linux Centos sedikit lebih baik dibandingan dengan linux Ubuntu dalam mengatasi serangan Brute Force.
5. Linux Ubuntu dan Linux Centos mampu mencatat dan memblock ip addres peyerang yang masuk .
6. Rules mengatasi serangan Brute Force pada linux Ubuntu maupun Linux Centos berfungsi untuk mencatat ip address yang masuk kemudian membock ip address yang dicurigai.

VI. SARAN

Saran yang mungkin akan berguna untuk pembaca yang ingin melakukan penelitian perbandingan dan pengujian sistem keamanan adalah :

1. Sebaiknya gunakan aplikasi tambahan seperti fail2ban pada linux Ubuntu,CentOS dan lakukan kombinasi rules di dalam IPTables agar sistem keamanan dapat bekerja lebih baik lagi.
2. Perhatikan protocol dari penyerang seperti icmp, tcp, dan udp. Agar rules yang dibuat dapat berfungsi.
3. Dalam membuat rules pastikan urutan rules benar-benar tepat agar rules dapat berfungsi dengan optimal dan mendapatkan hasil yang lebih baik.

VII. DAFTAR PUSTAKA

[1] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website," *J. Komput. dan Apl.*, vol. 07, no. 1, pp. 97–107, 2019.

[2] agustin setyo Wardani, "4,5

Miliar Data Dicuri Selama 6 Bulan Pertama 2018," *liputan6.com*, 2018.

[3] S. R. Ariyadi T., Kunang Y. N., "Implementasi Intrusion Prevention System(Ips) Pada Jaringan Komputer Kampus B Universitas Bina Darma," *J. Ilm. Tek. Inform. Ilmu Komput.*, vol. 14, no. 2, pp. 1–14, 2012.

[4] H. Huang, "Apa yang dimaksud dengan Analisis Perbandingan dalam Statistik," 2020.

[5] B. P. Mahasiswa, "AR," 2020.

[6] Dosen Universitas Mercubuana, "Keamanan Jaringan," pp. 1–75, 1969.

[7] J. Gondohanindijo, "IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan/Intrusi," *Maj. Ilm. Inform.*, vol. 03, no. 03, pp. 38–59, 2012.

[8] Simaremare, "Pengembangan Sistem Keamanan Jaringan Intranet UGM Menggunakan Metode IPS (Intrusion Prevention System)," *Ugm*, pp. 0–6, 2007.

[9] K. Penerbit and I. Bandung, "Iwan Sofana (Agustus Membangun Jaringan," p. 2015, 2014.

[10] F. Panjaitan *et al.*, "Pemanfaatan Notifikasi Telegram untuk Monitoring Jaringan Febriyanti," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 10, no. 2, pp. 725–732, 2019.