SISTEM PENGAMANAN JARINGAN ADMIN SERVER DENGAN METODE *INTRUSION DETECTION SYSTEM* (IDS) *SNORT*MENGGUNAKAN SISTEM OPERASI*CLEAROS*

Suhartono[1)], Abd.Rahman Patta[2)]

Abstrak:Jenis penelitian ini adalah penelitian R & D (*Research And Development*), yang bertujuan untuk membangun sistem monitoring keamanan jaringan admin server dengan basis sistem operasi adalah *ClearOS*. Metode yang digunakan dalam sistem monitoring keamanan jaringan admin server ini adalah dengan model 4D (four-D model). Model 4D (four-D model)terdiri dari beberapa tahapan – tahapan yaitu pendefinisian, perancangan, pengembangan dan uji coba. Hasil penelitian ini adalah sebuah sistem pengamanan jaringan admin server yang memberikan kemudahan terhadap admin server untuk memonitor kinerja server, monitoring serangan yang dilakukan oleh *hacker, attacker,* dan *intruder* serta mampu mendeteksi dan mengatasi serangan SSH *bruteforce* dan FTP *bruteforce*.

Kata Kunci : ClearOS, 4D, Admin Server,SSH *bruteforce*, FTP *bruteforce,Intrusion Detection System Snort*(IDS Snort).

Pendahuluan

Keamanan teknologi informasi (IT) merupakan sebuah hal mendasar yang penting untuk diperhatikan dalam sebuah lingkaran organisasi maupun individu. Berbagai serangan terhadap server pada organisasi hingga pembajakan akun pada individu, apapun bentuknya tindakan ini hanya mendatangkan kerugian. Menurut ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*). Adanya perangkat teknologi yang serba *modern* atau canggih akan tidak ada artinya tanpa diimbangi oleh pengaturan dan penggunaan secara tepat efektif dan efesien. Perangkat yang sederhana namun dikelola secara tepat bias menstabilkan bahkan akan sangat membantu terhadap perkembangan perusahaan, hal tersebut disebabkan keterbatasan *resource* sehingga harus betul-betul memanfaatkan teknologi yang dimiliki.

Dalam suatu teknologi jaringan diperlukan yang namanya manajemen jaringan yang fungsinya adalah untuk mengelola seluruh *resource* di jaringan agar bisa memberikan *good services* kepada penggunanya. Mengutip suatu definisi dari Mathews, D.C, bahwa proses suatu manajemen itu adalah "suatu proses yang ditunjukan untuk mempresentasikan pengetahuan suatu organisasi kepada suatu langkah kongkrut yang akan menghasilkan sesuatu yang diharapkan: (Kumar , 2002).

Tinjauan Pustaka

Internet

Internet sendiri berasal dari kata Interconnection Networking, bisa diartikan sebagai a global network of computers networks. Jaringan komputer berskala

http://dx.doi.org/10.31963/elekterika.v1i2.1220

internasional yang dapat membuat masing-masing komputer saling berkomunikasi. Dikembangkan dan diuji coba pertama kali pada tahun 1969 oleh US Department of Defense dalam proyek ARPAnet oleh (Jack Febrian & Farida Andayani, 2012).

Defenisi sistem

Menurut Mustakini (2009), sistem dapat didefinisikan dengan pendekatan prosedur dan pendekatan komponen, sistem dapat didefinisikan sebagai kumpulan dari prosedur-prosedur yang mempunyai tujuan tertentu.

Definisi Keamanan Jaringan Komputer

Jaringan komputer (*computer network*) menurut Sutanta (2005) merupakan interkoneksi sejumlah komputer dan peralatan (*peripheral*) yang dihubungkan dengan jalur transmisi dan alat komunikasi membentuk suatu sistem sehingga dapat saling bertukar data, informasi atau menggunakan peralatan secara bersama-sama untuk melaksanakan tugas pengolahan data.

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan yang lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama. Jaringan komputer dapat diartikan juga sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri lebih dari satu computer yang saling berhubungan, oleh (Sukmaaji & Rianto, 2008).

Proxy Server

Server Proxy adalah server yang diletakkan antara suatu aplikasi client dan aplikasi server yang dihubungi. Apalikasi client dapat berupa browser web, client FTP dan sebagainya. Sedangkan aplikasi server dapat berupa server web, server FTP dan sebagainya. Server Proxy yang diletakkan di antara aplikasi client dan aplikasi server tersebut, dapat digunakan untuk mengendalikan maupun memonitor lalu lintas paket data yang melewatinya oleh (Wagito.2007)

Firewall

Menurut O'brien (2011: 594) lebih spesifik menyatakan bahwa, "Firewalls adalah sebuah sistem atau perangkat yang mengizinkan pergerakan lalu lintas jaringan yang dianggap aman untuk dilalui dan mencegah lalu lintas jaringan yang tidak aman.

Snort

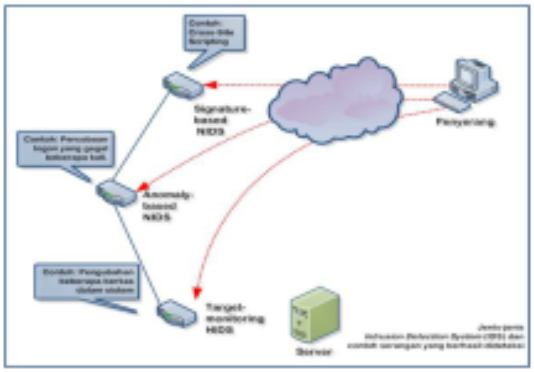
Snort adalah *Intrusion Detection System* jaringan *open source* yang mampu menjalankan analisis aliran *real-time* dan paket logging pada IP *network*. Dia dapat menjalankan analisis protokol, *content searching/matching*, dan dapat digunakan untuk mendeteksi berbagai serangan dan penyusupan, seperti *buffer overflow, stealth*

http://dx.doi.org/10.31963/elekterika.v1i2.1220

port scan, serangan CGI, penyusupan SMB, usaha-usaha OS *fingerprinting*, dan masih banyak lagi.(www.snort.org).

IDS (Intrusion Detection System)

Menurut Odon (2005:565) *Instrusion Detection System* atau IDS adalah suatu sistem aplikasi yang dapat memonitor lalu lintas jaringan dari paket-paket data yang mencurigakan atau yang melanggar aturan keamanan jaringan dan kemudian membuat laporan dari aktivitas jaringan tersebut.



Gambar 2.1

Contoh serangan yang berhasil di deteksi

Bagaimana Mendeteksi Penyusupan

Menurut Ariyus (2007)IDS memiliki implementasi TCP/IP khusus yang memungkinkan ia mengumpulkan paket dan selanjutnya memasang kembali paket-paket tersebut untuk dianalisis

IPS (Intrusion Detection System)

Intrusion Prevention System (IPS) adalah sebuah aplikasi yang bekerja untuk *monitoring traffic* jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya.

Squid

Squid adalah sebuah daemon yang digunakan sebagai proxy server dan web cache. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server web dengan melakukan caching permintaan yang berulang-ulang, caching DNS, caching situs web, dan caching pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanandengan cara melakukan penyaringan (filter) lalu lintas. Meskipun seringnya digunakan untuk protokol HTTP dan FTP, Squid juga menawarkan dukungan terbatas untuk beberapa protokol lainnya termasuk Transport Layer Security (TLS), Secure Socket Layer (SSL), Internet Gopher, dan HTTPS. Versi Squid 3.1 mencakup dukungan protokol IPv6 dan Internet Content Adaptation Protocol (ICAP) oleh (Oskar Pearson, 2003).

TCP/IP

TCP/IP (singkatan dari Transmission Control Protocol/Internet Protocol) adalah standar

http://dx.doi.org/10.31963/elekterika.v1i2.1220

komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokolyang terdiri dari sub-protokol, yang beroperasi pada lapisan yang berbeda. Merupakan standar protokol internet. Protokol ini memberikan nomor unik pada setiap komputer yang terkoneksi, oleh (Jack Febrian & Farida Andayani, 2012).

Authentikasi

Authentikasi adalah proses dalam rangka memvalidasi user pada saat memasuki sistem. Nama dan password dari user dicek melalui proses yang mengecek langsung ke daftar mereka yang diberikan hak untuk memasuki Sistem tersebut oleh (Jack Febrian & Farida Andayani, 2012)

Perangkat Lunak yang Digunakan

1. Visio

   Microsoft Visio merupakan salah satu keluarga dari Microsoft office yang memiliki kegunaan atau fungsinya sendiri. Berdasarkan akar katanya, visio berasal dari kata vision. Yang artinya penglihatan, daya lihat, dan pandangan. Salah satu contoh sketsa yang dapat dibuat menggunakan Microsoft Visio adalah sketsa sebuah ruangan, Peta, denah lokasi, diagram atau peta jaringan, oleh (Cheyantie, 2012).

2. ClearOS

   ClearOS adalah linux yang di kostumasi khusus untuk keperluan server. Dengan berbagai fitur yang powerfull dan setting yang simple, ClearOS menjadi alternative pilihan, baik untuk pemula yang tidak mengerti linux sama sekali maupun untuk professional yang memerlukan kemampuan terbaik dari OS linux server. Berbasis Linux Red Hat Enterprise 5, menjadikan ClearOS memiliki source base yang kuat dan stabil untuk dijalankan sebagai server di warnet, game online,kantor-kantor,dan perusahaan, oleh (Andi Micro, 2012)

METODE PENELITIAN

Identifikasi Masalah

Berdasarkan latar belakang masalah maka berhasil diidentifikasi masalah yang terjadi selama pengamatan dan wawancara terhadap owner LAB PTIK FT UNM yaitu antara lain:

1. Membutuhkan sebuah system jaringan yang memiliki authentikasi
2. Mendukung program pemerintah dalam menerapkan internet sehat kepada masyarakat dengan melakukan content filtering
3. Mengatur Akses pada jam tertentu bagi para pelajar agar internet bukan menjadi alasan untuk tidak melakukan aktifitas kampus

http://dx.doi.org/10.31963/elekterika.v1i2.1220

Analisis kondisi lapangan

Pengguna internet yang mayoritas mahasiswa, hampir setiap hari kurang lebih ada sekitar 10 sampai 14 orang user yang melakukan aktifitasnya melalui internet untuk melakukan berbagai hal mulai dari browsing, chating, download, game online, bisnis online, dan ada beberapa orang yang melakukan trading melalui Forex.

Jenis Penelitian

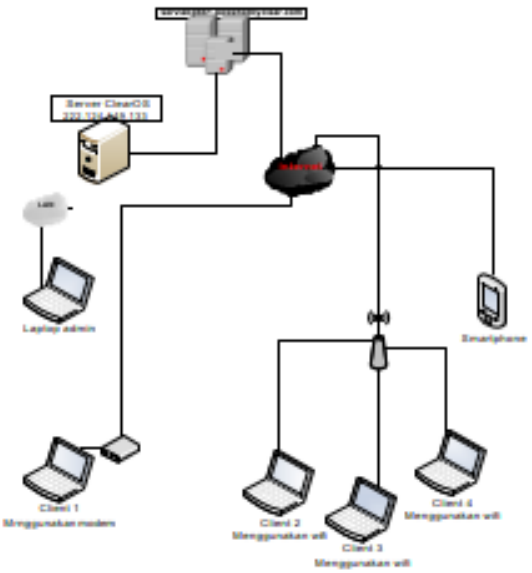
Dalam penelitian ini penulis menggunakan penelitian *Research and Development* (R&D). Menurut Sugiyono (2009:407) metode penelitian *Research and Development* yang selanjutnya akan disingkat menjadi R&D adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut.

Model Pengembangan Sistem

Penelitian ini akan menggunakan metode pengembangan *(development research)* dengan menggunakan pendekatan pengembangan model 4D (four-D model) yang dikemukakan oleh Sivasailam Thiagarajan dkk (1974). Adapun tahapan model pengembangan meliputi tahap pendefinisian *(define)*, tahap perancangan *(design)*, tahap pengembangan *(develop)* dan tahap ujicoba *(disseminate)*. Tahapan yang dilakukan pada penelitian ini baru sampai pada tahap pengembangan *(develop)*.

Desain Topologi Jaringan

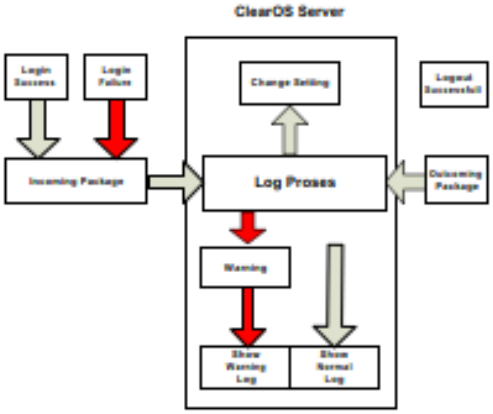
Laboratorium PTIK telah memiliki jaringan yang memadai untuk memberikan *service* kepada *client* dalam lingkup besar. Walaupun begitu, keamanan dan kelangsungan jaringan yang ada pada sistem tersebut harus dijaga dan harus dipikirkan strategi penerapan keamanan tersebut. Adapun gambaran umum dari topologinya seperti pada Gambar 3.2



Gambar 3.1
Desain Topologi Jaringan Lab PTIK

http://dx.doi.org/10.31963/elekterika.v1i2.1220

Alur kerja Server dapat dilihat pada Gambar 3.3



Gambar 3.2.
Alur Kerja ClearOS

Alur Kerja Server ClearOS sebagai *Intrusion Detection System*

Berdasarkan hasil studi literatur diambil simpulan dari berbagai penelitian serupa yang pernah dilakukan untuk menentukan alur sistem terbaik dan sesuai dengan studi kasus penelitian. Desain topologi jaringan yang digunakan tetap dengan model yang sama dengan desain topologi jaringan awal. Perubahan yang dilakukan untuk mengubah Mikrotik menjadi sistem RIDS yaitu penggunaan *firewall* dan mail. Alur kerja *Intrusion Detection System* berawal dari pendeteksian paket data yang dianggap berbahaya oleh *firewall*, berikut urutan tindakan yang dilakukan *firewall*.

HASIL DAN PEMBAHASAN

Konfigurasi Alert Notifications

Konfigurasi *alert notifications* ini merupakan tahap dimana setiap serangan yang akan masuk ke dalam system server akan terkirim ke *email admin server*.

```
IP="$(echo $SSH_CONNECTION | cut -d " " -f 1)"
HOSTNAME=$222.124.149.133/29
NOW=$(date +"%e %b %Y, %a %r")

echo 'SOMEONE from '$IP' logged into '$HOSTNAME'
on '$NOW'.' | mail -s 'SSH Login Notification'
servlabptik.unm@gmail.com
echo 'ALERT - SOMEONE Access on:' `date` `who` |
mail -s "Alert: Someone Access from `who | cut -d"(" -f2 |
cut -d")" -f1 `" servlabptik.unm@gmail.com
```

Konfigurasi snort yaitu Fail2ban

```
# JAILS
#
# SSH servers
#
[sshd]
enabled = true
filter = sshd
action = iptables[name=SSH, port=22, protocol=tcp]
         sendmail-whois[name=SSH,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com, sendername="ATTACK
DETECTOR"]
maxretry = 5
bantime = 600
logpath = /var/log/secure
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ban.
# The mail-whois action send a notification e-mail with a whois
request
# in the body.
enabled = true
filter = sshd-ddos
action = iptables[name=SSH, port=22, protocol=tcp]
         sendmail-whois[name=SSH,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com, sendername=ATTACK
DETECTOR""]
maxretry = 5
bantime = 600
logpath = /var/log/secure
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Gambar 4.9
Source code untuk mendeteksi serangan *SSH*

http://dx.doi.org/10.31963/elekterika.v1i2.1220

```
#
# FTP servers
#
[proftpd]
enabled = true
filter = proftpd
action = iptables[name=ProFTPD, port=21,
protocol=tcp]
      sendmail-whois[name=ProFTPD,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com,
sendername="FTP ATTACK DETECTOR"]
logpath = /var/log/secure
maxretry = 5
bantime = 600
port    = ftp,ftp-data,ftps,ftps-data
logpath = %(proftpd_log)s
backend = %(proftpd_backend)s
```

Gambar 4.10
Source code untuk mendeteksi serangan *FTP*

```
[sshd-ddos]
enabled = true
filter = sshd-ddos
action = iptables[name=SSH, port=22,
protocol=tcp]
        sendmail-whois[name=SSH,
dest=labptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com,
sendername=ATTACK DETECTOR""]
maxretry = 5
bantime = 600
```

Gambar 4.17
Source code untuk menangkal serangan *SSH*

```
proftpd]
enabled = true
filter = proftpd
action = iptables[name=ProFTPD, port=21,
protocol=tcp]
      sendmail-whois[name=ProFTPD,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com,
sendername="FTP ATTACK DETECTOR"]
logpath = /var/log/proftpd.log
maxretry = 5
```

Gambar 4.19
Source code untuk mendeteksi serangan FTP

Implementasi Sistem IDS

Secara umum, penerapan IDS dengan menggunakan data percobaan terhadap IP Public server1048m2yjx3.poweredbyclear.com secara langsung dilakukan dengan beberapa parameter yang dapat dilihat pada Tabel 4.2 agar mendapatkan hasil dengan kondisi yang sama.

Parameter Implementasi IDS terhadap jaringan Server *ClearOS*

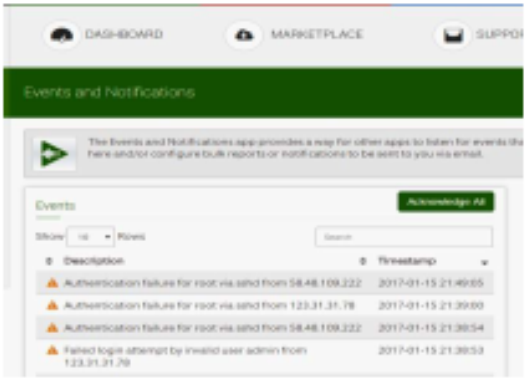
No.	Jenis Percobaan	Lama Percobaan	Tool yang digunakan	Objek Percobaan
1.	FTP Attack	15 hari	Login FTP di WinSCP	FTP Server ClearOS
2.	SSH Attack		PuTTY	Port SSH ClearOS

Table. 4.1

Tampilan Dasboard Sistem ClearOS

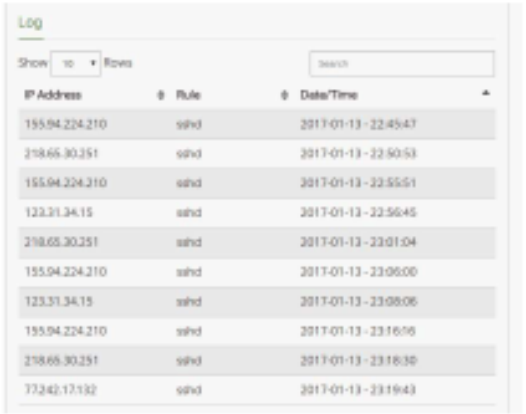
Hasil Pengiriman Email ke administrator

http://dx.doi.org/10.31963/elekterika.v1i2.1220



Hasil autentikasi user yang mencoba masuk

IP penyerang yang berhasil di Banned



Log report IP yang mencoba masuk kedalam Sistem

Uji Sistem Terhadap Serangan

Pengujian dilakukan untuk mengetahui keberhasilan sistem. *IDS* ini akan berhasil jika *admin* jaringan server ClearOS yang terdapat di Lab.PTIK UNM bisa dengan mudah melakukan monitoring jaringan, mengetahui jenis serangan yang sedang menyerang sistem yang di monitoringnya, dan menerima laporan serangan dimanapun admin jaringan berada dengan syarat admin jaringan memiliki *gadget* yang memungkinkan untuk terhubung ke email kapan saja.

Email ClearOS

Pengujian pada *email* merupakan tahapan perencanaan sebelum masuk ke inti sistem. Pengujian ini dilakukan untuk mengetahui bahwa email pengirim pada Server ClearOS telah terkoneksi dengan email penerima. Pengujian dilakukan dengan melakukan pengiriman secara manual tanpa terhubung ke *script* dan *scheduler* manapun. Berikut adalah perintah untuk melakukan pengiriman *email* secara manual.

```
echo "Percobaan dilakukan untuk menguji apakah server telah terhubung dengan gmail" | mailx –s "Testing Mail" servlabptik.unm@gmail.com
```

Gambar 4.22

Script untuk mengirim email secara manual

Implementasi Sistem IDS

Pengujian sistem IDS ini akan menghasilkan data dan informasi yang dibutuhkan untuk mengambil kesimpulan di akhir penelitian. Berdasarkan batasan masalah yang telah dibahas pada bab sebelumnya, pengujian sistem IDS akan dilakukan dengan melakukan serangan-serangan ke IP Publik server Lab PTIK.

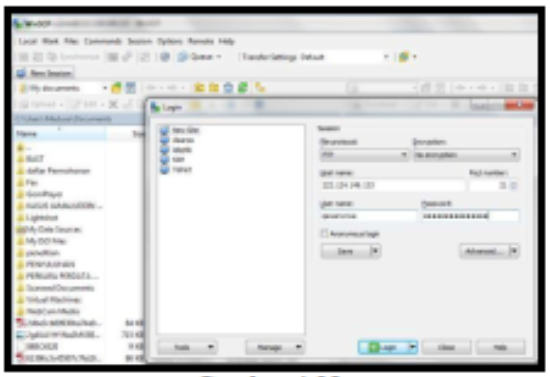
http://dx.doi.org/10.31963/elekterika.v1i2.1220

Adapun jenis-jenis serangan yang akan digunakan untuk pengujian akan dijabarkan di bawah ini.

a. *FTP Bruteforce*

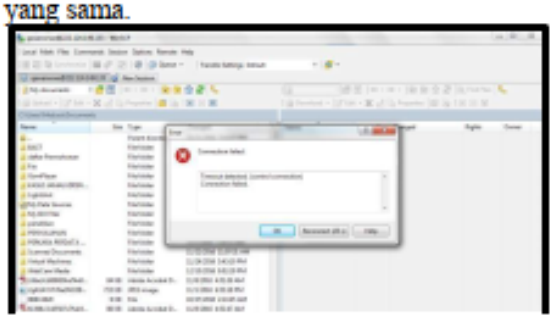
Sebelum menjalankan serangan *FTP Bruteforce* ke sistem, terlebih dahulu *rules* pada *attack detector* yang bertugas untuk menangani serangan FTP diaktifkan.

Serangan dilakukan dengan cara untuk login ke server melalui *FTP* dengan perintah "222.124.149.133" menggunakan *user* dan *password* yang salah.

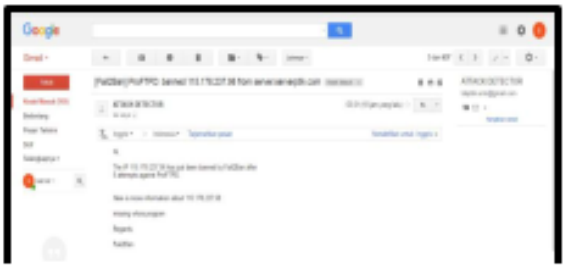


Gambar 4.32
Percobaan *login* melalui FTP menggunakan *user* dan *password* yang salah

tampilan 5 kali percobaan *login* gagal ke sistem dalam kurun waktu yang sangat dekat oleh IP yang sama.



Gambar 4. 36
Koneksi penyerang di drop oleh server

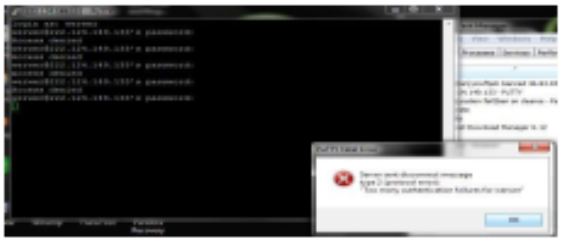


Gambar 4. 37
Report FTP *Attack* diterima melalui email

SSH *Bruteforce*

Sebelum menjalankan serangan SSH *Bruteforce* ke sistem, terlebih dahulu *script* dan *scheduler* yang bertugas untuk menangani serangan SSH diaktifkan.

Pada saat dilakukan percobaan login dengan *user* dan *password* yang salah, akan menampilkan pesan *error*



Gambar 4. 43
Pesan *errorlogin failure via ssh*

Pembahasan

Penulis melakukan percobaan melakukan serangan melalui dua port jaringan yaitu, *SSH* dan *FTP*. *SSH* dan *FTP* merupakan port yang paling rentan akan serangan yang dilakukan oleh attacker. Tipe serangan yang dilakukan adalah *SSH Bruteforce* dan *FTP bruteforce*. Serangan *SSH bruteforce* dan *FTP*

http://dx.doi.org/10.31963/elekterika.v1i2.1220

bruteforce ini bertujuan untuk mengeksploitasi sistem seseorang dengan mencoba masuk kedalam sistem menggunaka *user* dan *password* yang salah. Penulis merancang dan menkonfigirasi sistem keamanan dengan *IDS* dan mengunakan *ClearOS*. Dalam sistem keamanan ini *IDS* berfungsi untuk mendeteksi penyusupan yang coba dilakukan oleh *attacker*.

Kesimpulan

Berdasarkan penelitian dan pengujian yang sudah dilakukan mengenai system pengamanan jaringan server dengan metode IDS (*Intrusion Detection System) Snort* berbasis *ClearOS*, penulis dapat menarik beberapa kesimpulan sebagai berikut :

1. Sistem keamanan jaringan server dengan metode IDS menggunakan ClearOS pada Lab. PTIK dibangun dalam 2 langkah :
   a. Implementasi IDS
      Penerapan Sistem IDS dengan menggunakan data percobaan terhadap *traffic* jaringan server Lab.PTIK secara langsung dilakukan dengan beberapa parameter yaitu FTP *Brutefoce*, dan SSH *Brutefoce*
   b. Pengujian Sistem
      Pengujian dilakukan secara bertahap yang terdiri dari :
      a) Pengujian Email (Email Server)
         Pengujian dilakukan dengan melakukan pengiriman secara manual
      b) Sistem IDS
         pengujian sistem RIDS dilakukan dengan melakukan serangan-serangan ke jaringan server Lab. PTIK dengan parameter implementasi.
2. Untuk menampilkan *report* serangan dalam bentuk *log* dan *mailreport* secara otomatis pada mikrotik dilakukan dalam 4 cara yaitu:
   a. FTP *Brutefoce*
   b. SSH *Brutefoce*

DAFTAR PUSTAKA

Andri Kristanto. 2003. Jaringan Komputer. Graha Ilmu.

Cheyantie.2012 "About Microsoft Visio 2010" From http://blog.ub.ac.id/cheyantie/files/2012/10/Abo ut-Microsoft-Visio-20101.pdf (diakses 22:54 19 November 2012)

Jack Febrian & Farida Andayani. 2012 "Kamus Komputer dan Istilah Teknologi Informasi" Bandung:Informatika

Jogiyanto, Hartono. 2009. Analisis dan Desain Sistem Informasi, Edisi III. Yogyakarta: ANDI.

Kumar, 2002 . Management of Hospital. Hospital Administration In the 21 Century.

http://dx.doi.org/10.31963/elekterika.v1i2.1220

New Delhi: Deep &Deep Publication. PVT.LTD

Micro, Andi. 2012. Buku Hijau Clear OS 5.2 Edisi Revisi. Banjarbaru. Andi Micro.

O'Brien, James A. dan Marakas, George M. 2011. "Management Information Systems, 10th Edition". McGraw-Hill/ Irwin, New York

Odon, Wendel, 2005.Computer Network First Step, Penerbit Andi : Yogyakarta

Oskar Pearson. 2003 " Squid A User's Guide" From http://www.squid-cache.org (diakses 00.30 21 Desember 2012)

Setyosari, Punaji. 2010. Metode Penelitian Pendidikan dan Pengembangan, Jakarta : Kencana.

Sofana, Iwan. 2008. Membangun Jaringan Komputer (Membuat Jaringan Komputer (Wire & Wireless) untuk Windows dan Linux. Informatika. Bandung.

Sugiyono. (2009). Metode Penelitian Bisnis (Pendekatan Kuantitatif, Kualitatif, dan R&D). Bandung: Alfabeta.

Sukmaaji, Anjik, S.Kom & R Rianto S.Kom. 2008. "Jaringan Komputer: K'onsep Dasar Pengembangan Jaringan Dan Keamanan Jaringan" Yogyakarta: Andi Offset

Sutanta, Edhy. 2005. Komunikasi data dan Jaringan Komputer. Yogyakarta: Graha Ilmu.

Wagito. 2007. "Jaringan Komputer (Teori dan Implementasi Berbasis Linux)" Yogyakarta: Gava Media

http://dx.doi.org/10.31963/elekterika.v1i2.1220