SISTEM PENDEKTEKSIAN PENYUSUP BERBASIS SMS GATEWAY PADA PROSES OTENTIKASI *FILE TRANSFER PROTOCOL*(FTP)

Rahmad Abdillah
Jurusan Teknik Informatika Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
E-mail: rahmad.abdillah@uin-suska.ac.id

Abstrak
HIDS (*Host Based Intrusion Detection System*) yang ada pada saat ini belum mampu memberikan solusi tepat dalam hal notifikasi penyusup. Penelitian ini mengusulkan sebuah konsep notifikasi pada HIDS menggunakan SMS Gateway khususnya pada proses otentikasi layanan FTP. HIDS menggunakan konsep analisa terhadap file log meliputi proses pengumpulan informasi, ekstrak informasi dananalisa hasil ekstrak informasi. Sedangkan SMS Gateway sebagai model pengiriman laporan penyusup kepada administrator. Perpaduan HIDS dan SMS Gateway telah berhasil memberikan notifikasi penyusup lebih cepat kepada administrator.

Katakunci : HIDS dan SMS Gateway

Abstract
Today, HIDS (Host Based Intrusion Detection System) can not give the optimal solution about intruder notification.This study propose a concept about intruder notification on HIDS using SMS Gateway especially in authentication process at FTP service. That HIDS using log analysis concept which include information gathering process, information extraction and information extraction analysis. And SMS gateway as a notification report to administrator. By combination of these two kinds of technologies, administrator get the information about intrusion earlier.

Keyword : HIDS dan SMS Gateway

Pendahuluan

Sistem pendeteksian penyusup berbasis host atau host based intrusion detection system(HIDS) telah menempati peranan yang sangat penting di dalam melindungi sebuah host. Cara kerja HIDS tersebut adalah memberikan informasi penyusup kepada admin apabila terjadi penyusupan kedalam server ataupun host[1].Tentu saja dengan informasi yang dihasilkan tersebut, admin dapat segera mengambil tindakan. Ada banyak sistem pendeteksi penyusup yang telah beredar, seperti: Bro dan Snort. Penggunaan Bro IDS lebih optimal jika diterapkan pada jaringan yang lebih besar (Gbps), sedangkan Snort lebih optimal pada proses analisa paket data[2]. Namun untuk sistem pendeteksian pada proses otentikasi layanan FTP (File Transfer Protocol), Snort dan Bro belum optimal pada proses penyampaian informasi penyusup. Misalnya saja pada Snort, jika ingin mendapatkan informasi penyusup menggunakan media selain notifikasi sistem, maka harus menggunakan aplikasi tambahanseperti QuickPage [3][4].

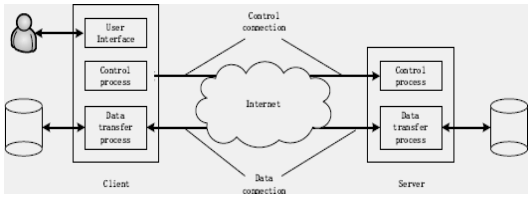
Aplikasi ini memberikan dukungan layanan penyampaian informasi melalui pager. Sedangkan pada Bro, notifikasi hanya sebatas informasi pada sistem bukan langsung kepada administrator. Pada

penelitian Wei Li dkk, Penyampaian informasi pada administrator hanya sebatas notifikasi sistem saja [5]

Pada penelitian ini, kami merancang dan mengimplementasikan metode HIDS dengan menggunakan konsep analisa terhadap file Log pada server khususnya Log FTP dan SMS Gateway sebagai perangkat untuk mengirimkan informasi penyusup kepada administrator. Langkah pertama pada aplikasi ini adalah menerapkan konsep HIDS, yaitu penggunaan file log sebagai resource utama. Kemudian file log tersebut akan dilakukan pemrosesan melalui tiga tahap yaitu mengumpulkan informasi log file, mengumpulkan informasi khusus pada log file (parsing) dan melakukan analisis terhadap log tersebut. Proses HIDS ini dilakukan secara berkala. Kedua, setelah berhasil melakukan analisa terhadap file log tersebut, diperoleh IP Adress yang ditetapkan sebagai penyusup, kemudian SMS Gateway akan mengirimkan informasi tersebut kepada administrator. Sehingga administrator dapat segera mengetahui informasi mengenai penyusup yang ada pada servernya.

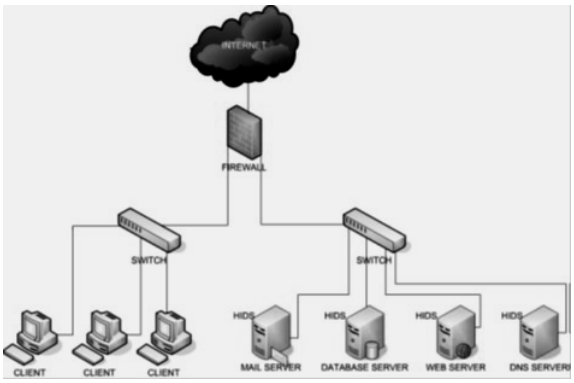
Bahan Dan Metode

File Transfer Protocol (FTP), salah satu protokol komunikasi jaringan yang paling sering digunakan saat ini, terutama di Internet. FTP merupakan sebuah layanan yang berjalan pada layer aplikasi yang mana melakukan kontrol dan monitoring file antara dua komputer yang melakukan komunikasi dua arah. Tujuan dari FT ini adalah bagaimana meningkatkan performa ketika saling berbagi file, terutama efiensi dan kehandalan serta transparansi ketika melakukan proses pengiriman data kepada pengguna [6].



Gambar 1. Proses Pertukaran Data Menggunakan FTP

Cara kerja HIDS (Host Based Intrusion Detection System) secara umum adalah setiap host atau server diimplementasikan HIDS, kemudian mulai menggali informasi seputar host tersebut. HIDS melakukan monitoring dan kontrol terhadap file tertentu seperti file Log pada host, serta memberikan informasi ataupun peringatan kepada administrator bahwa terdapat penyusup yang melakukan pengubahan atau melakukan akses terhadap host tersebut [7]. HIDS juga dapat melakukan monitoring terhadap proses yang sedang berjalan, aktivitas pada aplikasi dan segala bentuk event yang ada pada host [8].



Gambar 2. Implementasi HIDS[9]

Short Message Service (SMS) dapat mencapai panjang karakter hingga 160, yang mana setiap karakter merupakan referensi dari 7 bit alphabet [10].

Analisa terhadap File Log

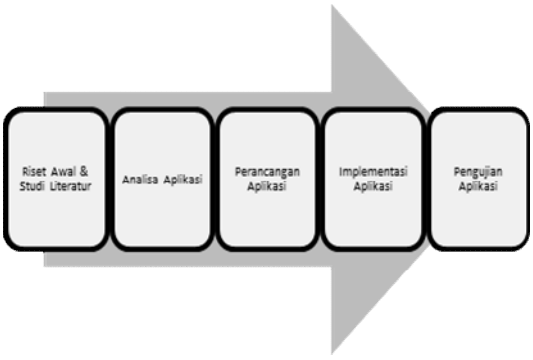
file log mengandung banyak sekali catatan ataupun rekaman peristiwa maupun perilaku pada system komputer serta segala event dari system operasi, aplikasi dan pola perilakunya. Biasanya file Log digunakan untuk melakukan proses debug, monitoring dan pendeteksian keamanan [5]. Ada beberapa tahapan di dalam melakukan analisa terhadap file Log yaitu:

1.Akses terhadap file Log
Penggunaan teknik yang tepat ketika mengakses sebuah file Log akan memberikan hasil yang maksimal terhadap informasi yang akan dicari.

2.Melakukan seleksi terhadap informasi di dalam file Log
Setelah berhasil melakukan akses terhadap file log dengan menggunakan teknik akses tertentu, maka selanjutnya adalah memilah-milah informasi yang akan diambil (proses Extract). Informasi yang diambil sepertinama host, layanan yang dimonitor dalam hal ini adalah FTP, IP address yang mengakses layanan dan username yang akan digunakan.

3.Analisa terhadap hasil seleksi
Proses ini melakukan analisa pada informasi yang telah diperoleh, seperti IP address yang berusaha melakukan akses terhadap layanan FTP khususnya gagal melakukan proses otentikasi.

Metode penelitian yang akan digunakan adalah sebagai berikut:



Gambar 3. Metode Penelitian

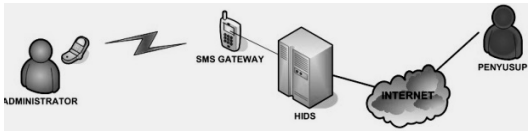
Berdasarkan Gambar 3, tahapan penelitian yang akan digunakan yaitu riset awal dan studi literatur, analisa aplikasi, perancangan aplikasi, implementasi aplikasi dan pengujian aplikasi. Berikut penjelasan masing-masing tahapan:

1.Riset Awal dan Studi Literatur
Tahapan ini mengulas tentang latar belakang penelitian seperti menemukan permasalahan yang ada bersumber dari penelitian, buku, jurnal ataupun media lainnya yang saling keterkaitan.

2.Analisa aplikasi
Aplikasi ini akan berjalan bersamaan dengan HIDS yang telah terpasang di dalam server. Misalkan pada sebuah server telah terpasang IDS yang mampu melakukan pendeteksian terhadap proses otentikasi FTP, kemudian aplikasi yang akan dibangun secara otomatis memberikan notifikasi jika terjadi penyusup kepada administrator melalui media SMS Gateway.
3.Perancangan aplikasi
Tahapan ini membahas tentang bagaimana aplikasi akan dibangun terutama informasi seperti apa saja informasi yang akan dibutuhkan oleh aplikasi.

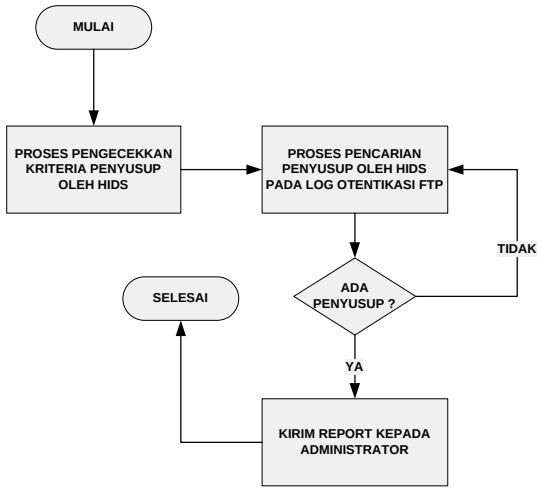
4.Implementasi Aplikasi
Tahapan ini membahas tentang lingkungan dari aplikasi yang akan menggunakan konsep SMS gateway, seperti kebutuhan system operasi, RAM, HDD, bahasa pemograman yang akan digunakan.

5.Pengujian aplikasi
Berdasarkan Gambar 4, aplikasi akan memberikan notifikasi penyusup jika menemukan beberapa kriteria yang telah ditetapkan sebagai penyusup oleh HIDS. Setelah dilakukan pengecekkan kriteria oleh HIDS, jika ditemukan penyusup maka HIDS akan memberikan perintah kepada aplikasi untuk mengirimkan informasi penyusup kepada administrator melalui SMS gateway.



Gambar 4. Implementasi HIDS

Hasil Dan Pembahasan
Flowchart dari cara kerja aplikasi dapat dilihat pada Gambar 5, berikut penjelasannya:

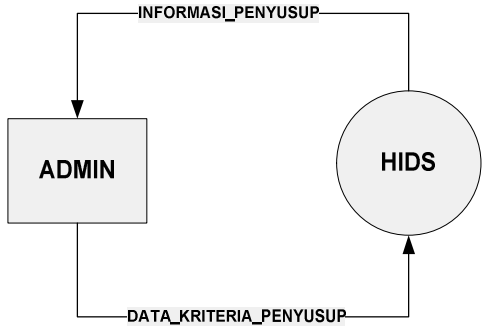


Gambar 5. Diagram alir sistem

Administrator server menentukan kriteria yang dianggap penyusup oleh HIDS, misalkan terdapat IP Address gagal melakukan proses otentikasi FTP sebanyak 3 kali maka HIDS akan menetapkan IP Address tersebut sebagai penyusup. Setelah ditetapkan kriteria yang dimaksud, maka HIDS akan mulai melakukan pengecekkan secara berkala terhadap log otentikasi FTP. Jika tidak ditemukan penyusup, maka HIDS akan terus menemukan sampai ada informasi penyusup berdasarkan kriteria yang telah ditetapkan. Jika terdapat penyusup sesuai dengan kriteria yang telah ditentukan, maka IP address yang dianggap sebagai penyusup dicatat pada server dan SMS gateway mulai menjalankan perintah untuk mengirimkan informasi penyusup kepada administrator.

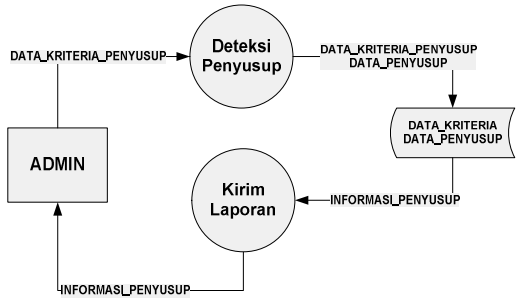
Analisa Aplikasi
Analisa aplikasi secara fungsional berkaitan dengan bagaimana data tersebut di dalam aplikasi beredar, seperti pembahasan Data Flow Diagram dan Context Diagram.Gambar 5 dan 6 menunjukkan bagaimana data beredar di dalam aplikasi. Context Diagram merupakan gambaran secara umum informasi apa saja yang beredar di dalam aplikasi. Pada gambar 6

tampak terlihat 2 aktor penting, yaitu admin dan HIDS. Admin memberikan kriteria tentang penyusup sedangkan HIDS memberikan informasi mengenai siapa saja penyusup yang telah terindikasi.



Gambar 6.Context Diagram

Gambar 7 menjelaskan tentang DFD yaitu penjelasan yang lebih rinci dari context diagram terutama pada aliran data. Ketika admin memasukkan data kriteria penyusup kedalam sistem, maka sistem akan menjadikan kriteria tersebut sebagai acuan untuk mendeteksi penyusup. Kriteria tersebut disimpan di dalam sebuah file.Setelah itu system mulai melakukan pendeteksian terhadap log file otentikasi FTP. Apabila ditemukan penyusup sesuai dengan kriteria yang telah ditentukan, maka system akan mengambil informasi data penyusup seperti IP address dan disimpan di dalam system. Setelah itu barulah sistem akan memberikan arahan untuk mengirimkan informasi penyusup kepada administrator melalui proses kirim laporan.



Gambar 7. Data Flow Diagram

Untuk dapat mengetahui detil secara fungsional dari DFD yang telah dijelaskan pada gambar 6, tabel 1 memberikan informasi secara detil dari aliran data pada aplikasi.

Tabel 1. Informasi mengenai proses pada DFD

No	Daftar proses	*Input*	*Output*	Keterangan
1	Deteksi Penyu-sup	Data Kriteria Penyu-sup	Data Penyu-sup	Pada proses ini, terdapat beberapa inputan data seperti kriteria penyusup meliputi gagal melakukan proses otentikasi FTP sebanyak x kali. Kemudian setelah system mendapatkan data kriteria penyusup, maka sistem akan mengecek log otentikasi untuk mendapatkan data penyusup.
2	Kirim Lapor-an	-	Informa si Penyu sup	Informasi yang akan dikirimkan oleh sistem menggunakan teknologi SMS Gateway kepada Administrator adalah data penyusup, seperti IP address.

Sedangkan pada tabel 2, berisikan informasi mengenai penjelasan dari tiap aliran data di dalam sistem.

Tabel 2.keterangan aliran data pada DFD level 1

No	*Nama*	*Deskripsi*
1	Data Kriteria Penyusup	Data ini berisikan tentang kriteria apa saja yang dapat dianggap sebagai penyusup. Misalkan terdapat IP address yang selalu gagal melakukan proses otentikasi menggunakan nama pengguna x.
2	Data Penyusup	Berupa informasi mengenai penyusup seperti IP address
3	Informasi Penyusup	Berupa informasi mengenai penyusup seperti IP address

Perancangan Aplikasi

Pada tahapan ini, konsep yang akan diterapkan pada perancangan aplikasi ini adalah procedural, maksudnya adalah rancangan dari algoritma *pseudo code* yang akan digunakan. Berikut daftar algoritma *pseudo code*:

A. Proses deteksi penyusup

```
Max_Fault()
{
Max_Fault=3
}
Crosscheck_log()
{
Max_Fault
```

```
find "Invalid user"  while
read i
do
Write_Intrusion
done
}
```

B. Proses Kirim Laporan

```
Write_Intrusion()
{
count= "Invalid user"
ip=ip
already=false
if already = false then
if count >Max_Faultthen
write ip
send ip
endif
endif
}
```

Implementasi Aplikasi

Aplikasi yang dibangun memiliki dua bagian utama yang tidak dapat dipisahkan, yaitu:

1.Implementasi Aplikasi Utama

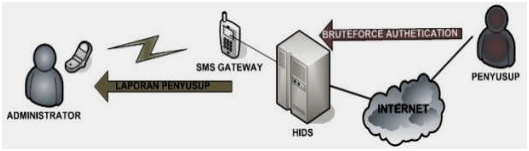
Implementasi ini meliputi proses utama yang terjadi pada HIDS yaitu proses untuk melakukan proses deteksi penyusup. Proses deteksi penyusup ini terdiri dari beberapa kegiatan yaitu proses untuk melakukan analisa file log otentikasi dan proses untuk mengambil informasi penyusup.

2.Implementasi Aplikasi Pendukung

Sedangkan pada implementasi aplikasi pendukung terdapat perangkat dan aplikasi SMS Gateway yang dapat melakukan broadcast SMS kepada administrator.

Pengujian Aplikasi

Pada tahapan ini, dilakukan pengujian terhadap server dengan cara melakukan tindakan serangan bruteforce authentication pada protokol ftp. Kemudian aplikasi HIDS mencoba melakukan tugasnya yaitu melakukan proses deteksi penyusup. Pada gambar 8 terlihat sekali bagaimana proses pengujian yang telah dilakukan.



Gambar 8. Pengujian penyusupan kedalam server

Berikut uraian penjelasan pada gambar 8 yaitu:

Penyusup melakukan tindakan *information gathering* terhadap server, yaitu suatu tindakan untuk mengumpulkan informasi pada suatu host atau server. Penyusup berhasil melakukan identifikasi terhadap server, bahwa terdapat layanan FTP yang sedang berjalan. Kemudian penyusup mulai melancarkan aksinya untuk dapat masuk kedalam layanan FTP. Penyusup memutuskan untuk melakukan tindakan *bruteforce authentication* terhadap proses otentikasi FTP.

Selama host telah dipasang atau diimplementasikan HIDS dan SMS gateway maka akan terjadi proses deteksi penyusup dan kirim laporan. HIDS akan selalu mendeteksi penyusup berdasarkan kriteria yang telah ditentukan. Jika telah berhasil menemukan penyusup maka HIDS akan menugaskan SMS gateway untuk memberikan informasi penyusup kepada administrator segera.

Kesimpulan yang telah dihasilkan dari tahapan pengujian ini adalah HIDS berhasil mendeteksi penyusup serta memberitahukan kepada administrator bahwa terdapat penyusup melalui teknologi SMS gateway. Gambar 9 tentang informasi yang diperoleh oleh administrator.

Gambar 9 . Hasil kirim laporan dari sistem

Kesimpulan

Hasil dari penelitian yang telah dilakukan adalah HIDS dan SMS Gateway telah berhasil diimplementasikan dan dikolaborasikan. HIDS dengan fitur untuk deteksi penyusup yang berada pada server khususnya pada

layanan FTP. Sedangkan SMS Gateway sebagai media pengirim informasi penyusup kepada administrator.

Sebaiknya sistem dapat mendeteksi lebih banyak lagi pola-pola penyusup seperti membatasi kelompok IP Address, apakah dummy atau bot yang mencoba mengakses layanan.

Daftar Pustaka

[1]Masoud Ghorbanian, Bharanidharan Shamugam, Ganthan Narayansamy, and Norbik Bashah Idris, "Signature-based hybrid Intrusion detection system (HIDS) for android devices," in Business Engineering and Industrial Applications Colloquium (BEIAC), 2013 IEEE, Langkawi, 2013, pp. 827 - 831.

[2] Pritika Mehra, "A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 6, pp. 383-386, August 2012.

[3] Andrew R. Baker and Joel Esler, Snort® IDS and IPS Toolkit, Toby Kohlenberg, Ed. Burlington: Syngress, 2007.

[4] Jacob Babbin, Simon Biles, and Angela D. Orebaugh, Snort Cookbook.: O'Reilly, 2005.

[5] Lin Ying, Zhang Yan, and Ou Yang-jia, "The Design and Implementation of Host-Based Intrusion Detection System," in Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium, Jian, China, 2010, pp. 595-598.

[6] Wei Li, Xin Hu, Yajing Jia, and Zhengguan Huang, "Proxy-based FTP secure audit technology," in Software Engineering and Service Science (ICSESS), 2014 5th IEEE, Beijing, 2014, pp. 667 - 670.

[7] Anuradha and A. Singhrova, "A host based intrusion detection system for DDoS attack in WLAN," in Computer and Communication Technology (ICCCT), 2011 2nd International Conference, Allahabad, 2011, pp. 433-438.

[8] Rahmad Abdillah, "Pencegahan Brute Force Authentication Via Protokol Ssh (Secure Shell) Menggunakan Metode Host Based Intrusion Detection System (HIDS)," in Konferensi Nasional Sistem Informasi (KNSI), Bali, 2012, pp. 1-6.

[9] Rahmad Abdillah, "QUICK REPORT FOR HOST BASED INTRUSION DETECTION SYSTEM (HIDS)," Jurnal Sains, Teknologi dan Industri, vol. 11, no. 2, 2014.

[10] N Croft, "On forensics: A silent SMS attack," in Information Security for South Africa (ISSA), Johannesburg, Gauteng, 2012, pp. 15-17.