PERANCANGAN PENGAMANAN *SERVER* SECARA OTOMATIS MENGGUNAKAN METODE ADAM *(AUTOMATIC EVENT DETECTION AND ACTIVITY MONITORING)*

Anggraini Kusumaningrum, Rolas Sianturi
Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Adisutjipto Yogyakarta
informatika@stta.ac.id

ABSTRACT

In an era like today's global, Internet-based information system security is a must to be considered, because of the public nature of the internet network and global is not safe. Basically the threat is coming from someone who wishes mempuyai gain illegal access to a computer network. Whenever there is a threat encountered on the server such as port scanning, the attacker IP addresses will be captured. Next will be used method Automatic Event Detection and Activity Monitoring (ADAM) to process security. ADAM will carry out retaliatory attacks in the form of a computer virus that was sent to the attacker. For this reason when a computer network is attacked by the intruder, then ADAM server will detect this type of attack is done, then asked for help from another server to strike back. Security server by applying the method ADAM able to do the blocking of port scanning the attacker did not end there ADAM will then send the file is a virus automatically. In terms of time efficiency, the method of securing the ADAM automatically faster than ıf all phases of the security is done manually. ADAM test non-adaptive systems this takes 4.4 minutes, while the time taken by the ADAM system to immobilize the attacker system only 1 minute 03:59 seconds, so the method ADAM works faster. Traffic normal state (RX 232B, 144B TX), but when encountered in the form of port scanning attacks become 21.46Kib TX RX 25.83Kib, and after working as RX 219B ADAM TX127B, resulting in a significant reduction in traffic.

Keywords: Information Systems Security, Server Monitoring, Threat Detection.

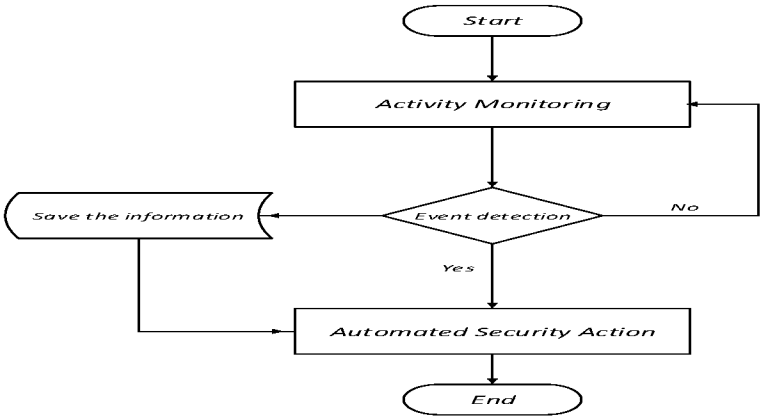
1. Pendahuluan

ADAM merupakan sebuah metode pengamanan jaringan yang mampu melakukan *monitoring* secara *real time*, dan menentukan kebijakan pengamanan secara otomatis ketika ditemui sebuah serangan. ADAM akan bekerja ketika ditemui serangan berupa *port scanning* dari IP yang berasal dari kelompok IP *whitelist*. Perumusan masalah pada metode ADAM yaitu merancang dan membangun sebuah keamanan *server* yang mampu mendeteksi adanya sebuah aktivitas serangan, membangun sistem yang adaptif dan mampu mengatasi masalah terhadap serangan dan mampu berkomunikasi dengan *server* lainnya untuk memberikan sebuah serangan balasan terhadap sistem *attacker* secara otomatis. Sistem automatisasi hanya bekerja ketika ditemui serangan *port server*, komunikasi antar *server* hanya pada dua buah *server* dengan bahasa pemrograman berbasis PHP dan sistem operasi *Ubuntu*.

2. Metodologi Penelitian

2.1 Analisa Metode ADAM

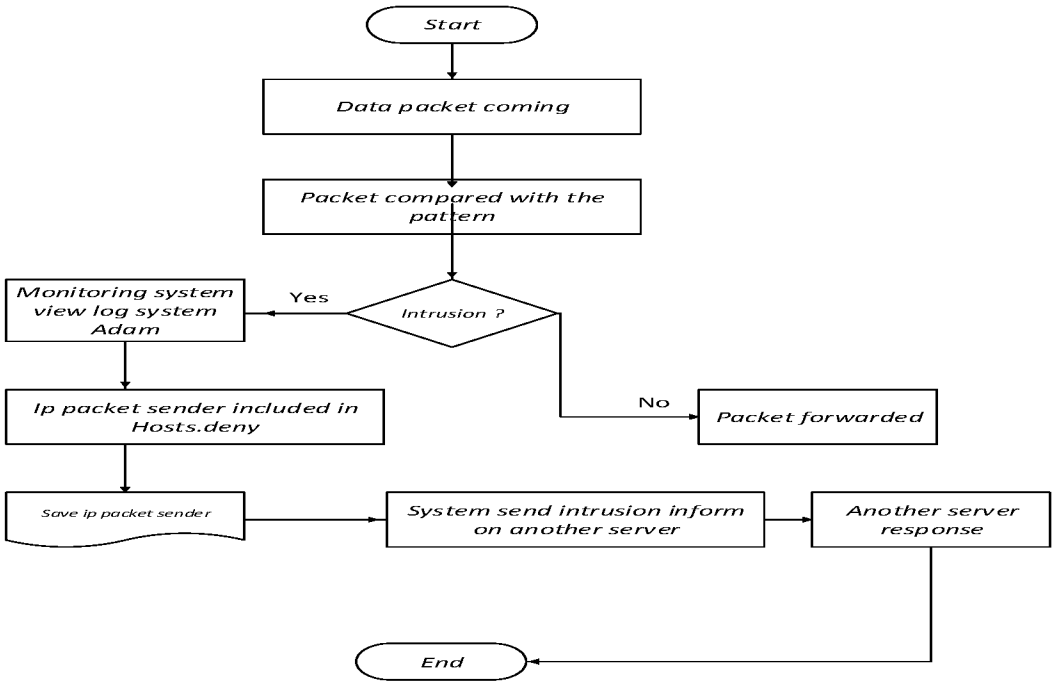
ADAM merupakan sebuah metode pengamanan jaringan yang mampu melakukan *monitoring* secara *realtime*, dan mendeteksi serangan *port scanning* terhadap *server*, kemudian melakukan tindakan sesuai kebijakan keamanan yang telah ditetapkan. Dalam perancangan metode ADAM dibutuhkan sistem *monitoring* yang mampu mendekteksi akan adanya serangan terhadap *server* untuk mendapatkan sebuah pemicu terjadinya automatisasi.



Gambar 1. Perancangan Metode ADAM

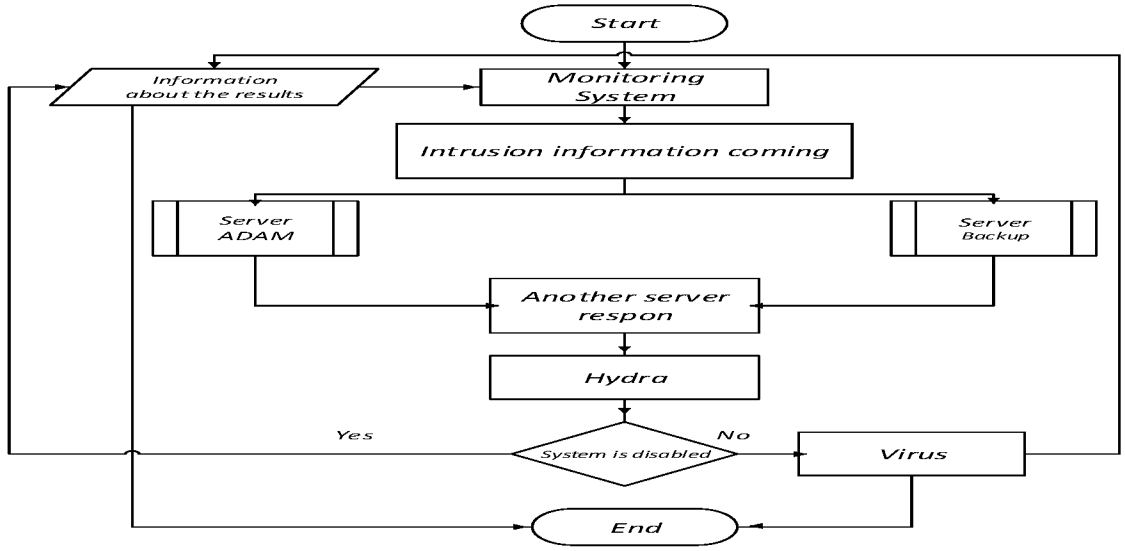
2.2 Perancangan Sistem

Bagan alur sistem *monitoring* pada *server* ini bekerja secara *real time*untuk memantau paket-paket data yang dilewatkan dalam jaringan komputer.



Gambar 2. Perancangan Sistem *Monitoring*

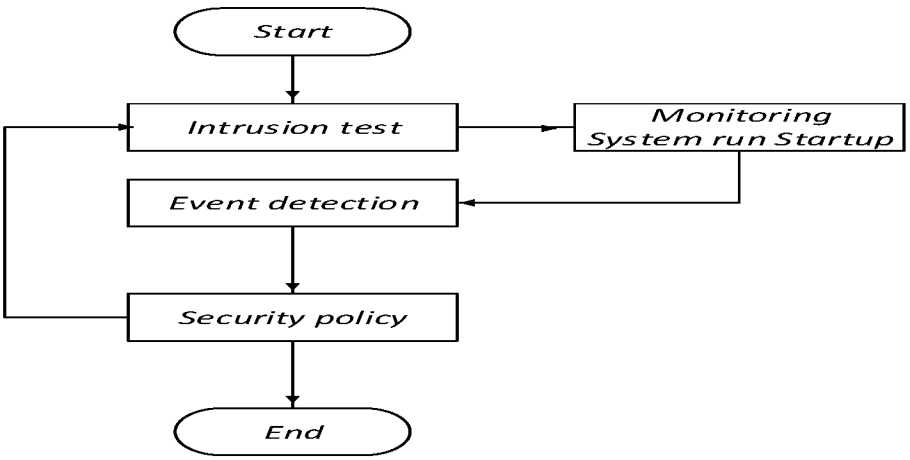
Pada kebijakan keamanan yang akan diterapkan pada sistem keamanan *server* yaitu ketika sistem *monitoring* mendeteksi adanya serangan, maka server menghubungi *server* lain untuk menginfomasikan adanya indikasi serangan.



Gambar 3. Perancangan Kebijakan Keamanan

2.3 Perancangan Uji Coba

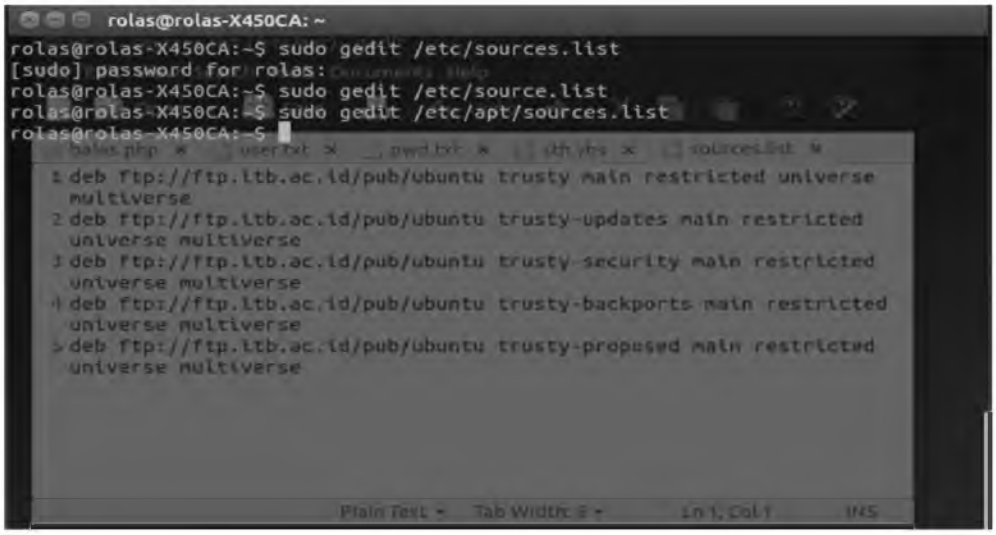
Pengujian sistem keamanan *server* dengan menerapkan metode *ADAM* dimulai dengan melakukan intrusi terhadap *server*, oleh sistem *monitoring* akan terdeteksi adanya sebuah ancaman maka secara otomatis *security policy*yang diterapkan pada *server* akan bekerja untuk memberikan kebijakan keamanan kepada pelaku intrusi. Uji serangan yang dilakukan menggunakan *Tools Zenmap*untuk*scanning port.*Dalam mengamankan sebuah *server* dengan sistem keamanan yang dibangun ini seorang *administrator* jaringan tidak banyak melakukan intruksi untuk sistem keamanan ini karena sistem keamanan bekerja secara adaptif dan automatisasi.



Gambar 4. Perancangan Uji Coba

3. Implementasi Dan Pembahasan

Sebelum melakukan instalasi dan konfigurasi *apache2* pastikan terlebih dahulu bahwa *repository Ubuntu 14.04 LTS* sudah diganti dengan repo local untuk mempercepat proses *update package Ubuntu.*



Gambar 5. *Source Repository* Ubuntu 14.04

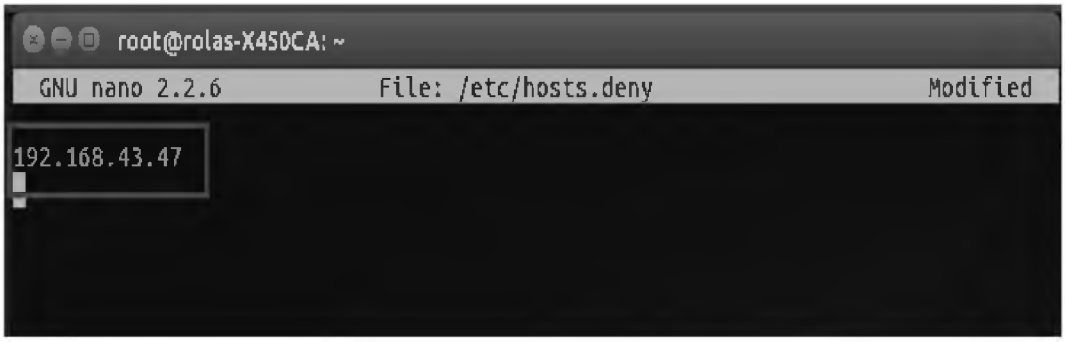
Konfigurasi system pada *server backup* terdapat beberapa proses konfigurasi yaitu *apache2, php5, ftp server, incrontab, lynx* dan *hydra.*

Gambar 6. *Cron Jobs Server Backup*

Informasi dari *server* ADAM diletakan pada direktori FTP s*erver backup* oleh *server* ADAM. Yang kemudian diambil oleh *server backup* untuk melakukan serangan terhadap *attacker.* Informasi dari *server* ADAM diletakan pada direktori FTP s*erver backup* oleh *server* ADAM. Yang kemudian diambil oleh *server backup* untuk melakukan serangan terhadap *attacker.*

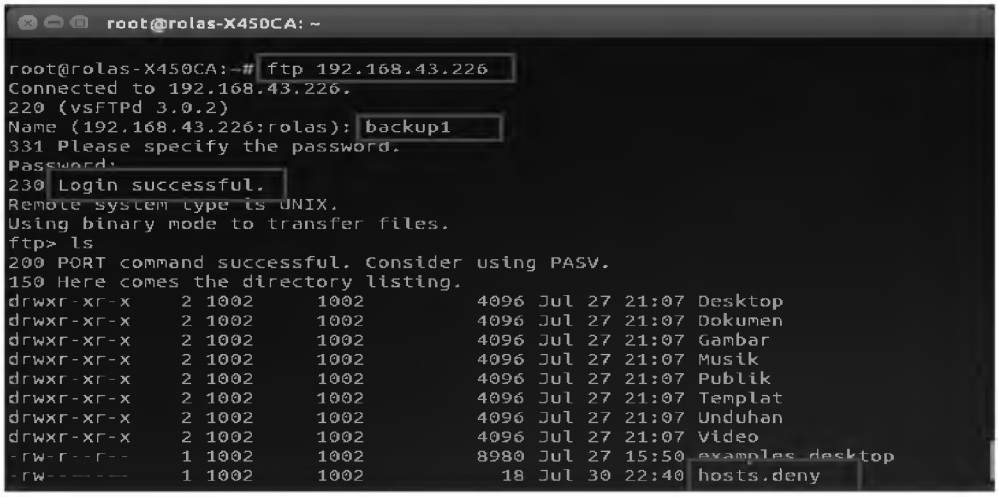
3.1 Penjelasan Sistem ADAM

Sistem pendeteksi serangan yang diterapkan pada sistem ADAM ini adalah kemampuan *server* dalam menangkap informasi *attacker* yang melakukan aktivitas *hacking*.



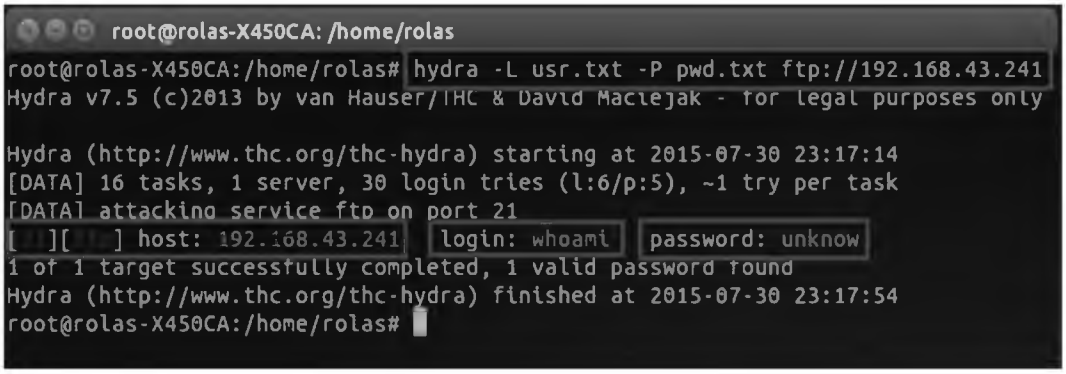
Gambar 7. Hasil Deteksi Serangan

Sistem komunikasi antar *server*, yakni *server* ADAM dan *server backup* bertujuan untuk berbagi informasi tentang *attacker*, yang kemudian melakukan serangan balasan secara bersama-sama.



Gambar 8. Hasil Komunikasi Antar *Server*

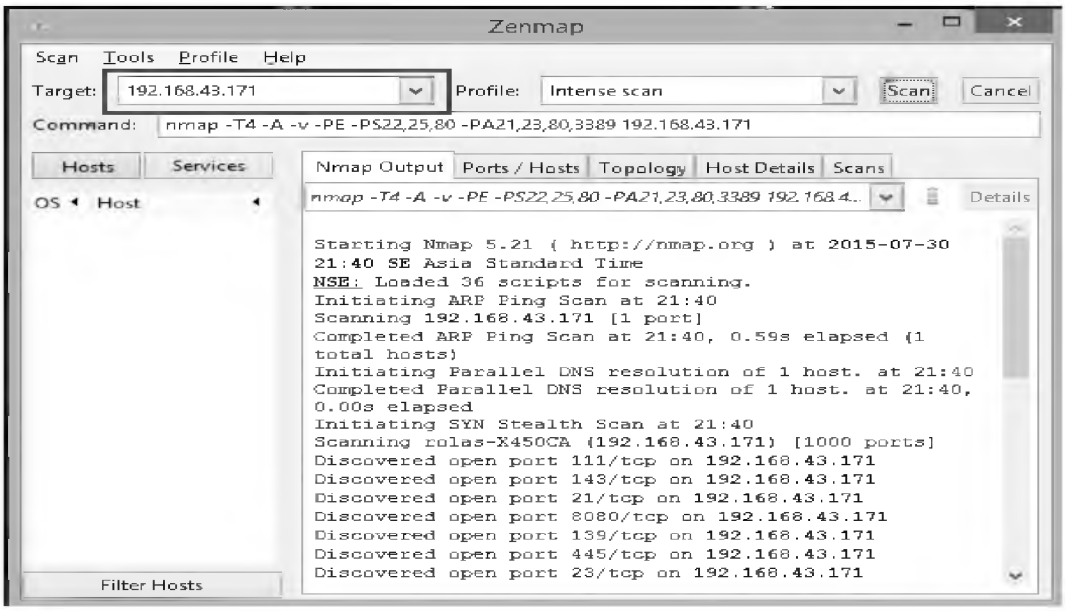
Sistem serangan balasan yang diterapkan pada sistem ADAM dimaksudkan untuk memberikan efek jera terhadap *attacker*.



Gambar 9. Hasil Serangan Balasan

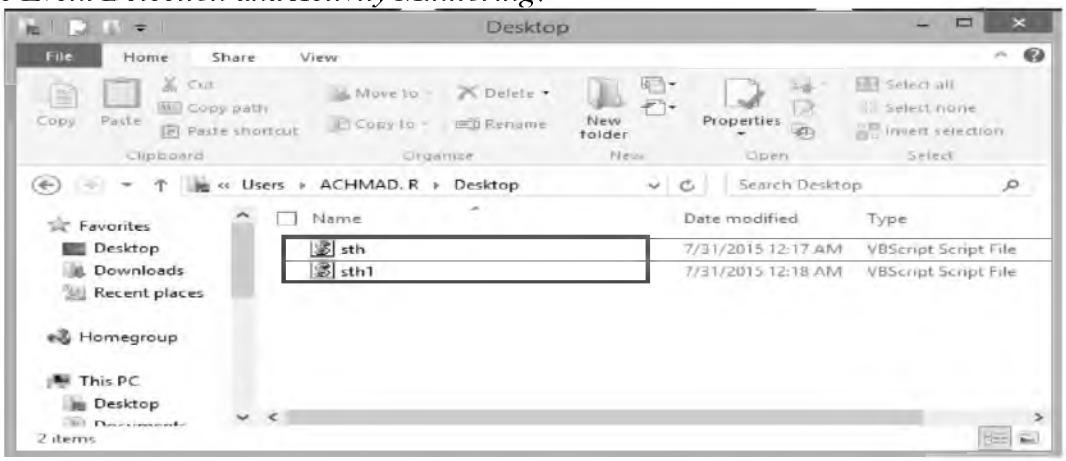
3.2 Uji Deteksi Serangan

Uji deteksi serangan pada *server* ADAM menggunakan *ports entry* yang bertugas untuk mendeteksi akan adanya serangan pada *port server* dan menangkap IP *attacker* serta menyimpannya ke dalam *file hosts.deny*.



Gambar 10. *Scanning port* dengan *nmap*

Uji otomatisasi sistem ADAM adalah pengujian system secara keseluruhan dengan metode *Automate Event Detection and Activity Minitoring*.



Gambar 11. *File Virus* Uji Otomatis

4. Penutup

4.1 Kesimpulan

1. Sistem otomatisasi ADAM mampu bekerja dalam menangani adanya jenis serangan terhadap *port server*, dan mampu menangkap IP *address* yang melakukan jenis serangan tersebut.
2. Sistem ADAM yang diterapkan pada *server* mampu berkomunikasi dengan *server* lainnya untuk berbagi informasi tentang *attacker* melalui FTP *server*.

3. Sistem ADAM mampu melakukan serangan balasan secara bersama-sama dengan *server backup* untuk melumpuhkan system *attacker* dengan menyisipkan virus ke dalam system *attacker* tersebut.
4. Sistem otomatisasi ADAM bekerja lebih cepat dibandingkan dengan sistem keamanan yang bekerja dengan cara manual.
5. Trafik jaringan setelah ADAM bekerja ketika ditemui serangan jenis *scanning port* akan lebih rendah dibanding sebelum ADAM bekerja.

4.2 Saran

1. Untuk pengembangan selanjutnya, system pendeteksi serangan lebih diperluas lagi agar dapat mendeteksi berbagai jenis serangan terhadap *server*.
2. *Server backup* yang bertugas membantu *server* ADAM dalam melakukan serangan balasan ditambahkan lebih dari satu *server*.

Daftar Pustaka

Eichel,Zee., Baster, James., Rizqi, Habibi., 2012. *Attacking Site With Backtrack*. Indonesian Backtrack Team.

Nikodemus, 2012. Network Hacking dengan Linux Backtrack. Penerbit : Andi Yogyakarta danWahana Komputer.

Rahman, Rizal. 2013. MahirAdministrasi Server dan Router dengan Linux Ubuntu Server 12.04 LTS.Bekasi, Creative Commons Attribution-ShareAlike 3.0 Unported License (CC by SA).

http://blog.pusheax.com/2014/01/dictionary-and-brute-force-attack-using.html. Diakses pada 10 Juli 2015, 02:01:17 AM.

http://blog.pusheax.com/2014/12/metasploit-port-scanning.html. Diakses pada 10 Juli 2015, 02:35:23 AM.

https://www.howtoforge.com/triggering-commands-on-file-or-directory-changes-with-incron. Diakses pada 14 Juli 2015, 2:04:13 PM.

http://www.w3schools.com/php/func_filesystem_fgets.asp. Diakases pada 14 Juli 2015, 2:03:09 PM.

http://www.ubuntugeek.com/bandwidth-monitoring-tools-for-ubuntu-users.html. Diakses pada 01 Agustus 2015, 20:18 WIB.

https://id.scribd.com/doc/171582542/Gilang-Instalasi-Konfigurasi-Portsentry. Diakses pada 2 Agustus 2015, 2:11:24 AM.

http://www.asus87.com/2011/05/aplikasi-ftp-client-di-linux-ubuntu/. Diakses pada 02 Agustus 2015, 02:33 WIB.