**Keamanan Sistem Komputer**

**Konfigurasi IDS Portsentry**

****

Disusun Oleh :

Agus Santoso (1641723006)

Erwin Heriana (1541180102)

Wahyu Arum R.P (1541180058)

KELAS : TI- 3E

**POLITEKNIK NEGERI MALANG**

**JURUSAN TEKNOLOGI INFORMASI**

**PRODI TEKNIK INFORMATIKA**

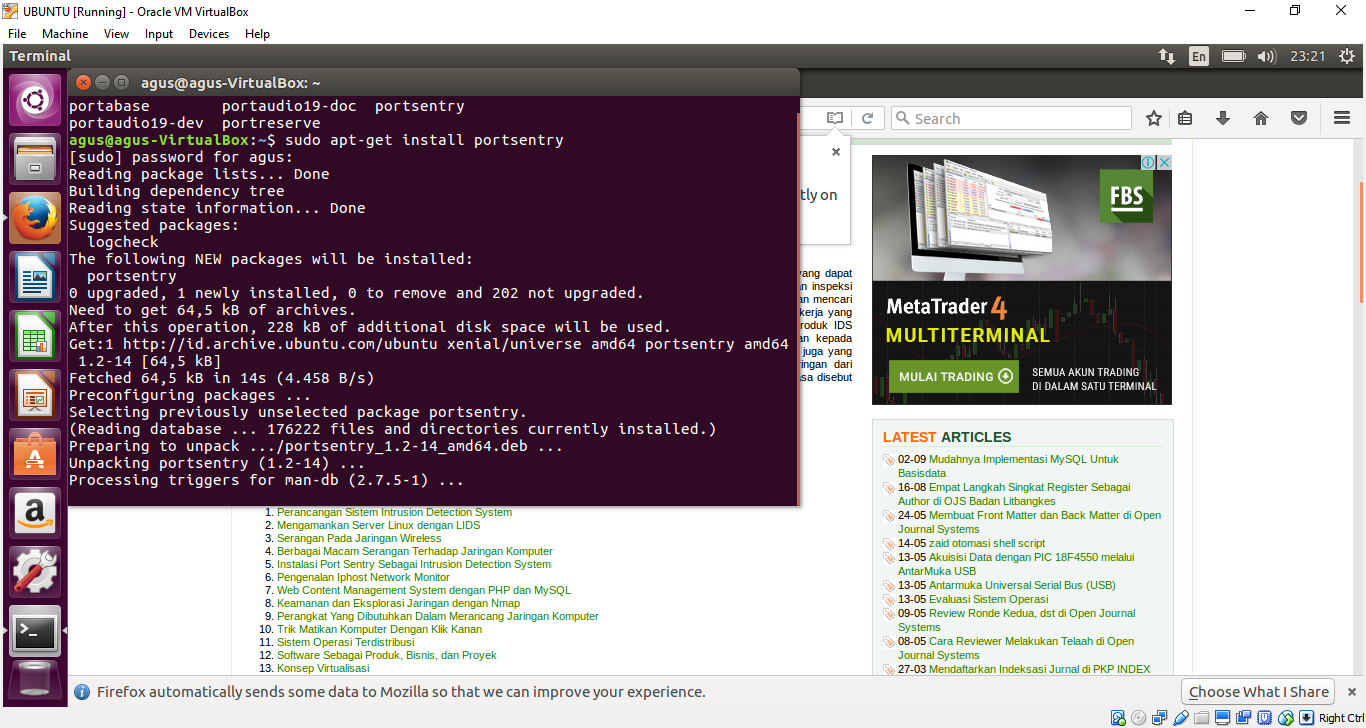
**2017**

**Portsentry** merupakan salah satu program aplikasi *firewall*, yang bisa melakukan pemblokiran terhadap *user*yang mencoba melakukan scanning port sistem atau mencoba melakukan aktivitas yang “tidak terpuji”, antara lain melakukan penyusupan melalui alamat port yang ada. Dengan adanya **portsentry**, semua alamat IP yang melakukan aktivitas yang dianggap “mencurigakan”, baik yang melalui port TCP maupun UDP akan segera diblokir.

Sehingga semua user yang menggunakan alamat IP yang sama seperti warnet, perkantoran, dan anggota ISP, tidak akan bisa mengakses server kita lagi

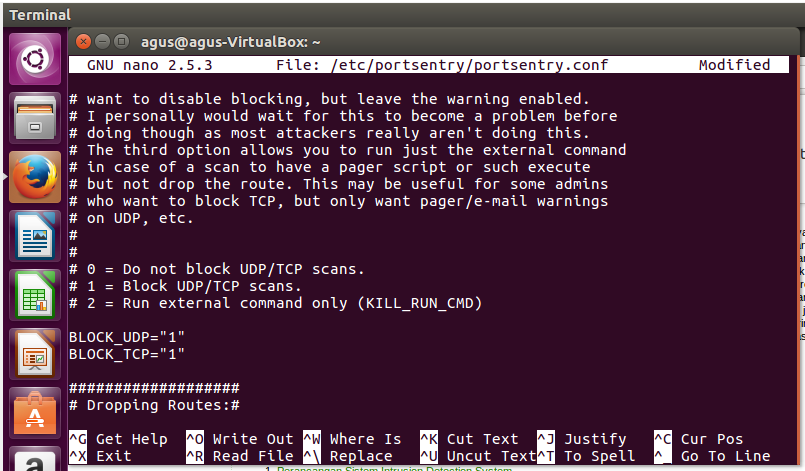
Berikut adalah langkah-langkah instalasi dan konfigurasi *portsentry* pada komputer IDS

1. Pada server IDS menjalankan *$ sudo apt-get install portsentry* untuk instalasi melalui terminal yang harus terkoneksi dengan *internet*, karena *portsentry* sudah ada di *repository* *ubuntu 11.04* seperti pada gambar 1



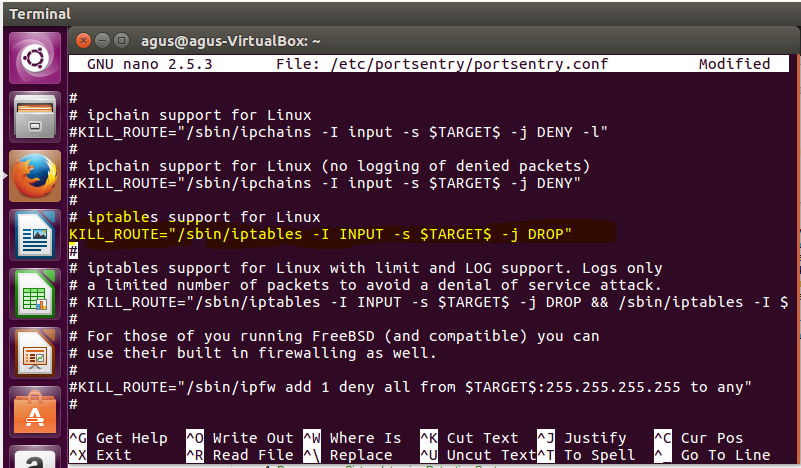
*Gambar 1 Instalasi Portsentry*

1. Pada server IDS terdapat file konfigurasi yang ada di direktori /*etc/portsentry/portsentry.conf* untuk mereject koneksipenyerang dengan *iptables* dan memfilter IP *host* penyerangmelalui *TCP wrapper*. Untuk mengedit file */etc/portsentry/portsentry.conf* dengan cara mengetikkan perintah *# nano /etc/portsentry/portsentry.conf.*



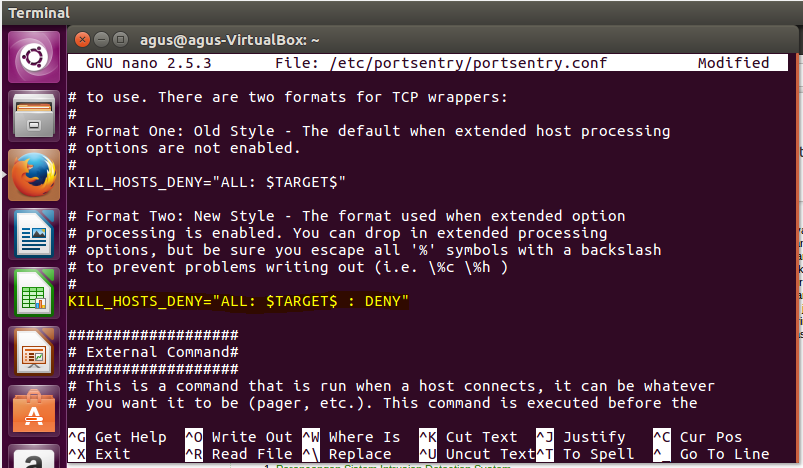
*Gambar 2 Konfigurasi Blocking TCP dan UDP scans*

Pada gambar 2 memperlihatkan konfigurasi *blocking* UDP/TCP *scans* pada *ignore options* , memilih angka 1 untuk memblock jika terjadi *scanning port* TCP dan UDP.



*Gambar 3 Konfigurasi Reject Connection Host dengan Iptables*

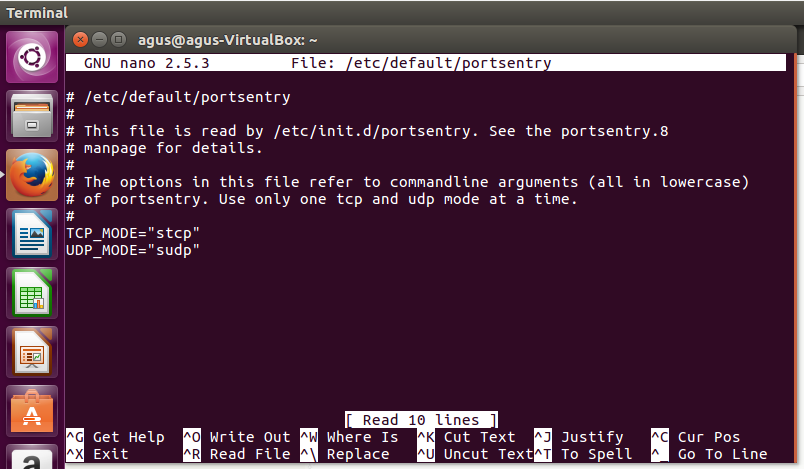
Pada gambar 3 memperlihatkan konfigurasi *blocking* *host* dengan *Ipchain* guna *memblokir* koneksi, untuk mereject koneksi *host* penyerang dengan menggunakan *iptables* ketika tertangkap melakukan kegiatan *scanning port* pada jaringandengan cara menghilangkan tanda # pada konfigurasi *KILL\_ROUTE=”/sbin/iptables –I INPUT –s $TARGET$ -j DROP”.*



*Gambar 4 Konfigurasi Filtering Host dengan TCP wrapper*

Pada gambar 4 memperlihatkan konfigurasi *filtering host* dengan *TCP wrapper*, menghilangkan tanda # pada konfigurasi *KILL\_HOSTS\_DENY=”ALL: $TARGET$ : DENY”* untuk memfilter *acces* IP *host* penyerang ketika tertangkap melakukan *scanning port* pada jaringan.

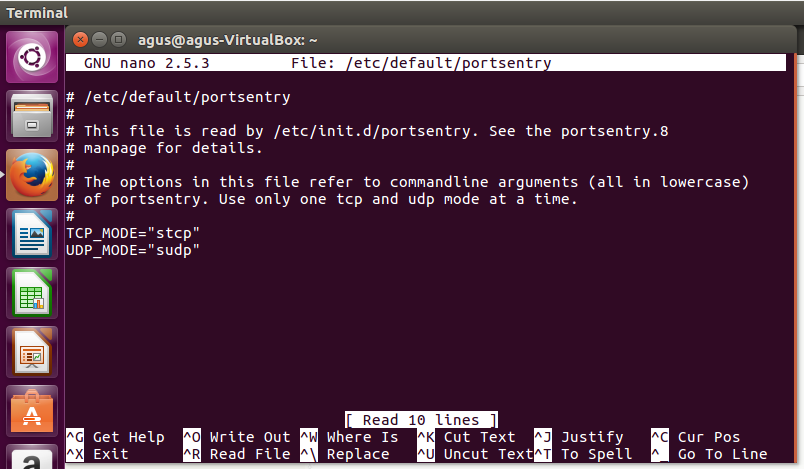
1. Pada sever IDS terdapat file */etc/portsentry/portsentry.ignore.static*, isi dengan IP yang tidak ingin terlindungi oleh *firewall portsentry*, untuk mengedit file */etc/portsentry/portsentry.ignore.static.* konfigurasi IP dapat dilakukan seperti pada gambar 5



*Gambar 5 Konfigurasi IP di /etc/portsentry/portsentry.ignore.static*

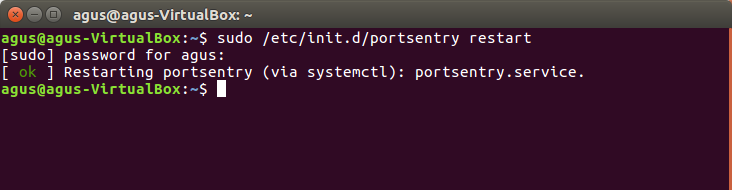
Dalam pengisian IP, jika tidak mencantumkan nilai mask *length-*nya maka akan diasumsikan nilai *subnet mask* 32 bit, semisal 192.168.1.0, maka akan diasumsikan sama dengan 192.168.1.0/32.

1. Pada server IDS terdapat file */etc/default/portsentry*, untuk memilih mode TCP dan UDP ketika *portsentry* mendeteksi *port* TCP/UDP, memilih mode deteksi *port* sesuai dengan yang ditentukan di *portsentry.conf* atau mode *advanced* dan menambah deteksi *stealth scan*.Untuk konfigurasi mode deteksi *port* di file */etc/default/portsentry* dapat dilihat pada gambar 6.

**

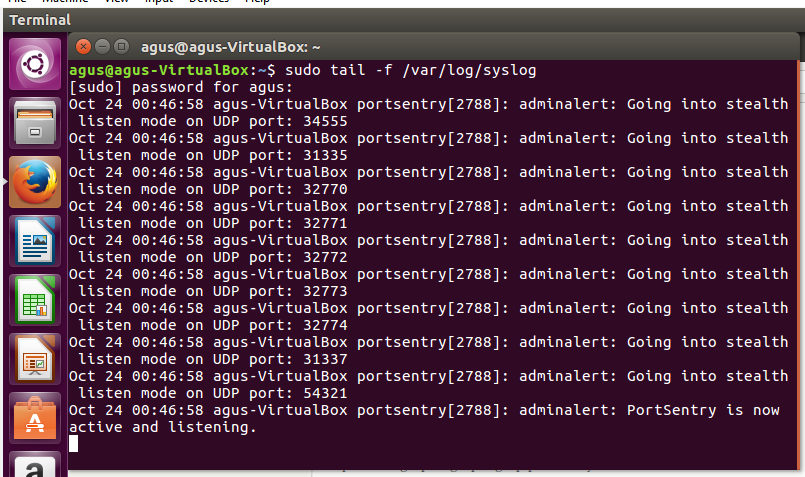
*Gambar 6 konfigurasi Mode Deteksi port TCP/UDP*

1. Pada server IDS mengaktifkan sistem *portsentry* dengan menginsialisasi *internet daemon* (*init.d*) yang secara *default* ada di sistem operasi. Untuk mengaktifkan *portsentry* dengan cara mengetik perintah *#* */etc/init.d/portsentry restart* seperti pada gambar 7.



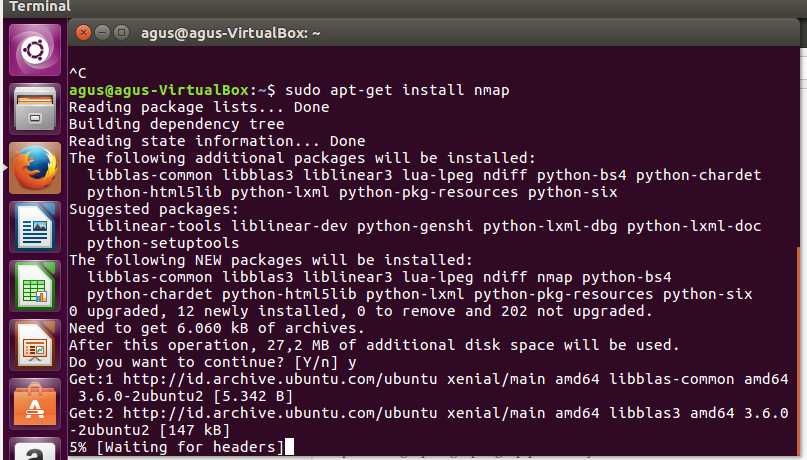
*Gambar* 7 Mgakyifkan Sistem Portsentry

1. Pada server IDS menjalankan perintah *# tail –f /var/log/syslog* untuk mengetahui aktifitas *portsentry* melalui data *syslog* seperti pada gambar 8.



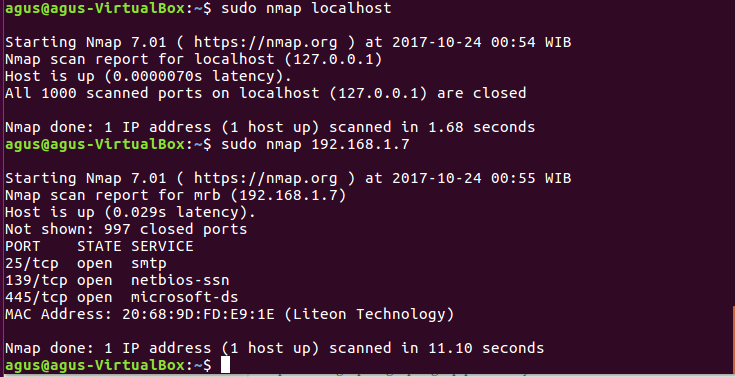
*Gambar 8 portsentry melalui data syslog*

1. Pada server IDS coba lakukan *scanning port* sendiri dengan menggunakan perintah *# nmap localhost* untuk mengetahui *port* yang dibuka dan dicek oleh *portsentry* seperti pada gambar 9 tetapi harus menginstall program *nmap* di *linux* dengan mengetikkan perintah *apt-get install nmap* yang sudah terkoneksi dengan *internet.*



*Gambar 9 cara install nmap*

1. tetapi harus menginstall program *nmap* di *linux* dengan mengetikkan perintah *apt-get install nmap* yang sudah terkoneksi dengan *internet.*



Gambar 9 *Port* yang dibuka dan dicek oleh *Portsentry*

Portsentry mempunyai kemampuan sebagai berikut: a. Berjalan di atas soket TCP & UDP untuk mendeteksi scanning port ke sistem. b. Mendeteksi stealth scan, seperti SYN/half-open, FIN, NULL, X-MAS. c. Portsentry akan bereaksi secara real time (langsung) dengan cara memblokir IP address penyerang. Hal ini dilakukan dengan menggunakan iptables dan memasukan ke file /etc/host.deny secara otomatis oleh TCP Wrapper. d. Portsentry mempunyai mekanisme untuk mengingat mesin/host yang pernah terhubung ke target. Dengan cara itu, hanya mesin/host yang terlalu sering melakukan sambungan (karena melakukan scanning) yang akan di blokir. e. Portsentry akan melaporkan semua pelanggaran melalui syslog dan mengindikasikan nama sistem, waktu serangan, IP mesin penyerang, TCP / UDP port tempat serangan dilakukan. f. Portsentry mampu memonitoring port UDP dan port TCP, yaitu : TCP\_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001, 4000,4001,5742,6000,6001,6667,12345,12346,20034,276 65,30303,32771,32772,32773,32774,31337,40421,40425, 49724,54320" UDP\_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,4 74,513,517,518,635,640,641,666,700,2049,31335,27444, 34555,32770,32771,32772,32773,32774,31337,54321"