**LAPORAN PRAKTIKUM**

**KEAMANAN KOMPUTER**

**Installasi Portsentry**

****

**Oleh :**

Oleh :

Nama : Siti Nur Haliza

NIM : 1600631013

**JURUSAN MANAJEMEN INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

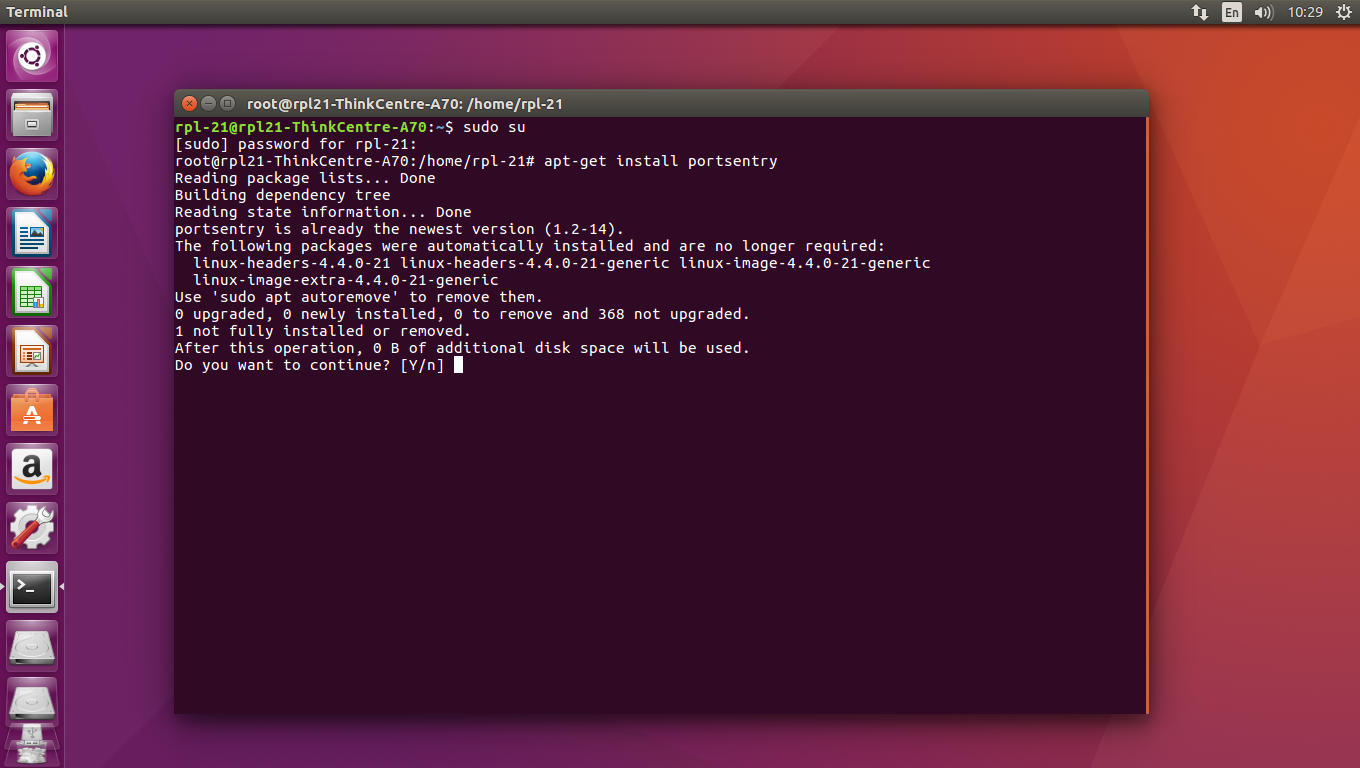
**2017/2018**

1. **Tujuan Praktikum**
2. Mengetahui Proses instalasi portsentry.
3. Mengetahui Cara konfigurasi portsentry.
4. Mengetahui Cara menjalankan dan menghentikan portsentry.
5. Mengetahui Cara uji coba port scanning dengan nmap.
6. Mengetahui Cara melihat log yang dihasilkan oleh portsentry
7. **Dasar Teori**

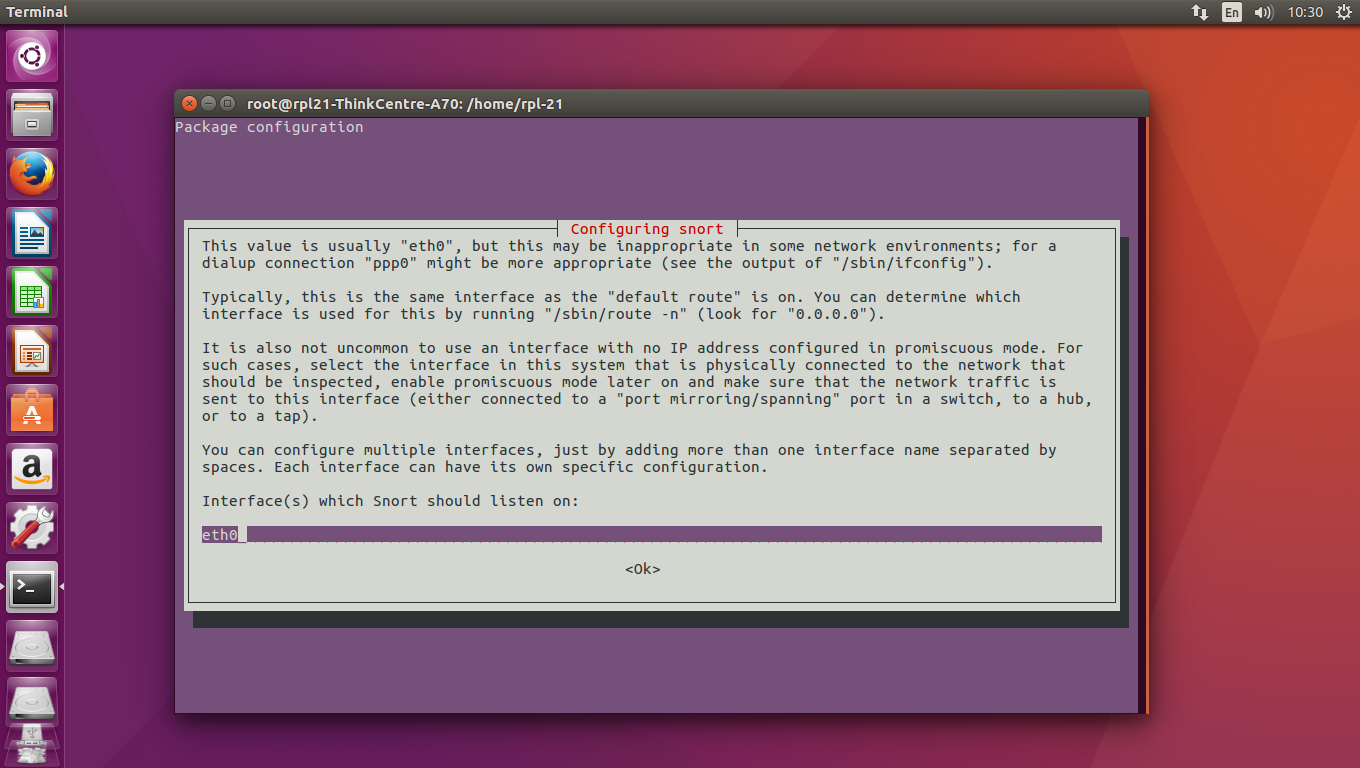
Portsentry merupakan tools yang digunakan untuk menghindari berbagai aktifitas scanning (terutama stealth scanning) yang dilakukan oleh hacker. Portsentry dapat mengingat ip address dari hacker. Portsentry juga dapat membuat server kita seolah-olah menghilang dari hadapan hacker bilamana terjadi aktifitas scanning.

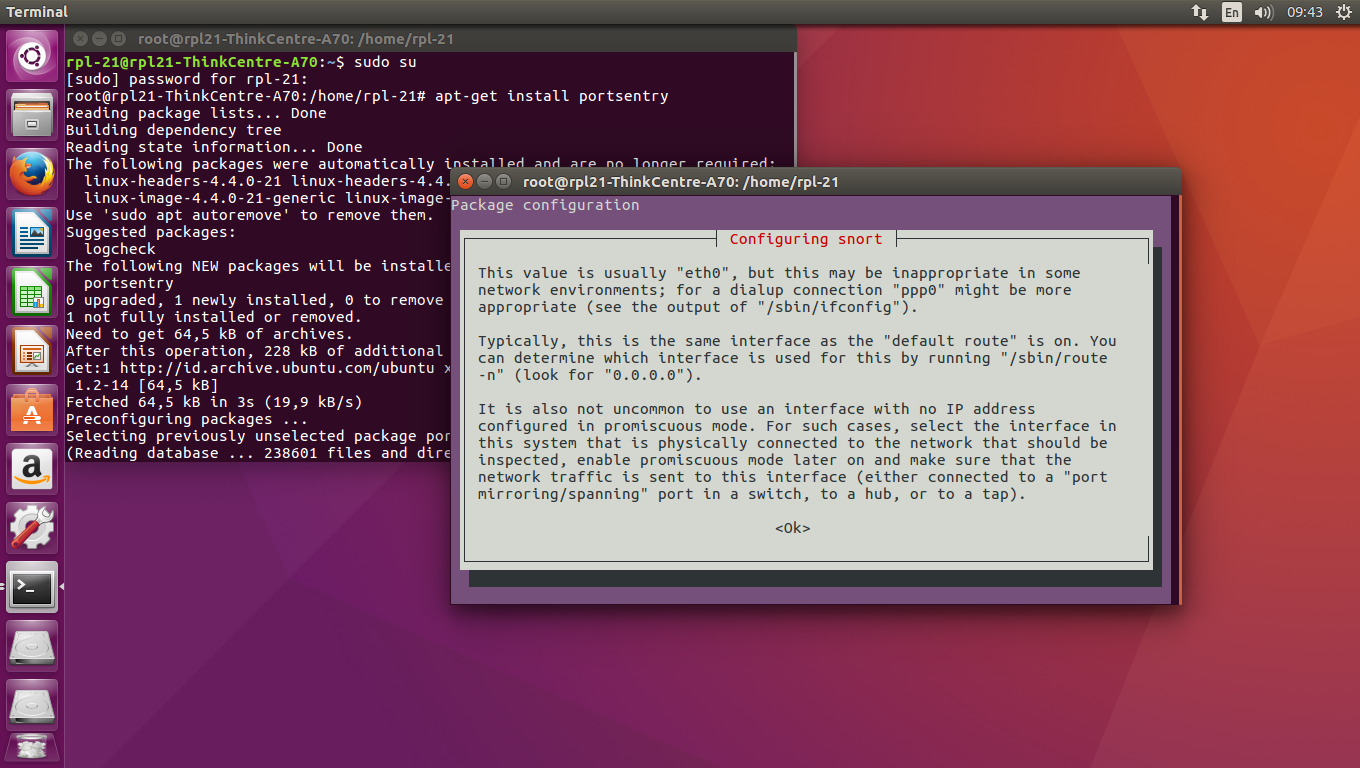
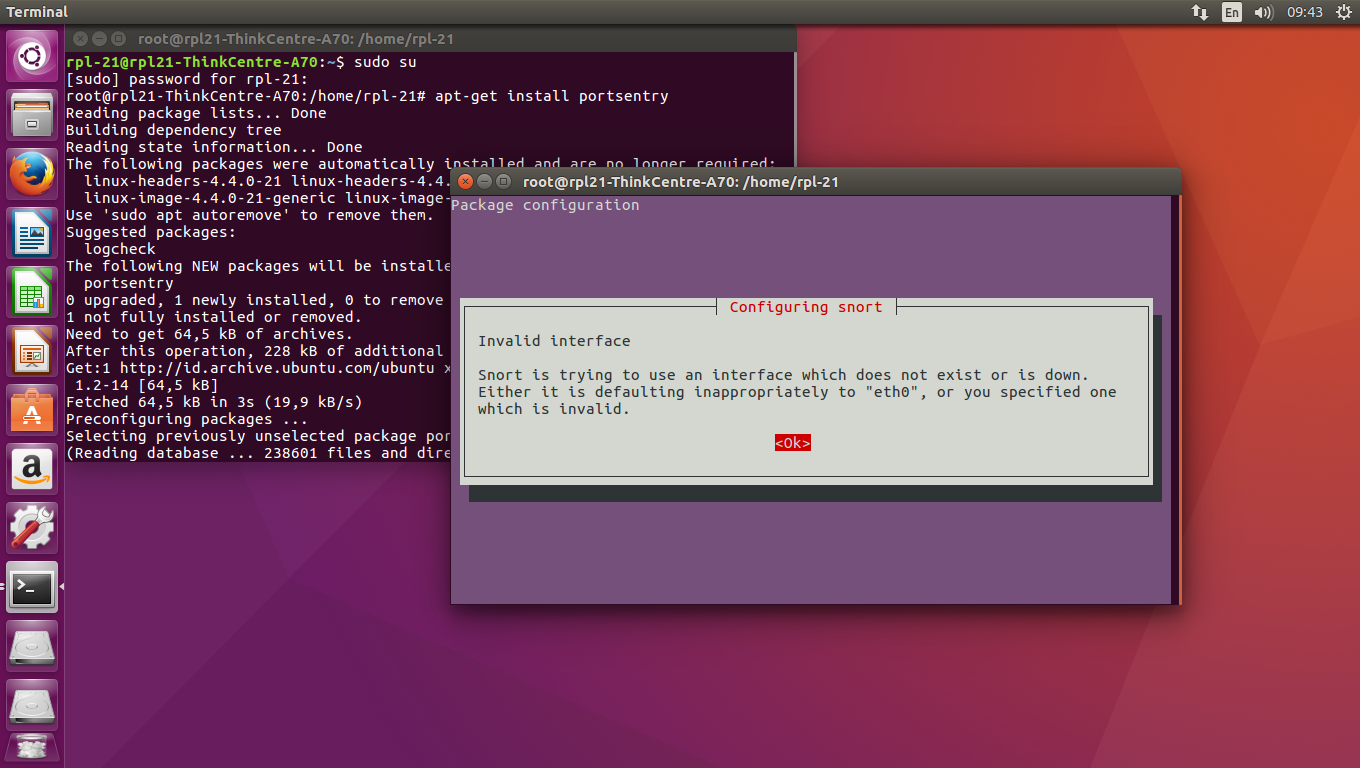
Kemampuan dari portsentry adalah

1. Portsentry akan mendeteksi berbagai teknik scan seperti SYN/half-open, FIN, NULL dan XMAS. Untuk mengetahui lebih jelas tentang berbagai teknik ini diharapkan untuk membaca manual dari software nmap yang merupakan salah satu software portscan terbaik yang ada.
2. Portsentry akan bereaksi terhadap usaha port scan dari lawan dengan cara memblokir penyerang secara real time dari usaha auto scanner, probe penyelidik, maupun serangan terhadap sistem.
3. Portsentry akan melaporkan semua kejanggalan dan pelanggaran kepada software daemon syslog lokal maupun remote yang berisi nama sistem, waktu serangan, IP penyerang maupun nomor port TCP atau UDP tempat serangan di lakukan.
4. Fitur lain Portsentry adalah pada saat terdeteksi sebuah port scan, sistem anda tiba-tiba menghilang dari hadapan penyerang. Fitur ini membuat penyerang tidak berkutik.
5. Portsentry selalu mengingat alamat IP penyerang, jika ada serangan port scan yang bersifat random maka portsentry akan bereaksi. Salah satu hal yang menarik dari portsentry adalah bahwa program ini dirancang agar dapat dikonfigurasi secara sederhana sekali dan bebas dari keharusan memelihara. (Dewannanta, 2013).
6. **Kegiatan Praktikum**
7. Ketik “sudo su”untuk login sebagai root/pengguna tertinggi
8. Ketik “apt-get install portsentry” untuk mendapatkan paket software linux secara online dan menginstallnya
9. Ketik “Y” untuk agreement, melanjutkan proses installasi



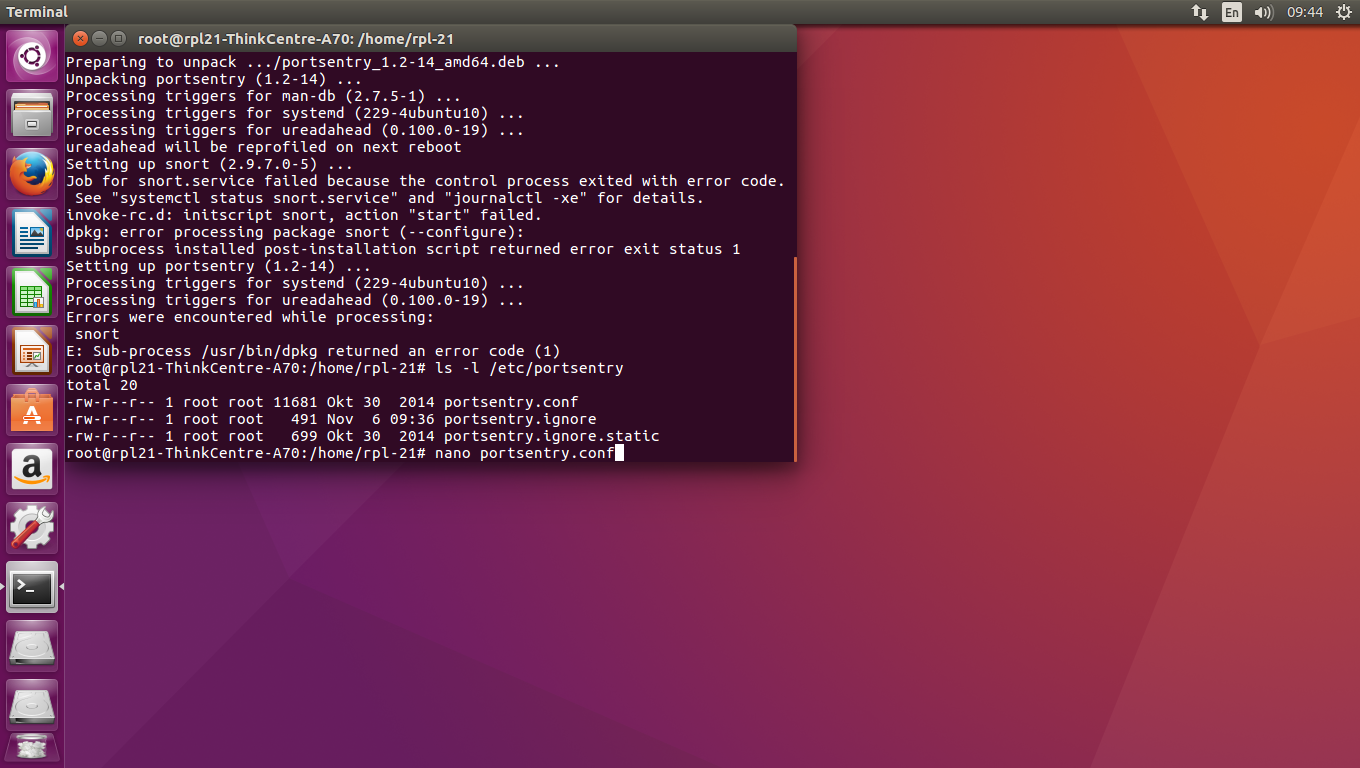
1. Tekan tombol tab untuk mengarahkan pointer ke nama interface dan pilih ok, hal ini berfungsi untuk mengkonfigurasi lancard .



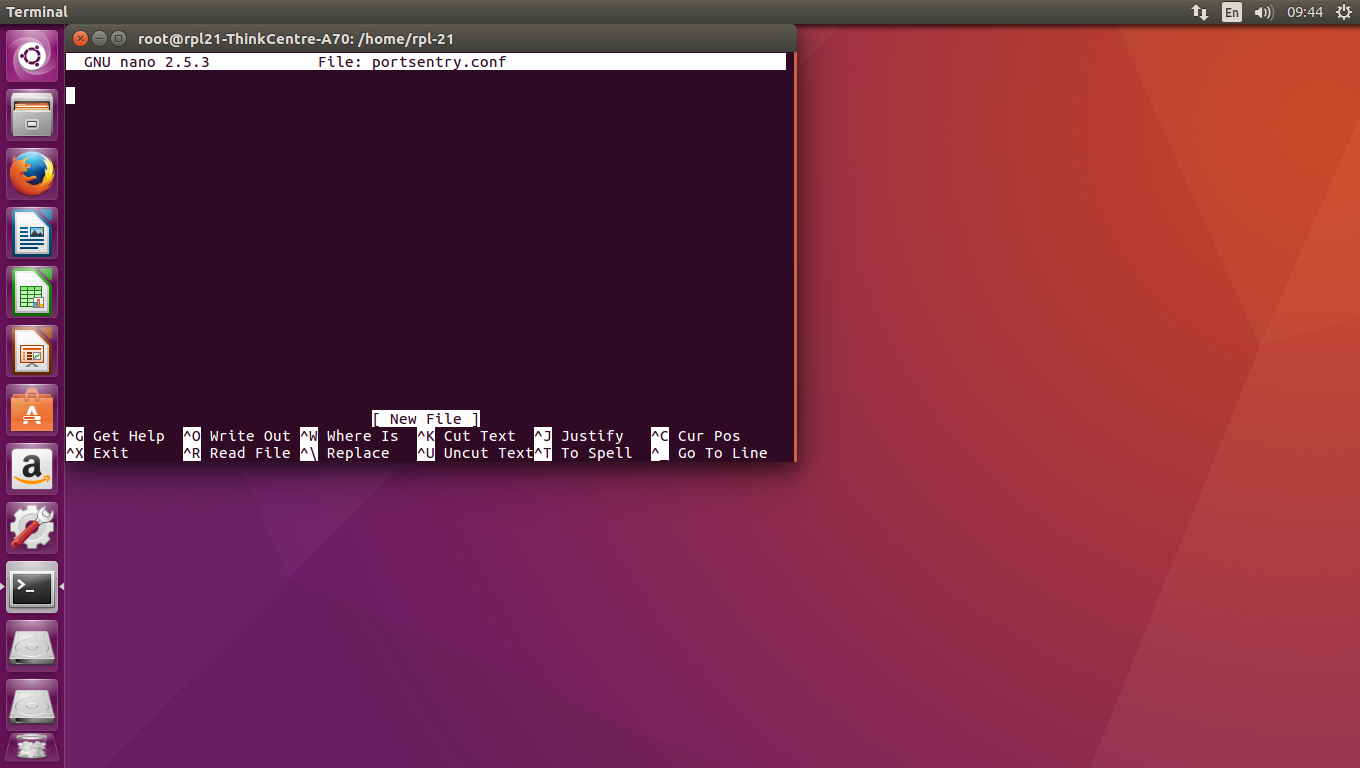
1. Tekan tab untuk mengarahkan pointer dan tekan enter untuk OK
2. Pilih Ok untuk konfigurasi
3. Setelah selesai proses installasi, untuk melihat konfigurasi portsentry

:ls -l /etc/portsentry.

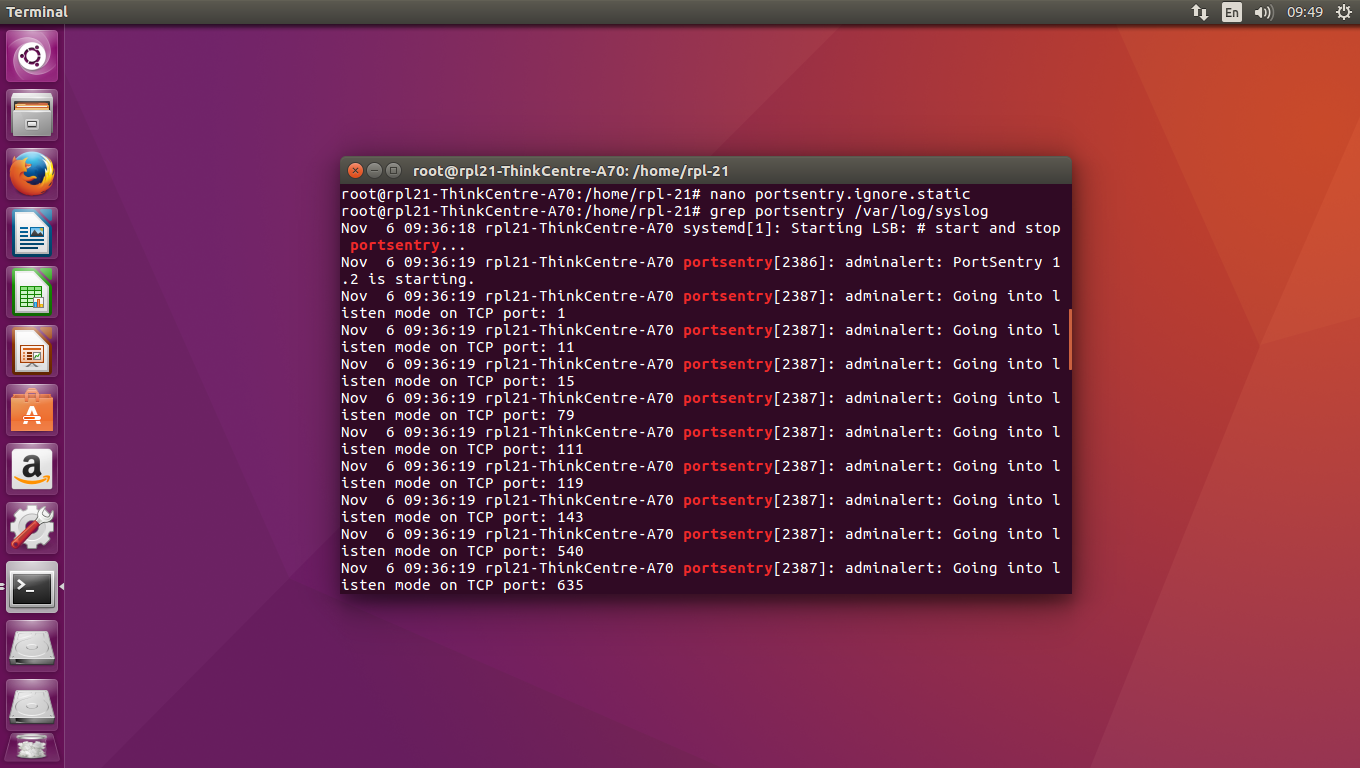
1. Ketik nano portsentry.ignore dan isi alamat ip komputer sebelahnya



1. Setelah mengisi alamat ip, tekan ctrl+s untuk menyimpan, tekan ctrl+x untuk exit dari halaman tersebut.



1. Untuk melihat pesan yang dibuat portsentry: grep portsentry /var/log/syslog



1. kode untuk menjalankan portsentry baik manual maupun otomatis :

ls -l /etc/init.d/portsentry.

1. untuk mencari identitas id portsentry:

find /etc/rc\*.d/\* -print | xargs ls -l | grep portsentry



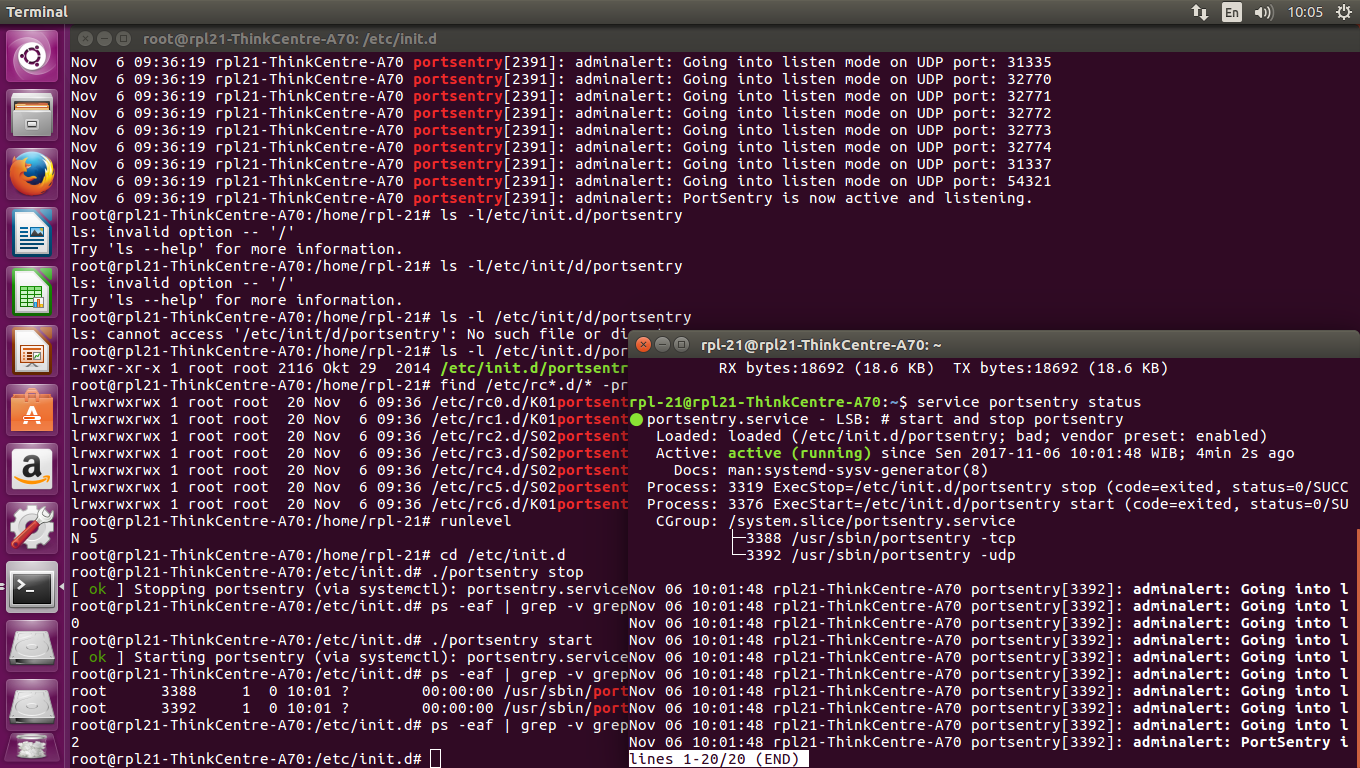
1. Menjalankan portsentry secara manual: cd /etc/init.d
2. Untuk menghentikan portsentry secara manual: ./portsentry stop
3. Mengecek portsentry sedang jalan apa tidak:

ps -eaf | grep -v grep | grep portsentry | wc –l

1. Untuk menjalankan Portsentry: ./portsentry start
2. Untuk melihat status portsentry: ps -eaf | grep -v grep | grep portsentry

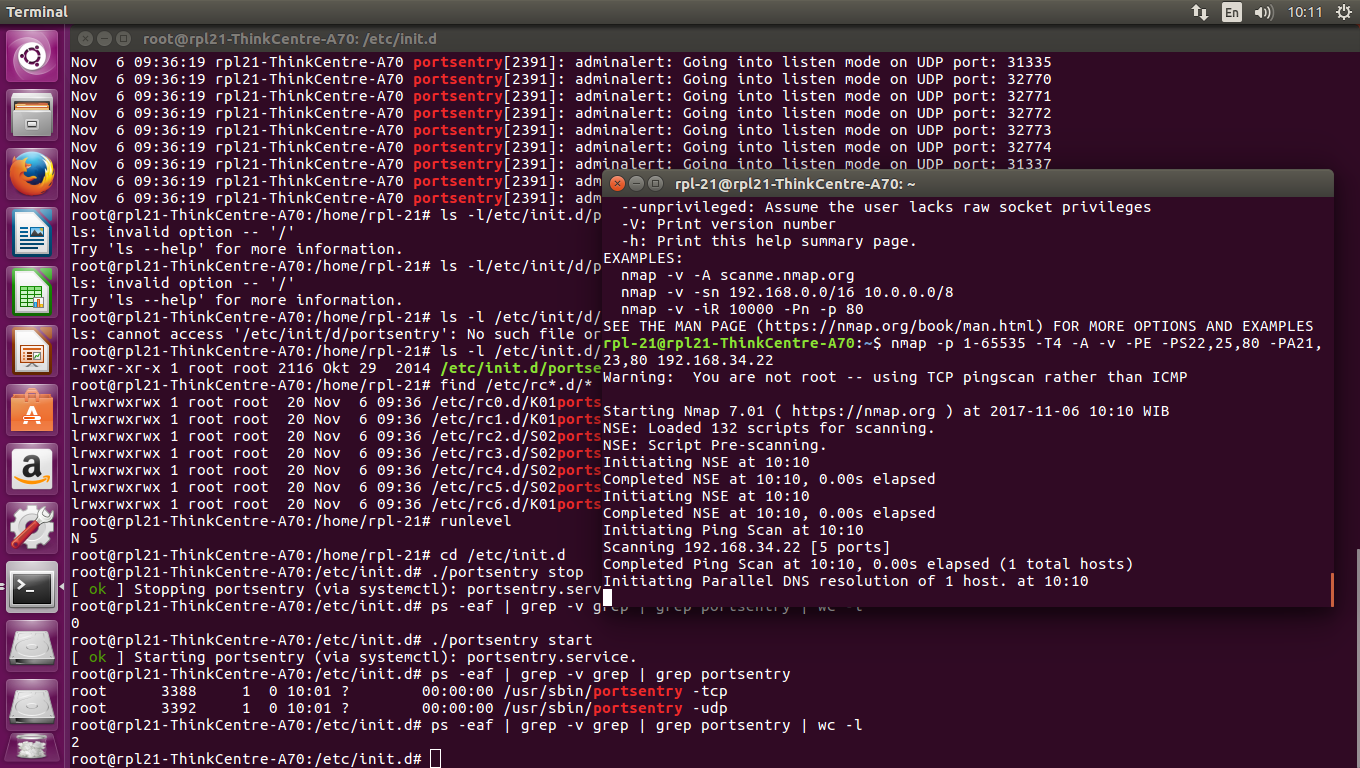


1. Buka terminal baru untuk cek status portsentry: service portsentry status



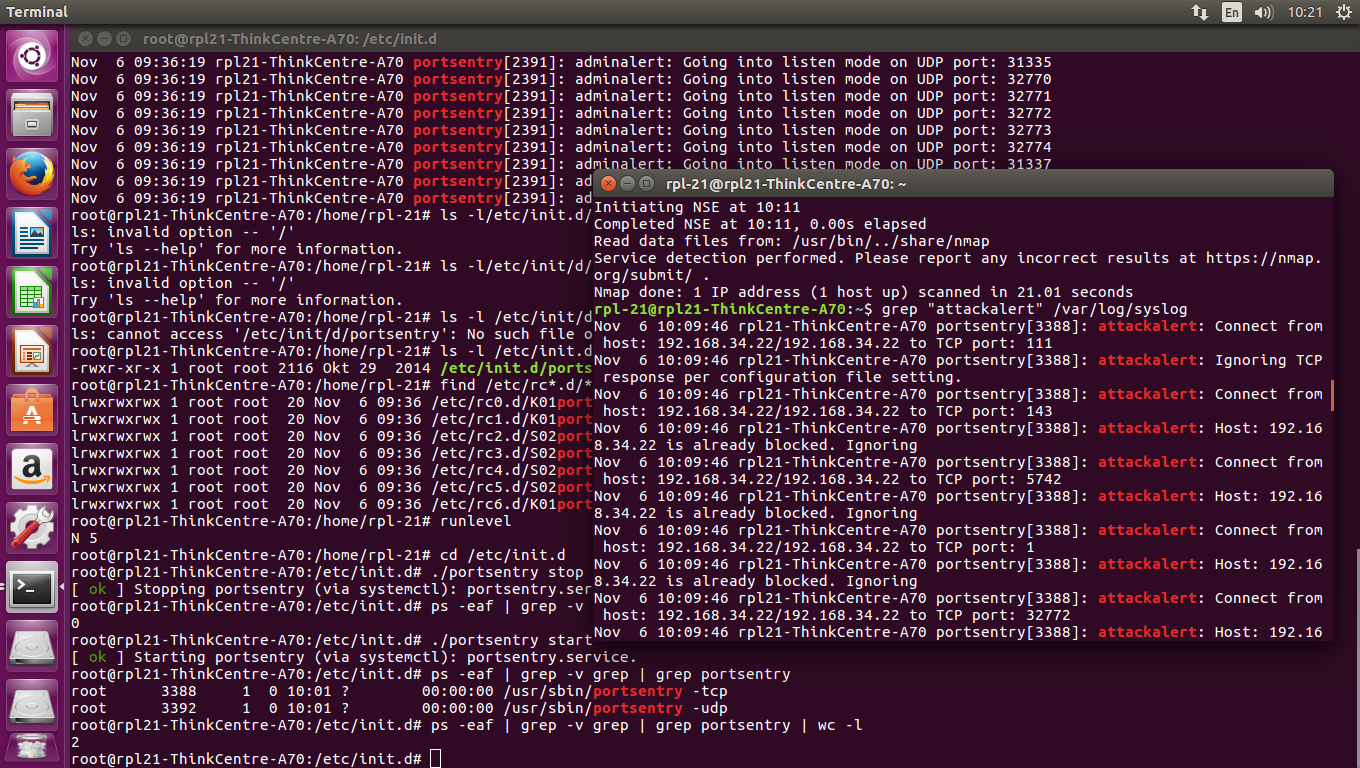
1. Untuk melakukan scanning dari port 1 - 65535

nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 IPKOMPUTER LAIN



1. Untuk mencari data serangan yang dibuat oleh port sentry:

grep “attackalert” /var/log/syslog



1. **Tugas Praktikum**

1. Proses instalasi portsentry

2. Cara konfigurasi portsentry

3. Cara menjalankan dan menghentikan portsentry

4. Cara uji coba port scanning dengan nmap

5. Cara melihat log yang dihasilkan oleh portsentry

1. **Kesimpulan**

Sebelum menginstal portsentry siapkan software nya, atau menggunakan perintah “apt-get install portsentry” untuk mendapatkan paket software secara online dan harus terhubung dengan internet terlebih dulu. Gambar di bawah ini menunjukkan proses root yang sedang berjalan, ketika status portsentry root nya 0 maka proses yang sedang berjalan tidak ada.