Welcome

Bienvenue

Willkommen

welkom

مرحبا بكم

yôkoso

Benvenuto

Bienvenida

tervetuloa

รับเสด็จ

欢迎

ubuntu-tn
tunisian team

SVP mettez votre portable en mode silencieux

Ubuntu GNU/Linux est-il un système sécuritairement sain?

Introduction

Augmentation d'utilisateurs d'Internet dans le monde:

- Plus qu'**un milliard et demi** dans le monde entier.
- Plus que **20%** de la population mondiale.

Source: Internet Word Stats, le 31 Mars 2009, www.internetworldstats.com/stats.htm

Augmentation d'utilisateurs d'Internet en Tunisie :

- **3%** de plus d'abonnés par mois.
- **262.986** abonnés en fin Mai 2009.
- **~2.960.000** utilisateurs d'internet en Tunisie.

Source : Agence Tunisienne de l'Internet, www.ati.tn

Introduction

La durée moyenne d'un PC ayant le système d'exploitation Windows non protégé connecté sur internet pour qu'il soit infecté passe de **40** minutes en 2003 à **4** minutes en 2009.

40 minutes en 2003

4 minutes en 2009

Source : Internet Storm Center, http://isc.sans.org/

Malwares sous Ubuntu GNU/Linux

Les malwares sous Ubuntu GNU/Linux sont au total 35 :

- Chevaux de Trois (Torjans) sont au nombre de deux seulement : Kaiten et Rexob
- Virus sont au nombre de 22 :
  - Le premier est sortie en septembre 1996
  - Le dernier virus est sorti en Juin 2007.
- Vers (Worms) : sont au nombre de 11 sous linux dont le petit dernier « SSH Bruteforce » sortie en 2008

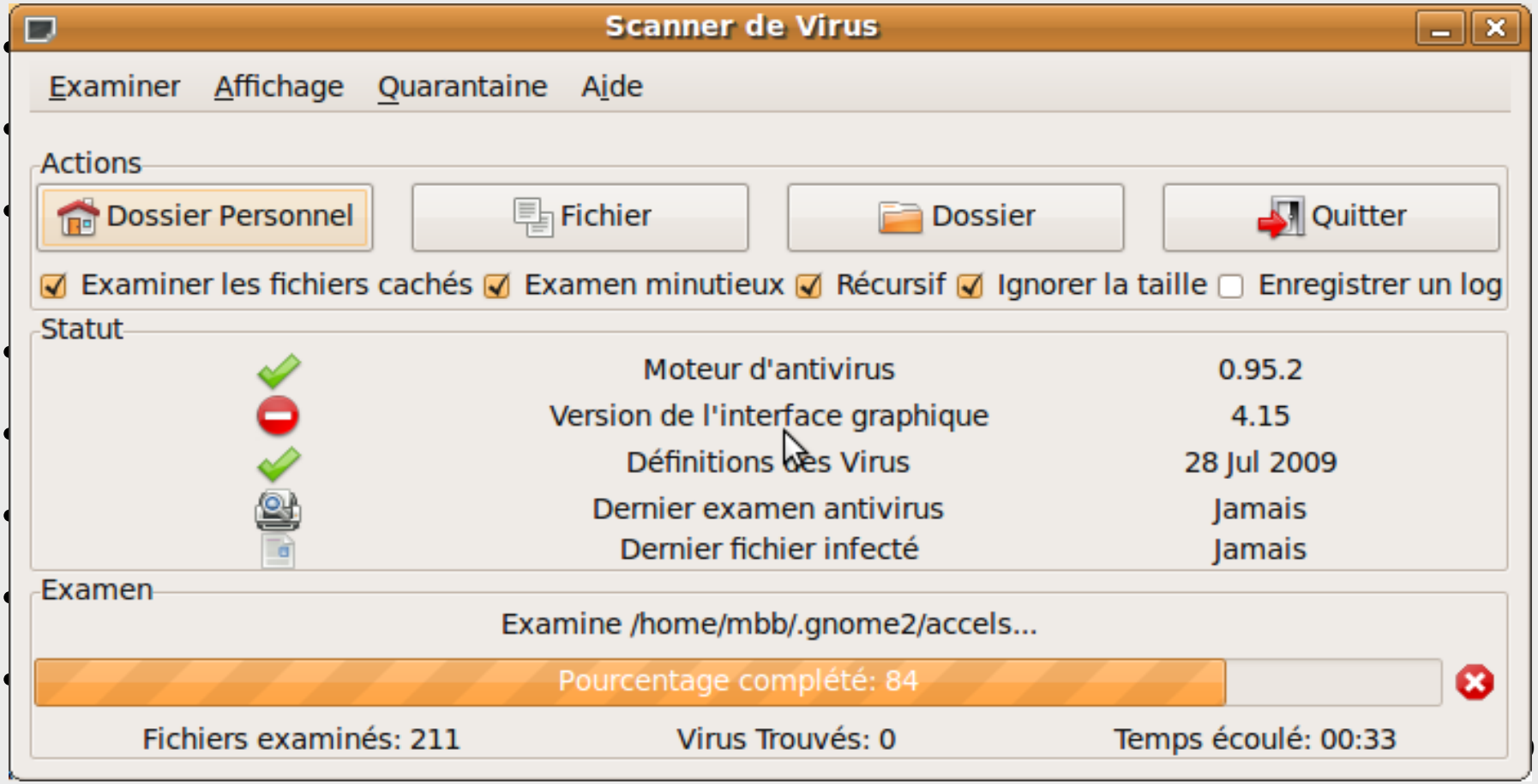
Limitation des Malwares sous Ubuntu

- Droit d'accès limités aux utilisateurs.
- Déclaration des fichiers exécutables est obligatoire.
- Configuration de Ubuntu est plus sûre que Windows.
- Les failles sont généralement plus vite corrigées.
- Ubuntu GNU/Linux est un OS open source.
- Téléchargement des logiciels à partir des dépôts.
- Grande variété de distributions Linux différentes.

Cibles des Hackers

- **Plusieurs types de pirates informatique :**
  - *Les Hacktivistes* : ils sont généralement « anti closed source », donc ils essayent toujours de casser la vulnérabilité des logiciels et des systèmes propriétaires
  - *Les Criminels* : ciblent toujours les systèmes et les applications les plus populaires afin de construire des réseaux de botnets énormes.
  - *Les newbies* : ce sont les nouveaux hackers, et qui cherche à faire des exploits personnel en ciblant les systèmes les plus connus.

ClamAV : caractéristiques



ClamAV : Installation

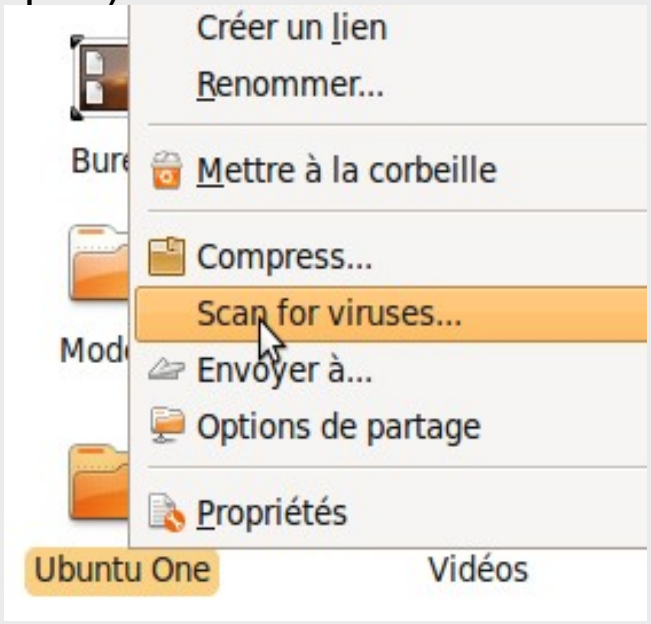
1- Dans « Système > Sources de mise à jour », activez le dépôt universe, puis rechargez

2- Dans « Système > Gestionnaire de paquets Synaptic », recherchez *clamav* et crochez *clamtk* qui vous permettra d'installer une interface graphique pour clamAV.

3- Acceptez toutes les dépendances et installez (Appliquer).

4- installation des addons :

- unrar-free ou unrar : permet de scanner les **fichiers compressés rar.**
- Nautilus-clamscan : est une extension qui **permet d'intégrer ClamAV avec Nautilus,**



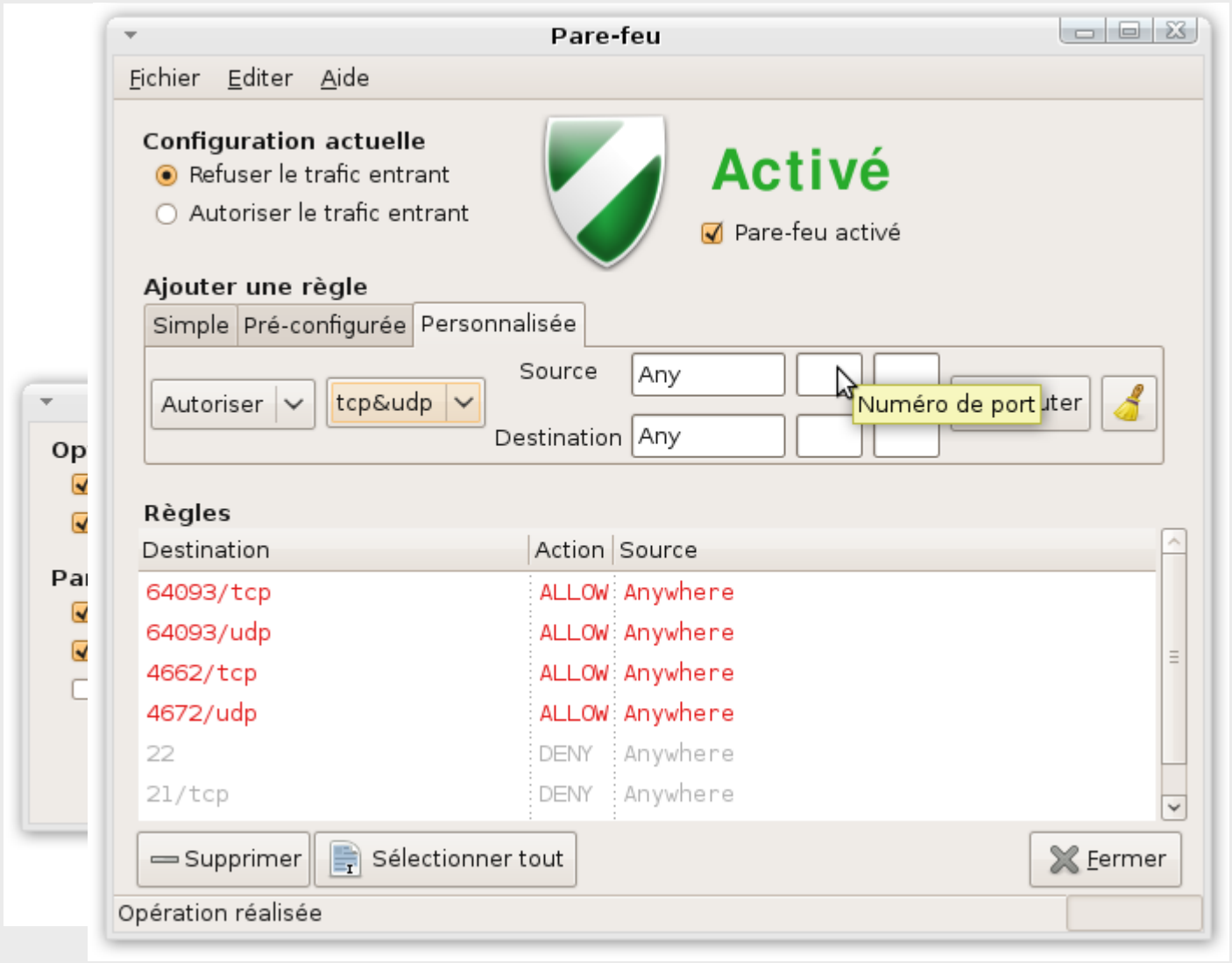
Firewall ou Pare-Feu

- Netfilter et IpTable :
  - Iptable l'interface de manipulation du système de filtrage de paquets *netfilter* qui sont fournit dans le noyau Linux.
  - Solution à la fois très flexible et hautement configurable.
  - Demande un certaine compétence dans Iptable.
- *Uncomplicated Firewall* (*ufw*) :
  - Interface en ligne de commande de gestion de *iptables*
  - *Sera pré-installé dans Ubuntu avec la version 0.27.1-2*
  - Fournir une interface facile à utiliser pour des utilisateurs peu familiers avec les concepts de pare-feu
  - GUFW est une interface graphique de gestion de UFW.

UFW en ligne de commandes

- **Activation/Désactivation d'ufw**
  - sudo ufw [enable|disable]
- **Autoriser/Refuser le trafic entrant suivant les règles par défaut :**
  - sudo ufw default [allow|deny]
- **Afficher l'état actuel des règles**
  - sudo ufw status
- **Activer/Désactiver la journalisation :**
  - sudo ufw logging [on|off]
- **Autoriser/Refuser/Supprimer une règle:**
  - sudo ufw [allow|deny|delete [allow|deny]] proto [tcp|udp] from [any|ipAdresse] to [any|ipAdresse] port [N°Port]

UFW avec une interface graphique : GUFW



Outils de sécurité

- **Firewall**
  - Netfilter, IP-Filter, UFW, FireStarter ...
- **Chiffrement**
  - OpenSSL, OpenSSH, Free S/Wan, PGP…
- **Authentification**
  - OpenLdap, FreeRadius, S/Key…
- **Antivirus**
  - Amavis, clamAV ...
- **Détecteur de sniffeurs**
  - Neped , Sentinel, Cpm…

Outils de sécurité

- **PKI**
  - Open_PKI, EuPKI…
- **Honey-Pots**
  - Honeyd , HoneyNet, Deception Toolkit, Specter …
- **Détection d'intrusion**
  - Snort , Prelude, Ntop, Shadow …
- **Scanner des vulnérabilités**
  - Nessus, Dsniff, Nmap, Sara, Whisker, Nikto, THC-Amap ...
- **Anti-Spam**
  - Spam Assassin (solution serveur ou client), SamSpade…

Conclusion

- Ubuntu GNU/Linux représente un étui mature et sécuritairement sain.
- Codes sources disponibles → auditables
- Documentation assez fournie
- Assistance communautaire disponible sur le Net
- On n'a pas besoin d'installer un antivirus.
- La configuration d'un firewall est à la porté de tout le monde.

Adresse Utiles

http://www.insecure.org/tools.html

http://www.linuxsecurity.com

http://www.linux-sec.net/

http://sourceforge.net

http://www.clamav.com/

http://www.ubuntu.com

http://www.ubuntu-tn.org

http://doc.ubuntu-fr.org/gufw

Contact

Pour nous rejoindre, ou
pour tout renseignements, veuillez
contacter notre LoCoTeam Ubuntu-tn.

ubuntu-tn
tunisian team

Réalisé par :
Mohamed Ben Bouzid - Abd Elmonoam Kouka
www.ubuntu-tn.org

Merci pour votre attention!

Des Questions?