

OUTILS ET LOGICIELS LIBRES EN SÉCURITÉ INFORMATIQUE

Patrick Boucher, CISSP, CISA
Gardien Virtuel Inc.



Gardien Virtuel
s é c u r i t é
i n f o r m a t i q u e

19 juin 2007

Plan

- 1- Définition
- 2- Création des logiciels libres
- 3- Personnes impliquées
- 3- Sécurité informatique – Concept de base
- 4- Les outils
- 5- L'avantage
- 6- L'inconvénient
- 7- Les références



Définition

- Se réfère au quatre grandes libertés de Richard Stallman :
 - Liberté de copier
 - Liberté de modifier
 - Liberté d'analyser
 - Liberté de publier des versions améliorées



Création des logiciels libres

- Gens qui ont un besoin spécifique
- Fausse croyance que le logiciel libre est gratuit
 - Chacun sert les besoins de tous
- Contributeurs sont attirés par :
 - Connaissances techniques
 - Besoins
 - Technologies disponibles



Personnes impliquées

- Utilisateurs
 - Parlent de la technologie, recherche la confiance et le sentiment de sécurité en utilisant la même technologie que les autres
- Supers utilisateurs
 - Aident les gens avec les problèmes
- Rédacteurs / Experts
 - Discutent de la technologie dans les forums



Personnes impliquées (suite)

- Initiés

- Prend une part dans le processus d'assurance-qualité

- Joueurs

- Très actifs dans le développement de la technologie

- Joueurs clés

- Rôle majeur dans le développement de la technologie



Personnes impliquées (suite)

- Supporteur
 - Fournit un apport financier dans le projet



Sécurité informatique – Concept de base

- Confidentialité , Intégrité, Disponibilité
- Concept du triple A
 - Authentification
 - Qui es-tu?
 - Autorisation
 - Que peux-tu faire?
 - Accounting
 - Qu'as tu fais?



Les outils

- Très précieux pour attaquer, diagnostiquer, analyser un réseau ou un système informatique.



Les outils (suite)

■ Nmap

- Permet le balayage automatisé des ports TCP et UDP d'un système distant

```
Nmap -sS -v -P0 -g 53 -p- --data-length 128 -T INSANE -sV -O -f -oN  
./résultat.txt 192.168.0.0-255
```

■ Wireshark

- Outil d'écoute de réseau

■ Nessus

- Outil de balayage des vulnérabilités

■ Netcat

- Permet de générer des connexions UDP et TCP



Les outils (suite)

- Snort
 - Permet de détecter les intrusions
- OpenSSH
 - Permet de se brancher à d'autres ordinateurs sans mots de passe
- OpenSSL
 - Protocole d'encapsulation sécuritaire
- Join the Ripper
 - Attaque des mots de passe par force brute ou dictionnaires.



Les outils (suite)

- VNC
 - Connexion distance facile et légère
- Iptables
 - Permet de tout bloquer
- SpamAssasin
 - Anti-pourriel
- ClamAv
 - Anti-virus gratuit



Les outils (suite)

- Firefox
 - Plug-ins qui font une partie du travail
- Dig
 - Permet d'interroger un service DNS avancé
- NsLookUp
 - Permet d'interroger un service DNS
- Traceroute
 - Permet de découvrir des réseaux



Les outils (suite)

- Ping
 - Vérification de la présence d'un système
- NbtStat
 - Affiche les statistiques du protocole NetBios
- DBAN
 - Supprime les informations sur les disques
- GPG
 - Permet le chiffrement



Les outils (suite)

- TrueCrypt
 - Permet le chiffrement du disque dur
- NetStumbler
 - Permet de détecter les réseaux sans-fils
- ToneLoc
 - Balayage des lignes téléphoniques pour les modems



Les outils un peu plus avancés

- SeLinux
 - Permet d'analyser les actions présent par les utilisateurs
- Kismet
 - Outil d'écoute réseau sans-fils
- TripWire
 - Gestion des changements sur les systèmes
- Nikto
 - Outil automatisé des services Web



Les outils un peu plus avancés (suite)

- JMeter
 - Permet de tester le comportement d'un système Web Apache
- IDSWakeUp
 - Permet de tester la fiabilité d'un système de détection d'intrusion
- DSNIF
 - Permet d'écouter et de capturer les informations communiquées entre deux postes réseaux



Les outils un peu plus avancés (suite)

- HPing2
 - Outil de reconnaissance réseau
- FlawFinder
- RATS
- Achilles
 - Permet d'intercepter et de modifier les requêtes http(s)
- TsCrack
 - Attaque par force brute d'un service de bureau distant



Les outils un peu plus avancés (suite)

- Stunnel
 - Permet d'établir un tunnel SSL
- Packit
 - Outil de création de paquet



L'avantage – Logiciels libres

- Permet de savoir ce que l'outil va faire et à quel moment il le fait
- Les copies vont toujours fonctionner même si le développeur abandonne le projet



Inconvénients – Logiciels libres

- Support offert



Les références

■ PFSense

- <http://www.pfsense.com/>

■ Outil de chiffrement pour Linux

- <http://linuxhelp.blogspot.com/2006/08/disk-encryption-tools-for-linux-a>

■ Alternative Linux

- <http://www.linuxalt.com/>
- <http://www.econsultant.com/i-want-open-source-software/>
- <http://www.damicon.com/resources/opensoftware.html>

■ Test de performance Apache Jmeter

- <http://jakarta.apache.org/jmeter/>



Les références (suite)

- IDS WakeUP

- <http://www.hsc.fr/ressources/outils/idswakeup/>

- MetaSploit

- <http://www.metasploit.org/>



Questions?

MERCI !



Gardien Virtuel
s é c u r i t é
i n f o r m a t i q u e