LINUX SCHOOL
Magazine

Pur et dur

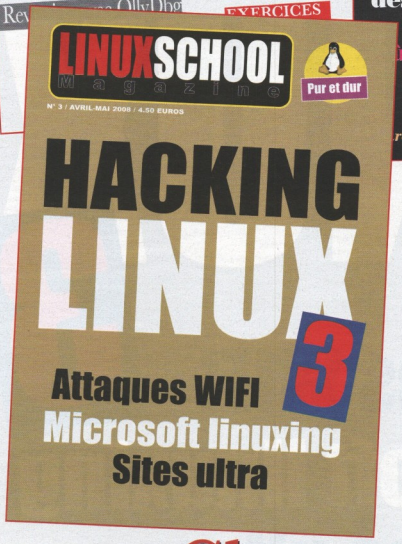
N° 3 / AVRIL-MAI 2008 / 4.50 EUROS

HACKING LINUX 3

Attaques WIFI

Microsoft linuxing

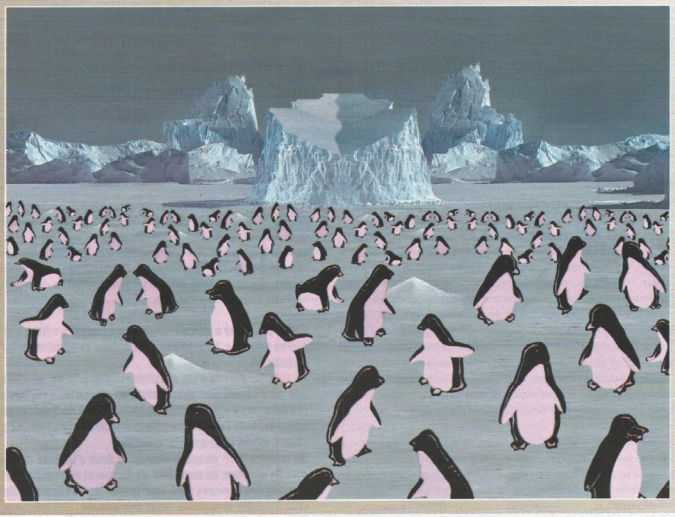
Sites ultra



Les rebelles sont de retour !

Chez votre marchand de journaux

Sommaire



LINUXSCHOOL MAGAZINE est édité par LPN 15 RUE CHEVREUIL - 94 700 MAISONS-ALFORT
Redaction en chef : Linux Community • **Directeur de Publication et représentant légal :** André Olivier
Imprimé en France par ROTO GARONNE 47310 Estillac • La Rédaction accepte toutes les contributions de la Communauté
Commission paritaire en cours • Dépôt légal à parution • ISSN en cours •

Bien choisir sa distribution

Pour se lancer dans l'aventure Linux, la première chose à faire est d'acquérir une distribution qui saura répondre à vos besoins. Linux est un univers vague et l'utilisateur lambda peut parfois se trouver dérouté face à la multitude de choix qui s'offrent à lui… Dans cet article, nous allons vous donner les clés qui vous permettront d'opter pour le bon choix pour faire de Linux votre système principal...

1. Pourquoi linux ?

Depuis maintenant plusieurs années, Linux est réputé pour être un système fiable, d'une grande stabilité et qui a fait ses preuves dans les entreprises. Mais ce qui fait avant tout la grande force de Linux, c'est son prix. En effet, bien qu'il existe certaines versions de linux payantes, la grande majorité demeurent gratuites.

De plus, linux est un système qui saura faire les preuves de ses performances même sur un ordinateur datant déjà de plusieurs années. Ce qui fait une des forces de Linux est le fait qu'il s'agisse d'un système « open souce » qui attire un grand nombre de développeurs. De très nombreux logiciels sont désormais disponibles sous Linux et si vous avez l'habitude d'utiliser des logiciels libres comme la suite bureautique openoffice ou le navigateur firefox, vous ne serez surement pas dépaysés sous Linux… Alors, pourquoi ne pas abandonner votre vieux Windows ?

2. Connaître ses besoins

Avant de faire un choix, vous devez avant tout savoir quelle utilisation vous souhaitez faire d'un environnement Linux. Linux offre un large choix de distributions à usage personnel de type « Workstation », c'est-à-dire une utilisation courante correspondant à la grande majorité des utilisateurs, mais il est également possible d'utiliser Linux pour en faire un serveur ou encore un pare-feu pour votre réseau domestique. Vous devez également avoir conscience de votre connaissance du système. Un utilisateur de Linux averti portera son choix sur des distributions plus performantes, mais aussi souvent plus complexes à mettre en œuvre. Vous devez donc prévoir si vous cherchez simplement à découvrir Linux, si vous souhaitez vous débarrassez de Windows définitivement ou si Linux sera sur une machine destinée à en faire un serveur ou un pare-feu.

3. Les distributions

Linux est distribué par des communautés ou des entreprises qui gèrent le développement de nouveaux outils et veillent au maintien à jour des applications disponibles sur le système.

Une distribution est donc composée d'un noyau Linux, d'un ensemble d'outils qui permettent l'administration et la personnalisation du système et enfin d'un grand nombre de logiciels gratuits et souvent open source.

Faites attention à ne pas confondre « gratuit », « libre » et « open source ». La subtilité réside dans l'utilisation faite du logiciel.

Un logiciel gratuit n'est simplement pas payant. Ce n'est pas pour autant que vous pouvez en faire n'importe quoi. Les licences d'utilisations des logiciels qui définissent le cadre légal de l'utilisation diffèrent souvent d'un logiciel à l'autre, même chez un unique éditeur.

Un logiciel libre donne à chacun le droit d'utiliser, d'étudier, de modifier, de dupliquer, de donner et de vendre ledit logiciel. Ces licences sont, pour la plupart, des licences de type GPL/LGPL et définies sur le site gnu.org

Enfin, un logiciel open source est un logiciel dont le code source est accessible par qui veut. Un logiciel peut cependant est open source est payant.

Linux est un système libre et open source

Il existe deux grandes familles de distributions Linux, les distributions « gratuites » et les distributions « officielles ».

Les distributions officielles sont des distributions à caractères « commercial » (donc payantes) généralement vendues sous forme de « packs » comprenant plusieurs CD/DVD, une docu-

mentation complète du système imprimée, une assistance technique, ainsi que quelques logiciels commerciaux.
Les distributions gratuites représentent la grande majorité des distributions Linux. Ce sont des distributions téléchargeables gratuitement sur internet qui offrent pour la plupart l'essentiel des logiciels de configuration du système et d'outils internet et bureautique.

4. Un moyen de découvrir Linux : le live cd

Linux est disponible sous forme de distributions dites « live cd ». Il s'agit d'une image disque (CD ou DVD selon les distributions) qui, une fois gravée, vous offre un Linux tout à fait fonctionnel sans aucune installation sur le disque dur. Il s'agit ici de distributions qui permettent de découvrir Linux et son univers sans risquer d'endommager vos données sauvegardées sous Windows. Cela vous permet de mettre Linux au banc d'essai, comme si vous l'aviez installé. Vous vous rendrez alors compte par vous-même si Linux est un système pour vous ou non…
Attention cependant à ne pas vous arrêter au test d'une seule distribution ; les distributions Linux sont différentes et offre un large choix d'environnement graphique et de gestions des « paquets » logiciels… Le live cd Linux sera également à même de vous sauver la mise en cas de crash grave de Windows en vous permettant une récupération de vos données que vous pensiez perdues à tout jamais.
Parmi les live cd, certaines distributions offrent également la possibilité d'être installées.
Knoppix est le pionner du live cd ! C'est la distribution qui a le plus fortement fait parler des live cd… Encore aujourd'hui, une majorité des distributions live cd se basent sur knppix. C'est la distribution idéale pour découvrir Linux en douceur, elle est livrée avec le gestionnaire de fenêtre KDE (il existe deux grands gestionnaires de fenêtre sous Linux, qui sont Gnome et KDE). KDE a tendance à plus se rapprocher de Windows que son cousin Gnome.
Désormais, les plus grandes distributions grand public sont hybride et à la fois live cd et permettent d'installer le système sur le disque dur.

5. Choix d'une distribution Linux pour un usage de tous les jours

Ubuntu : Le phénomène

Ubuntu est une distribution qui contribue fortement à la popularité de Linux depuis maintenant plus d'un an. Cette distribution a pris d'assaut le petit monde des distributions Linux et s'est vite imposée comme une valeur montante. Pourquoi ? Elle propose un environnement fonctionnel et facile d'utilisation sur un seul CD. Les outils de configuration sont eux aussi simples et performants. Ici, la démarche n'est pas de noyer l'utilisateur sous une centaine d'applications, mais de lui offrir seulement l'essentiel. Si vous souhaitez ajouter un grand nombre de logiciels, Ubuntu vous offre tout de même cette opportunité grâce à son logiciel de gestion de paquetage : Synaptic !
Ubuntu offre un design très épuré et ergonomique basé sur l'environnement. Une version est également disponible avec les environnements de bureau KDE (kubuntu) et XFCE (Xubuntu)

Mandriva : la star du monde Linux francophone

Mandriva, anciennement appelé Mandrake, œuvre depuis des années pour rendre Linux accessible au grand public. Leur distribution a toujours été un modèle du genre, souvent pionnière en ce qui concerne avant tout la facilité d'installation, mais également d'utilisation du système. C'est un des premiers Linux à avoir offert une installation en mode graphique, Linux étant alors réservé à un public initié, les installations se faisaient en mode console (sans la souris).
Avec Suse, Mandriva est sans doute la distribution Linux qui s'approche le plus des systèmes « grand public » comme Windows ou Mac OSX. De plus, son support français est le plus conséquent du monde Linux, Mandriva étant une entreprise française…

Opensuse : Le Linux sponsorisé par Novell

Opensuse est une distribution communautaire mais sponsorisée par Novell. C'est ni plus ni moins qu'un Linux Suse mais sans les binaires propriétaires. Il s'agit d'une distribution accessible à tous par sa simplicité. Cependant, un minimum de puissance est requis, ce n'est pas le Linux le plus léger.

Fedora : Le « fork » de red hat

Fedora est un projet mené par red hat dans le but d'avoir une version gratuite de son système. C'est la Red Hat pour les particuliers. Anciennement nommée Fedora Core, elle ne comporte pas de binaires propriétaires. Cette distribution possède une forte communauté. Elle est connue pour sa sécurité et ses performances mais un peu moins pour sa simplicité d'utilisation. La gestion des paquetages peut parfois être déroutante sur cette distribution…

Debian : Le linux qui a fait ses preuves

Une distribution communautaire qui est source de beaucoup d'autres distributions. Elle est très stable car les binaires sont longuement éprouvés. De ce fait, vous n'y trouverez pas les dernières versions de binaires. De fait, il existe 3 versions :
- **Stable :** version figée où les mises à jour sont uniquement des correctifs de sécurité,
- **Testing :** future version stable où seuls les paquets suffisamment testés peuvent être intégrés
- **Unstable :** version active et instable, où de nouveaux paquetages sont sans cesse ajoutés ou mis à jour (surnommée Sid).

Gentoo : Pour les fous de la compilation...

La Gentoo est à part dans le monde linux. C'est une distribution qui s'adresse à un public averti. Avec cette distribution, votre système sera très performant (car compilé spécialement pour votre processeur), mais pas forcément toujours simple à utiliser. Une bonne lecture de la documentation en ligne est indispensable avant de se lancer dans l'aventure Gentoo…

6. Les linux spécialisés

De nombreuses distributions Linux sont conçues pour un usage spécifique… en voici quelques exemples :

Garbure pour la création multimédia

Garbure rassemble 5 Lives cd pour l'animation, la mise en page, la vidéo, la musique et la création de sites web. Si vous avez une âme de réalisateur ou de graphiste, c'est la distribution qu'il vous faut !

SystemRescueCD : récupérez vos données avant qu'elles ne soient vraiment perdues

Voilà un Live cd élaboré dans le but de partitionner, créer des images de partitions, rechercher les virus, sauvegarder et restaurer la table des partitions, sauvegarder des données, graver, tester la mémoire vive. Le cd de petite taille (100 Mo) peut être personnalisé (pour cela, suivez le Howto du site). Cette distribution, si vous choisissez de la graver, vous sauvera sûrement la mise un jour ou l'autre !

BackTrack : Le professionnel de la sécurité

BackTrack permet de tester la sécurité des réseaux. Elle est installable et personnalisable, c'est la distribution idéale pour tous ceux qui souhaitent se familiariser avec les nombreux outils de sécurité Linux de scan réseau, de crack wifi ou autre.

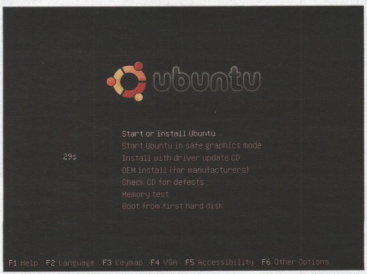
Installez Linux sur le même disque que Windows !

Précédemment dans le magazine, nous vous avons donné des conseils pour choisir la distribution Linux qui correspond le mieux à vos besoins… et, j'en suis sûr, beaucoup d'entre vous auront retenu *Ubuntu*. Cette distribution connaît un large succès depuis son lancement car elle offre une interface conviviale et des outils de configuration simples et performants.

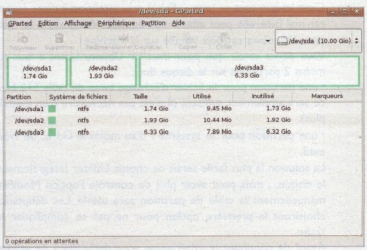
La première chose à faire est bien entendu de récupérer Ubuntu et de le graver… Cette distribution est disponible sur : http://ubuntu-fr.org

Sélection des paramètres linguistiques

Appuyez juste sur Entrée pour lancer le programme d'installation. Le système chargera alors…

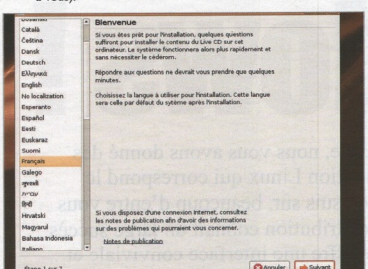


Une fois l'environnement Live CD chargé, vous aurez à l'écran l'interface graphique gnome et un système Ubuntu complet prêt à être utilisé, même sans installation... En effet, une des particularités d'Ubuntu est qu'il s'agit d'une distribution live cd installable. Cette interface graphique vous présente votre système d'exploitation tel qu'il sera quand il sera installé sur votre ordinateur. N'hésitez pas à explorer les différents menus afin de regarder les applications préinstallées. La première étape va consister à éditer la table des partitions pour faire de la place sur notre disque : rendez-vous donc dans le menu Système puis Administration et pour finir Editeur de partition.



Vous voici sur la fenêtre principale de l'éditeur de partition. Cet outil affiche votre disque dur avec la place disponible. Faites un clic droit sur la barre représentant votre disque dur puis cliquez

sur Redimensionner. Spécifiez une taille au moins égale à 3500 Mo. C'est le minimum pour avoir un système opérationnel avec des outils comme openoffice, firefox, gimp etc. N'oubliez pas de valider vos changements en faisant Edition -> Valider.
Une fois notre disque prêt, nous allons pouvoir lancer la procédure d'installation. Cliquez donc sur l'icône « Install » se trouvant sur votre bureau. L'installation affiche un écran Choisissez Français et validez (à moins que vous ne souhaitiez installer votre système dans une des autres langues disponibles… Libre à vous).



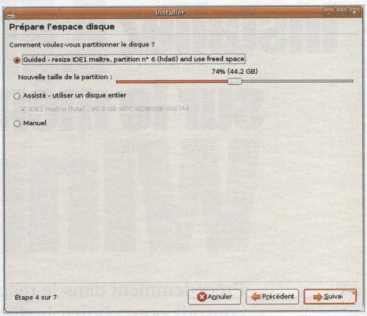
A l'étape suivante, choisissez la zone géographique dans laquelle vous vous trouvez (certainement Paris…).
[IMG5]
Choisissez ensuite la langue de votre clavier… N'hésitez pas à utiliser la barre d'en bas pour tester la validité de la configuration !

Partitionnement

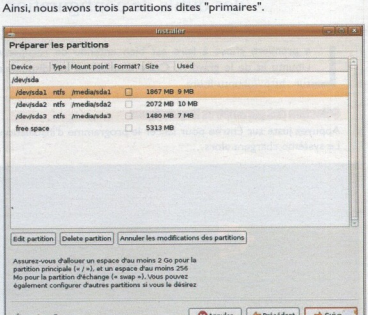
Voici l'étape la plus sensible : le partitionnement du disque dur. C'est ici que tout se joue… Faites très attention à cette étape, car, mal faite, elle peut effacer vos données Windows si un système Windows est déjà installé sur la machine.
Vous devez savoir que pour installer Ubuntu Linux, il faut au moins 2 partitions sur le disque dur :

- une partition pour le fichier d'échange swap de taille 512 Mo, ce sera amplement suffisant (il n'est pas nécessaire d'en mettre plus),
- une partition pour le système / d'au moins 4 Go et de type ext3.

La solution la plus facile serait de choisir Utiliser intégralement le disque..., mais pour avoir plus de contrôle l'option Modifier manuellement la table de partition sera idéale. Les débutants choisiront la première option pour ne pas se compliquer la tâche.
Avant de continuer, le programme vous demandera de valider les modifications :
Nous entrons dans la partie " difficile " de l'installation. C'est à partir d'ici que nous allons organiser l'espace disque pour installer Linux. Sur l'écran montré ci-dessous, cliquez sur le bouton "Manuel", puis sur "Suivant".

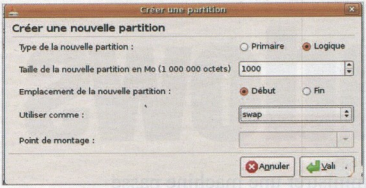


Ici, tous vos disques durs sont listés, ainsi que les partitions présentes. Sur notre exemple, la première partition est une partition NTFS contenant Windows XP, la deuxième partition est une partition NTFS contenant Windows Vista et la troisième partition est au format NTFS elle aussi, et contient des données personnelles. Ainsi, nous avons trois partitions dites "primaires".

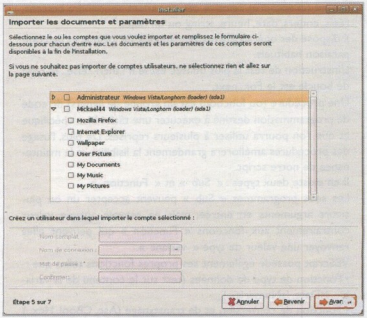


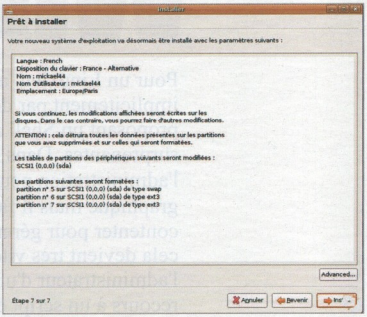
Attention :
Un disque dur peut accueillir au maximum 4 partitions primaires. Cependant, si vous désirez posséder plus de 4 partitions, une partition étendue permet d'avoir autant de disques logiques que l'on veut.
Nous allons créer en premier la partition pour la mémoire d'échange. Nous n'aborderons pas ici l'utilité de la mémoire d'échange. Toujours est-il que cette dernière est indispensable au fonctionnement de Linux. Cliquez sur la ligne " Free Space " puis

sur le bouton "New partition"
La fenêtre suivante apparaît :

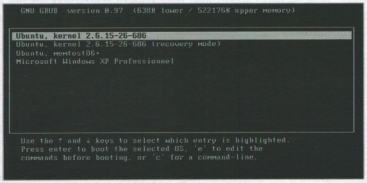


En ce qui concerne la place à allouer à la partition d'échange, il est conseillé de laisser un espace équivalent à la quantité de RAM que votre ordinateur embarque. Cependant, avoir une SWAP légèrement plus grande que sa RAM permet de profiter de la veille prolongée car le stockage de la RAM s'effectue dans cette partition SWAP lors de cette opération.
Vous retournez à l'écran précédent. Faites la même manipulation afin de créer la partition système.
• Taille de la nouvelle partition en Mo : mettez au moins 2000 Mo. 2500 Mo si vous ne possédez pas beaucoup d'espace disque. Cependant, 4500 Mo s'avère être un maximum correct.
• Emplacement de la nouvelle partition : début
• Utiliser comme : ext3
• Point de montage : /
Validez et faites la même opération afin de créer la partition abritant les fichiers personnels.
• Taille de la nouvelle partition en Mo : le reste de votre espace disque libre alloué à Linux.
• Emplacement de la nouvelle partition : début
• Utiliser comme : ext3
• Point de montage : /home
Vos partitions sont maintenant terminées ! Vous venez d'achever l'étape la plus difficile de l'installation. Cliquez sur le bouton suivant. Inscrivez votre nom, le nom d'utilisateur voulu, le mot de passe lié au nom d'utilisateur et le nom du PC.
Sur l'écran suivant, vous pouvez importer quelques préférences de Windows afin de les avoir sous Linux. Sélectionnez ce que vous désirez importer puis cliquez sur suivant.
Votre système est enfin prêt à être installé, cliquez sur le bouton installer afin de lancer l'installation.





L'installation prendra environ 20 minutes selon la puissance de l'ordinateur.
Redémarrez votre ordinateur et admirez le travail … GRUB vous demande de choisir si vous souhaitez démarrer Windows ou Linux.



Linuxez votre Windows

Pour un Linuxien, administrer une machine passe implicitement par des scripts d'administration, Linux proposant un Shell aux performances et possibilités surprenantes. Dans le monde Windows, toute l'administration peut se faire par le biais d'une interface graphique mais il faut bien admettre que si on peut s'en contenter pour gérer une dizaine d'utilisateurs ou machines, cela devient très vite lourd et fastidieux pour l'administrateur d'un parc machines conséquent et que le recours à un script d'automatisation s'impose rapidement.

Introduction

On pourra se dépanner avec quelques scripts DOS (fichiers.bat) pour de petits scripts mais pour de gros traitements sur des OS comme Windows XP ou 2003 server, il faut passer à un autre utilitaire.

Nous allons utiliser VBScript qui est un langage de script sous Windows. Il peut fonctionner dans différents conteneurs tels que :

• Internet Explorer. Il est alors utilisé au sein de pages HTML auxquelles il amène une certaine inter activité impossible à atteindre avec le seul langage HTML.

• Internet Information Server (IIS) le serveur Web de Microsoft sur NT/2000 et son équivalent Personal Web Server (PWS) sur Win9x. Dans ce cas, vbscript est utilisé pour faire de la programmation côté serveur web, technologie appelée ASP (Active Server Pages) par Microsoft.

• Windows Scripting Host (WSH) pour une utilisation directe sous Windows notamment pour écrire des scripts d'administration système, c'est bien évidemment ce dernier cas qui nous intéresse.

Un programme VBSCRIPT ne s'exécute pas directement sous Windows mais dans un conteneur qui lui fournit un contexte d'exécution et un certain nombre d'objets qui lui sont propres.

Pour travailler dans le conteneur WSH deux exécutables sont disponibles : wscript.exe et cscript.exe .

Le « W » de wscript veut dire windows et le « C »de cscript veut dire console. Un script peut être exécuté indifféremment par wscript ou cscript. La différence réside dans le mode d'affichage de messages à l'écran :

• wscript les affiche dans une fenêtre.

• cscript les affiche à l'écran.

Bon, faisons maintenant un rapide tour d'horizon du fonctionnement de Vbscript.

VBScript manipule un seul type de données que l'on appelle variant (cf encadré), selon le cas, ce variant contiendra boléens, réels, entiers, date, heure, string ou un objet.

Il dispose des opérateurs mathématiques, de logique et de comparaison habituels.

L'instruction de test la plus utilisée est le If ..then ..else.. et celle de boucle est le For...next.

Une procédure (ou fonction) est un groupe de ligne(s) de code de programmation destiné à exécuter une tâche bien spécifique et que l'on pourra utiliser à plusieurs reprises. De plus, l'usage des procédures améliorera grandement la lisibilité et la maintenance de notre script.

Il en existe deux types : « Sub » et « Function ».

Les sous programmes « Sub » peuvent accepter un ou plusieurs arguments en entrée, mais ne renvoie aucune valeur contrairement aux fonctions « Function » qui peuvent elles renvoyer une valeur de type « variant ».

VBScript possède également ses propres fonctions telles que :

• Fonction de type de données (test sur le contenu de la variable, IsDate, IsNumeric...)

• Fonction de conversion et de transtypage (Asc, CBool, Hex..)

Les variables en VBscript

Les variables contiennent des données qui peuvent être modifiées lors de l'exécution d'un programme. On y fait référence par le nom de cette variable.
Les noms de variables :
• ne doivent pas dépasser 255 caractères.
• doivent commencer par une lettre (caractère alphabétique).
• ne peuvent contenir une virgule, un point ou un espace.
• ne peuvent reprendre des mots clés de VBscript.
• doivent être uniques à l'intérieur de leur portée (voir variables globales et locales).
Ajoutons pour nous les francophones, qu'il faut employer l'alphabet ASCII, donc les lettres sans accents.
Pour rappel, VBscript est sensible à la casse. Attention donc aux majuscules et minuscules !

La déclaration de variable

Les variables peuvent se déclarer de deux façons :
• De façon explicite. On dit à VBscript que ceci est une variable. La commande qui permet de déclarer une variable est le mot clé « Dim » suivi du nom de la variable (et ce généralement en début de script).
Dim Numero
Dim x, y, z
• soit de façon implicite. On écrit directement dans le code VBscript, le nom de la variable suivi de la valeur que l'on lui attribue et VBscript s'en accommode.
Numero = 2
Prenom = "ReZoR"
On peut exiger la méthode de déclaration explicite et empêcher les déclarations implicites. Cela se réalise par la commande « Option Explicit »
Cette commande se place dans la première ligne de code de votre VBscript :
OptionExplicit
Dim variable
la suite du code...

Les types de données sous VBscript
VBscript utilise un seul type de données nommé Variant . Ce type Variant est véritablement un fourre-tout de différents types d'informations. En voici quelques-uns :
Des nombres:
Tout nombre entier ou avec virgule tel que 22 ou 3.1416
Des chaînes de caractères:
Toute suite de caractères alphanumérique comprise entre guillemets telle que "suite de caractères". On emploiera aussi le terme "strings".
Des Booléens:
Contient True (vrai) ou False (faux).
Empty:
La variable n'a pas encore été initialisée. Sa valeur est égale à 0 pour les variables numériques et " " pour les strings.
Null:
Contient (intentionnellement) des données incorrectes.
Error:
Contient un numéro d'erreur. Utile pour corriger un script (voir chapitre les messages d'erreur).

Variables locales et variables globales

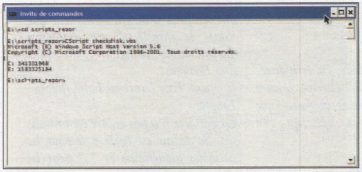
Les variables déclarées dans les procédures ont une portée dite locale, elles ne sont utilisables que dans le cadre de cette seule procédure.
Une variable est dite globale, lorsqu'elle pourra être partagée partout dans le code du script. Pour qu'une variable soit globale, elle doit être déclarée en dehors de toutes procédures. Pour ce faire, on les déclare tout au début du script.

• Fonction de chaîne (Len, Join, Chr..)
• Fonction de date et d'heure (Date, Hour, ...)
• Fonction mathématique (Cos, Exp, Randomize..)
• Fonction d'interaction avec l'utilisateur (MsgBox, InputBox..)

On dit de VBScript qu'il est un langage orienté Objet capable de manipuler ce que l'on appelle des « objets ».
En terme de programmation objet, on utilise les termes « propriétés » et « méthodes » de l'objet.
Pour faire simple, considérons un objet comme une boîte noire qui a des caractéristiques (propriétés) que l'on pourra atteindre de l'extérieur comme par exemple un objet fenêtre, celle ci a une couleur, une taille et d'autre propriétés.
On pourra agir sur cet objet par l'intermédiaire de commandes (redimensionner...) que l'on appellera méthodes.
Donc, pour se servir d'un objet il suffira de lui appliquer la bonne « méthode » en lui passant les bons paramètres.
Bon assez parlé, mettons nous au travail et écrivons un script (checkdisks.vbs) qui scanne les différents lecteurs de l'ordinateur et affiche l'espace libre de chaque unité.

```
Option Explicit
On Error Resume Next
Dim fs, unites, disque
Set fs = createObject("Scripting.FileSystemObject")
Set unite = fs.Drives
For Each disque In unites
Wscript.Echo disque.path & " " & disque.FreeSpace
Next
```

Analysons ce script:
Tout d'abord les deux premières lignes constituent ce que l'on appelle les informations « d'en tête » du programme.
Option Explicit (cf encadré), cette instruction indique que toutes les variables employées doivent être déclarées au préalable.
On Error Resume Next, scindons cette instruction en deux parties. On Error indique à l'ordinateur que l'on veut faire quelque chose en cas d'erreur , Resume Next indique que l'on souhaite passer à l'instruction suivante. On conseille généralement de ne pas utiliser cette instruction dans la phase de création du programme afin de ne pas masquer des erreurs éventuelles.



Une sortie console avec CScript

Une sortie boîte de dialogue Wscript

Un message d'erreur en mode WScript

Dim sert à déclarer une variable (cf encadré), on essaye toujours de donner un nom parlant aux variables que l'on déclare dans un programme, ic fs pour file system et disque et unites qui parlent d'eux même.

Dans un programme VBScript vient ensuite, si besoin est, une section « informations de référence » dans laquelle on donne des valeurs aux variables déclarées et dont les objectifs sont les suivants :

- Diminuer la frappe pour le programmeur.
- Rendre le script plus lisible.
- Permettre de modifier facilement un script.

Nous pourrions par exemple créer un script lisant les valeurs des clés de registre comme le nom du pc et nous trouverions dans les informations de référence une ligne du style :

regComputerName="HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName\ComputerName\"

Avouez que si vous devez utiliser cette variable plusieurs fois, ceci vous simplifiera la tâche ! :-)

Le programme que nous étudions ne contient pas de section « Informations de référence ».

On passe ensuite à la section « Informations de travail » où seront exécutées les actions souhaitées.

Examinons la première ligne de code de cette section :

Set fs = createObject("Scripting.FileSystemObject")

Nous attribuons à la variable fs la référence de l'objet FileSystem grâce au mot clé Set, cet objet permet d'effectuer des opérations sur les disques, dossiers et fichiers.

Set unites=fs.Drive permet de définir l'objet Drive en interrogeant la propriété Drive de l'objet FileSystem.

Dans les trois dernières lignes du script, nous balayons l'ensemble des lecteurs (disques)

avec la ligne « For Each disque In unites » et nous affichons à l'aide de l'instruction « Wscript.Echo » les propriétés path (nom) et FreeSpace (espace libre) dans deux boîtes de dialogues successives si vous le lancer en Wsript ou l'une après l'autre si vous le lancer avec cscript dans une console.

Ce script (checkdisk.vbs) met en évidence l'intérêt de l'utilisation de l'instruction « On Error Resume Next », supprimez cette ligne et vous vous rendrez compte qu'une erreur programme est générée.

Ceci est du au fait que l'on scanne les lecteurs du PC, y compris le CDROM et que celui-ci est vide.

On ajoute donc la ligne « On Error Resume Next » pour que le programme ne s'arrête pas.

En VBScript, on se rend vite compte que le choix de l'objet est primordial en fonction de ce à quoi on désire accéder.

Ainsi le programme nom_pc.vbs (cf encadré) utilise l'objet « WscriptShell » pour lire dans la base de registre du système.

A ce stade vous savez créer des objets et les utiliser via leurs méthodes et propriétés.

Les objets VBScript et Wsh accesibles en VBScript sont respectivement au nombre de 3 et de 6.

Pour VBScript, il s'agit des objets Err, RegExp et Dictionnary, nous n'étudierons pas les deux derniers car ils ne sont pas essentiels pour une bonne compréhension de WSH.

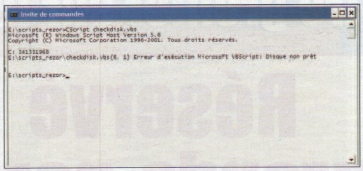
En ce qui concerne les objets WSH, il s'agit de Wscript, Wscript.Arguments, WscriptNetwork, Wscript.Shell, Wscript.Environnement et Wscript.Shortcut.

Quelques adresses utiles :

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/1c457e66-a6b2-4545-b2dd-33a59d8661e8.asp

http://www.secretswindows.com/

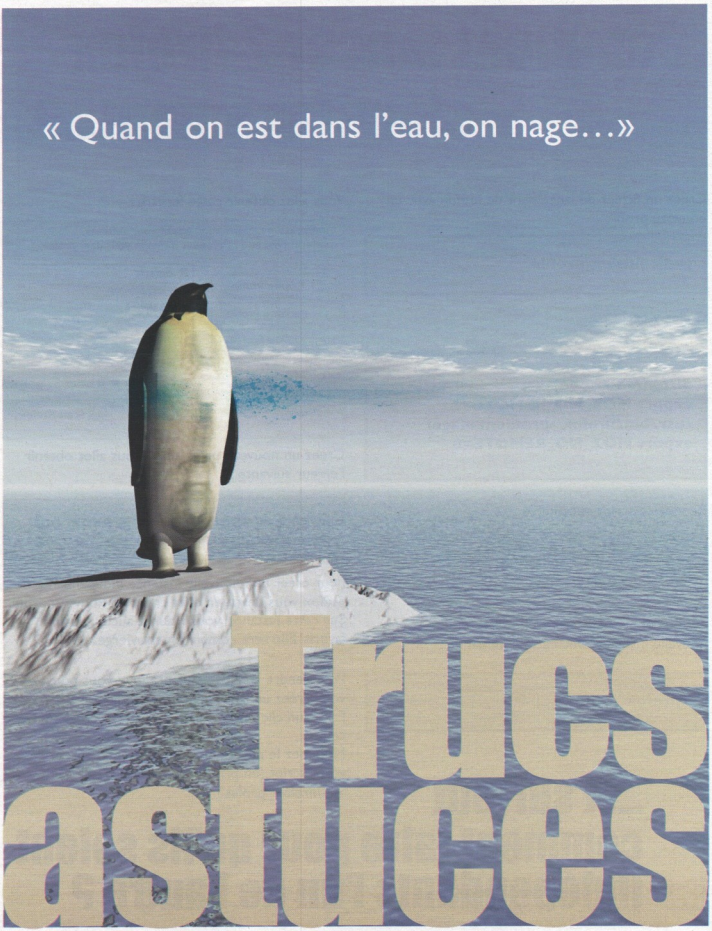
```
'nom_pc.vbs
'=================================================
'scrip affichant le nom actif, le nom et le host du pc
'=================================================
' informations d'entête
Option Explicit
On Error Resume Next
'
'déclaration des noms de variables
Dim objshell
Dim regActiveComputerName, regComputerName, regHostName
Dim ActiveComputerName, ComputerName, HostName
regActiveComputerName = "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\" &_
"ComputerName\ActiveComputerName\ComputerName"
'les caractères &_ sont utilisés pour dire au script de concaténer deux chaînes de caractères se suivant à la ligne
regComputerName="HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\Compute
rName\ComputerName"
regHostName                                                                    =
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Hostname"
'informations de travail
Set objshell = CreateObject("Wscript.Shell")
ActiveComputerName = objshell.RegRead(regActiveComputerName)
ComputerName = objshell.RegRead(regComputerName)
HostName = objshell.RegRead(regHostName)
'
'on dirige les informations recueillies vers la sortie standard grâce à la commande WScript.Echo qui 'affiche le contenu des
variables que l'on peut concaténer avec du texte
WScript.Echo ActiveComputerName & " est le nom du pc actif"
WScript.Echo ComputerName & " est le nom du pc "
WScript.Echo HostName & " est le nom d'hôte"
```



Message d'erreur en mode CScript

Réservé aux grands-parents !

Information et abonnement
www.ordisenior.com



Trucs astuces

Comment lancer 2 firefox simultanément...?

Créez un fichier de lancement de firefox avec un nouveau profil :

```
gedit firefox_profils
```

Collez-y ceci :

```
#!/bin/sh
export MOZ_NO_REMOTE=1
/usr/bin/firefox -profilemanager
export MOZ_NO_REMOTE=0
```

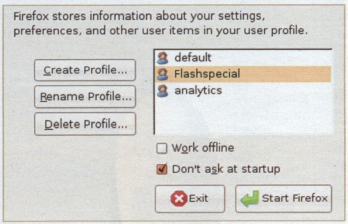
Rendez ce script exécutable

```
sudo chmod u+x firefox_profils
```

Et vous pouvez lancer ensuite directement votre nouvelle instance avec cette commande :

```
./firefox_profils
```

Vous allez obtenir cette fenêtre :



Créez un nouveau profil sinon vous allez obtenir l'erreur suivante :

```
Firefox is already running, but is not responding.
```

Pour créer une nouvelle instance indépendante de firefox vous devez en effet créez un nouveau profil. Sur cette instance, vous n'aurez aucun plugin ni favoris. Elle sera completement vierge.

Pour rendre la chose plus pratique vous pouvez vous créez un lanceur pour ce script :
Faites un clic droits sur le bureau >> créer un lanceur.
Nommez le puis donnez lui le chemin absolu de votre script (en principe '/home/VOTRENOMUSER/firefox_profils').

...Et surtout comment faire pour qu'ils soient indépendants l'un de l'autre ?

Vixta. Comme Vista, mais... gratuit

Vista vous plaît mais vous préférez les logiciels libres ?
Il existe une solution : un excellent compromis entre les deux mondes qui vous permettra de faire le grand saut sans perdre vos marques !
Nommé Vixta, il s'agit d'un système d'exploitation Linux basé sur une distribution Fedora Core 8 dans un environnement KDE, et par conséquent totalement gratuit ! Il n'est malheureusement disponible qu'en anglais et portugais, mais vu sont succès, on peut espérer une version française dans peu de temps :)
Comme on peut le voir sur ces images, la copie avec l'interface Aero de Vista est bluffante, étonnant d'ailleurs que Microsoft n'ait pas encore élevé la voix !

Tous les éléments sont bien là : la barre des tâches, le menu démarrer, les icônes, le poste de travail, la barre de démarrage… Même les écrans d'accueil et de fermeture sont imités et la skin de Firefox rappel beaucoup IE7.
Bien évidemment, il y a quelques différences propres au monde de l'open source : Au revoir IE, explorer et Office et bienvenue Firefox, Konqueror et openoffice.org !
Dernier avantage : une facilité d'installation hors du commun (4 "ok" et un password d'après le site officiel !) ce qui n'est pas courant et qui repousse nombre d'utilisateurs…
Pour conclure, on peut dire que cette facilité d'utilisation (pour les windowsiens) et cette ressemblance font que vixta est idéalement conseillé pour un débutant qui souhaite passer sans douleur à linux.
Un des objectifs de Vixta n'est il d'ailleurs pas "Spread linux to the "masses" ?

Pour aller plus loin, visitez le site officiel : www.vixta.org

Quelques commandes Vi ...bien utiles

Rechercher

/word	Recherche "word" de haut en bas
?word	Recherche "word" de bas en haut
/jo[ha]n	Recherche "john" ou "joan"
/\< the	Recherche "the", "theatre" ou "then"
/the\>	Recherche "the" ou "breathe"
/\< the\>	Recherche "the"
/\< ....\>	Recherche tous les mots de 4 lettres
/\	Cherche "fred" mais pas "alfred" ou "frederick"
/fred|joe	Recherche "fred" ou "joe"
/\<\d\d\d\d\d\>	Recherche exactement 4 nombres entiers
/^\n\{3}	Trouve 3 lignes vides
:bufdo /searchstr/	Effectue une recherche dans tous les fichiers ouverts

Remplacer

:%s/old/new/g	Remplace toutes les occurences de "old" par "new" dans le fichier
:%s/old/new/gw	Remplace toutes les occurences avec confirmation
:2,35s/old/new/g	Remplace toutes les occurences entre les lignes 2 et 35
:5,$s/old/new/g	Remplace toutes les occurences de la ligne 5 à la fin du fichier
:%s/^/hello/g	Remplace le début de chaque ligne par "hello"
:%s/$/Harry/g	Remplace la fin de chaque ligne par "Harry"
:%s/onward/forward/gi	Remplace "onward" par "forward" sans tenir compte de la casse
:%s/ *$//g	Supprime les espaces blancs
:g/string/d	Supprime toutes les lignes contenant "string"
:v/string/d	Supprime toutes les lignes ne contenant pas "string"
:s/Bill/Steve/	Remplace la première occurence de "Bill" par "Steve" dans la ligne courante
:s/Bill/Steve/g	Remplace "Bill" par "Steve" dans la ligne courante
:%s/Bill/Steve/g	Remplace "Bill" par "Steve" dans tout le fichier
:%s/\r//g	Supprime les caractères de retour DOS (^M)
:%s/\r/\r/g	Transforme les caractères de retour DOS en retours
:%s#<[^>]\+>##g	Supprime les tags HTML en laissant le texte
:%s/^\(.*\)\n\1$/\1/	Supprime les lignes en doublon
Ctrl+a	Incrémente le nombre sous le curseur
Ctrl+x	Decrémente le nombre sous le curseur
ggVG g?	Transforme le texte en Rot13

Casse

Vu	**Transforme la ligne en minuscule**
VU	**Transforme la ligne en majuscule**
g~~	**Inverse la casse de la ligne**
vEU	**Mets le mot en majuscule**
vE~	**Modifie la casse du mot**
ggguG	**Mets tout le texte en majuscule**
:set ignorecase	**Ignore la casse lors des recherches**
:set smartcase	**Ignore la casse lors des recherches sauf si une majuscule est utilisée**
:%s/.*/\U&	**Mets toutes les lettres en majuscule**
:%s/.*/\L&	**Mets toutes les lettres en minuscule**
:%s/\<./\u&/g	**Mets la première lettre de chaque mot en majuscule**
:%s/\<./\l&/g	**Mets la première lettre de chaque mot en minuscule**
:%s/.*/\u&	**Mets la première lettre de chaque ligne ne majuscule**
:%s/.*/\l&	**Mets la première lettre de chaque ligne en minuscule**

Lecture/Ecriture sur d'autres fichiers

:1,10 w outfile	**Enregistre les lignes 1 à 10 dans outfile**
:1,10 w >> outfile	**Ajoute les lignes 1 à 10 dans outfile**
:r infile	**Insère le contenu de infile**
:23r infile	**Insère le contenu de infile sous la ligne 23**

Explorateur de fichiers

:e .	**Ouvre l'explorateur de fichiers intégré**
:Exp	**Ouvre l'explorateur de fichiers intégré**
:Sex	**sépare la fenetre et ouvre l'explorateur de fichiers**
:browse e	**Explorateur graphique**
:ls	**Liste les buffers**
:cd ..	**Se déplacer au dossier parent**
:args	**Liste de files**
:args *.php	**Ouvre une liste de fichiers**
:grep expression *.php	**Retourne une liste de fichiers .php contenant expression**
gf	**Ouvre le nom de fichier sous le curseur**

Interaction avec Unix

:!pwd	**Execute la commande unix "pwd" et retourne à vi**
!!pwd	**Execute la commande unix "pwd" et insère la sortie dans le fichier**
:sh	**Quitte temporairement vi**
$exit	**Retourne sous vi**

Alignement

:%!fmt	Aligne toutes les lignes
!}fmt	Align toutes les lignes à la position courante
5!!fmt	Aligne les 5 lignes suivantes

Onglets

:tabnew	Crée un nouvel onglet
gt	Affiche l'onglet suivant
:tabfirst	Affiche le premier onglet
:tablast	Affiche le dernier onglet
:tabm n(position)	Réarrange les onglets
:tabdo %s/foo/bar/g	Execute une commande dans tous les onglets
:tab ball	Mets tous les fichiers ouverts dans des onglets

Partage de fenêtre

:e filename	Edite filename dans la fenêtre courante
:split filename	Divise la fenêtre et charge filename
ctrl-w up arrow	Déplace le curseur dans la fenêtre du haut
ctrl-w ctrl-w	Déplace le curseur dans la fenêtre suivante
ctrl-w_	Maximise la fenêtre courante
ctrl-w=	Donne la même taille à toutes les fenêtres
10 ctrl-w+	Agrandis la fenêtre courante de 10 lignes
:vsplit file	Divise la fenêtre verticalement
:sview file	Identique à :split mais en mode lecture seule
:hide	Ferme la fenêtre courante
:only	Fais de la fenêtre courante la seule à l'écran
:b 2	Ouvre le buffer #2 dans cette fenêtre

Complétion

Ctrl+n Ctrl+p (en insertion)	Compléter le mot
Ctrl+x Ctrl+l	Compléter la ligne
:set dictionary=dict	Definit dict comme dictionnaire
Ctrl+x Ctrl+k	Compléter en utilisant le dictionnaire

Marqueurs

mk	Marque la position actuelle
'k	Déplace le curseur à la marque k
d'k	Supprime le texte jusqu'à la marque k

Abréviations

:ab mail mail@provider.org	**Définit mail comme abbréviation de mail@provider.org**
Indentation	
:set autoindent	**Active l'indentation automatique**
:set smartindent	**Indentation automatique intelligente**
:set cindent	**Règles d'indentation pour programmes en C**
:set shiftwidth=4	**Défini 4 espaces comme taille d'indentation**
ctrl-t, ctrl-d	**Indente/désindente en mode insertion**
>>	**Indente**
<<	**Désindente**

Coloration syntaxique

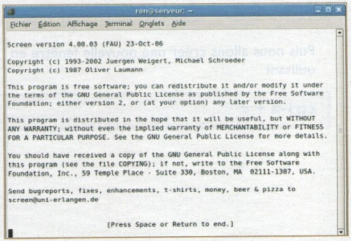
:syntax on	**Active la coloration syntaxique**
:syntax off	**Désactive la coloration syntaxique**
:set syntax=perl	**Force la coloration syntaxique**

Utilisations et commandes de screen

Vous avez un serveur dédié et vous aimeriez bien laissez un client irc ou un client torrent tourner dessus, si une seule session suffit vous pouvez peut être regarder du coter de la commande nohup mais si vous avez besoin de plusieurs sessions ou plusieurs fenêtres alors vous aurez sûrement besoin de screen ;)

Tout d'abord on installe et on lance screen :

```
apt-get install screenscreen
```



>>

>> Faites entrée vous arrivez sur la 1ere fenêtre, comment le sait-on ?

Tout simplement avec la commande

 # appuyer sur Ctrl et A en même temps, puis sur w après #
ctrl-a +w

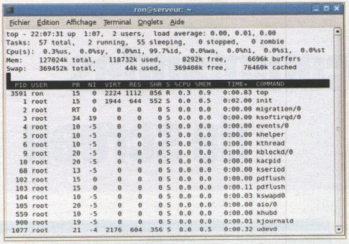
Cela vous affiche

0*$ bash

Le numéro de la fenêtre est ici en rouge ;)

Dans cette fenêtre 0 nous lancerons une commande comme

Top



Puis nous allons créer une nouvelle fenêtre en utilisant

ctrl-a + c

Vous pouvez lancer une autre commande comme wget, un client irc en mode texte comme irssi ou encore un client torrent ;)

Vous pouvez réessayer la commande pour vérifier que vous êtes bien dans la fenêtre numéro 1

ctrl-a + w

1*$ bash, nous sommes bien dans la fenêtre 1

Revenons à la première fenêtre avec les commandes

ctrl-a + p
ctrl-a + [numéro de fenetre]

Le principal intérêt est de pouvoir laisser les commandes tourner tout en fermant notre terminal. Sortons de screen grâce à la commande

ctrl-a + d

Vous pouvez fermer puis rouvrir la connexion ssh ou le terminal et la faites :

screen -r

Vous retrouvez bien les 2 fenêtres avec la commande top dans la fenêtre 0 et votre client irc ou torrent fans la fenêtre 1.

Installer les drivers AR5007EG sous ubuntu feisty

1/ Téléchargez ndiswrapper ICI :

```
wget http://wifix.sourceforge.net/software.php?title=ndiswrapper
```

2/ Téléchargez les derniers drivers atheros pour win XP (oui on va les utiliser avec ndiswrapper !!!)

Si vous avez une version 32 bits:

```
wget http://blakecmartin.googlepages.com/ar5007eg-32-0.2.tar.gz
```

Si vous avez une 64 bits

```
wget http://blakecmartin.googlepages.com/ar5007eg-64-0.2.tar.gz
```

3/ Décompresser les archives téléchargées:

```
tar xvf ar5007eg-*.tar.gz
tar xvf ndiswrapper-newest.tar.gz
```

4/ Installez tout le necessaire à la compilation automatique:

```
sudo aptitude update && sudo aptitude install linux-headers-$(uname -r) build-essential
```

5/ Blacklistez le module ath_pci kernel (il ne supporte pas notre chipset).

```
echo "blacklist ath_pci" | sudo tee -a /etc/modprobe.d/blacklist
```

6/ Compilez ndiswrapper:

```
pushd ndiswrapper-*/
sudo make uninstall
make
sudo make install
popd
```

7/ Installez les drivers windows à partir ndiswrapper

```
pushd */ar5007eg/
sudo ndiswrapper -i net5211.inf
popd
```

8/ Automatisez le lancement d'ndiswrapper au démarrage:

```
sudo modprobe ndiswrapper
echo "ndiswrapper" | sudo tee -a /etc/modules
```

9/ Rebootez

```
sudo init 6
```

ENJOY !

Testez la résistance aux attaques de votre réseau wifi

Le meilleur moyen de vous prémunir des attaques de personnes malintentionnées sur votre réseau wifi est sûrement de jouer vous-même le rôle de la personne malintentionnée. Pour ce type d'attaque, la distribution Linux backtrack sera votre fidèle partenaire…

La préparation

Avant toute chose, téléchargez la distribution Linux backtrack gratuitement sur http://www.remote-exploit.org/backtrack_download.html. Gravez-la après avoir vérifié son intégrité (md5sum). Une fois gravée, mettez-la de côté afin de préparer une partition FAT32 de 2 ou 3 giga… L'avantage du FAT32 c'est qu'il est lisible par Windows et linux.

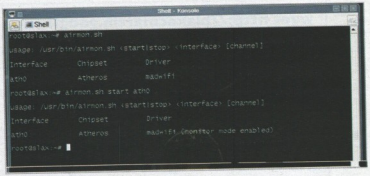
Cette partition va en fait servir à stocker les paquets capturés et les différents fichiers nécessaires pour le crack de la clé wep. Cette partition n'est pas indispensable mais recommandée, surtout si vous ne disposez que de peu de RAM car backtrack étant un live cd, tout ses fichiers sont stockés en RAM. Le fait d'avoir une partition fat32 vous permet aussi d'arrêter le pc et de redémarrer sans perdre tous les paquets déjà capturés, ce qui représente un avantage non négligeable…

Vous pouvez ensuite démarrer sur votre backtrack…

Le login est *root*, le mot de passe est *toor* et pour lancer le mode graphique tapez *startx* (il se peut que vous deviez taper *stqrtx* car le clavier est configuré en anglais par defaut…)

A l'attaque !

Afin de se lancer, l'ouverture de plusieurs terminaux s'avèrera utile… Prenez-en un puis tapez " airmon.sh " pour détecter les interfaces wifi, puis sélectionnez celle que vous voulez démarrer par la commande " airmon.sh start « l'interface wifi » "



Ici on voit que la carte est correctement reconnue et que le mode monitor est directement activé. Le mode monitor permet de capter tous les paquets qui transitent même ceux qui ne vous sont pas adressés.

Maintenant que nous sommes sûrs que notre carte est correctement détectée, il nous faut scanner les réseaux… L'outil qui est utilisé pour scanner les réseaux est *airodump*.

Tapez dans la console : "airodump « interface » « nom du fichier de sortie » « canal à scanner » ".

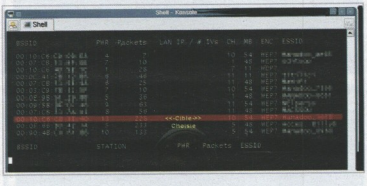
Pour choisir de scanner tous les canaux, mettez 0

Vous pouvez rajouter le paramètre 1 à la fin, pour n'enregistrer dans le fichier de sortie (ici out) que ce qui va nous servir à cracker la clef wep :

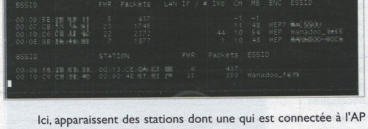
Sh# airodump ath0 out 0 1

Le fait de rajouter ce paramètre crée un fichier de sortie dont l'extension est différente: .ivs à la place de .cap. Le principal avantage est que ce fichier ne contient pas toutes les informations de paquets mais uniquement les IVs, sa taille est donc beaucoup plus petite. Si vous n'avez pas créé de partition pour stocker les captures, utilisez cette option. Préférez cependant enregistrer en .cap si vous avez une partition Fat32

Fait « cd .. » pour remonter à la racine. Puis "cd mnt" pour aller dans le dossier qui correspond au poste de travail sous windows. Puis faites "cd « partition fat32 » "
L'interface d'airodump se présente comme ceci :



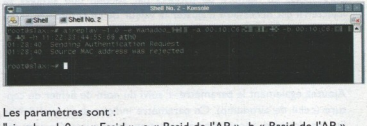
La colonne BSSID correspond à l'adresse mac des points d'accès (AP)
La colonne ESSID correspond au nom du réseau (Wanadoo-XXXX, WiFI-freebox.)
La première partie correspond aux points d'accès et la seconde partie aux stations (comprendre les ordinateurs connectés aux différents réseaux).
Ici il n'y a pas encore de stations.
La colonne qui nous intéresse est la colonne des IVs. Ce sont ces fichiers qui vont nous permettre de cracker les clefs wep.
Ici, notre AP est le seul dont l'Essid n'est pas totalement masqué. Afin de gagner du temps, il est conseillé de se concentrer sur le canal où se trouve le réseau a cracker… On relance donc *airodump* en choisissant seulement le canal où il se situe : dans notre exemple… le 10
« airodump ath0 out 10 »
Pour arrêter la capture et pouvoir entrer des commandes, faites Ctrl+C.
Vous êtes également obligés de stopper la capture si vous souhaitez copier une adresse mac car l'écran se rafraîchit. Pour copier quelque chose, sélectionnez simplement avec la souris et faites clic droit copy. Idem pour coller ou utiliser shift+insert.
Pour plus de détails sur *airodump*, tapez uniquement « airodump » dans la console et l'aide apparaîtra (idem pour aircrack et airplay).



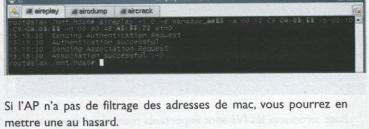
Ici, apparaissent des stations dont une qui est connectée à l'AP qui nous intéresse.
Les accès-point ont parfois un filtrage des adresses mac, appelé mode association. C'est le cas par exemple des livebox.
Pour *aireplay*, nous aurons besoin de cette adresse mac. Le but sera donc de se faire passer pour l'ordinateur ayant accès a l'AP.
Dès qu'*airodump* commence sa récupération des IVs, il indique le type de cryptage utilisé sur le réseau. Il peut être de trois types : WEP WPA ou OPN. Le WEP étant le plus rapide à « cracker ».
Nous savons désormais que le cryptage de notre réseau est WEP, qu'une station est présente et qu'il y a du trafic (350 paquets pour la station en peu de temps). Nous allons donc pouvoir utiliser le second outil indispensable pour crackerun reseau wifi : *aireplay*, un injecteur de paquets pour accélérer le trafic et surtout stimuler l'envoi d'IVs Il faut savoir que pour cracker la clef WEP d'un réseau wifi, il est préférable qu'il y ait un maximum de trafic. La capture de IVs n'en sera que beaucoup plus rapide.
Si le trafic est nul ou quasi nul, nous devrons injecter des paquets, c'est là qu'*aireplay* intervient…

La Fake authentification

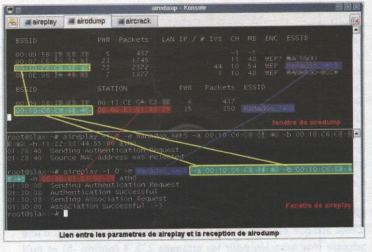
Cette attaque est seulement utile lorsque vous avez besoin d'une adresse mac associée pour les attaques 2, 3, 4 (option -h) et qu'il n'y a pas de clients associés pour le moment. Il est recommandé d'utiliser l'adresse MAc d'un client réel (par exemple, 00:09:5B:EB:C5:2B) dans les attaques 2, 3 et 4. L'attaque *fake authentification* ne génère pas de requêtes ARP.
On lance *aireplay* une première fois sans se soucier du bssid de la station :



Les paramètres sont :
"aireplay -1 0 -e « Essid » -a « Bssid de l'AP » -b « Bssid de l'AP » -h « Bssid de la station » « interface » "
« -1 0 » correspond à une attaque par "fake authentification" le zéro indiquant le délai de réponse accepté.
Remarquez que si nous mettons une adresse mac aléatoire, l'AP nous refoule. Nous devons indiquer le BSSID fourni par airodump :



Si l'AP n'a pas de filtrage des adresses de mac, vous pourrez en mettre une au hasard.
Une fois « association succesful » obtenu, nous savons que l'AP nous autorise à nous connecter. C'est une première victoire…
L'authentification successful peut se faire attendre dans le cas d'une mauvaise réception du signal. Ne vous inquiétez pas… Plusieurs « sending authentification Request » peuvent être nécessaires. Considérez tout de même qu'après une centaine d'envois, si aireplay n'affiche toujours pas l'athentification succesfull, il n'y parviendra probablement jamais…
Voici un petit schéma qui vous montre les relations entre les paramètres d'aireplay et la capture d'airodump (voir page suivante) :
Il se peut que l'association ne fonctionne pas, passez tout de même à l'étape suivante qui consiste à injecter des paquets dans le trafic…



Lien entre les parametres de aireplay et la reception de airodump

L'injection de paquets

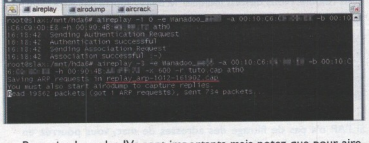
Une fois que l'association est bonne, on relance aireplay en changeant et rajoutant quelques paramètres.

Il faut changer le premier paramètre et le remplacer par "-3", ce qui correspond à une attaque par injection de paquets.

Il faut également rajouter le paramètre "-x" suivi d'une valeur qui correspond au nombre de paquets par second que aireplay va injecter. Il est nécessaire d'ajuster la valeur de ce paramètre selon la réception du signal. Si la réception est excellente, n'hésitez pas, injectez 1000 paquets par seconde. Si la réception est mauvaise, vous pourrez descendre jusque 150 ou 200, ce sera plus long mais plus fiable …

Ajoutez également le paramètre -r suivi du nom de fichier de capture (celui de airodump). Ce paramètre indique dans quel fichier lire les données nécessaires à l'injection de paquets. Ce sont les ARP présent dans ce fichier qui nous seront utiles pour influencer le trafic.

N'oubliez pas de vous placer dans le même répertoire.



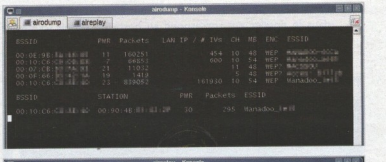
Pour airodump, les IVs sont importants mais notez que pour aireplay, les ARP le sont tout autant, ce sont eux qui vont vous permettre d'augmenter la production de IVs.

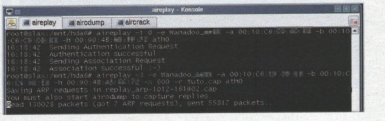
Aireplay sauvegarde les ARP dans un fichier qu'il crée à chaque fois qu'il est lancé (souligné sur la capture d'écran). C'est ce fichier que vous mettrez ensuite après le paramètre -r si les récupérations d'ARP ont fonctionné.

Les ARP sont obtenus en lisant le fichier indiqué mais aussi en écoutant le réseau comme le fait airodump.

Ici, on voit que l'on a un ARP. Dès qu'un ARP a été trouvé, aireplay commence à envoyer des paquets et c'est là que la magie opère et que vous verez les IVs augmenter à vue d'œil…

Normalement, les ARP augmentent également… Une limite imposée par aireplay est de 1024 ARP.





Dernière étape : Récupération de la clé WEP avec aircrack…

Pour lancer aircrack, il faut environ 300.000 IVs pour une clé WEP 64bits et 1.000.000 d'IVs pour une clé de 128 bits.

Ouvrez donc un nouveau Shell et lancez aircrack.

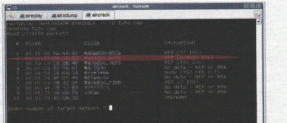
Sh# aircrack -x -0 nomduFichierDeCapture

Le paramètre -x permet de ne pas bruteforcer les 2 derniers bits. Le paramètre -0 met aircrack en couleur pour plus de lisibilité

Ensuite, le dernier paramètre est le nom du fichier de capture d'airodump.

Vous pouvez également utiliser la syntaxe « *.cap » et « *.ivs » pour ouvrir tous les fichiers .cap et .ivs.

Sh# aircrack -x -0 *.cap *.IVs

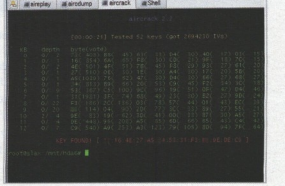


Une fois lancé, aircrack nous affiche tous les réseaux qu'il a rencontrés, leur cryptage et le nombre d'IVs correspondant. Il vous suffit d'entrer le numéro du réseau.

Un peu de patience devrait nous amener à trouver la clé. Aircrack incrémente automatiquement les IVs et s'en sert pour cracker la clef WEP. Lorsque qu'aircrack a trouvé la clé, il l'affichera en rouge.

Voilà, vous avez réussi à cracker votre réseau, il n'est donc pas assez sécurisé. L'utilisation du WPA est fortement conseillé, car beaucoup plus d'IVs sont nécessaires…

N'oubliez surtout pas que vous n'avez pas le droit de cracker le réseau wifi de vos voisins ;).



Partager ses fichiers sous Linux avec NFS

Sans doute êtes-vous habitués au partage de fichiers sous Windows. Mais savez-vous qu'il est possible de partager ses fichiers sous Linux. Cette fonction existe depuis bien longtemps et va bien au delà de ce que propose les autres systèmes d'exploitation car Linux a été conçu pour le réseau. Le mécanisme de partage s'appelle un montage NFS. Je vous propose de le découvrir dans cet article. Mais avant, nous ferons un petit rappel sur le système de fichier ext3.

L'ORGANISATION DES FICHIERS SOUS LINUX

Le système de fichiers

Actuellement, le système de fichier le plus utilisé sous Linux est l'ext3. Celui-ci succède à l'ext2 en intégrant une journalisation permettant une récupération plus facile, et sans perte de données, du système en cas de crash. Sous Windows, le système de fichiers est NTFS qu'il ne faudra pas confondre avec le NFS sous Linux que je vais vous expliquer dans la suite de l'article. Avant de passer au sujet principal de cet article et de faire du partage avec NFS, je vous propose de voir ou de revoir l'arborescence des fichiers sur notre système préféré.

L'arborescence des fichiers sous Linux

Sous Linux, vous ne trouvez pas de lettre pour désigner vos lecteurs comme sous Windows, mais une arborescence qui intègre tout. Celle-ci part évidemment d'une racine « / ».Vous rencontrez sous celle-ci une multitude de dossiers et de sous-dossiers. Si vous

RépertoireContenubinBinaires (exécutables) des commandes essentiellesbootFichiers statiques pour le programme d'amorçagedevFichiers des pilotes de périphériquesetcConfiguration système propre à la machinehomeRépertoires personnels des utilisateurslibBibliothèques partagées et modules noyaux essentielsmediaPoints de montage pour les supports amovibles mntPoint de montage pour les montages temporairesprocRépertoire virtuel pour les informations système (noyaux 2.4 et 2.6)rootRépertoire personnel de l'utilisateur rootsbinExécutables système essentielssysRépertoire virtuel pour les informations système (noyaux 2.6)tmpFichiers temporairesusrHiérarchie secondairevarDonnées variablesoptRépertoire pour d'autres logiciels

source : www.commentcamarche.net/linux/linarb.php3

souhaitez connaître la signification de chacun d'eux, lisez l'encadré ci-dessous qui vous donnera une description succinte du rôle de chaque dossier.
Petite remarque, j'utilise dans cet article indifféremment le terme de dossier ou répertoire.
Vous constatez que certains répertoires ont un sens particulier sous Linux. En effet, dans ce système d'exploitation, pratiquement tout peut être considéré comme un fichier. Par exemple, le répertoire « /proc » vous permet d'obtenir une multitude d'informations sur votre système. Ceci est rendu possible car Linux établit une communication entre votre matériel et un pseudo-système de fichiers. Si vous voulez par exemple obtenir des informations sur votre CPU, vous pouvez taper la commande suivante qui est normalement sensée afficher le contenu du fichier « cpuinfo » du répertoire « /proc » :

```
more /proc/cpuinfo
```

Explorez un peu ce dossier. Vous ne risquez pas grand-chose en appliquant la commande « more » aux fichiers qu'il contient. De plus, les noms des sous-répertoires ainsi que des fichiers sont souvent très explicites. Si je vous demande que peut bien contenir le fichier /proc/version, je suis certain que vous avez une petite idée. Mais voyons à présent comment se présentent les différents périphériques de stockage sous Linux.

Le principe du montage

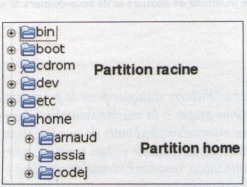
Pour qu'un périphérique de stockage, amovible ou non, soit visible et utilisable par votre système, il doit être monté. Généralement vous avez partitionné votre disque lors de l'installation. Dans ce cas, vous avez probablement trois partitions : une pour le système, une pour les répertoires personnels des utilisateurs et une d'échange pour la mémoire virtuelle. Et bien, chacune d'elle est montée au démarrage de Linux à un endroit bien précis. La partition système est obligatoirement montée à la racine « / », la partition contenant les répertoires des utilisateurs est montée en « /home ». Ce qui veut dire que le système vient « coller » l'arborescence de cette partition dans le répertoire « /home », celui-ci étant présent dans la partition du système, elle même montée en « / ».
Vous pouvez ainsi, d'une certaine façon, « emboîter » toute arborescence, donc toute partition, dans n'importe qu'elle répertoire d'une partition déjà montée. Souvent, la règle veut que l'on monte les supports amovibles dans « /media » et les montages temporaires d'autres types dans « /mnt ». Mais vous êtes entièrement libre. Personnellement, je monte mes mémoires USB dans les dossiers « /mnt/clef1 » et « /mnt/clef2 », que j'ai bien sûr pris soin de créer avant.
Ce mécanisme est très puissant. Surtout que les partitions montées peuvent être dans une multitude de systèmes de fichiers différents. Par exemple, si vous montez votre CDROM dans « /media/cdrom » le système de fichiers est probablement de l'iso9660. En revanche, si c'est une mémoire USB que vous montez dans « /media/usbdisk » le système de fichiers peut être en FAT32 (système issus de Windows).
Je vous parle depuis un moment de montage, mais je ne vous ai pas encore expliqué comment faire, et quelle commande il faut utiliser. Celle permettant le montage d'une partition est « mount » :

```
mount [-option] périphérique répertoire
```

Par exemple, lorsque vous insérez votre mémoire USB, le système détecte un nouveau périphérique, souvent « /dev/sdXX ». En effet, tous les périphériques sont dans le répertoire « /dev » comme devices. Si vous êtes sur une Ubuntu, le montage va se faire automatiquement. Sur d'autres distributions, il faut parfois le faire « à la main ». C'est à dire taper la commande :

```
mount /dev/sda1 /media/usbdisk -t vfat
```

Ceci est un exemple. Votre mémoire USB peut ne pas être en « /dev/sda1 ». Pour voir comment le système fait la détection sur votre ordinateur, vous pouvez comparer le contenu du pseudo-système de fichier « /proc/partition » avant et après insertion de votre mémoire USB.
Pour monter une mémoire amovible de la sorte, il faut être l'utilisateur Root. Or, bien souvent, et c'est même plus que conseillé, il vaut mieux monter les périphériques sous le compte utilisateur avec lequel vous travaillez. Pour cela, Root doit donner le droit à un utilisateur lambda de monter telle ou telle partition. De plus, certaines partitions doivent se monter automatiquement lors du démarrage du système. Pour configurer tout ceci,



la partition des utilisateurs est montée dans le répertoire home de la partition racine.

```
# /etc/fstab: static file system information.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
/dev/hda6       /               ext3    defaults,errors=remount-ro 0       1
/dev/hda8       /home           ext3    defaults        0       2
/dev/hda7       none            swap    sw              0       0
/dev/hdb        /media/cdrom0   iso9660 ro,user,noauto            0       0
/dev/sda1       /mnt/clef1      vfat    rw,user,noauto  0       0
/dev/sdb1       /mnt/clef2      vfat    rw,user,noauto  0       0
/dev/hda5       /mnt/donnees    vfat    rw,user,noauto  0       0
```

il existe un fichier spécial : « /etc/fstab ». Je vous livre un extrait du fichier que j'ai sur ma machine et nous allons le parcourir ensemble afin d'en comprendre sa signification.

Toutes les lignes qui commencent par un # sont des commentaires, comme toujours sous Linux. Chaque ligne représente un périphérique de stockage et précise comment il doit être monté. Les lignes sont décomposées en 4 colonnes principales et 2 autres un peu spéciales. La première indique où se trouve le périphérique, la seconde le répertoire où il faut le monter, la troisième le système de fichiers qui est utilisé, la quatrième des options de montage, la cinquième est un indicateur pour l'utilitaire de sauvegarde dump et la sixième un indicateur pour l'ordre de vérification du système de fichiers au démarrage.

Dans mon fichier, après les commentaires, la première ligne déclare le montage du pseudo-système de fichiers « proc ». La ligne suivante monte la partition « /dev/hda6 » comme racine du système. Le type de fichier est de l'ext3. L'option « defaults » est utilisée pour indiquer qu'il faut monter la partition avec les options par défaut du système. Les options sont séparées par des « , ». Nous voyons ici une deuxième option : errors=remount-ro.

Cela veut dire que s'il y a eu une erreur lors du montage, on

```
# sampl . /etc/exports file
/               master(rw) trusty(rw,no_root_squash)
/projects       proj*.local.domain(rw)
/usr            *.local.domain(ro) @trusted(rw)
/home/joe       pc001(rw,all_squash,anonuid=150,anongid=100)
/pub            (ro,insecure,all_squash)
```

refait une tentative en lecture seule. La troisième ligne indique le montage de la partition « /dev/hda8 » dans le répertoire « /home ». Ensuite vient le montage de la partition d'échange qui présente une syntaxe un peu particulière et sur laquelle je ne m'étendrai pas. Les lignes suivantes présentent des options différentes. « ro » et « rw » stipulent si le montage doit se faire en lecture seule ou en lecture écriture. « user » indique au système qu'un utilisateur quelconque a le droit de monter cette partition. Enfin, « noauto » précise qu'il ne faut pas tenter de monter automatiquement la partition. Ceci est en effet préférable pour les supports amovibles, car ils sont rarement connectés au système lors de son démarrage.
Nous avons donc vu que le fichier fstab donnait des informations au système sur les unités de stockage qu'il faut monter au démarrage, mais aussi sur celles qui peuvent être montées par l'utilisateur. Ce fichier est donc systématiquement lu quand un utilisateur fait une tentative de montage. Si le périphérique que vous souhaitez monter correspond à une ligne dans dans le fichier fsatb, la commande s'en trouve simplifiée. Par exemple, pour exploiter ma clef USB, je tape la commande :

```
mount /mnt/clef1
```

Les options de montage sont lues dans le fichier fstab et la clef est montée si cela est possible. Si en revanche, la ligne n'existe pas dans le fichier, il faut tout préciser dans la commande et de plus, être l'utilisateur Root. Attention avec les supports amovibles, il doivent être démontés avant d'être retirés physiquement de l'ordinateur. La commande qui le permet est :

```
umount /dev/xxx
```

Nous venons de voir le système du montage des fichiers sous Linux. C'est la même technique qui est utilisée pour partager des fichiers entre plusieurs machines. Une fraction de l'arborescence d'un ordinateur peut être montée à un endroit de l'arborescence d'une autre machine. Encore faut-il en avoir le droit et savoir comment faire. C'est ce que nous allons voir.

Le montage NFS sous Linux

Imaginez que vous souhaitiez monter une partie de l'arborescence d'un ordinateur A dans l'arborescence d'un ordinateur B. La première chose à faire est d'indiquer à l'ordinateur A la branche qu'il est autorisé à partager. Pour ce faire, vous devez installer un service sur cette machine. Le serveur NFS. Cela se fait très facilement si vous êtes sur Ubuntu ou Debian mais ce n'est pas beaucoup plus compliqué sur d'autres distributions. Un petit « apt-get install » et le tour est joué. Mais avant tout, soyons curieux et faisons une petite recherche sur les paquets qui concernent nfs :

```
root@ubuntu:~# apt-cache search nfs
```

Dans la liste importante qui s'affiche à l'écran, seuls deux paquets vont nous intéresser. Le premier est le support nfs pour le système. Installons le :

```
root@ubuntu:~# apt-get install nfs-common
```

Le deuxième va permettre à la machine de devenir serveur NFS. Installons-le aussi :

```
root@ubuntu:~# apt-get install nfs-kernel-server
```

Voilà tout est prêt pour le partage. Il faut indiquer maintenant quelle est la partie de votre arborescence que vous souhaitez partager et quelles machines seront autorisées à accéder à ce partage. Cette configuration se fait dans le fichier « /etc/exports ». Il faut évidemment être l'utilisateur Root pour pouvoir écrire dans celui-ci. Il est relativement simple à écrire. Chaque ligne indique un partage. Le premier élément de la ligne indique le répertoire partagé tandis que le second précise les droits.
Nous avons dit un peu plus haut que nous souhaitions partager une partie de l'arborescence de l'ordinateur A sur l'ordinateur B. Supposons que le répertoire partagé soit le « /home » des utilisateurs de la machine A. Voici les lignes qui devront apparaître dans le fichier « /etc/exports » de l'ordinateur A.

```
# /etc/exports: the access control list for filesystems which may be
exported
#                       to NFS clients.  See exports(5).
/home     192.168.1.3(rw)
```

Classiquement, les # représentent des commentaires. La ligne qui suit ceux-ci précise que nous partageons le répertoire « /home » uniquement pour la machine dont l'IP est 192.168.1.3 et que l'accès peut se faire en lecture comme en écriture. Voilà, vous voyez que c'est assez simple. La déclaration des machines autorisée à accéder au partage peut se faire d'une multitude de façons. De plus, bon nombre d'options peuvent être précisées sur la ligne du partage. Voici quelques exemples issus du manuel Linux :
La première ligne indique que l'on partage tout le système de fichier pour la machine « master » en lecture/écriture ainsi que la machine « trusty ». L'option no_root_squash précise que l'utilisateur Root sur l'ordinateur client aura aussi les droits Root sur l'ordinateur serveur. La ligne suivante précise que le répertoire /projects est accessible en lecture/écriture pour tou-

tes les machines dont le nom commence par « prof » et qui font partie du domaine « local.domaine ». Je ne vais pas aller plus loin pour le moment, car les autres options sont un peu plus complexes et ne nous sont pas d'une grande utilité pour le moment.
Voyons à présent comment faire pour monter le répertoire sur la machine client, donc notre ordinateur B. Voici la ligne qui doit apparaître dans le fstab de cette machine :

```
#montage nfs
pcB:/home  /home/pcB  nfs
rsize=8192,wsize=8192,timeo=14,intr
```

Ici nous n'avons pas indiqué l'IP de l'ordinateur B, mais son nom. Ceci n'est possible que si vous disposez d'un système capable de faire la résolution des noms (soit avec un DNS, soit en indiquant explicitement la relation entre le nom et les IP des machines dans le fichier « /etc/hosts » de vos ordinateurs). Nous aurions pu aussi utiliser dans ce cas, le nom de l'ordinateur dans le fichier « exports ». Vous constatez que le montage se fait dans le dossier « /home/pcB » de l'ordinateur client et que l'on précise que le système de fichiers est nfs. Les options qui suivent sont conseillées dans le man Linux et semblent être un bon compromis. Elle précise la taille des blocs de lecture et d'écriture et d'autres petites choses que je vous laisse découvrir dans le man Linux pour ne pas trop alourdir cet article. En effet, il nous reste à traiter le problème lié aux propriétaires des fichiers.

Et les droits des utilisateurs ?

Quand vous vous identifiez sur une machine Linux, vous avez un nom d'utilisateur et vous faites partie d'un groupe. Le groupe porte généralement le même nom que celui de l'utilisateur, mais ce n'est pas une obligation, et rarement le cas dans des grosses structures. Le système vous attribue donc un UID et un GID correspondant respectivement à votre identifiant utilisateur et groupe pour Linux. Ce sont toujours les mêmes, pour un utilisateur donné sur une machine donnée, et vous pouvez les connaître en tapant la commande « id » ou en consultant le contenu des fichiers « /etc/passwd » et « /etx/group ». Quand un utilisateur crée un fichier sur le système, il possède son UID et son GID pour que le système puisse déterminer qui a les droits sur celui-ci. Vous pouvez lister les fichiers d'un dossier en visualisant l'ID de l'utilisateur et du groupe auquel il appartient avec la commande « ls -n ».

Dans un montage NFS tel que nous l'avons fait, les fichiers de la machine serveur gardent leurs UID et GID sur la machine cliente. Il faut donc que les identifiants utilisateur et groupe de la machine client soient les mêmes que ceux de la machine serveur si vous souhaitez que tout le monde retrouve ses fichiers. Il existe une alternative qui consiste à attribuer un UID et GID d'utilisateur anonyme à la machine qui se connecte et non l'UID et le GID de l'utilisateur qui tente de faire l'opération. Par exemple, considérons la ligne suivante :

```
/home/joe
pc001(rw,all_squash,anonuid=150,anongid=100)
```

Dans ce cas, le montage nfs ne peut se faire que sur la machine pc001 et, de plus, quel que soit l'utilisateur accédant à ce partage, il sera considéré comme portant l'UID 150 et le GID 100 sur la machine serveur. C'est l'option « all_squash » qui le permet. Il me semble à présent que vous avez toutes les cartes en mains pour faire vos partages. Si vous voulez des renseignements complémentaires, je vous conseille ces quelques sites et surtout de lire le man Linux.

Conclusion

J'espère avoir pu vous donner des solutions pour le partage de fichiers sous Linux en utilisant NFS. Ce n'est pas toujours simple de bien comprendre le mécanisme au premier abord, car il change beaucoup par rapport aux partages sous Windows. Néanmoins, vous constaterez que ce n'est qu'une question d'habitude. De plus, il n'existe pas que cette solution pour partager des fichiers avec Linux et nous aurons l'occasion d'en voir d'autres dans les prochains magazines. Alors bon partage...

les Si des initiés

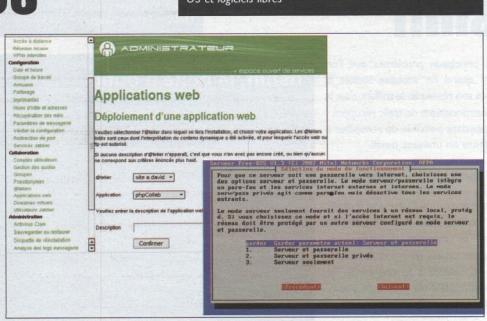
Hacking Linux

FreeEOS

URL : http://free-eos.org/
OS et logiciels libres

FreeEOS est une solution basée sous Gnu/Linux qui va vous permettre d'héberger facilement et rapidement les services internet dont vous aurez besoin.

L'installation est des plus enfantines. Une fois installé, FreeEOS vous permettra de partager votre connexion Internet entre plusieurs machines, de les protéger grâce à son firewall automatisé, d'héberger vos sites, emails et messagerie instantanée ou gérer un domaine, que ce soit pour des stations sous GNU/Linux, MacOS ou Windows.



Vous pourrez également profiter de nombreuses applications dynamiques (comme des forums, galeries de photos, gestion d'association, CMS et bien d'autres), partager des imprimantes et bien plus encore... Toute l'administration peut s'effectuer simplement via une interface web accessible directement depuis votre poste de travail.

Bref, FreeEOS est la solution à tous les administrateurs débutant comme confirmés n'ayant pas le temps (ou la motivation ;>) de s'adonner à la configuration manuelle de leur serveur !

Proxychains

OS : Linux
URL : http://proxylabs.netwu.com/proxychains

Qui a dit que les proxys ne servaient qu'aux navigateurs Web ? Le gros reproche que l'on peut faire à tous les outils d'anonymats actuel semble être leur manque de fonctionnalités et la difficulté de leur mise en place. Une solution excellente est Proxychains.
Proxychains est un programme au concepteur novateur qui s'utilise de façon totalement transparente. Pour ce faire, il va intercepter les appels aux fonctions utilisant les sockets (grâce au Preload de librairies) et intercaler lors de vos connexions un ou plusieurs proxys de votre choix. Les types de proxys supportés sont : http (connect), socks4 et socks5.
Etant donné qu'il intercepte toutes les fonctions de types sockets, aucune configuration des logiciels utilisés n'est nécessaire et ceux-ci sont tous compatibles. Ainsi, au lieu de taper :

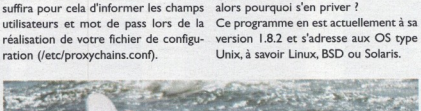
```
ssh monordi.com
```

vous taperez :

```
proxychains ssh monordi.com
```

et vous serez connecté au travers d'un ou plusieurs proxies à votre destination. Le gros point fort de ce programme est que sa configuration est relativement simple, puisqu'il vous suffit d'entrer une série de proxys valides dans votre fichier de configuration et de spécifier le mode de chaînage parmi les 3 suivants : Random, Strict ou Dynamic. L'authentification sur les proxys est elle aussi gérée, et il vous suffira pour cela d'informer les champs utilisateurs et mot de pass lors de la réalisation de votre fichier de configuration (/etc/proxychains.conf).

Le nombre de proxies à chaîner n'est pas limité, bien que le temps de latence augmente de façon proportionnelle au nombre de proxies utilisés. Vous pourrez utiliser ce logiciel en toutes circonstances : navigateurs internets, mails, ssh, ftp, telnet, etc… L'utilisation de proxies reste à ce jour la meilleure forme d'anonymat et de protection de la vie privée sur le Web et plus généralement sur Internet. Ce programme permet leur utilisation de façon vraiment simplifiée, alors pourquoi s'en priver ?
Ce programme en est actuellement à sa version 1.8.2 et s'adresse aux OS type Unix, à savoir Linux, BSD ou Solaris.



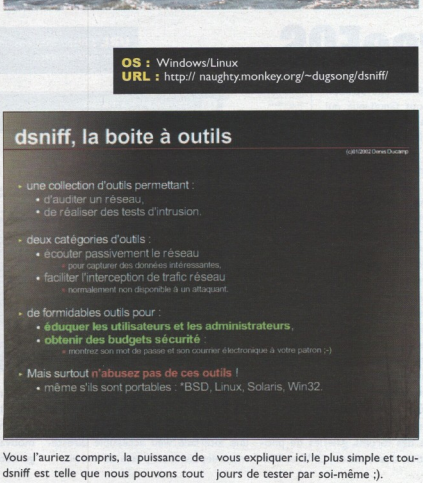
Dsniff

OS : Windows/Linux
URL : http:// naughty.monkey.org/~dugsong/dsniff/

L'un des principaux problèmes que l'on rencontre quand on souhaite auditer la sécurité de son réseau en le sniffant, c'est la quantité astronomique de trafic récupéré. Il est cependant possible de remédier à ce problème en utilisant dsniff.

En effet, dsniff est un renifleur réseau de mot de passe uniquement.
Dsniff c'est aussi une collection d'outils pour le réseau : dsniff, le filesnarf, le mailsnarf, le msgnarf, l'urlsnarf et webspy permettent de surveiller passivement un réseau à la recherche de données intéressantes (mots de passe, emails, dossiers, etc.).

Mais attention, comme dit l'auteur, ce programme a été concu afin d'auditer son propre réseau et de démontrer la faiblesse des mots de passe circulant en « clair », c'est à dire voyageant de manière non cryptée sur le réseau.



Vous l'auriez compris, la puissance de dsniff est telle que nous pouvons tout vous expliquer ici, le plus simple et toujours de tester par soi-même ;).

Bmap

OS : Linux
URL : http://packetstormsecurity.org/linux/security/bmap-1.0.17.tar.gz

Vous connaissez sûrement l'art de la steganographie qui consiste à dissimuler un fichier dans un autre. L'intérêt de cette méthode est permettre de faire passer des informations confidentielles à l'intérieur même d'un fichier apparemment anodin.
Pour cela diverses méthodes sont utilisées, à commencer par la plus connue qui nécessite l'utilisation d'un éditeur hexadécimal afin d'ajouter par exemple à l'intérieur même d'une image un message secret.
Ensuite, il existe une autre méthode de dissimulation d'information qui consiste à cacher les informations confidentielles à l'intérieur du Slackspace. Le slackspace correspond à l'espace disque libre d'un fichier. En effet, grosso modo, le système alloue toujours un peu plus de place sur le disque dur aux fichiers qu'ils ne leurs faut véritablement (du au découpage par blocs.) Cette deuxième méthode est celle utilisée par Bmap.
Illustrons maintenant l'utilisation de celui-ci par un exemple.
Ici nous allons copier la ligne correspondant au super utilisateur root depuis le fichier /etc/shadow vers le slackspace d'exemple.gif :

```
/* Vérifions d'abord si quelqu'un a eu la même idée que nous, apparemment non, le slackspace est vide */
nitryx:~/bmap# bmap -checkslack exemple.gif
exemple.gif does not have slack

/* On regarde la taille du Slackspace. Ici on va pouvoir y mettre 2ko de données ! */
nitryx:~/bmap# bmap -slackbytes exemple.gif
2006

/* Copions la ligne correspondant au root de /etc/shadow dans le slackspace de notre image */
nitryx:~/bmap# cat /etc/shadow | grep root | bmap -putslack exemple.gif
stuffing block 206909
file size was: 18474
slack size: 2006
block size: 4096

/* L'opération a fonctionnée */
nitryx:~/bmap# bmap -check-slack exemple.gif
exemple.gif has slack

/* On regarde maintenant le contenu du slackspace de exemple.gif */
nitryx:~/bmap# bmap -slack exemple.gif
getting from block 206909
file size was: 18474
slack size: 2006
block size: 4096
root:$1$qBeNJPe8$gVUd.fwBNxln5pFXNhLdJ0:12877:0:99999:7:::
```

Burneye

OS : Linux
URL : http://www.packetstormsecurity.org/groups/teso/burneye-1.0.1-src.tar.bz2

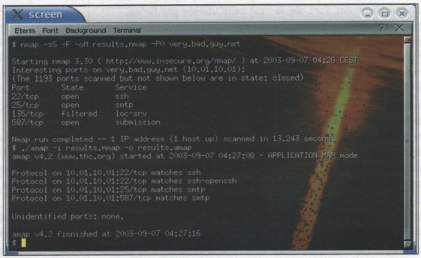
Garder ses binaires secrets n'est pas chose aisée. Cependant, afin d'assurer de la confidentialité d'un programme dont on ne souhaite dévoiler le fonctionnement, un outil formidable a été dévoilé par scut de la team Teso, il s'agit de burneye. En effet, burneye permet d'encrypter un exécutable au format ELF Linux sur machine Intel x86. Afin d'éviter les techniques dites de reversing, il offre plusieurs options telle que l'obfuscation rendant le code exécutable beaucoup plus difficile à débugger ou encore des options telles que la mise en place d'un mot de passe afin de crypter le binaire et d'empêcher son exécution sans la connaissance de celui-ci.
La version actuelle est la 1.0.1 et à ce jour, il n'existe aucun moyen de reverser un binaire encrypté par cette méthode si on a oublié le mot de passe, attention à ne pas vous brûler les yeux ...

```
Matrix:/tmp/burneye-1.0.1/src# ./burneye
burneye - TESO ELF Encryption Engine
version 1.0.1
------------------------------------------------------------------------------

usage: ./burneye [options] <program>

banner options
        -b file         display banner from 'file' before start
        -B file         display banner from 'file' on tty before start

password protect options
        -p pass         use password encryption with 'pass' as password
        -P env          first try to read password from environment 'env',
                        will use password from 'env' now, too, if its there
        -i              ignore invalid entered password and execute junk
                        not recommended (default: off)

fingerprinting options
        -S              SEAL mode (options F,f,t are ignored)
        -f file         use fingerprint from 'file' to protect binary
        -F              use fingerprint of current host (do not use -f and -F)
        -t num          tolerate 'num' deviations in fingerprint
        -q              be quiet about wrong fingerprint, just exit
```

AMAP

OS : Linux
URL : http://thc.org.segfault.net/thc-amap/

AMAP fait ce qu'on pourrait appeler du scanning intelligent : il se base sur les résultats de nmap (ou est capable de scanner directement les ports d'une machine) pour deviner les types d'applications qui se trouvent derrière les ports. Pour cela, il se connecte sur chacun des ports et cherche à obtenir une réponse de la part de l'application qui tourne derrière. Soit l'application lui envoie directement des informations correspondant à un protocole facilement reconnaissable (exemple : SSH ou POP3), soit il faut lui envoyer des séquences de paquets pour obtenir une réponse (par exemple pour le protocole HTTP). Grâce à cet outil, il est possible de savoir qu'un serveur FTP tourne sur le port 8765. Les administrateurs s'amusent rarement à modifier un numéro de port (surtout pour les services qu'ils ouvrent à Internet), mais



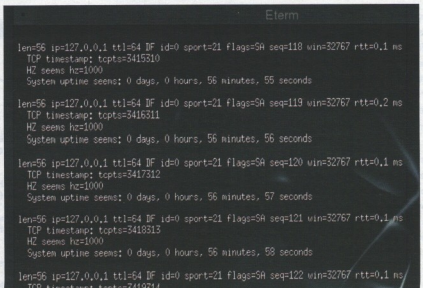
il arrive que l'on souhaite identifier le service tournant derrière un port élevé... AMAP fera cela très bien, très vite et très facilement !
Les protocoles supportés nécessitant un envoi sont : dns, ftp, http, jrmi, ldap, ms-ds, ms-remote-desktop-protocol, ms-sql, netbios-session, ntp, oracle-tns-listener, rpc, sap-r3, smtp, snmp-public, ssl et x-windows. En ajoutant les protocoles identifiables dès la connection, on obtient un total de 147 protocoles différents supportés !

Hping

OS : Unix
URL : http://www.hping.org

Peu d'entres nous n'ont jamais entendu parler de Hping et c'est bien normal. En effet, sa puissance fait toute sa popularité dans le monde de la sécurité des réseaux.
Hping est un outil de création et d'analyse de traffic TCP/IP.
Hping est un outil complet et peut par exemple servir à tester la sécurité de votre firewall, tester le fnctionnement de votre réseau, s'entrainer à l'OS fingerprinting, découvrir les techniques du man in the middle, de l'idle host scanning et j'en passe…

Hping gère plusieurs protocoles tels que TCP, UDP et ICMP.
Lors de l'utilisation de HPING est souvent intéressant de travailler avec un analyseur de trafic comme tcpdump ou ethereal. En effet lorsqu'on génére du traffic avec Hping il est impératif d'analyser les réactions du réseau ou du système cyble.



Les fonctionnalités offertes par HPING sont donc énormes et permettent ainsi de comprendre et maîtriser les possibilités et les lacunes de TCP/IP.

P0f

OS : *BSD, Linux, Windows
URL : http://lcamtuf.coredump.cx/p0f.shtml

D'abord, P0f est l'outil de fingerprinting passif le plus évolué à ce jour.
Le fingerprinting passif consiste à détecter le système d'exploitaiton de machines dialoguant sur le réseau en ne faisant qu'écouter le trafic. Ainsi, aucun paquet n'est envoyé vers les machines, ce qui rends cette méthode de fingerprinting redoutablement indétectable ! Bien entendu, pour qu'une machine puisse être analysée, il faut qu'elle émette des paquets sur le réseau, et le résultat d'un scan de réseau est à construire avec le temps (plusieurs journées de sniff permettent d'avoir une bonne vision des différents systèmes d'exploitation qui dialoguent sur le réseau).
De plus, le fonctionnement de cet outil est d'une simplicité déconcertante. Il s'installe et se lance très simplement.
Enfin, pour permettre de rendre P0f plus fiable encore, l'auteur nous invite à augmenter la base de fingerprint en visitant la page de son site située à l'url http://lcamtuf.coredump.cx/p0f-help/.

```
firewall:~/p0f# ./p0f -i eth0 -U -q -p
192.168.0.1:1399 - Windows 2000 SP4, XP SP1
  -> 216.239.57.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1400 - Windows 2000 SP4, XP SP1
  -> 66.102.9.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1401 - Windows 2000 SP4, XP SP1
  -> 66.102.9.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1402 - Windows 2000 SP4, XP SP1
  -> 216.166.85.97:80 (distance 0, link: ethernet/modem)
192.168.0.1:1403 - Windows 2000 SP4, XP SP1
  -> 216.166.85.97:80 (distance 0, link: ethernet/modem)
192.168.0.1:1403 - Windows 2000 SP4, XP SP1
  -> 216.166.85.97:80 (distance 0, link: ethernet/modem)
192.168.0.1:1404 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1405 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1406 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1407 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1408 - Windows 2000 SP4, XP SP1
  -> 207.68.178.16:80 (distance 0, link: ethernet/modem)
192.168.0.1:1409 - Windows 2000 SP4, XP SP1
```

Scapy

OS : Linux • Logiciel Libre
URL : http://www.secdev.org/projects/scapy/

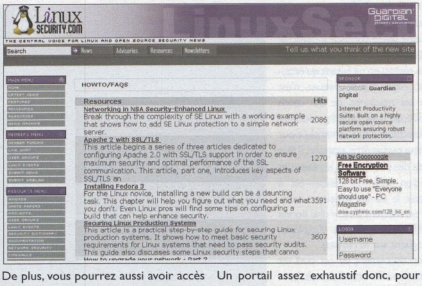
Il y a quelques jours sur le salon officiel de l'Net secret's une personne est venue en demandant quel était le meilleur langage de programmation pour débuter. Je lui ai proposé le Python qui est simple et complet pour débuter. On m'a alors interpellé en me disant que le C était le meilleur, le plus puissant et pas si complexe que ça. Pour prouver ma bonne foie, j'ai trouvé Scapy qui est un programme très intéressant en Python, et oui :-).
Scapy est un outil très performant de manipulation de paquet réseau. Il permet, selon l'auteur, de remplacer hping, nmap dans 85% des cas, arpspoof, arpsk, arping, tcpdump, ethereal et p0f. Scapy peut en effet générer et sniffer toutes sortes de paquets. L'avantage est qu'il permet de manipuler tout cela à un haut niveau d'abstraction, sous la forme d'objet Python sur lesquels on peut agir de manière interactive ou scriptée, assez simplement (voir la séance de sniff directement dans l'interpréteur en capture et les nombreuses démos du site). Packages disponibles pour RedHat et Debian.

```
Fichier  Edition  Affichage  Terminal  Onglets  Aide
>>> a=sniff(filter="tcp and ( port 25 or port 110 )",
 prn=lambda x: x.sprintf("%IP.src%:%TCP.sport% -> %IP.dst%:%TCP.dport
%  %2s,TCP.flags% : %TCP.payload%"))
192.168.8.10:47226 -> 213.228.0.14:110   S :
213.228.0.14:110 -> 192.168.8.10:47226  SA :
192.168.8.10:47226 -> 213.228.0.14:110   A :
213.228.0.14:110 -> 192.168.8.10:47226  PA : +OK <13103.1048117923@po
p2-1.free.fr>

192.168.8.10:47226 -> 213.228.0.14:110   A :
192.168.8.10:47226 -> 213.228.0.14:110  PA : USER toto

213.228.0.14:110 -> 192.168.8.10:47226   A :
213.228.0.14:110 -> 192.168.8.10:47226  PA : +OK

192.168.8.10:47226 -> 213.228.0.14:110   A :
192.168.8.10:47226 -> 213.228.0.14:110  PA : PASS tata

213.228.0.14:110 -> 192.168.8.10:47226  PA : -ERR authorization faile
```

Linuxsecurity

LANGUE : Anglais
URL : http://www.linuxsecurity.com

Quand notre pingouin se transforme en gardien efficace de votre vie privée, de votre réseau ou simplement de votre station de travail, alors c'est que vous êtes sur Linux Security. Même si notre système préféré offre par défaut une sécurité accrue pour ses utilisateurs, il convient de bien connaître sa machine et de configurer convenablement un certaine nombre de services pour que cet adage devienne pleinement une réalité. Je ne saurais trop vous conseiller de faire un tour sur ce site, qui contient l'une des meilleurs bases de données dans ce domaine pour les machines fonctionnant sous linux.



Sur celui-ci vous pourrez trouver les meilleurs tutoriaux et How-To à télécharger (en anglais) pour optimiser au mieux les performances de votre système.

De plus, vous pourrez aussi avoir accès à bon nombre de textes de référence ou de liens selon vos besoins : firewalls, IDS, sécurité réseau, serveurs, cryptographie et j'en passe.

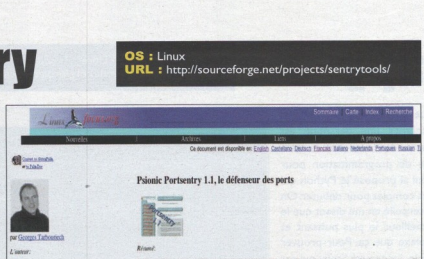
Un portail assez exhaustif donc, pour tout ce qui concerne la sécurité sous linux que tous les administrateurs et utilisateurs devraient connaître et avoir dans leurs bookmarks.

Portsentry

OS : Linux
URL : http://sourceforge.net/projects/sentrytools/

PortSentry est un programme qui fonctionne sous de multiples Unix. Il s'adapte aux comportements de chacun d'eux. Son unique objectif est de prévenir les tentatives d'intrusion sur un système.

Quand un pirate veut s'attaquer à une machine, il va souvent commencer par scanner les ports de sa cible à la recherche de services potentiellement vulnérables. C'est dans cette configuration qu'intervient PortSentry. Lorsqu'il détecte le scan, il bloque immédiatement toute communication de la machine équipée de PortSentry avec la machine attaquante. Pour y parvenir, il peut par exemple créer une règle de firewalling et ajouter une entrée dans /etc/hosts.deny. Tout cela, bien entendu, loggé dans /var/log/messages. Pour les plus paranos d'entre nous, il est également possible d'exécuter une commande lorsqu'un scan est détecté. Exemple: ifconfig -i eth0 down. ;)



PortSentry marque alors un point essentiel par rapport aux programmes passifs qui se contentent seulement de détecter les scans en cours.

Tripwire

OS : Linux
USL : http://sourceforge.net/projects/tripwire/

Ce logiciel open source est en priorité destiné au monde *nix et fera le bonheur de tous les administrateurs et root en tout genre.
Il est intéressant de noter qu'une version commerciale est également disponible pour les systèmes : Solaris, Windows NT, HP-UX et IBM AIX. Tripwire est un programme qui permet de vérifier en temps réel la modification des fichiers les plus importants sur votre système.
C'est donc un contrôleur d'intégrité, qui compare les propriétés des dossiers et des fichiers contre l'information stockée dans une base de données précédemment produite lors de l'installation. Tous les changements sont notés, y compris ceux qui ont été ajoutés ou supprimés, avec la possibilité d'être averti directement par mail. De plus, les dossiers contenant les informations (bases de données, rapports…) sont cryptés, ce qui permet d'en assurer la confidentialité. C'est un outil qui devrait être installé juste après la mise à jour de votre système pendant le processus d'installation de votre distribution afin de garantir que les fichiers marqués ne soient pas déjà corrompus..

Cmospwd

OS : Dos, Windows, Linux, FreeBSD, NetBSD
URL : http://www.cgsecurity.org

```
firewall1:~/cmospwd-4.6/src# ./cmospwd --help

CmosPwd - BIOS Cracker 4.6, February 2005, Copyright 1996-2005
GRENIER Christophe, grenier@cgsecurity.org
http://www.cgsecurity.org/

Usage: cmospwd [/k[de|fr]] [/d]
       cmospwd /k[de|fr]] [/d] /[r|w] cmos_backup_file              restore/loa
rite
       cmospwd /k                                                  kill cmos
       cmospwd [/k[de|fr]] /m[01]*       execute selected module

 /kfr french AZERTY keyboard, /kde german QWERTY keyboard
 /d to dump cmos
 /m0010011 to execute module 3,6 and 7

NB: For Award BIOS, passwords are differents than original, but work.
firewall1:~/cmospwd-4.6/src#
```

Le mot de passe du bios est souvent une des premières protections logicielles qu'un attaquant physique pourra avoir affaire.
La majorité d'entre nous savons qu'il suffit simplement d'enlever la pile de la mémoire du bios pour la réinitialiser et donc supprimer toutes protections au niveau du bios et donc de faire sauter le mot de passe.
Cependant il existe des méthodes plus subtiles qui consistent à réinitialiser ce mot de passe en interférant directement avec le bios.
Cmospwd est ici le logiciel qu'il nous faut car il permet en effet de cracker différentes marques de bios. Cmospwd permet de sauvegarder, restaurer et effacer la cmos. Ainsi il est possible de récupérer, restaurer et effacer le mot de passe du bios. La compatibilité du programme avec votre matériel n'est pas un problème, cmospwd est open source, et cela lui permet de bénéficier de nombreuses contributions afin de travailler sur de nombreux bios à partir de nombreux OS.
Cmospwd est donc une alternative intéressante à la, n'hésitez pas à lire le fichier README pour de plus amples informations sur ce soft !

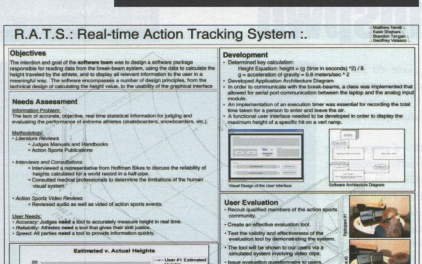
Admin-sys

LANGUE : Français
URL : http://www.admin-sys.com

« Site d'aide à l'administration, pour les administrateurs et toutes les personnes qui souhaitent en savoir plus sur leurs systèmes UNIX, LINUX. », tels sont les mots qui ouvrent le site et qui résument bien sa raison d'être.
Admin-sys.com vous offre l'opportunité de résoudre vos problèmes d'administration grâce à sa documentation complète. Vous pourrez donc apprendre, comprendre et maîtriser le fonctionnement de Linux ou de Solaris. Par exemple : les bases essentielles du système Unix, mettre en place un système RAID sous Solaris, faire des sauvegardes sous hpux, et même quelques notions de sécurité.
Ainsi, les débutants comme les initiés pourront être satisfaits de leur visite sur ce site car ils trouveront toujours quelques astuces pour les aider à surmonter leurs petites défaillances...
Admin-sys.com est le fruit d'un travail de passionné qui désir offrir au monde les ressources nécessaire à une administration efficace de son système et de son réseau.

RATS

OS : Linux, Windows
URL : http://www.securesoftware.com

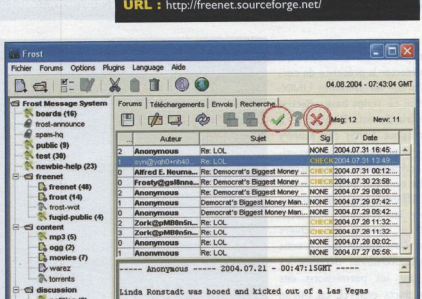


Quel programmeur n'a jamais rêvé d'un outil qui audite son code à la recherche de failles de sécurité ou de buffer overflow ? Et bien, avec RATS c'est aujourd'hui une réalité. Ce logiciel est développé et maintenu par les ingénieurs de sécurité de Secure Software. RATS est un outil qui permet de scanner son code C, C++, Perl, PHP ou Python à la recherche des erreurs de programmation qui pourraient poser des problèmes de sécurité. Il permet ainsi d'identifier rapidement les appels potentiellement dangereux des fonctions par exemple. Il exécute également une analyse de base pour essayer d'éliminer les conditions qui ne sont pas forcement des problèmes à l'origine mais peuvent le devenir dans une utilisation détournée du programme audité. De plus, le logiciel donne, si possible, les modifications à apporter pour régler le problème.
Bien évidemment, même si il permet de voir rapidement les problèmes rencontrés les plus fréquemment dans les codes sources, vous ne devriez pas exclure de faire ce travail vous-même et n'oubliez pas de le tester comme pourrait le faire un hacker.
Couplé à votre bon sens, RATS deviendra alors un outils indispensable.

Freenet

OS : Linux, Windows
URL : http://freenet.sourceforge.net/

Freenet est un réseau informatique anonyme et décentralisé, bâti au dessus d'Internet et conçu pour exercer une liberté d'expression totale et résistant à la censure. Sa nature permet donc à chacun de lire et de publier du contenu. Il offre la plupart des services actuels d'Internet (email, téléchargement, web, etc.). Le contenu de Freenet est extrêmement varié on y trouve vraiment n'importe quoi et surtout n'importe quoi. Étant le seul réseau vraiment anonyme à large échelle, on y trouvera donc des sites de hacking très underground ne respectant pas la loi en vigueur...
Néanmoins la liberté à un prix ! Les deux principaux défauts de Freenet sont son insupportable lenteur (chaque utilisateur héberge une partie du réseau) mais aussi le contenu parfois extrêmement trash que l'on peut y trouver. Néanmoins si l'utilisation reste réfléchie il n'y aura aucun problème : on ne trouve que ce que l'on cherche.



Le logiciel d'échange de fichiers Frost

Tcpdump

OS : Linux
URL : http://www.tcpdump.org

Tcpdump est la référence en matière de sniffer ! En effet, c'est le sniffer par excellence sous linux, c'est le plus abouti et le plus malléable.
Son utilisation est des plus simples, la prise en main est rapide et il vous suffira de lire le man (man tcpdump) pour connaître toutes les possibilité que vous offre ce soft.
Admirons alors quelques unes des possibilités offertes par TCPDump grâce à un exemple.
Dans le cas suivant, la passerelle (qui est donc la machine à partir de laquelle est exécuté TCPDump) filtre tout ce qui arrive de la machine 192.168.0.1 à destination d'un serveur FTP sur internet (port 21). Grâce à) l'option –X de TCPDump, nous pouvons avoir une visualisation du contenu des paquets en ASCII et en hexadécimal :

```
# tcpdump -X -s 0 src
192.168.0.1 and port 21

On obtient alors quelque chose du
style:

[..]
00:34:03.145837
192.168.0.1.2698 >
ftpperso.free.fr.ftp: P
44:56(12) ack 182 win 65205
(DF)
0x0000    4500 0034 31d3
4000 8006 0b30 c0a8 0001
E..41.@....0....
0x0010    d41b 28fc 0a8a
0015 dc77 67ee 7b1d 4ffe
..(.....wg.{.O.
0x0020    5018 feb5 e852
0000 4357 4420 6e69 7472
P....R..CWD.nitr
0x0030    7978 0d0a
yx..
[..]
```

On voit clairement que la commande FTP 'CWD nitryx' (la commande FTP 'CWD' correspond au 'cd' sur une machine unix.) a été lancée par 192.168.0.1 sur le serveur.

Bien entendu, cela ne reste qu'un exemple. Il y a en effet des utilisation bien plus intéressantes que celle-ci à faire de tcpdump. Par exemple, auditer votre réseau pour découvrir ce qui transite ou non en « clair » sur votre réseau (donc non-crytpé), vérifier l'efficacité de votre forgeur de paquets et j'en passe…

TCPDump est donc un outil que tout le monde devrait avoir sous la main afin de mieux comprendre, par exemple, le fonctionnement de son réseau.

Rootkithunter

OS : Unix
URL : http://www.rootkit.nl

RootKit Hunter est un logiciel libre qui permet de détecter la présence de certains rootkits sur les systèmes UNIX. Pour y arriver, ce script bash effectue une longue série de tests. D'abord, il y a un test d'intégrité (md5) des fichiers importants – notamment des binaires utilisés par le script même – en fonction d'une base de données de divers systèmes et leur différentes version (surtout pertinent sur les système propriétaires). Ensuite, il cherche des fichiers connus pour être utilisés par certains rootkits. Enfin, RkHunter détecte des anomalies dans les permissions des fichiers, des ports ouverts, ou même des LKM et KLD suspects. RootKit Hunter s'adapte à l'OS testé et effectue les tests les plus appropriés. Sur Linux par exemple, le programme compare le contenu de /proc avec la sortie de ps. Complémentaire à chkrootkit (www.chkrootkit.org), cet outil peut s'avérer très utile si vous craignez que votre système ait été compromis. Mais n'oubliez pas que ce genre de tests ne pourra que vous prouver que vous avez bien été piraté, mais certainement pas l'inverse.

```
   /usr/bin/du                                              [ OK ]
   /usr/bin/file                                            [ OK ]
   /usr/bin/find                                            [ OK ]
   /usr/bin/head                                            [ OK ]
   /usr/bin/kill                                            [ OK ]
   /usr/bin/login                                           [ OK ]
   /usr/bin/lsattr                                          [ OK ]
   /bin/netstat                                             [ BAD ]
   /bin/ps                                                  [ OK ]
   /bin/sh                                                  [ OK ]
   /bin/su                                                  [ OK ]
   /usr/bin/chattr                                          [ OK ]
   /usr/bin/wc                                              [ OK ]
   /usr/bin/wget                                            [ OK ]
   /usr/bin/whereis                                         [ OK ]
   /usr/bin/who                                             [ OK ]

[Press <ENTER> to continue]


Check rootkits
* Default files and directories
   Rootkit '55808 Trojan - Variant A'...                    [ OK ]
   Rootkit 'AjaKit'...                                      [ OK ]
   Rootkit 'aPa Kit'...                                     [ OK ]
```

John The Ripper

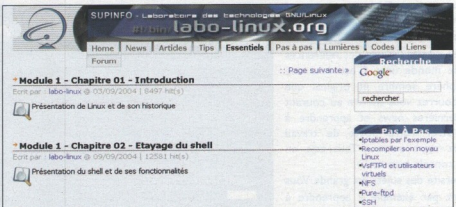
OS : *NIX, DOS, Win32, BeOS, OpenVMS
URL : www.openwall.com/john/

John the Ripper est le plus célèbre cracker de mots de passe. Il est développé par Solar Designer en licence GNU. Le plus rapide de sa catégorie, il permet d'auditer la sécurité de vos passwords et leurs résistances à une attaque par « brute force ». Conçu à l'origine pour les mots de passe Unix, la dernière version (1.6) supporte de nombreux type de hachage, ce qui en fait un outil complet pour tout type de plateforme : *NIX, DOS, Win32, BeOS et OpenVMS. S'il peut paraître un peu rebutant aux newbies par sa prise en main en ligne de commande, il suffit pourtant d'un peu d'entraînement et de lecture avec john --help pour découvrir toutes les possibilités de ce logiciel incontournable dans le monde de la sécurité informatique.

```
C:\WINDOWS\system32\cmd.exe
C:\unzipped\john-16w\john-16\run>john.exe

John the Ripper  Version 1.6  Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-single                 "single crack" mode
-wordfile:FILE -stdin   wordlist mode, read words from FILE or stdin
-rules                  enable rules for wordlist mode
-incremental[:MODE]     incremental mode [using section MODE]
-external:MODE          external mode or word filter
-stdout[:LENGTH]        no cracking, just write words to stdout
-restore[:FILE]         restore an interrupted session [from FILE]
-session:FILE           set session file name to FILE
-status[:FILE]          print status of a session [from FILE]
-makechars:FILE         make a charset, FILE will be overwritten
-show                   show cracked passwords
-test                   perform a benchmark
-users:[-]LOGIN|UID[,..] load this (these) user(s) only
-groups:[-]GID[,..]     load users of this (these) group(s) only
-shells:[-]SHELL[,..]   load users with this (these) shell(s) only
-salts:[-]COUNT         load salts with at least COUNT passwords only
-format:NAME            force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL          enable memory saving, at LEVEL 1..3

C:\unzipped\john-16w\john-16\run>
```

Labo Linux

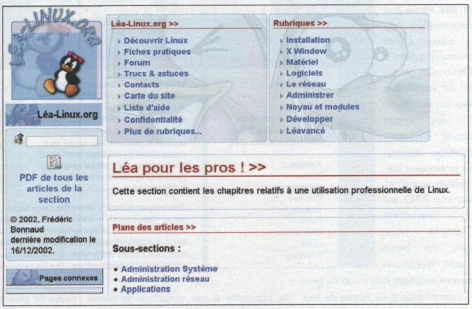
LANGUE : Français
URL : http://www.labo-linux.org



Le labo linux est l'un des labos de l'école d'informatique supinfo. Une fois arrivé sur la page d'accueil, on a déjà une vue d'ensemble du site. L'interface permet de se repérer facilement. Un système d'icônes différencie les types d'articles, de news ou de tips. On peut également trier les documents du site par type, date ou popularité. Les dernières news, les derniers articles comme les plus populaires ou même le dernier kernel disponible sont visibles en un coup d'oeil ! Ceci donne un ensemble convivial, simple et pratique. Par ailleurs, il faut noter que les concepteurs on fait des efforts pour toucher un large éventail d'utilisateurs. L'ensemble est classé selon les compétences de chacun pour permettre une compréhension aisée des articles. Ainsi les débutants pourront comprendre facilement les informations présentes sur le site. Nous soulignerons enfin que tous le labo linux est régulièrement en mouvement et la rubrique news est actualisée quotidiennement.

Linux Entre Amis (Léa)

LANGUE : Français
URL : http://www.lea-linux.org



Comme il se définit lui-même « le site d'aide Linux francophone », Linux Entre Amis (Léa) est une référence pour tous les utilisateurs francophones de Linux qui souhaitent obtenir une aide en ligne sur un problème précis. Ce site est l'un de mes préférés en la matière. Il possède une base de données d'articles qui s'enrichit continuellement pour vous offrir la solution à votre problème. Parmi les nombreuses rubriques qui composent ce site, vous pourrez trouver de nombreux conseils et astuces dans les domaines aussi variés que les réseaux, X-Window, l'administration de votre poste, le noyau et j'en passe. Vous pourrez également apprendre à vous servir de vieux minitel comme terminal ! Bref de quoi vous scotcher à votre écran et votre console un bon bout de temps. Mais Léa c'est aussi la possibilité de télécharger au format PDF l'ensemble des informations disponibles sur le site pour une consultation hors-ligne. C'est un geste très appréciable de la pars des concepteurs du site. A consulter sans modération !

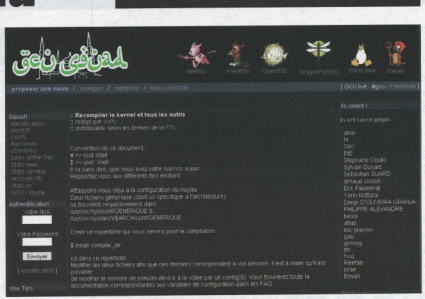
Gcu Squad

LANGUE : Français
URL : http://www.gcu-squad.org

Avis aux amateurs d'Unix en tous genres ! Nous n'aurions pu envisager une partie Unix sans parler du célèbre gcu-squad ! En effet, ce site est une des références dans le monde unix. C'est dans une atmosphère sombre et original que vous pourrez vous mettre au courant des dernières news et apprendre à administrer votre poste de travail comme votre serveur. Tout cela en mode console bien sur :).

La diversité des sujets est grande. Vous pourrez par exemple y apprendre à sécuriser votre Unix, recompiler votre kernel OpenBSD, crypter votre swap, monter un firewall sous linux ou BSD, accélérer le système de fichier de NetBSD (qui a tendance à être un peu lent à la base) et j'en passe …

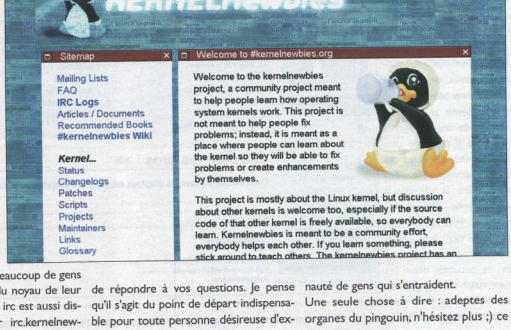
N'hésitez pas à faire un tour sur leur canal irc (irc.freenode.com #gcu), ça peut toujours aider !



Bref,gcu-squad a de quoi vous scotcher à votre écran pendant de longues et belles heures !

Kernelnewbies

LANGUE : Anglais
URL : http://www.kernelnewbies.org



Kernelnewbies est, comme son nom l'indique, un site dédié aux débutants voulant s'initier à cette chose extraordinaire qu'est le kernel linux. On peut y trouver de nombreux tutoriaux explicatifs, un glossaire très complet permettant d'obtenir une définition exhaustive des principaux éléments relatifs au kernel. De plus, une FAQ est mise à la disposition des usagés pour répondre de façon claire aux questions que peuvent se poser beaucoup de gens sur le fonctionnement du noyau de leur Linux adoré. Un channel irc est aussi disponible sur le serveur irc.kernelnewbies.org, salon #kernelnewbies, où tout un tas de passionnés se feront une joie de répondre à vos questions. Je pense qu'il s'agit du point de départ indispensable pour toute personne désireuse d'explorer le fonctionnement du kernel linux. Ce site est vraiment celui d'une communauté de gens qui s'entraident.

Une seule chose à dire : adeptes des organes du pingouin, n'hésitez plus ;) ce site est pour vous.

Offre spéciale d'abonnement

LINUXSCHOOL
Magazine

LE NOUVEAU MAGAZINE 100% LINUX

1 an

de pur linux (6numéros)

24 euros !!!

A découper ou à recopier et à envoyer accompagné de votre réglement de 24 euros à l'ordre de LPN à LINUXSCHOOL Magazine15 rue Chevreul - 94700 MAISONS-ALFORT

NOM : _____ PRENOM : _____

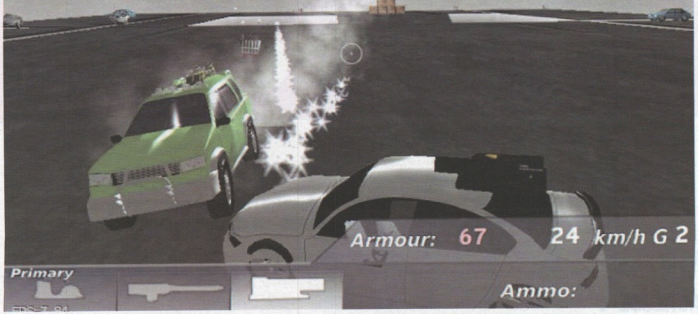
ADRESSE : _____

CODE POSTAL : _____ VILLE : _____

Ce mois-ci, le pingouin se défoule avec

Automanic

Oubliez la course ! Le but du jeu est de froisser la carrosserie de ses adversaires tout en gardant sa voiture en état de marche. Automanic fonctionne en mode "deathmatch". Quelques armes plus ou moins efficaces mais toujours amusantes sont disponibles sur les véhicules. Elles vous permettent de détruire un peu plus vite les armures des autres joueurs. Le reste est à découvrir sur : **http://automanic.sourceforge.net/download.html**



Chez votre marchand de journaux