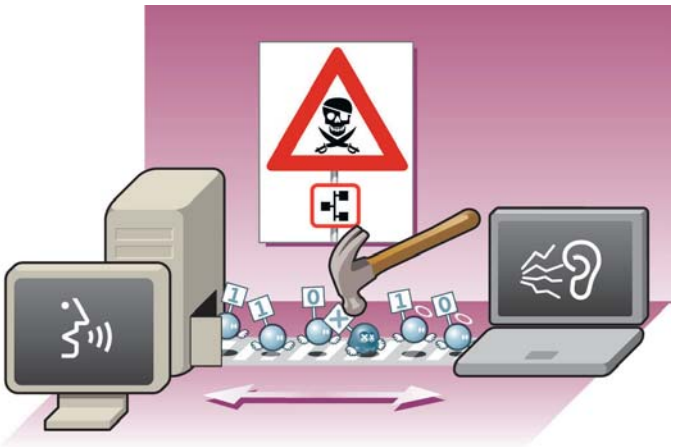
Smb Cifs

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Les pratiques de partage de ressources se sont amplifiées, corrélativement à la généralisation, notamment via Internet, de logiciels faciles d'utilisation (Samba,...) répondant à ce besoin. Cependant, la méthode la plus courante et la plus connue pour pénétrer une machine, notamment un ordinateur ou un serveur, correspond justement à l'exploitation de fonctionnalités de partage de ressources, souvent actives par défaut. Ce type de faille permet à un pirate informatique (Cracker) de prendre le contrôle d'une machine et d'en manipuler les données et les ressources.

Table des matières



1 Le protocole SMB/CIFS

Afin de partager des ressources sur un réseau, qu'il soit public ou privé, il est nécessaire d'utiliser un protocole de mise à disposition de ces ressources. Ce protocole de haut niveau sera transporté sur l'ensemble du réseau par les protocoles de transport/session habituels tels que TCP/IP, Netbios, IPX...

Le protocole SMB pour « Server Message Block » est utilisé pour le partage de fichiers, d'imprimantes, de ports série et les liens de communication type « canal nommé » (named pipes). Ce protocole a fait son apparition au milieu des années 80 et a initialement été mis au point par IBM. Ensuite, les sociétés Intel et Microsoft se sont chargées de son développement.

SMB est un protocole Client Serveur

Ce protocole est basé sur des dialogues « demande-réponse » entre un client SMB et un serveur SMB. C'est de cette manière que des serveurs mettent à disposition des ressources sur le réseau. Le client va donc se connecter au serveur « SMB », à l'aide d'un autre protocole, et obtenir ainsi les ressources accessibles, pouvant ensuite demander accès à ces ressources partagées (disques, périphériques,...etc).

CIFS « Common Internet File System »

CIFS est la nouvelle évolution du protocole « SMB », c'est ce nouveau protocole qui est utilisé par MS Windows 2000 pour permettre le partage de fichiers et périphériques sur des réseaux IP (Protocole Internet). CIFS est supporté sur la majorité des systèmes informatiques tels que Linux, Unix, Ms Windows NT, Ms Windows 98, MS Windows 95, MS OS2 Lan Manager,... Cette évolution est optimisée pour le partage de ressources sur Internet.

suite au verso

Smb Cifs

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

2 Quels sont les risques potentiels liés au partage de ressources ?

Le partage de ressources peut concerner les fichiers stockés sur la machine, mais également les périphériques tels que les imprimantes ou tout autre matériel connecté par les ports série, parallèle ou encore « USB » (Universal Serial Bus). Cet accès ne se limite pas nécessairement à la consultation ou à l'utilisation de ces ressources mais peut éventuellement permettre leur modification, ou leur effacement, voire leur mise hors d'état de fonctionnement.
Si le partage de ressources est évidemment le but premier de la mise en place d'un réseau local, la mise à disposition de ces mêmes ressources hors de ce réseau n'est certainement pas à conseiller.

Les conséquences peuvent être :

- **Consultation, vol ou destruction de données**
- **Destruction de fichiers systèmes informatiques**
- **Vol de UID/mot de passe (UID = User-ID = nom de l'utilisateur)**
- **Attaques de type denial of service**
- **Infection virale**
- **...**

3 Qui est concerné ?

Tous les citoyens, PME et administrations confondues, connectés à un réseau public ou privé mettant à disposition des données ou des ressources par une fonction de partage activée sur leur machine, de manière volontaire ou par défaut.

4 Suis-je exposé aux risques liés au partage de ressources ?

Les utilisateurs isolés n'ont généralement aucune raison d'autoriser le partage de ressources au contraire des utilisateurs qui sont habituellement connectés sur un réseau local. Toutefois il faut savoir que certains systèmes d'exploitation (OS) activent par défaut les capacités de partage de ressources. De fait, il appartient aux utilisateurs isolés de vérifier si leur configuration répond à cette exigence de sécurité.

Afin de savoir si une machine est exposée, y compris en tant qu'utilisateur isolé, il y a lieu de se rendre dans la fenêtre « configuration réseau » de la machine et de vérifier si la fonction « Partage de fichiers et d'imprimantes » est activée. Si c'est le cas, la machine est une cible potentielle pour les pirates informatiques (« Cracker »).

Pour valider votre configuration, vous pouvez également lancer le test se trouvant à l'adresse ci-dessous :
http://security.symantec.com/sscv6/

5 Comment se protéger ?

Si votre machine, notamment un ordinateur ou un serveur, est isolée

Dans le cas où votre machine n'est pas connecté en réseau local, la meilleure chose est de :

- **désactiver la fonctionnalité de « Partage de fichiers et d'imprimantes ».**

Vous trouverez, en annexe, les manipulations à réaliser selon le type de système d'exploitation (OS) dont votre machine est équipée.

Smb Cifs

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

Si votre machine est connectée en réseau local

Dans le cas où vous avez vraiment besoin de cette fonctionnalité, nous vous conseillons de mettre en place les recommandations suivantes :

- **Utilisez un équipement pare-feu** ou paramétrez des fonctionnalités pare-feu de Ms Windows XP afin de cantonner le protocole de partage de fichiers au sein de votre réseau local et d'en interdire toute propagation sur les réseaux publics. (Blocage des ports 445, 135, 137, 138, 139).
- **Créez un et un seul disque partagé** situé à la racine de votre disque dur et protégez son accès par un mot de passe sûr.
- **Supprimez le compte «Guest»** de votre système informatique et protégez tous les autres comptes utilisateurs mots de passe sûrs et un blocage du compte après un certain nombre de tentatives d'accès erronées ou frauduleuses.
- **Veillez à ce que la plate-forme antivirale soit toujours active** et à jour, afin d'éviter la propagation de virus.
- **Evitez de travailler avec des adresses IP** (protocole Internet) **fixes**, utilisez plutôt une distribution d'adresse IP (protocole Internet) dynamique.

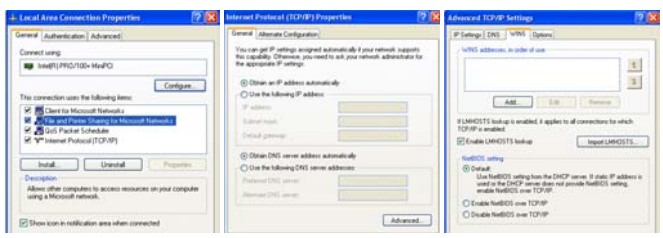
6 Annexes

6.1 Désactivation sous Ms Windows XP

- **Désactivez le protocole Netbios** dans les propriétés de la connexion distante utilisée.

Note : en tant qu'utilisateur isolé vous pouvez également désactiver le partage de fichier au niveau de votre fonction réseau local.

- **Utilisez les fonctionnalités "pare-feu"** de Ms Windows XP.



6.2 Désactivation sous Ms Windows 2000

- **Désactivez le protocole Netbios** dans les propriétés de la connexion distante utilisée.

Note : en tant qu'utilisateur isolé vous pouvez également désactiver le partage de fichiers au niveau de votre fonction réseau local.