Groupe de travail Réseau
Request for Comments : 2179
Catégorie : Information

A. Gwinn, Networld+Interop NOC Team
juillet 1997
Traduction Claude Brière de L'Isle

Sécurité du réseau pour les manifestations commerciales

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Le présent mémoire ne spécifie aucune forme de norme de l'Internet. Sa distribution n'est soumise à aucune restriction.

Résumé
Le présent document est conçu pour aider les fabricants et autres participants aux manifestations commerciales, comme Networld+Interop, à concevoir une protection efficace contre les attaques sur le réseau et les systèmes par des individus non autorisés. On a généralement observé que de nombreux administrateurs de système et coordinateurs de manifestations commerciales tendent à surestimer l'importance de la sécurité des systèmes dans les manifestations commerciales. En fait, les systèmes dans les manifestations commerciales sont au moins aussi enclins aux attaques que les plates-formes de bureau. Les systèmes des manifestations commerciales devraient être traités aussi sérieusement que les ordinateurs dans les bureaux. Une brèche dans la sécurité d'un système d'une manifestation commerciale peut rendre – et a rendu – les démonstrations d'un exposant non fonctionnelles – parfois pour toute la durée de l'événement !

Le présent document n'est pas destiné à remplacer la multitude des ouvrages très complets sur le sujet de la sécurité de l'Internet. Son objet est plutôt de fournir une collection sous la forme d'une liste de vérifications de façons simples, fréquemment négligées, de minimiser les chances d'une attaque coûteuse. On encourage les exposants à prêter une attention particulière à ce document et à le partager avec tous les représentants associés.

1. Sécurité physique

Avant de traiter les questions de sécurité techniques, une des failles le plus fréquemment sous estimée et répandue de la sécurité est la simple attaque non technologique. La victime courante est celui qui laisse une console en connexion, peut-être comme racine, et quitte le système. D'autres fois, une "bonne âme" anonyme peut demander un mot de passe pour aider l'usager à "identifier un problème". Ce type de méthode permet à un intrus, en particulier celui qui va être connecté comme "racine", d'accéder aux fichiers systèmes.

Conseils :
* Former le personnel de vente et de soutien aux connexions système, en particulier aux comptes "racines" ou autres comptes privilégiés.
* Identifier les individus qui utilisent les systèmes de démonstration à des fins différentes de celles prévues, en particulier , le personnel qui n'est pas du stand d'exposition.
* Demander l'identification de toute personne qui souhaite accéder aux systèmes pour des besoins de maintenance, sauf si leur identité est connue.

2. Sécurité système

Cette section discute des procédures de sécurité techniques pour les stations de travail sur le réseau de l'exposant. Bien que les spécificités tendent à être celles des systèmes Unix, les procédures générales s'appliquent à toutes les plates-formes.

Sécurité des mots de passe

L'absence de mot de passe ou des mots de passe faciles à deviner est une porte d'entrée relativement peu technique dans les systèmes,mais est responsable d'un nombre significatif d'intrusions. De bons mots de passe sont la pierre angulaire de la sécurité des systèmes.

Par défaut, les systèmes d'exploitation d'ordinateurs personnels (PC) comme Windows 95 et MacOS ne fournissent pas de sécurité adéquate du mot de passe. Le mot de passe de connexion Windows n'assure aucune sécurité (frapper la touche "Entrée" permet à l'usager de contourner l'entrée du mot de passe). La sécurité du mot de passe pour ces machines est possible, mais sort du domaine d'application du présent document.

Conseils :
* Vérifier dans /etc/passwd sur les systèmes Unix et dans l'application d'administration d'utilisateur sur les autres systèmes qu'il y a bien un mot de passe. Certains systèmes vendus tout prêts ont un mot de passe nul, dans certains cas même pour les comptes privilégiés.
* Changer les mots de passe, en particulier les mots de passe système et racine.
* Mêler les casses, les nombres et la ponctuation, en particulier sur les comptes privilégiés.
* Changer régulièrement les mots de passe système.
* Ne pas utiliser de mot de passe se rapportant à l'événement, à la société, ou aux produits exposés. Le personnel système à Networld+Interop, lorsque on lui demande d'aider le personnel des stands, devine souvent même les mots de passe racine !

Comptes ultra privilégiés

Certains fabricants de systèmes sont connus pour fournir des systèmes avec plusieurs comptes privilégiés (par exemple, les systèmes Unix avec des comptes qui ont les privilèges racine [UID=0]). Certains fabricants peuvent inclure un compte d'administration système séparé qui met un utilisateur dans un programme administratif spécifique. Chaque compte privilégié supplémentaire présente en fait une nouvelle opportunité de tromperie.

Généralement, si un système Unix n'a pas besoin de comptes racines supplémentaires, ceux-ci peuvent être désactivés en plaçant "*" dans le champ mot de passe de /etc/passwd, ou en utilisant l'outil administratif lorsque un système utilise la sécurité améliorée. Vérifier dans tous les systèmes les comptes avec des super privilèges et soit les désactiver, soit changer leur mot de passe en tant que de besoin.

S'assurer que les comptes privilégiés sont inaccessibles de partout sauf de la console système. Les systèmes s'appuient fréquemment sur des fichiers tels que /etc/securettys pour avoir une liste de terminaux "sûrs". En règle générale, sauf si un terminal est dans ce fichier, une connexion racine n'est pas possible. Une utilisation spécifique de ce dispositif devrait être couverte dans les fichiers de documentation du système.

Conseils :
* Vérifier /etc/passwd sur les systèmes Unix et l'application d'administration d'utilisateur sur les autres systèmes pour voir si il y a des comptes privilégiés supplémentaires.
* Désactiver la connexion à distance pour les comptes privilégiés.
* Désactiver tout compte privilégié qui n'est pas nécessaire.
* Limiter la connexion à partir des comptes racine aux terminaux "sûrs" ou à la console système.

Utilisation de jetons d'authentification

Les jetons d'authentification tels que SecureID, Cryptocard, DES Gold et autres, fournissent une méthode pour produire des mots de passe à "utilisation unique". Le principal avantage dans un environnement de manifestation commerciale est de rendre sans valeur les paquets capturés par des reniflages sur le réseau. On devrait considérer comme un fait qu'il y a de nombreux renifleurs de paquets et d'autres outils d'administration qui observent constamment (en toute légitimité) le réseau – en particulier lors d'une grande manifestation commerciale centrée sur les réseaux. Des mots de passe typés, par défaut, sont envoyés en clair à travers le réseau, permettant aux autres de les voir. Les jetons d'authentification fournissent un mot de passe qui n'est valide que pour une instance, et n'est plus utile ensuite. Une extension logique de l'utilisation des jetons d'authentification serait de les utiliser pour "l'accès à la maison" (du réseau de la manifestation au site de l'entreprise) pour minimiser les chances de problèmes de sécurité hors site.

Une solution de remplacement à ces jetons est le protocole de coquille sécurisée (SSH, *secure shell*) qui fournit une connexion chiffrée entre les clients et les serveurs. Cette connexion peut porter à la fois du trafic de connexion et une communication arbitraire d'accès à accès, et c'est un outil puissant pour sécuriser un réseau entre les stands et les communications de et vers les systèmes distants.

Conseils :
* Contacter les vendeurs de jetons/cartes d'authentification pour avoir des informations sur la façon de les intégrer dans des environnements spécifiques, ou sur des plateformes spécifiques.
* L'utilitaire du domaine public "cryptosu" (csu), lorsque utilisé avec une Cryptocard, fournit un remplacement pour la commande Unix "su", employant un style mise au défi/réponse d'authentification de l'accès racine.
* Explorer l'utilisation de clients et serveurs ssh.

FTP anonyme

Les comptes FTP anonymes peuvent facilement devenir un trou dans la sécurité. Désactiver ce service si il n'est pas spécifiquement nécessaire. Si FTP anonyme doit être utilisé, les conseils suivants peuvent aider à le sécuriser :
* Lorsque un usager se connecte comme "anonymous", il devrait être cantonné dans une arborescence de répertoire

spécifique. S'assurer que FTP prend correctement sa racine dans le répertoire approprié. Un "cd /" devrait mettre un usager anonyme au sommet de l'arborescence "public", et non au répertoire racine du système.
* Certains systèmes peuvent permettre que des liaisons symboliques (ou "raccourcis") emmènent un usager en dehors de l'arborescence permise. Vérifier tous les liens à l'intérieur de la hiérarchie FTP anonyme.
* S'assurer que le répertoire racine de FTP est "possédé" par quelqu'un d'autre que le compte 'ftp'. Normalement, il devrait être possédé par "root".
* Ne pas utiliser un répertoire entrant sur lequel on puisse écrire du monde entier, sauf si c'est absolument nécessaire. De nombreux sites utilisent cela comme moyen pour que les usagers transfèrent les fichiers sur le site. Cela peut, et l'est souvent, devenir un site d'archivage de logiciels volés (que la communauté des pirates appelle des "warez").
* Retirer les permissions de lecture des permissions du répertoire (chmod 733 sur les systèmes Unix) interdit à un usager anonyme la capacité de faire la liste du contenu d'un répertoire. Les fichiers peuvent être déposés comme d'habitude, mais ne sont restitués que si l'usager connaît le nom exact du fichier .

Partage de fichiers réseau

Les partages de fichiers en écriture sans aucune forme de sécurité sont une invitation à la destruction des informations et des démonstrations. Qu'on utilise NFS sur les systèmes Unix ou des facilités de partage de PC comme CIFS, AppleShare, ou NetWare, on devrait porter la plus grande attention à la sécurité des fichiers exportés. Se souvenir que ce sont vos concurrents qui partagent le même réseau que vous dans une manifestation commerciale ! La sécurité des accès aussi bien en lecture qu'en écriture devrait être assurée et chaque point d'accès examiné.

Exporter le système de fichiers NFS en écriture pour le monde entier accorde à tout le monde la capacité de lire et écrire tout fichier dans le point de montage exporté. Si on fait cela, par exemple, avec un répertoire système tel que "/" ou "/etc", c'est très simple d'éditer des fichiers de mots de passe pour se créer un accès personnel au système. Donc, /etc/exports devrait être examiné attentivement pour être certain que rien de nature sensible n'est exporté à quiconque sauf un autre hôte de confiance. Tout ce qui est exporté au grand public devrait l'être en "lecture seule", et les informations qui sont disponibles devraient être vérifiées via le partage de fichiers.

Conseils :
* Ne pas fournir d'espace de partage de fichier sauf nécessité.
* Vérifier où les informations exportées seront "visibles".
* Ne pas conserver de partages en écriture sauf absolue nécessité !

Hôtes de confiance

Les entrées d'hôtes de confiance sont une méthode pour permettre à d'autres hôtes d'une sécurité "équivalente" d'accéder à un autre ordinateur hôte. Certains fabricants offrent des systèmes avec des fichiers d'hôtes de confiance ouverts. S'assurer que cette question est traitée.

Conseils :
* Sur les systèmes Unix, vérifier l'entrée '+' (tous les systèmes sont de confiance) dans les fichiers /etc/hosts.equiv et ".rhosts" (il peut y avoir plusieurs fichiers .rhosts) et les retirer.
* Vérifier si il y a une entrée "xhost +" dans le fichier "...X11/xdm/Xsession". Le plus souvent, une entrée "xhost" va apparaître avec un nom de chemin tel que "/usr/local/lib/xhost +". La retirer.

SetUID et SetGID binaires (systèmes Unix)

Sur les systèmes Unix , le bit "suid" sur un programme système exécutable permet au programme de s'exécuter comme si il était le propriétaire. Un programme qui a le setUID réglé à "racine" va permettre au programme de s'exécuter avec les privilèges de racine. Il y a plusieurs raisons légitimes pour qu'un programme ait les privilèges de racine, et beaucoup les ont. Cependant, il peut être inhabituel d'avoir des programmes suid dans des répertoires d'utilisateur individuel ou d'autres endroits non systèmes. Un examen des systèmes de fichiers peut activer tout programme qui a son bit suid ou sgid établi. Avant de désactiver un programme, vérifier la légitimité des fichiers.

Conseils :
* "find / -user root -perm -4000 -print" va trouver toutes les occurrence d'un fichier setuid n'importe où dans le système, y compris ceux sur les partitions montées sur NFS.
* "find / -group kmem -perm -2000 -print" va faire la même chose pour les permissions de groupe kmem.

Propriété de l'annuaire système et permissions d'écriture

Vérifier la propriété de tous les répertoires système et les permissions nécessaires pour écrire ou modifier les fichiers. Il n'y a pas de façon simple de le faire sur les systèmes d'exploitation de PC comme Windows NT sans vérifier simplement tous les fichiers et répertoires ou en utilisant une version de "ls" qui va faire la liste des ACL.

Sur les systèmes Unix, un répertoire avec des permissions comme "drwxrwxrwx" (comme /tmp) est en écriture pour le monde entier et n'importe qui peut créer ou modifier les fichiers dans une telle zone. Porter une attention particulière à "/" et "/etc". Ils devraient être la propriété d'un compte système et non d'un utilisateur individuel. Si il y a un doute, contacter le fabricant du logiciel système pour avoir confirmation du répertoire approprié ou des permissions du fichier.

Services réseau

Tout serveur non indispensable devrait être désactivé. Les "R services" (rexec, rsh, et rlogin) bien connus sont particulièrement enclins aux problèmes de sécurité et devraient être désactivés sauf besoin spécifique. Porter une attention particulière aux fichiers d'hôtes de confiance, et soyez conscients du risque des attaques par usurpation d'identité IP de la part de machines qui "prétendent" être des hôtes de confiance.

Conseils :
* Sur les systèmes Unix, supprimer les "R services" (rexec, rsh, rlogin) dans /etc/inetd.conf.
* Chercher d'autres services inconnus ou inutiles.

Protocole trivial de transfert de fichiers (TFTP)

TFTP peut être un moyen d'accès facile dans les fichiers système pour un intrus. Il est en général de bonne pratique de désactiver TFTP. Si TFTP est nécessaire, vérifier que seuls les fichiers ciblés pour l'export sont accessibles. Une façon simple de vérifier la sécurité est de tenter d'exécuter TFTP sur des fichiers comme /etc/passwd ou /etc/motd pour vérifier l'accessibilité des fichiers système.

Surveillance des connexion TCP

Les logiciels du domaine public (TCP Wrappers ou "tcpd" pour les systèmes Unix) permettent de restreindre et de surveiller les connexions TCP sur chaque hôte. Les systèmes peuvent être configurés pour notifier à un administrateur et au journal système *(syslog)* quand une personne non autorisée tente d'accéder à l'hôte. Ce logiciel est accessible à :

* ftp://info.cert.org/pub/tools/tcp_wrappers/

BIND (Berkeley Internet Name Daemon)

Les versions antérieures de BIND ont été victimes de diverses attaques. Si un hôte doit agir comme DNS, utiliser la dernière version de BIND. Elle est disponible à :

* ftp://ftp.isc.org/isc/bind

Sécurité d'envoi de messagerie et de messageur

Un grand nombre de versions antérieures de Sendmail ont connu des failles de sécurité. Vérifier que le sendmail installé est bien de la version la plus récente. Autrement, consulter le fabricant du système d'exploitation pour obtenir la livraison la plus récente pour la plateforme.

Sécurité des écritures de serveur de la Toile

On devrait chercher dans les scripts et fichiers binaires de tous les serveurs de la Toile (en particulier dans les répertoires "...httpd/cgi-bin") ceux qui permettent d'exécuter des commandes coquilles *(shell commands)*. De nombreuses attaques de ces derniers mois se sont concentrées sur l'utilisation d'utilitaires tels que "phf" pour accéder à /etc/passwd sur un système cible. Retirer tout script qui n'est pas nécessaire dans le cours du fonctionnement d'un serveur de la Toile.

Autres suggestions

* Vérifier avec le fabricant du système d'exploitation les problèmes de sécurité connus. S'assurer que tous les systèmes ont la dernière version du logiciel – en particulier les pansements de sécurité pour guérir des problèmes spécifiques.

* Examiner fréquemment les fichiers de journaux d'événements sur l'hôte. Sur les systèmes Unix, la commande "last" va

fournir les informations sur les connexions récentes et sur leur origine. Les fichiers "syslogs" ou "Event Viewer" vont contenir des informations plus spécifiques sur les événements du système.

* Les journaux d'événements de serveur de la Toile (...httpd/log/access_log et ...httpd/log/error_log) vont contenir des informations sur ceux qui ont accédé à un serveur de la Toile mondiale, ce à quoi il a été fait accès, et ce qui a échoué.

* De bonnes sauvegardes sont la meilleure défense contre les dommages au système. Effectuer des sauvegardes avant de placer un système sur le réseau d'une manifestation commerciale puis continuer les sauvegardes pendant l'événement et à nouveau après la manifestation. Un ensemble de sauvegarde final est utile pour examiner de possibles tentatives (ou réussites) de pénétrations de la sécurité du système.

Sécurité du réseau général

Comme on peut s'y attendre dans des manifestations commerciales sur les réseaux (grandes ou petites) il y a de nombreuses entités qui utilisent des renifleurs de paquets. La plupart sont des exposants qui ont un besoin légitime de les utiliser dans le cours de leurs démonstrations de produits. Cependant, il faut être conscient qu'il y a beaucoup "d'oreilles qui écoutent" sur les segments de réseau – dont chacune peut "entendre" ou "voir" les informations lorsque elles croisent le réseau. Les sessions telnet sont particulièrement enclines à l'espionnage. Une bonne règle d'approximation est de supposer que "quand on entre son mot de passe, on est le seul à ne pas le voir !"

Il est de bonne pratique de ne pas se connecter (ou "su") à un compte avec privilèges à travers le réseau, pour autant que ce soit possible. Comme mentionné précédemment, les jetons d'authentification et ssh sont un moyen simple d'ajouter de la sécurité à l'accès à un compte système.

Filtrage de paquets

De nombreux routeurs prennent en charge le filtrage de base de paquet. Si un routeur peut être déployé entre le réseau local et le réseau de la manifestation, le filtrage général de base de paquet devrait être employé. Ci-dessous figure une bonne approche de filtre "général" de paquet. L'approche elle-même est ordonnée en catégories :
* refus/acceptation générale globale.
* refus spécifiques de service global.
* acceptation spécifique de service/hôte.
* refus final de tous les autres services TCP/UDP.

Sur la base de la théorie du refus de tout ce dont on ne sait pas si c'est du trafic acceptable, une bonne approche de réglage d'un filtre, dans l'ordre des priorités d'exécution, pourrait être :

refus/acceptation générale globale
1 Filtrer les adresses de source déguisées par interface. Confronter les adresses de source aux informations d'acheminement disponibles pour l'interface. Éliminer les paquets avec une adresse de source qui arrivent sur une interface (de "l'extérieur" par exemple) qui prétendent avoir une adresse de source sur une autre interface ("l'interne").
2 Filtrer tous les paquets à acheminement de source sauf si l'acheminement de source est spécifiquement nécessaire.
3 Permettre les connexions sortantes à partir des hôtes "internes".
4 Permettre les connexions TCP établies (le champ Protocole contient 6 et le champ Fanions TCP contient soit ACK soit NE contient PAS le bit SYN). Ne filtrer les demandes que pour les 'nouvelles' connexions.
5 Filtrer les 'nouvelles' connexions avec l'accès de source 25. Empêcher les gens de prétendre être un serveur de messagerie distant.
6 Filtrer l'adresse de bouclage (adresse de source 127.0.0.1). Arrêter les paquets provenant d'un résolveur DNS mal configuré.

refus spécifiques de service global
1 Bloquer spécifiquement tous les accès de "R-command" (accès de destination 512-515).
2 Bloquer telnet (accès de destination 23) à partir de tout hôte qui ne demande pas l'accès telnet depuis l'extérieur. (Si on utilise ssh, on peut le bloquer à partir de tous les hôtes !)
3 Ajouter des filtres spécifiques pour refuser tous les autres protocoles spécifiques au réseau, comme nécessaire.

acceptation spécifique de service/hôte
1 Ajouter des accès spécifiques aux services spécifiques d'hôtes "publics" (serveurs FTP ou de la Toile mondiale non sûrs).
2 Permettre SMTP (accès de source et de destination 25) pour la messagerie électronique aux serveurs de messagerie.
3 Permettre les connexions FTP entrantes (accès de source 20) aux serveurs FTP.
4 Permettre le DNS (accès de source et de destination 53, UDP & TCP) aux serveurs de noms. Si les transferts de zone ne sont pas nécessaires, bloquer l'accès à TCP.
5 Permettre les paquets RIP entrants (accès de source et de destination 520, UDP), si c'est approprié.

6 Ajouter des filtres spécifiques pour permettre d'autres protocoles spécifiques désirés ou pour ouvrir certains accès à des machines spécifiques.

refus final de service
1 Refuser tous les autres services UDP et TCP non permis par les filtres précédents.

Adresse de l'auteur

R. Allen Gwinn, Jr.
Associate Director, Computing
Business Information Center
Southern Methodist University
Dallas, TX 75275
téléphone : 214/768-3186
mél : allen@mail.cox.smu.edu ou allen@radio.net

Contributeur

Stephen S. Hultquist
Worldwide Solutions, Inc.
4450 Arapahoe Ave., Suite 100
Boulder, CO 80303
téléphone : +1.303.581.0800
mél : ssh@wwsi.com