tiger

Analyseur de sécurité UNIX

Tiger est un package consistant de scripts shell, code C, et de fichiers de données utilisées pour vérifier les problèmes de sécurité dans un système UNIX. Il scanne les fichiers de configuration système, les systèmes de fichiers, et les fichiers de configuration utilisateur pour de possible problèmes de sécurité et les affiche.

tiger peut être configuré en ajustant les variables Tiger_ dans le fichier de configuration tigerrc. Pour chaque module disponible, il y a une variable qui determine si le module est lancé.

OPTIONS

-B tigerdir Spécifie le répertoire où tiger est installé.

-l logdir|@logserver Spécifie le nom du répertoire où tiger écrit le rapport de sécurité, ou le nom d'un serveur de log tiger.

-w workdir Spécifie un répertoire à utiliser pour créer des fichiers scratchs.

-b bindir Spécifie le répertoire qui contient les binaires générés depuis les modules C.

-c tigerrc Spécifie l'emplacement du fichier tigerrc

-e Insert des explication dans les rapports de sécurité suivant chaque message.

-E Créé un rapport explicatif séparé

-G Génère les signatures (hashs MD5 et permissions de fichier) pour les fichiers binaires système

-H Formatte le rapport en html

-S Indisque qu'une vérification des fichiers de configuration des clients sans disque servis par cette machine devraient être vérifiés en même temps.

-q Supprime les messages pour être le plus silencieux possible

-A arch Spécifie l'architecture au lieu de laisser tiger l'obtenir

-O os Spécifie l'os au lieu de laisser tiger l'obtenir

-R release Spécifie la version de l'os au lieu de laisser tiger l'obtenir

Modules

Tiger est composé d'une série de modules. Chacun de ces modules vérifie les problèmes de sécurité liés aux systèmes UNIX. Les modules peuvent être exécutés seul, depuis cron ou via le programme tiger.

check_accounts Vérifie les comptes fournis dans le système, recherche les comptes désactivés avec cron, rhosts, .forward et les shells valides

check_aliases Effectue une vérification pour les alias mail et les configuration non-correct

check_anonftp Vérifie si le service FTP anonyme est configuré correctement

check_cron Valide les entrées cron dans le système

check_embedded Détermine si les chemins embarqués sont configurés correctement

check_exports Analyse les fichiers de configuration des exports NFS

check_group Vérifis les groupes UNIX disponible dans le système

check_inetd Vérifie le fichier de configuration inetd

check_known Recherche les signes d'intrusion connus, incluant les backdoors et les mail spools.

check_netrc Vérifie si le fichiers netrc des utilisateurs sont configurés correctement

check_nisplus Recherche les erreurs de configuration dans les entrées NIS+

check_path Valide les binaires dans le PATH de l'utilisateur, et les définitions PATH utilisés par les scripts pour déterminer les définitions non-sécurisé

check_perms Vérifie les permissions de fichiers et les inconsistances

check_printcap analyses la configuration pour le fichier de contrôle d'imprimante

check_rhosts Vérifie les fichiers rhosts pour vois si la configuration utilisateur laisse le système ouvers à des attaques

check_sendmail Vérifie les fichiers de configuration sendmail

check_signatures Compares les signatures des fichiers binaires avec ceux stockés dans la base locale (fournie avec le programme)

check_system Ce module appelle les modules spécifique de l'os dans /usr/lib/tiger/systems/

check_apache Vérifie la configuration Apache

check_devices Vérifie les permissions des périphérique

check_exrc Analyse les fichiers .exrc qui ne sont pas dans les répertoires home.

check_finddeleted Vérifie si les fichiers supprimés sont utilisé par un processus dans le système

check_ftpusers Analyse /etc/ftpusers et détermine si les admins sont dans ce fichier

check_issue Vérifie /etc/issue et /etc/issue.net pour déterminer s'ils contiennent le contenu approprié

check_logfiles Vérifie l'existence de fichiers de log (wtmp, btmp, lastlog, et utmp). Vérifie le umask

check_lilo Analyse les fichiers de configuration de lilo et grub

check_listeningprocs Vérifie les processus écoutant sur des sockets TCP/IP dans le système et les utilisateurs qui les lances

check_passwdformat Vérifie le format de /etc/passwd pour déterminer les inconsistances indiquant une intrusion ou une mauvaise configuration

check_patches Vérifie si les patchs sont disponibles pour le système. Utilise autorpm ou apt-get.

check_root Vérifie si le login root distant est autorisé

check_rootdir Vérifie les permission de /root

check_rootkit Tente de trouver les systèmes rootkités, en recherchant les commandes ls et find qui sont des trojans. inclus également un wrapper pour chkrootkit

check_single Vérifie si le système est configuré correctement et interdit l'accès single-user.

check_release Analyse la version de l'os et détermine s'il n'est plus à jours.

check_runprocs Vérifie si les processus configurés dans tigerrc sont lancés dans le système.

check_services Vérifie quils services sont configurés dans le système (généralement /etc/services) et ceux qui devraient être configurés

check_tcpd Test l'existance de tcp-wrappers et change la configuration et détermine quels services tournent sous tcp-wrappers

check_umask Vérifie le paramètre umask dans les fichiers de configuration

check_xinetd Vérifie si les services xinetd sont activés ou non

crack_run Lance une installation locale du programme Crack qui peut être utilisé pour déterminer si les mots de passe locaux sont trop simple

tripwire_run

aide_run

Integrit_run Wrappers pour des vérificateurs d'intégrité, ces programmes améliore le support de tiger pour les signatures binaires MD5 et SHA1 et les vérifications de permission de fichier.

deb_checkadvisories Vérifie une liste d'avertissement de sécurité pour voir si le système a des paquets installés dont la version peut être sujet à une vulnérabilité

deb_checkmd5sums Compare les MD5 des fichiers binaires avec ceux fournis après l'installation.

deb_nopackfiles Recherche les fichiers installés dans les répertoires système qui ne sont pas fournis par un package Debian