tigerrc

Fichier de configuration pour tiger

Ce fichier est pré-traité, et ne peut contenir que des assignements de variables et des commentaires

TigerNoBuild=Y Les fichiers C sont corrompus
Tiger_Check_PASSWD=Y Rapide
Tiger_Check_PASSWD_FORMAT=N Non nécessaire dans les systèmes avec pwck
Tiger_Check_PASSWD_SHADOW=Y le temps dépend du nombre d'utilisateurs
Tiger_Check_PASSWD_NIS=N idem
Tiger_Check_GROUP=Y rapide
Tiger_Check_ACCOUNTS=Y le temps dépend du nombre d'utilisateurs
Tiger_Check_RHOSTS=Y idem
Tiger_Check_NETRC=Y idem
Tiger_Check_ALIASES=Y rapide
Tiger_Check_CRON=Y rapide
Tiger_Check_ANONFTP=Y rapide
Tiger_Check_EXPORTS=Y rapide
Tiger_Check_INETD=Y rapide pour inetd, varie pour xinetd
Tiger_Check_SERVICES=Y assez rapide
Tiger_Check_KNOWN=Y rapide
Tiger_Check_PERMS=Y assez rapide
Tiger_Check_SIGNATURES=N plusieurs minutes
Tiger_Check_FILESYSTEM=Y Dépend de la taille du système de fichier. peut prendre des heures
Tiger_Check_ROOTDIR=Y Rapide
Tiger_Check_ROOT_ACCESS=Y Rapide
Tiger_Check_PATH=Y rapide pour root.
Tiger_Check_EMBEDDED=Y Plusieurs minutes
Tiger_Check_BACKUPS=Y Rapide
Tiger_Check_LOGFILES=Y Rapide
Tiger_Check_USERUMASK=Y Rapide
Tiger_Check_ETCISSUE=N Rapide, doit être personnalisé
Tiger_Check_STRICTNW=Y Rapide
Tiger_Check_LISTENING=Y Rapide
Tiger_Check_SYSTEM=Y Dépend des vérification du système
Tiger_Check_RUNPROC=N rapide, doit être personnalisé
Tiger_Check_DELETED=N Dépend du nombre de processus dans le système
Tiger_Check_APACHE=N Rapide
Tiger_Check_SSH=Y Rapide
Tiger_Check_SENDMAIL=N Rapide
Tiger_Check_PRINTCAP=Y Rapide
Tiger_Check_EXRC=N Dépend de la taille du système de fichier

Tiger_Check_ROOTKIT=Y Lent si chkrootkit est disponible

Tiger_Check_FTPUSERS=Y Rapide

Tiger_Check_OMNIBACK=N Rapide

Tiger_Check_NTP=Y Rapide

Tiger_Check_PATCH=N dépend de la connexion réseaux

Tiger_Check_SINGLE=Y Rapide

Tiger_Check_BOOT=Y Rapide

Tiger_Check_INITTAB=Y Rapide

Tiger_Check_RCUMASK=Y Rapide

Tiger_Check_NEVERLOG=Y Rapide

Tiger_Check_OS=Y Rapide

Tiger_Check_NETWORKCONFIG=Y Rapide

Tiger_Cron_SendOKReports=N Indique si les rapports sans informations sont envoyés à cron

TigerCron_Log_Keep_Max=10 Nombre de rapports à conserver pour chaque vérification lancé depuis crontab

Tiger_Cron_Template=N Indique si les rapports sont comparés avec un template, si disponible

Tiger_Cron_CheckPrev=Y Indique si les rapports sont comparés avec un précédent rapport, si disponible

Tiger_Show_INFO_Msgs=N Indique si les massages taggés INFO sont affichés

Tiger_Run_CRACK=N lance Crack

Tiger_CRACK_LOC_OVERRIDE=/mnt/cdrom/crack/Crack Emplacement du binaire Crack

Tiger_CRACKREPORTER_LOC_OVERRIDE=/mnt/cdrom/crack/Reporter

Tiger_CRACKDIR_LOC_OVERRIDE=/usr/local/crack Doit être accessible en écriture

Tiger_Output_FQDN=Y Indique si les fqdn sont utilisés

Tiger_Run_TRIPW=N Lance le vérification d'intégrité Tripwire

Tiger_TRIPW_LOC_OVERRIDE=/mnt/cdrom/tripw/tripwire Emplacement du binaire tripwire

Tiger_Run_AIDE=N Lance le vérification d'intégrité de fichier AIDE

Tiger_Run_AIDE_VERBOSE=1 Rapport verbeux (pas encore implémenté)

Tiger_AIDE_LOC_OVERRIDE=/mnt/cdrom/aide/aide.bin Emplacement du binaire aide

Tiger_AIDE_CFG_OVERRIDE=/mnt/cdrom/aide/aide.conf Emplacement de la configuration de aide

Tiger_AIDE_DB_OVERRIDE=/mnt/cdrom/aide/in.db Emplacement de la base de données de aide

Tiger_Run_INTEGRIT=N Lance le vérificateur d'intégrité de fichier Integrit

Tiger_INTEGRIT_CFG=/etc/integrit/integrit.conf Emplacement de la configuration d'integrit

Tiger_INTEGRIT_LOC_OVERRIDE=/mnt/cdrom/integrit/integrit.bin Emplacement du binaire integrit

Tiger_Output_Width=79 Pour le formattage de la sortie

Tiger_CRON_Output_Width=0 Largeur de la sortie quand utilisé via tigercron

Tiger_Global_PATH="/etc/profile /etc/csh.login" PATH global

Tiger_Passwd_Constraints="PASS_MIN_DAYS PASS_MAX_DAYS PASS_WARN_AGE PASS_MIN_LEN" Vérifications opérées sur les mots de passe

Tiger_Passwd_Hashes='crypt3|md5|sha512' Type de hash de mot de passe acceptés

Tiger_Dormant_Limit=60 Nombre de jours des fichiers non-modifiés dans le répertoire home avant d'être considéré comme dormants

Tiger_Admin_Accounts='adm|bin|daemon|games|lp|mail|news|operator|sync|sys|uucp|man|proxy|majordom|postgres|www-data|oper Comptes autres que root considérés comme administratifs (non utilisés par des humains, et dont sans mot de passe)

Tiger_Embed_Max_Depth=3 Si un chemin embarqué réfère à un fichier exécutable, il est vérifié. cela continue récursivement jusqu'à ce qu'il n'y ait plus de nouveaux exécutables trouvé, ou une profondeur max atteinte.

Tiger_Embed_Check_Exec_Only=Y Ne recherche que les exécutables dans les chemins embarqués

Tiger_Embed_Check_SUID=Y Vérifie les exécutables setuid trouvés

Tiger_Embed_Report_Exec_Only=Y Ne reporte que les exécutables qui sont en écriture ou non possédés par root

Tiger_Embedded_OK_Owners='root|bin|uucp|sys|daemon' Qui est autorisé à posséder des fichiers système

Tiger_Embedded_OK_Group_Write='root|bin|uucp|sys|daemon' Quels groupes peuvent accéder en écriture aux fichiers systèmes

Tiger_Check_PATHALL=N Spécifie si le PATH de tous les utilisateurs doivent être vérifiés. Peut potentiellement être dangereux

Tiger_ROOT_PATH_OK_Owners='root|uucp|bin|news|sys|daemon|lp' Qui peut posséder les exécutables dans /root ?

Tiger_ROOT_PATH_OK_Group_Write='root|uucp|bin|sys|daemon' Quels groupes peuvent accéder en écriture dans /root

Tiger_PATH_OK_Owners=$Tiger_ROOT_PATH_OK_Owners Qui peut posséder quelque chose dans les PATH utilisateurs

eval Tiger_PATH_OK_Group_Write='$Tiger_ROOT_PATH_OK_Group_Write' Quels groupes peuvent avoir un accès en écriture sur les exécutables dans le PATH utilisateur (non-root)

Tiger_Collect_CRACK=Y Indique si tiger doit attendre que Crack se termine.

Tiger_Crack_Local=Y Lance Crack dans les sources de mot de passe locaux uniquement

Tiger_Mail_FROM="root@`uname -n`" Nom de l'émetteur pour l'envoie de la sortie de tigercron

Tiger_Mail_RCPT=root Destinataire de la sortie de tigercron

Tiger_Files_of_Note=".. [!.]*/.* */.* */.[!.]/.log/.FSP*" Liste de globs de nom de fichier à regarder dans le système de fichier

Tiger_FSScan_Setuid=N Vérifie les exécutables setuid

Tiger_FSScan_Setgid=N Vérifie les exécutables setgid

Tiger_FSScan_Devs=Y Vérifie les fichiers de périphérique

Tiger_FSScan_SymLinks=Y Vérifie les liens symboliques étranges

Tiger_FSScan_ofNote=Y Vérifie les noms de fichier étranges

Tiger_FSScan_WDIR=N Vérifie les répertoire accessible en écriture par tout le monde

Tiger_FSScan_Unowned=Y Vérifie les fichiers avec un propriétaire/groupe non-définis

Tiger_FSScan_WarnUnknown=Y Alerte sur les systèmes de fichier inconnus utilisés

Tiger_FSScan_Local=" Système de fichiers considérés comme local dans le système

Tiger_FSScan_NonLocal=" Systèmes de fichiers considérés comme non-local.

Tiger_FSScan_ReadOnly=N Spécifie si les systèmes de fichiers en lecture seul sont scannés

USERDOTFILES=".alias .kshrc .cshrc .profile .login .mailrc .exrc .emacs .forward .tcshrc .zshenv .zshrc .zlogin .zprofile .rcrc .bashrc Liste de fichiers cachés communéments trouvés dans les répertoires home qui sont vérifiés par check_accounts

RHOST_SITES='*.tamu.edu|jupiter' Site Rhost qui sont attendus dans .rhosts. Tout ce qui ne matche pas est reportés

Tiger_Accounts_Trust=999 Quels uid ne doivent pas générer d'alerte pour les shells valides

Tiger_SSH_Protocol='1|2' Version de SSH attendue

Tiger_SSH_RhostsAuthentication='no' variable sshd_config attendue

Tiger_SSH_PasswordAuthentication='no' variable sshd_config attendue

Tiger_Listening_Every=Y Indisque si une alerte est données pour les services qui écoutent sur toutes les interfaces

Tiger_Listening_ValidUsers='root' Indique quel utilisateur est autorisé à avoir des processus en écoute pour les connections entrantes

Tiger_Listening_ValidProcs=" Quels processus sont toujours considérés comme valides, sans regarder s'il écoutent les connections entrantes dans le système.

Tiger_Running_Procs='syslogd cron atd klogd' Quels processus doivent être vérifiés par tiger. Les processus de cette liste qui ne sont pas vu dans la table de processus génère un FAIL

Tiger_DPKG_Optimize=Y Indisque si les vérification DPKG sont optimisés

Tiger_CHKROOTKIT_ARGS="-q" Arguments utilisé pour chkrootkit.