Rapport d'audit

27 juillet 2015, 11:58:02 - UTC

Version de l'outil	5.6
Nombre de cibles scannés	4
Nombre de vulnérabilités identifiées	151

Sommaire

Introduction

L'outil d'audit DenyAll Vulnerability Manager Enterprise Edition permet d'identifier de potentielles failles de sécurité informatique et le risque qu'elles pourraient engendrer en cas d'exploitation par un attaquant malveillant.

La première partie du rapport offre une vision synthétique et managériale des vulnérabilités de sécurité découvertes. La seconde partie liste exhaustivement ces vulnérabilités en apportant une évaluation de leur risque potentiel et des indications pour vous guider dans leur compréhension et leur résolution. Enfin, vous trouverez en annexe l'ensemble des serveurs et services découverts ce qui vous permettra le cas échéant d'approfondir leur examen.

Méthodologie

Ce rapport ne peut prétendre à être exhaustif et ne se substitue donc en aucun cas à l'analyse qu'un expert en test d'intrusion mènerait. De plus, l'exactitude des informations qu'il contient doit être validée auprès de l'administrateur du système ciblé par l'audit, ce afin d'écarter toute erreur d'identification (faux positif) de l'outil.

Appréciation du risque

L'évaluation du risque inhérent à chaque vulnérabilité figurant dans ce rapport repose sur la méthodologie

- l'impact potentiel d'une attaque exploitant cette vulnérabilité, en termes de disponibilité de l'application, confidentialité et intégrité des informations,
- l'exploitabilité (c'est-à-dire la facilité d'exploitation) de la vulnérabilité, une vulnérabilité plus facile à exploiter augmentant le nombre d'attaquants potentiels et donc la probabilité d'occurrence d'une attaque.

Les notes CVSS (risque global, impact et exploitabilité) s'échelonnent entre 0 et 10.

Priorisation de traitement des vulnérabilités

La priorité de traitement suggérée pour chaque vulnérabilité a cinq niveaux : critique (risque égal à 10), majeur (risque compris entre 8 et 10), élevé (risque compris entre 7 et 8), moyen (risque compris entre 4 et 7) et faible (risque inférieur à 4).

Pour apprécier le risque réel de chaque vulnérabilité, il faut pondérer l'impact potentiel par la valeur de l'actif, c'est-à-dire l'importance opérationnelle d'une application ou la criticité de l'information pouvant être compromise ; et l'exploitabilité par l'exposition intrinsèque de l'entreprise - certaines activités type financières motivant plus d'attaques que d'autres.

Enfin, ces risques peuvent être couverts par des contrôles préventifs, dissuasifs ou palliatifs.

Rapport à la direction

Récapitulatif

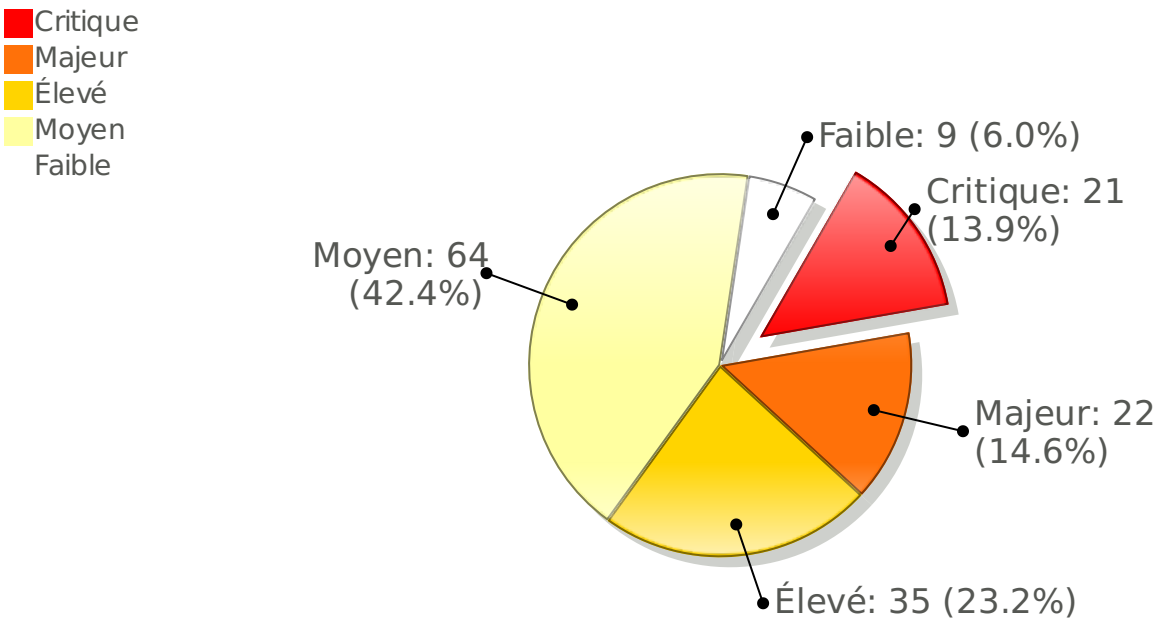
Parmi les 4 serveurs testés, 4 ont présenté des vulnérabilités dont **4 des vulnérabilité(s) de priorité critique**.

Ces vulnérabilités sont présentées graphiquement ci-dessous et détaillées dans la partie technique du rapport.

	Risques					
	Critique	Majeur	Élevé	Moyen	Faible	**TOTAL**
DBMS	8	6	7	12	1	34
Réseau	1	1	1	6	2	11
Unix	0	2	1	15	3	21
Web	2	3	8	30	3	46
Windows	10	10	18	1	0	39
TOTAL	21	22	35	64	9	151

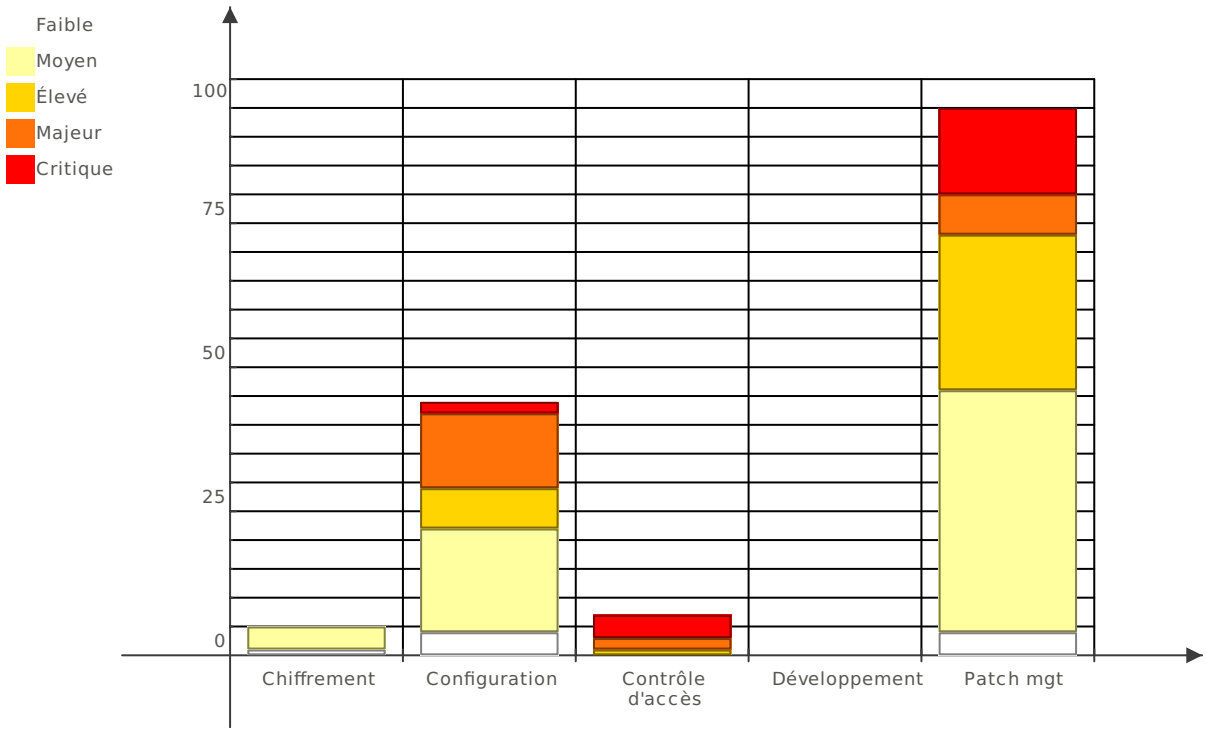
Vulnérabilités par priorité

Ce graphique présente le nombre de vulnérabilités identifiées, par priorité.

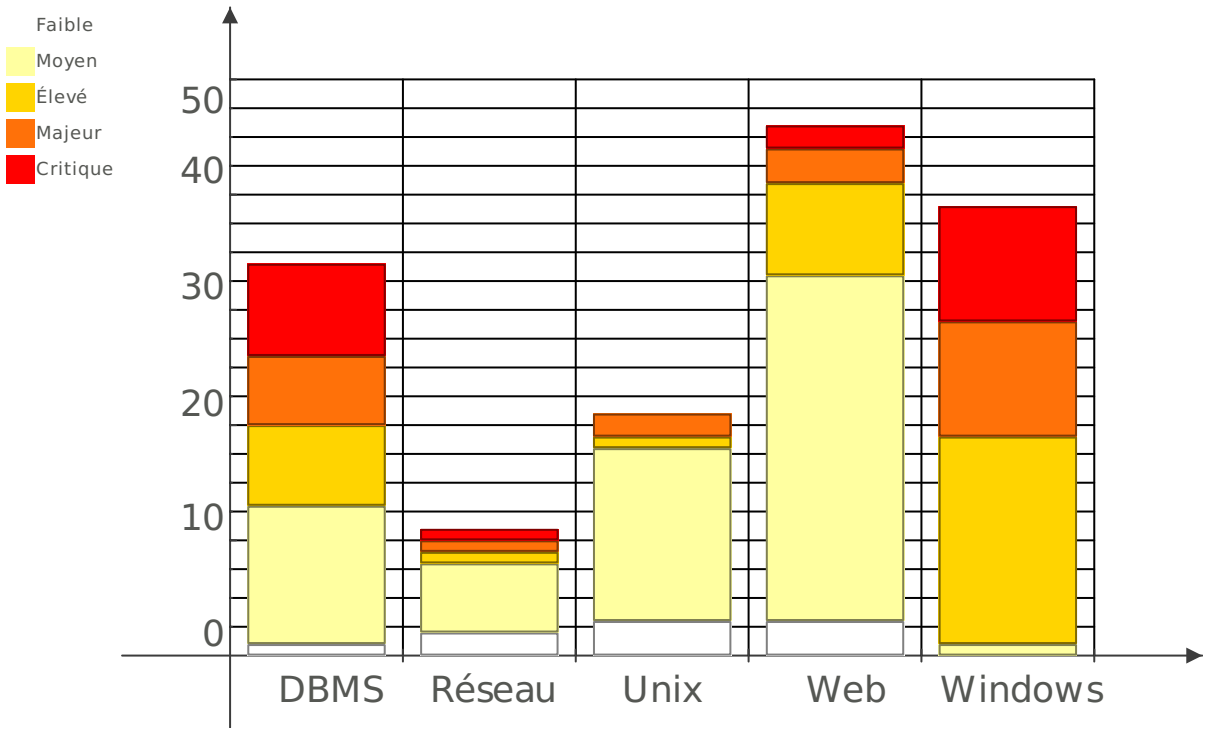


Vulnérabilités, par fonction et objet

Ce graphique présente le nombre de vulnérabilités classées par fonction de contrôle.

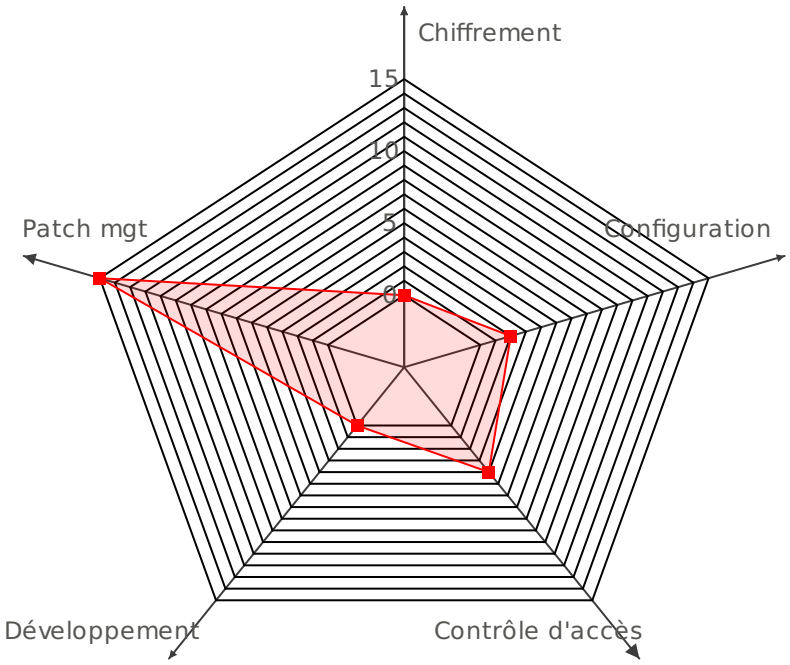


Ce graphique présente le nombre de vulnérabilités classées par objet de contrôle.

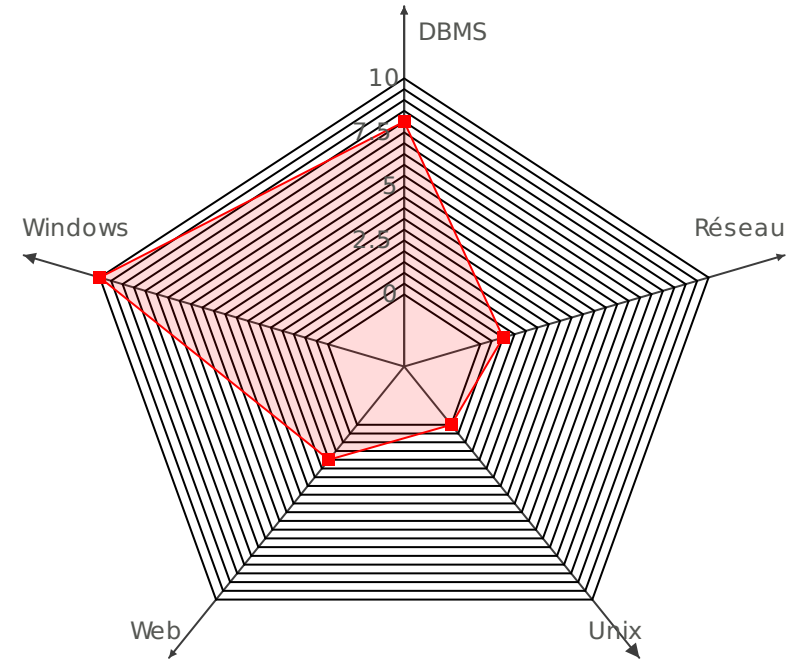


Vulnérabilités de priorité critique par type

Ce graphique présente le nombre de vulnérabilités de priorité critique classées par fonction de contrôle.

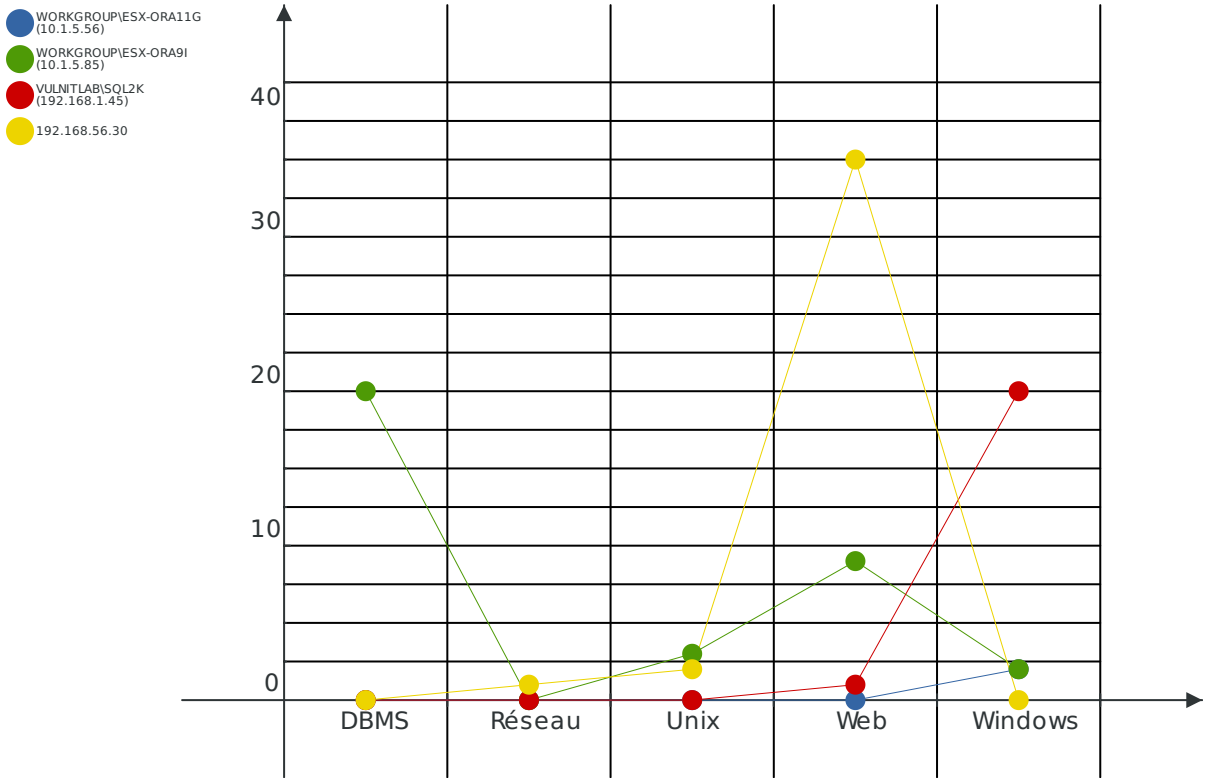


Ce graphique présente le nombre de vulnérabilités de priorité critique classées par objet de contrôle.



Nombre de correctifs manquants, par IP et objet

Ce graphique présente le nombre de correctifs (*patchs*) manquants pour chaque cible, classés par objet de contrôle.



Rapport technique

Inventaire

WORKGROUP\ESX-ORA11G (10.1.5.56)

Informations sur la machine distante :

- DNS : esx-ora11g
- NetBios : WORKGROUP\ESX-ORA11G
- Nom libre : WORKGROUP\ESX-ORA11G

Date de dernier scan : 2013-08-13 08:41:35

Compte administrateur validé : non

Cible testée : oui

Nombre de vulnérabilités :

- Critique : 4
- Majeur : 10
- Élevé : 2
- Moyen : 5
- Faible : 0

Ports ouverts : 7

Services :

- 135/tcp : RPC - Microsoft EPMAP - non testé
- 137/udp : Netbios name service - non testé
- 139/tcp : NETBIOS Services - non testé
- 445/tcp : SMB - Microsoft File Sharing - non testé
- 1025/tcp : RPC - Microsoft EPMAP - non testé
- 1031/tcp : BBN IAD - non testé
- 1521/tcp : Oracle - non testé

WORKGROUP\ESX-ORA9I (10.1.5.85)

Informations sur la machine distante :

- DNS : esx-ora9i
- NetBios : WORKGROUP\ESX-ORA9I
- Nom libre : WORKGROUP\ESX-ORA9I

Date de dernier scan : 2013-08-13 08:41:35

Compte administrateur validé : non

Cible testée : oui

Nombre de vulnérabilités :

- Critique : 8
- Majeur : 4
- Élevé : 8
- Moyen : 21
- Faible : 2

Ports ouverts : 11

Services :

- 80/tcp : HTTP - World Wide Web - non testé
- 135/tcp : RPC - Microsoft EPMAP - non testé
- 137/udp : Netbios name service - non testé
- 139/tcp : NETBIOS Services - non testé
- 443/tcp : HTTPS - Secure HTTP - non testé
- 445/tcp : SMB - Microsoft File Sharing - non testé
- 1025/tcp : RPC - Microsoft EPMAP - non testé
- 1032/tcp : BBN IAD - non testé
- 1521/tcp : Oracle - non testé
- 2100/tcp : FTP - File Transfer Protocol - non testé
- 8080/tcp : HTTP - World Wide Web - non testé

VULNITLAB\SQL2K (192.168.1.45)

Informations sur la machine distante :

- DNS : sql2k
- NetBios : VULNITLAB\SQL2K
- Nom libre : VULNITLAB\SQL2K

Date de dernier scan : 2013-08-13 09:42:21

Compte administrateur validé : non

Cible testée : oui

Nombre de vulnérabilités :

- Critique : 8
- Majeur : 3
- Élevé : 18
- Moyen : 1
- Faible : 0

Ports ouverts : 23

Services :

- 7/tcp : echo - non testé
- 9/tcp : discard server - non testé
- 13/tcp : daytime - non testé
- 17/tcp : Quote of the Day - non testé
- 19/tcp : ttytst source Character Generator - non testé
- 25/tcp : SMTP - Simple Mail Transfer Protocol - non testé
- 42/tcp : WINS - Windows Internet Naming Service - non testé
- 53/tcp : DNS - Domain Name Server - non testé
- 80/tcp : HTTP - World Wide Web - non testé
- 135/tcp : RPC - Microsoft EPMAP - non testé
- 139/tcp : NETBIOS Services - non testé
- 161/udp : SNMP - non testé
- 443/tcp : HTTPS - Secure HTTP - non testé
- 445/tcp : SMB - Microsoft File Sharing - non testé
- 515/tcp : Spooler - LPD - non testé
- 548/tcp : AFP - Apple Filing Protocol - non testé
- 1029/tcp : ms-lsa - non testé
- 1032/tcp : BBN IAD - non testé
- 1033/tcp : netinfo-local - non testé
- 1036/tcp : pcg-radar - non testé
- 1040/tcp : netarx - non testé
- 1433/tcp : MSSQL - Microsoft SQL Server - non testé
- 3372/tcp : MDTC - Microsoft Distributed Transaction Coordinator - non testé

192.168.56.30

Informations sur la machine distante :

- DNS : inconnu
- NetBios : inconnu

Date de dernier scan :

Compte administrateur validé : oui

Cible testée : non

Nombre de vulnérabilités :

- Critique : 1
- Majeur : 5
- Élevé : 7
- Moyen : 37
- Faible : 7

Ports ouverts : 7

Services :

- 22/tcp : SSH - Secure Shell Login [OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)] - non testé
- 80/tcp : HTTP - World Wide Web [Apache httpd 2.2.14 ((Ubuntu) mod_mono|2.4.3 PHP|5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python|3.3.1 Python|2.6.5 mod_perl|2.0.4 Perl|v5.10.1)] - non testé
- 139/tcp : NETBIOS Services [Samba smbd 3.X (workgroup: WORKGROUP)] - non testé
- 143/tcp : IMAP - Internet Mail Access Protocol [Courier Imapd (released 2008)] - non testé
- 445/tcp : NETBIOS Services [Samba smbd 3.X (workgroup: WORKGROUP)] - non testé
- 5001/tcp : commplex-link [Oracle VM Manager] - non testé
- 8080/tcp : HTTP - World Wide Web - non testé

Résumé

- WORKGROUP\ESX-ORA11G (10.1.5.56) - Patch mgt / Application des correctifs Windows - Critique
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Le rôle n'a pas de fonction de vérification des mots de passe - Critique
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Contrôle d'accès / Mot de passe SYSDBA trivial - Critique
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Nom d'instance trivial - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Aucun pare-feu trouvé - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Logiciel désactivé - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Contrôle d'accès / Mot de passe trivial - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Configuration Windows - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Compte invité activé - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Longueur minimale des mots de passe trop courte - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Exigences de complexité des mots de passe désactivées - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Mot de passe n'expirant jamais - Majeur

- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Historique des mots de passe trop faible - Majeur
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Les comptes inutilisés doivent être verrouillés - Élevé
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Machine hors du domaine - Élevé
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Les limites de ROLES doivent être activées - Moyen
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / AUDIT_SYS_OPERATIONS devrait être mis à TRUE - Moyen
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / GLOBAL_NAMES devrait être à TRUE - Moyen
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / os_authent_prefix devraient être une chaine nulle - Moyen
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Durée de vie minimale des mots de passe trop courte - Moyen
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Application des correctifs de bases de données - Critique
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Application des correctifs Web - Critique
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Application des correctifs Windows - Critique
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Contrôle d'accès / Mot de passe SYSDBA trivial - Critique
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Contrôle d'accès / Mot de passe trivial - Majeur
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Configuration / Liste d'instances accessible - Élevé
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Configuration / Configuration Windows - Élevé
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Chiffrement / Chiffrement faible - Moyen
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Application des correctifs Unix - Moyen
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Chiffrement / SSLv2 - Moyen
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Chiffrement / Certificat SSL non valide - Moyen
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Chiffrement / SSLv3/TLSv1 mode CBC faible - Moyen
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Chiffrement / Renegotiation SSL - Faible
- VULNITLAB\SQL2K (192.168.1.45) - Contrôle d'accès / Dossier partagé publiquement accessible - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Communauté SNMP en écriture - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Contrôle d'accès / Mot de passe trivial - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Application des correctifs Windows - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Communauté SNMP publique - Majeur
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Informations par RPC - Majeur
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Liste d'utilisateurs accessible - Élevé
- VULNITLAB\SQL2K (192.168.1.45) - Contrôle d'accès / Relai mail ouvert - Élevé
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Liste d'instances accessible - Élevé
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Application des correctifs Web - Élevé
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Service Discard - Moyen
- 192.168.56.30 - Patch mgt / Application des correctifs Web - Critique
- 192.168.56.30 - Configuration / [device] L'appareil a des droits publics. - Majeur
- 192.168.56.30 - Configuration / [account] Mauvais droits sur le dossier parent du

home. - Majeur
- 192.168.56.30 - Configuration / Liste d'utilisateurs accessible - Élevé
- 192.168.56.30 - Patch mgt / Application des correctifs Unix - Élevé
- 192.168.56.30 - Configuration / Configuration Web - Moyen
- 192.168.56.30 - Configuration / [local network] Processus en cours d'écoute. - Moyen
- 192.168.56.30 - Configuration / [network] Il n'y a pas de fichier FTPUSERS. - Moyen
- 192.168.56.30 - Configuration / [ssh] La directive PasswordAuthentication est mise à une valeur désapprouvée. - Moyen
- 192.168.56.30 - Configuration / [root] Login root distant autorisé dans SSHD_CONFIG. - Moyen
- 192.168.56.30 - Configuration / [inet] Le port pour le service est aussi assigné à un autre service. - Moyen
- 192.168.56.30 - Configuration / [pass] Le compte est désactivé, mais a un shell valide. - Moyen
- 192.168.56.30 - Patch mgt / Application des correctifs Réseau - Moyen
- 192.168.56.30 - Configuration / [cron] L'utilisation de cron ne semble pas restreinte. - Moyen
- 192.168.56.30 - Configuration / [cron] La crontab root ne semble pas exister. - Moyen
- 192.168.56.30 - Configuration / [account] Le home de l'utilisateur n'est pas accessible. - Moyen
- 192.168.56.30 - Configuration / [pass] L'intégrité des mots de passe est douteuse. - Moyen
- 192.168.56.30 - Configuration / [local network] Processus en cours d'écoute. - Moyen
- 192.168.56.30 - Configuration / Configuration Réseau - Faible
- 192.168.56.30 - Configuration / [account] Le compte semble être inactif. - Faible
- 192.168.56.30 - Configuration / [path] Le fichier n'exporte pas de paramètre initial pour PATH. - Faible
- 192.168.56.30 - Configuration / [pass] Le compte n'a pas un shell valide. - Faible

WORKGROUP\ESX-ORA11G (10.1.5.56)

Patch mgt / Application des correctifs Windows — Critique

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Critique

Méthodologie : boîte noire

- Correctif manquant : MS10-012
  Résumé : Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
  Script de test et informations relatives à cette vulnérabilité : 902269
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0022 , CVE-2010-0231
- Correctif manquant : MS09-001
  Résumé : Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
  Script de test et informations relatives à cette vulnérabilité : 900233
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-4114 , CVE-2008-4834 , CVE-2008-4835

Configuration / Le rôle n'a pas de fonction de vérification des mots de passe — Critique

Description : Les mots de passe devraient être au moins de 10 caractères alphanumériques. Cela devrait être contrôlé par une fonction de vérification desmots de passe.

Résolution : Créez la fonction, puis:
ALTER PROFILE profile_name LIMIT PASSWORD_VERIFICATION_FUNCTION new_value

Priorité : Critique

Méthodologie : boîte blanche

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:P/).

Informations :
- DEFAULT

Contrôle d'accès / Mot de passe SYSDBA trivial — Critique

Description : L'accès à cette base de données Oracle dispose d'un ou plusieurs comptes triviaux avec le privilège SYSDBA (i.e. mot de passe publiquement connu, voir la liste des instances et comptes ci-dessous).

Résolution : Changer les mots de passe de ces comptes ou les verrouiller.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Informations : SID : ORA11G (SYS/Compl3x3)

Configuration / Nom d'instance trivial	Majeur

Description : Le nom d'instance de cette base de données Oracle est commun (ie. il fait partie des noms courants donnés aux instances Oracle).

Résolution : Modifier le nom de cette instance.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).

Informations : [ORA11G]

Configuration / Aucun pare-feu trouvé	Majeur

Description : Aucun pare-feu n'a été trouvé sur la machine

Résolution : Installer un pare-feu

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).

Références : PCI DSS 1.4

Configuration / Logiciel désactivé	Majeur

Description : Le logiciel de sécurité est désactivé

Résolution : Activer le produit

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).

Informations : WindowsFirewall - Domain profile, WindowsFirewall - Standard profile

Contrôle d'accès / Mot de passe trivial	Majeur

Description : L'accès à cette base de données Oracle dispose d'un ou plusieurs comptes triviaux (i.e. mot de passe publiquement connu, voir la liste des instances et comptes ci-dessous).

Résolution : Changer les mots de passe de ces comptes ou les verrouiller.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

Informations : [ORA11G:OUTLN/OUTLN, ORA11G:DIP/DIP, ORA11G:WMSYS/WMSYS,

ORA11G:XDB/CHANGE_ON_INSTALL, ORA11G:ORDSYS/ORDSYS, ORA11G:ORDPLUGINS/ORDPLUGINS, ORA11G:MDSYS/MDSYS, ORA11G:MDDATA/MDDATA, ORA11G:WFS_USR_ROLE/WFS_USR_ROLE, ORA11G:CSW_USR_ROLE/CSW_USR_ROLE, ORA11G:OWB$CLIENT/S, ORA11G:SCOTT/TIGER, ORA11G:DEMO/DEMO]

Configuration / Configuration Windows — Majeur

Description : La configuration actuelle de ce serveur Windows présente des défauts.

Résolution : Corriger la configuration de ce serveur.

Priorité : Majeur

Méthodologie : boîte noire

- Résumé : Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 801991
  Risque : 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-1999-0519

Configuration / Compte invité activé — Majeur

Description : Le compte invité est activé

Résolution : Désactiver les comptes "invité" locaux et du domaine

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).

Informations : Invité

Configuration / Longueur minimale des mots de passe trop courte — Majeur

Description : Un mot de passe trop court permet d'augmenter les chances de réussite d'une attaque par brute force

Résolution : Augmenter la longueur minimale des mots de passe (au moins 6 caractères)

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).

Références : PCI DSS 8.5.10

Configuration / Exigences de complexité des mots de passe désactivées — Majeur

Description : Les exigences de complexité des mots de passe permettent d'éviter l'utilisation de mots de passe simples

Résolution : Activer les exigences de complexité des mots de passe

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).

Références : PCI DSS 8.5.11

Configuration / Mot de passe n'expirant jamais	Majeur

Description : Le mot de passe n'expire jamais, ce qui permet d'augmenter les chances de réussite d'une attaque par brute force

Résolution : Retirer l'option permettant la non-expiration du mot de passe

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.1 (Impact : 8.3, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).

Références : PCI DSS 8.5.9

Informations : Administrateur

Configuration / Historique des mots de passe trop faible	Majeur

Description : L'historique des mots de passe évite aux utilisateurs de réutiliser d'anciens mots de passe

Résolution : Augmenter la valeur d'historisation des mots de passe (au moins 4)

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.1 (Impact : 8.3, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).

Références : PCI DSS 8.5.12

Configuration / Les comptes inutilisés doivent être verrouillés	Élevé

Description : Les comptes inutilisés peuvent être une source potentielle d'attaque. Vous devez les verrouiller.

Résolution : ALTER USER <user> ACCOUNT LOCK;

Priorité : Élevé

Méthodologie : boîte blanche

Risque : 7.9 (Impact : 8.3, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:P/A:P/).

Informations :
- Username: OSCANNER_TEST, OS Username: None, Timestamp: 2010-05-14 10:56:46, Log off time: None, Return code: 1017, Terminal: None, User host: ubuntu-base
- Username: OWBSYS_AUDIT, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log

off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: OWBSYS, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: APEX_030200, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: APEX_PUBLIC_USER, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: FLOWS_FILES, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: MGMT_VIEW, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 1017, Terminal: None, User host: ubuntu-base
- Username: MGMT_VIEW, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 1017, Terminal: None, User host: ubuntu-base
- Username: MGMT_VIEW, OS Username: None, Timestamp: 2010-05-14 10:56:50, Log off time: None, Return code: 1017, Terminal: None, User host: ubuntu-base
- Username: SPATIAL_CSW_ADMIN_USR, OS Username: None, Timestamp: 2010-05-14 10:56:57, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: SPATIAL_WFS_ADMIN_USR, OS Username: None, Timestamp: 2010-05-14 10:56:57, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: ORDDATA, OS Username: None, Timestamp: 2010-05-14 10:56:57, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: XS$NULL, OS Username: None, Timestamp: 2010-05-14 10:56:57, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: APPQOSSYS, OS Username: None, Timestamp: 2010-05-14 10:56:57, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: ORACLE_OCM, OS Username: None, Timestamp: 2010-05-14 10:56:58, Log off time: None, Return code: 28000, Terminal: None, User host: ubuntu-base
- Username: JLroot, OS Username: 2010-05-14 11:36:53, Timestamp: None, Log off time: 1017, Return code: unknown, Terminal: Ubuntu-LAMP, User host: ?
- Username: PUBLIC, OS Username: gcastagnino, Timestamp: 2012-04-17 15:45:16, Log off time: 2012-04-17 15:45:16, Return code: 0, Terminal: pts/4, User host: natty-dev
- Username: DEMO9, OS Username: root, Timestamp: 2012-05-22 12:18:47, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: DES, OS Username: root, Timestamp: 2012-05-22 12:18:47, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: DES2K, OS Username: root, Timestamp: 2012-05-22 12:18:47, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: DEV2000_DEMOS, OS Username: root, Timestamp: 2012-05-22 12:18:47, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MDSYS, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 28000, Terminal: unknown, User host: natty-dev
- Username: ME, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MFG, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MGR, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MGWUSER, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MIGRATE, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MILLER, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MODTEST, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MMO2, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MMO2, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time:

None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MOREAU, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MRP, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MSC, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MSD, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MSO, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MSR, OS Username: root, Timestamp: 2012-05-22 12:18:50, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MTS_USER, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MTSSYS, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MWA, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: MXAGENT, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NAMES, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NEOTIX_SYS, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NNEUL, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NOM_UTILISATEUR, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NOME_UTILIZADOR, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NOMEUTENTE, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: NUME_UTILIZATOR, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: OAIHUB902, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: OAS_PUBLIC, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: OAS_PUBLIC, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: OCITEST, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: OCM_DB_ADMIN, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: OCM_DB_ADMIN, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: ODM, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: ODM_MTR, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: ODS, OS Username: root, Timestamp: 2012-05-22 12:18:51, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: REP_OWNER, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: REP_OWNER, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: REP_USER, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: REPADMIN, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off

time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: REPORTS, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: REPORTS_USER, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RG, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RHX, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RLA, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RLM, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RMAIL, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RMAN, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: RRS, OS Username: root, Timestamp: 2012-05-22 12:18:54, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SAP, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SAMPLE, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SAP, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SAPR3, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SDOS_ICSAP, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SECDEMO, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SERVICECONSUMER1, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SH, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SH, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SI_INFORMTN_SCHEMA, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 28000, Terminal: unknown, User host: natty-dev
- Username: SITEMINDER, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SLIDE, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SPIERSON, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SSP, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: STARTER, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: STRAT_USER, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SWPRO, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SWUSER, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SYMPA, OS Username: root, Timestamp: 2012-05-22 12:18:55, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev
- Username: SCOTT, OS Username: root, Timestamp: 2012-05-22 12:19:00, Log off time: None, Return code: 1017, Terminal: unknown, User host: natty-dev

- Username: SYS, OS Username: rh, Timestamp: 2013-02-26 13:41:15, Log off time: None, Return code: 28009, Terminal: unknown, User host: rhouyvet.DenyAll.local
- Username: SYSDBA, OS Username: rh, Timestamp: 2013-02-26 13:41:24, Log off time: None, Return code: 1017, Terminal: unknown, User host: rhouyvet.DenyAll.local
- Username: RHOUYVET, OS Username: rh, Timestamp: 2013-02-26 14:14:13, Log off time: None, Return code: 0, Terminal: unknown, User host: rhouyvet.DenyAll.local
- Username: RHOUYVET, OS Username: rh, Timestamp: 2013-02-26 14:14:13, Log off time: 2013-02-26 14:14:13, Return code: 0, Terminal: unknown, User host: rhouyvet.DenyAll.local
- Username: RHOUYVET, OS Username: rh, Timestamp: 2013-02-26 14:14:13, Log off time: None, Return code: 0, Terminal: unknown, User host: rhouyvet.DenyAll.local
- Username: ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ABM, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADAMS, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADLDEMO, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADMINISTRATOR, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADMINISTRATOR, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADMINISTRATEUR, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ADMINISTRATEUR, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AHL, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AHM, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AK, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ALHRO, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ALHRW, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ALR, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AMS, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AMV, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ANDY, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ANONYMOUS, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ANONYMOUS, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AP, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPLMGR, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPLSYS, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPLSYS, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPLSYSPUB, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off

time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPLSYSPUB, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPLYSYSPUB, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPS_MRC, OS Username: root, Timestamp: 2013-03-07 15:32:09, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPS, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: APPUSER, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AQ, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AQDEMO, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AQJAVA, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AQUSER, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AR, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ASF, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ASG, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ASL, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ASO, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ASP, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AST, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ATM, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AUDIOUSER, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AURORAJISUTILITY$, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AURORAJISUTILITY$, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AURORAORBUNAUTHENTICATED, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AURORAORBUNAUTHENTICATED, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AX, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: AZ, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BC4J, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BEN, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BIC, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BIL, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BIM, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time:

None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BIS, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BIV, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BIX, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BLAKE, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BLEWIS, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BOM, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BRIO_ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BRUGERNAVN, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BRUKERNAVN, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BSC, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: BUG_REPORTS, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CALVIN, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CATALOG, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CCT, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CDEMO82, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CDEMO82, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CDEMOCOR, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CDEMORID, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CDEMOUCB, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CDOUGLAS, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CENTRA, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CE, OS Username: root, Timestamp: 2013-03-07 15:32:10, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CENTRAL, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CIDS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CIS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CIS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CISINFO, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CISINFO, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CLARK, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CLKANA, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time:

None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CLKRT, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CN, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: COMPANY, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: COMPIERE, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CQSCHEMAUSER, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CQUSERDBUSER, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CRP, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSC, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSD, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSE, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSF, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSI, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSL, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSMIG, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSP, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSR, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CSS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CTXDEMO, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CTXSYS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: CTXSYS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: CUA, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUE, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUF, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUG, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUI, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUN, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUP, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CUS, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: CZ, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None,

Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DATA_SCHEMA, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DBI, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DBVISION, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DCM, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DDIC, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DEMO, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 28001, Terminal: unknown, User host: da-auditor
- Username: DEMO8, OS Username: root, Timestamp: 2013-03-07 15:32:11, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DIANE, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DIP, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: DISCOVERER_ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DISCOVERER5, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DMSYS, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DSGATEWAY, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DPF, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DSGATEWAY, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DSSYS, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DTSP, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EAA, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EAM, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EARLYWATCH, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EAST, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EC, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ECX, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EJB, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EJSADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EJSADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EMP, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ENG, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ENI, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ESTOREUSER, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off

time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EVENT, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EVM, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EXAMPLE, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EXFSYS, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: EXTDEMO, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: EXTDEMO2, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FA, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FEM, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FII, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FINANCE, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FINPROD, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FLM, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FND, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FOO, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FPT, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FRM, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FROSTY, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FTE, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: FV, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GL, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GMA, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GMD, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GME, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GMI, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GMF, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GML, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GMP, OS Username: root, Timestamp: 2013-03-07 15:32:12, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GMS, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GPFD, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GPLD, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time:

None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: GR, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HADES, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HCPARK, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HLW, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HR, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HR, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HRI, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HVST, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HXC, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: HXT, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IBA, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IBE, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IBU, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IBP, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IBY, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ICDBOWN, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ICX, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IDEMO_USER, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IEB, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IEC, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IEM, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IEO, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IES, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IEU, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IEX, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IFSSYS, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IGC, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IGF, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IGI, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IGS, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time:

None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IGW, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IMAGEUSER, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IMC, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IMEDIA, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IMT, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: INTERNAL, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 9275, Terminal: unknown, User host: da-auditor
- Username: INTERNAL, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 9275, Terminal: unknown, User host: da-auditor
- Username: INV, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IPA, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IPD, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: IPLANET, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ITG, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ISC, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JA, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JAKE, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JE, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JG, OS Username: root, Timestamp: 2013-03-07 15:32:13, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JILL, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JL , OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JMUSER, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JOHN, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JONES, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JTF, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JTM, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JTS, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: JWARD, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: KWALKER, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: L2LDEMO, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: LBACSYS, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: LIBRARIAN, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off

time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MANPROD, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MARK, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MASCARM, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MASTER, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MDDATA, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: MDDEMO, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MDDEMO_CLERK, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MDDEMO_CLERK, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: MDDEMO_MGR, OS Username: root, Timestamp: 2013-03-07 15:32:14, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ODS_SERVER, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ODSCOMMON, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OEM_REPOSITORY, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OEMADM, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OEMREP, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKB, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKC, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKI, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKO, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKR, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OKX, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OLAPDBA, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OLAPSVR, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OLAPSVR, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OLAPSYS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: OLAPSYS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: OMWB_EMULATION, OS Username: root, Timestamp: 2013-03-07 15:32:15,

Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ONT, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OO, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OPENSPIRIT, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OPI, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORACACHE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORACACHE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORACLE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORADBA, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORANGE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORAPROBE, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORAREGSYS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORASSO, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORASSO_DS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORASSO_PA, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORASSO_PS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORASSO_PUBLIC, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORASTAT, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORCLADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORDCOMMON, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ORDPLUGINS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: ORDSYS, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: OSE$HTTP$ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OSE$HTTP$ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OSM, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OSP22, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OSSAQ_HOST, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OSSAQ_PUB, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OSSAQ_SUB, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OTA, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OUTLN, OS Username: root, Timestamp: 2013-03-07 15:32:15, Log off time:

None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: OWA, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OWA_PUBLIC, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OWF_MGR, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OWF_MGR, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OWNER, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OZF, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OZP, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: OZS, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PA, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PANAMA, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PATROL, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PAUL, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PERFSTAT, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PERSTAT, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PJM, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PLANNING, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PLEX, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PLSQL, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PM, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PM, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PMI, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PN, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PO, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PO7, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PO8, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: POA, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: POM, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL_APP, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL_DEMO, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log

off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL_DEMO, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL_PUBLIC, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL_SSO_PS, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_DEMO, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_PS, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_PUBLIC, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_SSO, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_SSO_ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_SSO_PS, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PORTAL30_SSO_PUBLIC, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: POS, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: POWERCARTUSER, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PRIMARY, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PSA, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PSB, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PSP, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PUBSUB, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PUBSUB1, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: PV, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QA, OS Username: root, Timestamp: 2013-03-07 15:32:16, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QDBA, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QP, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_ADM, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_ADM, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_CB, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time:

None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_CB, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_CBADM, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_CBADM, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_CS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_CS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_ES, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_OS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_ES, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_OS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_WS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: QS_WS, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: RE, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: REP_MANAGER, OS Username: root, Timestamp: 2013-03-07 15:32:17, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: SYSADM, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: SYSADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: SYSADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: SYSTEM, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: SYSTEM, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1005, Terminal: unknown, User host: da-auditor
- Username: TAHITI, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TALBOT, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TDOS_ICSAP, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TEC, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TEST, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TEST, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TEST_USER, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TESTPILOT, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: THINSAMPLE, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TIBCO, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TIP37, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TRACESVR, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off

time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TRAVEL, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TSDEV, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TSMSYS, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TSUSER, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: TURBINE, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: UDDISYS, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: ULTIMATE, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: UM_ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: UM_CLIENT, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER_NAME, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER0, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER1, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER2, OS Username: root, Timestamp: 2013-03-07 15:32:18, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER3, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER4, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER5, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER6, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER7, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER8, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USER9, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: USUARIO, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: UTILITY, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: UTLBSTATU, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VEA, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VEH, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VERTEX_LOGIN, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VIDEOUSER, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VIF_DEVELOPER, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VIRUSER, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time:

None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VPD_ADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VRR1, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: VRR1, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WEBCAL01, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WEBDB, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WEBREAD, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WEBSYS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WEBUSER, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WEST, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WFADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WH, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WIP, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WIRELESS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WK_PROXY, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WK_SYS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WK_TEST, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WKADMIN, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WKPROXY, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WKSYS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WKPROXY, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WKUSER, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WKSYS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WMS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WMSYS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: WOB, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WPS, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WSH, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WSM, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WWW, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: WWWUSER, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off

time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XADEMO, OS Username: root, Timestamp: 2013-03-07 15:32:19, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XDB, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 28000, Terminal: unknown, User host: da-auditor
- Username: XDP, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XLA, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XNC, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XNI, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XNM, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XNP, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XNS, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XPRT, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: XTR, OS Username: root, Timestamp: 2013-03-07 15:32:20, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: DBSNMP, OS Username: root, Timestamp: 2013-03-07 15:32:21, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor
- Username: SYSMAN, OS Username: root, Timestamp: 2013-03-07 15:32:31, Log off time: None, Return code: 1017, Terminal: unknown, User host: da-auditor

Configuration / Machine hors du domaine	**Élevé**

Description : La machine n'appartient pas à un domaine Windows

Résolution : Ajouter la machine au domaine

Priorité : Élevé

Méthodologie : boîte blanche

Risque : 7.8 (Impact : 6.8, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:N/).

Informations : DenyAll.local, WORKGROUP, DENYALL

Configuration / Les limites de ROLES doivent être activées	**Moyen**

Description : Un nombre limité de ROLES doit être mis en place.

La recommendation du CIS benchmark est de 30, mais avec SYS qui en nécessite environ 20, 50 est une cible plus réaliste.

Résolution : alter system set max_enabled_roles=50 scope=spfile sid='*';

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.8 (Impact : 6.8, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:P/A:N/).

Informations :

- Current value: NONE

Configuration / AUDIT_SYS_OPERATIONS devrait être mis à TRUE	Moyen

Description : Recommandation CIS. Défaut : FALSE. Mettre à TRUE pour auditer toutes les activités effectuées en tant que SYSDBA ou SYSOPER.

Résolution : alter system set AUDIT_SYS_OPERATIONS=TRUE scope=spfile;

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.8 (Impact : 10.0, Exploitabilité : 3.1) CVSS : (AV:L/AC:L/AU:S/C:C/I:C/A:P/).

Informations :
- Current value: 0

Configuration / GLOBAL_NAMES devrait être à TRUE	Moyen

Description : Définir GLOBAL_NAMES=TRUE assure que le nom du lien à la base de données correspond au nom de la base de données distante.

Recommendation du CIS benchmark. Soyez prudent avec les applications qui ont plus de un lien vers la même base de données (Oracle E-Business Suite, par exemple), car vous aurez besoin de spécifier un nom unique qui par conséquent ne pourra pas correspondre à tous les noms de la base distante.

Résolution : alter system set global_names=true scope=spfile;

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.7 (Impact : 8.3, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:P/I:P/A:P/).

Informations :
- Current value: None

Configuration / os_authent_prefix devraient être une chaine nulle	Moyen

Description : La recommandation CIS est de mettre os_authent_prefix à la valeur nulle. La valeur par defaut est OPS$.

Résolution : alter system set os_authent_prefix='' scope=spfile sid='*';

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.2 (Impact : 6.8, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:P/I:P/A:N/).

Informations :
- Current value: ora11g

Configuration / Durée de vie minimale des mots de passe trop courte	**Moyen**

Description : Une durée de vie minimale des mots de passe peut permettre à un utilisateur de changer plusieurs fois de suite son mot de passe pour rédifinir à sa valeur actuelle, contournant ainsi la politique d'historique

Résolution : Augmenter la valeur de durée de vie minimale du mot de passe (conseillé : 1 jour)

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.0 (Impact : 4.3, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:P/A:N/).

Références : PCI DSS 8.5.9

WORKGROUP\ESX-ORA9I (10.1.5.85)

Patch mgt / Application des correctifs de bases de données — Critique

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Critique

Méthodologie : boîte noire

- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server Multiple Unspecified Vulnerabilities - Jan 08
  Script de test et informations relatives à cette vulnérabilité : 802528
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-0339 , CVE-2008-0340 , CVE-2008-0341 , CVE-2008-0342 , CVE-2008-0343 , CVE-2008-0344 , CVE-2008-0345
- Paquet affecté : -ORACLE DATABASE AND APPLICATION SERVER
  Résumé : Oracle Database Server and Application Server Ultra Search Component Unspecified Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 802524
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-0347
- Paquet affecté : -ORACLE DATABASE AND APPLICATION SERVER
  Résumé : Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 802526
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2006-0282 , CVE-2006-0283 , CVE-2006-0285 , CVE-2006-0286 , CVE-2006-0287 , CVE-2006-0290 , CVE-2006-0291
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server Multiple Unspecified Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 802527
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2006-0256 , CVE-2006-0257 , CVE-2006-0258 , CVE-2006-0259 , CVE-2006-0260 , CVE-2006-0261 , CVE-2006-0262 , CVE-2006-0263 , CVE-2006-0265 , CVE-2006-0266 , CVE-2006-0267 , CVE-2006-0268 , CVE-2006-0269 , CVE-2006-0270 , CVE-2006-0271 , CVE-2006-0272 , CVE-2006-0547 , CVE-2006-0548 , CVE-2006-0549 , CVE-2006-0551 , CVE-2006-0552 , CVE-2006-0586
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server Multiple Unspecified Vulnerabilities - April 06
  Script de test et informations relatives à cette vulnérabilité : 802538
  Risque : 9.1 (Impact : 10.0, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2006-1868 , CVE-2006-1871 , CVE-2006-1872 , CVE-2006-1873 , CVE-2006-1874
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server Multiple Vulnerabilities - Oct 06
  Script de test et informations relatives à cette vulnérabilité : 802520
  Risque : 9.1 (Impact : 10.0, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2006-5332 , CVE-2006-5333 , CVE-2006-5334 , CVE-2006-5335 , CVE-2006-5336 , CVE-2006-5339 , CVE-2006-5340 , CVE-2006-5341 , CVE-2006-5342 , CVE-2006-5343 , CVE-2006-5344 , CVE-2006-5345
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server MDSYS.MD Buffer Overflows and Denial of Service Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 802523
  Risque : 8.5 (Impact : 9.2, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:N/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2007-0272
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server 'RDBMS' component Denial of Service Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 802539
  Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
  Références : PCI DSS 6.1 , CVE-2007-5506

- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server Upgrade and Downgrade Component Multiple Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 802519
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2007-2113 , CVE-2007-2118
- Résumé : Oracle 9iAS SOAP Default Configuration Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 11227
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2001-1371
- Paquet affecté : -ORACLE DATABASE AND APPLICATION SERVER
  Résumé : Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 802525
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2006-0435
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database Server Multiple Components Multiple Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 802522
  Risque : 6.5 (Impact : 6.4, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2007-3855
- Résumé : Oracle 9iAS default error information disclosure
  Script de test et informations relatives à cette vulnérabilité : 11226
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2001-1372
- Résumé : Oracle 9iAS access to SOAP documentation
  Script de test et informations relatives à cette vulnérabilité : 11223
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1
- Résumé : Oracle 9iAS Jsp Source File Reading
  Script de test et informations relatives à cette vulnérabilité : 10852
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2002-0562
- Résumé : Oracle 9iAS Java Process Manager
  Script de test et informations relatives à cette vulnérabilité : 10851
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2002-0563
- Résumé : Oracle 9iAS Dynamic Monitoring Services
  Script de test et informations relatives à cette vulnérabilité : 10848
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2002-0563
- Résumé : Oracle 9iAS iSQLplus XSS
  Script de test et informations relatives à cette vulnérabilité : 12112
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1
- Paquet affecté : -ORACLE DATABASE
  Résumé : Oracle Database 'XML DB component' Unspecified vulnerability
  Script de test et informations relatives à cette vulnérabilité : 902043
  Risque : 4.0 (Impact : 2.9, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-0851
- Résumé : Oracle 9iAS SOAP configuration file retrieval
  Script de test et informations relatives à cette vulnérabilité : 11224
  Risque : 2.1 (Impact : 2.9, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2002-0568

Patch mgt / Application des correctifs Web — Critique

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Critique

Méthodologie : boîte noire

- Paquet affecté : -OPENSSL
  Résumé : OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100527
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2009-3245
- Paquet affecté : -OPENSSL
  Résumé : OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100668
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-0742
- Résumé : mod_ssl hook functions format string vulnerability
  Script de test et informations relatives à cette vulnérabilité : 13651
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2004-0700
- Résumé : http TRACE XSS attack
  Script de test et informations relatives à cette vulnérabilité : 11213
  Risque : 5.8 (Impact : 4.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2003-1567 , CVE-2004-2320
- Résumé : Allaire JRun directory browsing vulnerability
  Script de test et informations relatives à cette vulnérabilité : 10814
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2001-1510
- Résumé : JServ Cross Site Scripting
  Script de test et informations relatives à cette vulnérabilité : 10957
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1
- Résumé : Web Server Cross Site Scripting
  Script de test et informations relatives à cette vulnérabilité : 10815
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1
- Résumé : Apache Web Server ETag Header Information Disclosure Weakness
  Script de test et informations relatives à cette vulnérabilité : 103122
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2003-1418
- Résumé : FastCGI samples Cross Site Scripting
  Script de test et informations relatives à cette vulnérabilité : 10838
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1

Patch mgt / Application des correctifs Windows — Critique

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Critique

Méthodologie : boîte noire

- Correctif manquant : MS09-001
  Résumé : Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
  Script de test et informations relatives à cette vulnérabilité : 900233
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-4114 , CVE-2008-4834 , CVE-2008-4835
- Correctif manquant : MS10-012
  Résumé : Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
  Script de test et informations relatives à cette vulnérabilité : 902269
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0022 , CVE-2010-0231

Contrôle d'accès / Mot de passe SYSDBA trivial	Critique

Description : L'accès à cette base de données Oracle dispose d'un ou plusieurs comptes triviaux avec le privilège SYSDBA (i.e. mot de passe publiquement connu, voir la liste des instances et comptes ci-dessous).

Résolution : Changer les mots de passe de ces comptes ou les verrouiller.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Informations : SID : ORA9I (SYS/ORACLE)

Contrôle d'accès / Mot de passe trivial	Majeur

Description : L'accès à cette base de données Oracle dispose d'un ou plusieurs comptes triviaux (i.e. mot de passe publiquement connu, voir la liste des instances et comptes ci-dessous).

Résolution : Changer les mots de passe de ces comptes ou les verrouiller.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 9.0 (Impact : 8.5, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:C/A:P/).

Informations : SID : ORA9I (DBSNMP/DBSNMP, SCOTT/TIGER)

Configuration / Liste d'instances accessible	Élevé

Description : La configuration de la base de données Oracle permet d'obtenir la liste des instances de bases de données.

Résolution : Migrer vers une version plus récente (Oracle 10g minimum) et s'assurer que le fichier listener.ora ne contient pas la ligne "LOCAL_OS_AUTHENTICATION_LISTENER = OFF".

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).

Informations : [ORA9I]

Configuration / Configuration Windows	Élevé

Description : La configuration actuelle de ce serveur Windows présente des défauts.

Résolution : Corriger la configuration de ce serveur.

Priorité : Élevé

Méthodologie : boîte noire

- Résumé : Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 801991
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-1999-0519

Chiffrement / Chiffrement faible — Moyen

Description : Le serveur SSL accepte des connexions utilisant des algorithmes de chiffrement faibles (dont la longueur de clé est inférieure à 128 bits), ce qui pourrait permettre de déchiffrer en un temps raisonnable les identifiants de connexion et données transmises sur le réseau.

Résolution : Restreindre le choix d'algorithmes de chiffrement aux seuls algorithmes dont les clés sont au moins de longueur 128 bits.

Priorité : Moyen

Méthodologie : boîte noire

Risque : 5.4 (Impact : 6.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:N/A:N/).

Références : PCI DSS 2.2.2

Informations : DES-CBC-MD5 (SSLv2 - 56 bits), EXP-RC4-MD5 (SSLv2 - 40 bits), EDH-RSA-DES-CBC-SHA (SSLv3 - 56 bits), DES-CBC-SHA (SSLv3 - 56 bits), EXP-EDH-RSA-DES-CBC-SHA (SSLv3 - 40 bits), EXP-DES-CBC-SHA (SSLv3 - 40 bits), EXP-RC4-MD5 (SSLv3 - 40 bits), EDH-RSA-DES-CBC-SHA (TLSv1 - 56 bits), DES-CBC-SHA (TLSv1 - 56 bits), EXP-EDH-RSA-DES-CBC-SHA (TLSv1 - 40 bits), EXP-DES-CBC-SHA (TLSv1 - 40 bits), EXP-RC4-MD5 (TLSv1 - 40 bits)

Patch mgt / Application des correctifs Unix — Moyen

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Moyen

Méthodologie : boîte noire

- Paquet affecté : -OPENSSL
  Résumé : OpenSSL 'ssl3_get_record()' Remote Denial of Service Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100587
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-0740
- Résumé : Apache Connection Blocking Denial of Service
  Script de test et informations relatives à cette vulnérabilité : 12280
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2004-0174
- Paquet affecté : -OPENSSL
  Résumé : OpenSSL 'dtls1_retrieve_buffered_fragment()' Remote Denial of Service Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100588
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-0433

Chiffrement / SSLv2	Moyen

Description : Le serveur HTTPS supporte SSLv2 ou SSLv3 qui est vulnérable à une attaque Man In The Middle

Résolution : Désactiver le support de SSLv2 sur le serveur

Priorité : Moyen

Méthodologie : boîte noire

Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).

Références : PCI DSS 2.2.2

Informations : SSLv2 supported

Chiffrement / Certificat SSL non valide	Moyen

Description : Le certificat est invalide, ou n'est pa sun certificat de confiance

Résolution : Installer un certificat valide délivré par une autorité de confiance

Priorité : Moyen

Méthodologie : boîte noire

Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).

Références : PCI DSS 2.2.2

Informations : Certificate not trusted: 21 (unable to verify the first certificate)

Chiffrement / SSLv3/TLSv1 mode CBC faible	Moyen

Description : Le protocole de chiffrement SSLv3 et TLSv1, utilisé dans certaines configuration chiffrant les données en utilisant le mode CBC avec vecteurs d'initialisation chaînés est vulnérable à une attaque de type man-in-the-middle permettant d'obtenir les en-têtes HTTP d'une transaction HTTPS, en conjonction avec du code javascript utilisant l'API WebSocket HTML5, les URLConnection Java, ou l'API WebClient de Silverlight. Cette attaque est aussi nommée BEAST.
Des détails théoriques sur la mise en œuvre de cette attaque sont disponibles dans les publications de Gregory V. Bard :
- http://eprint.iacr.org/2004/111.pdf
- http://eprint.iacr.org/2006/136.pdf
Une description pratique de l'attaque a été présentée par Rizzo et Duong :
http://www.educatedguesswork.org/2011/09/security_impact_of_the_rizzodu.html

Résolution : La meilleure solution consiste à migrer le service sur TLSv1.1 ou TLSv1.2 pour lesquels la faiblesse a été corrigée.
Cependant, peu de clients et serveurs sont compatible avec cette possibilité. Par conséquent, un contournement consiste à privilégier les méthodes de chiffrement RC4 de SSLv3/TLSv1 et à désactiver les modes CBC. La façon de faire dépend du logiciel serveur.

Pour un serveur Apache, on pourra par exemple prioriser des méthodes TLSv1.2, puis RC4 pour les clients ne permettant que TLSv1 ainsi :
> SSLHonorCipherOrder On
> SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH

Pour un serveur Postfix :
> tls_preempt_cipherlist = yes
> tls_high_cipherlist = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH

Priorité : Moyen

Méthodologie : boîte noire

Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

Références : CVE-2011-3389

Informations : EDH-RSA-DES-CBC-SHA (SSLv3 - 56 bits), DES-CBC-SHA (SSLv3 - 56 bits), EXP-EDH-RSA-DES-CBC-SHA (SSLv3 - 40 bits), EXP-DES-CBC-SHA (SSLv3 - 40 bits), EDH-RSA-DES-CBC-SHA (TLSv1 - 56 bits), DES-CBC-SHA (TLSv1 - 56 bits), EXP-EDH-RSA-DES-CBC-SHA (TLSv1 - 40 bits), EXP-DES-CBC-SHA (TLSv1 - 40 bits)

Chiffrement / Renegotiation SSL	**Faible**

Description : Le serveur HTTPS supporte la renégociation non sécurisée qui est vulnérable à une attaque Man In The Middle

Résolution : La renégociation non sécurisée doit être désactivée

Priorité : Faible

Méthodologie : boîte noire

Risque : 2.6 (Impact : 2.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:N/I:P/A:N/).

Références : PCI DSS 2.2.2

Informations : SSL insecure renegotiation supported

VULNITLAB\SQL2K (192.168.1.45)

Contrôle d'accès / Dossier partagé publiquement accessible — Critique

Description : La configuration actuelle permet à tout un chacun (disposant ou non d'un compte sur le domaine) d'accéder aux partages Windows et aux fichiers qu'ils contiennent.

Résolution : Restreindre l'accès à ce partage aux seuls utilisateurs autorisés.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Informations : [TESTSMB]

Configuration / Communauté SNMP en écriture — Critique

Description : La communauté SNMP décrite ci-dessous est accessible à tous en écriture, ce qui permet d'administrer le serveur à distance (et en particulier l'arrêter).

Résolution : Migrer vers SNMP v3 pour ajouter une authentification. A défaut, changer le nom de la communauté ou restreindre les machines habilitées à accéder au service SNMP.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Informations : [private]

Contrôle d'accès / Mot de passe trivial — Critique

Description : L'accès à cette base de données Microsoft SQL Server dispose d'un compte administrateur trivial (i.e. mot de passe nul ou identique à l'identifiant).

Résolution : Modifier le mot de passe du compte administrateur.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Informations : SID : SQL2KVINCENT ([sa])

Patch mgt / Application des correctifs Windows — Critique

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Critique

Méthodologie : boîte noire

- Correctif manquant : MS10-012
  Résumé : Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
  Script de test et informations relatives à cette vulnérabilité : 902269
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0022 , CVE-2010-0231
- Correctif manquant : MS09-048
  Résumé : Microsoft Windows TCP/IP Remote Code Execution Vulnerability (967723)
  Script de test et informations relatives à cette vulnérabilité : 900838
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-4609 , CVE-2009-1925 , CVE-2009-1926
- Correctif manquant : MS09-001
  Résumé : Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
  Script de test et informations relatives à cette vulnérabilité : 900233
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-4114 , CVE-2008-4834 , CVE-2008-4835
- Résumé : IIS .IDA ISAPI filter applied
  Script de test et informations relatives à cette vulnérabilité : 10695
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2001-0500
- Correctif manquant : MS03-039
  Résumé : Microsoft RPC Interface Buffer Overrun (KB824146)
  Script de test et informations relatives à cette vulnérabilité : 102015
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2003-0528 , CVE-2003-0605 , CVE-2003-0715
- Correctif manquant : MS09-055
  Résumé : Microsoft Windows ATL COM Initialization Code Execution Vulnerability (973525)
  Script de test et informations relatives à cette vulnérabilité : 900880
  Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2009-2493
- Résumé : Microsoft RPC Interface Buffer Overrun (823980)
  Script de test et informations relatives à cette vulnérabilité : 11808
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2003-0352
- Correctif manquant : MS03-007
  Résumé : Unchecked Buffer in ntdll.dll (Q815021)
  Script de test et informations relatives à cette vulnérabilité : 11413
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2003-0109
- Correctif manquant : MS02-050
  Résumé : Certificate Validation Flaw Could Enable Identity Spoofing (Q328145)
  Script de test et informations relatives à cette vulnérabilité : 11145
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2002-0862 , CVE-2002-1183
- Correctif manquant : MS02-055
  Résumé : Unchecked Buffer in Windows Help(Q323255)
  Script de test et informations relatives à cette vulnérabilité : 11147
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2002-0693 , CVE-2002-0694
- Correctif manquant : MS03-043
  Résumé : Buffer Overrun in Messenger Service (828035)
  Script de test et informations relatives à cette vulnérabilité : 11888
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2003-0717
- Correctif manquant : MS02-063
  Résumé : Unchecked Buffer in PPTP Implementation Could Enable DOS Attacks (Q329834)
  Script de test et informations relatives à cette vulnérabilité : 11178
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2002-1214
- Correctif manquant : MS03-041
  Résumé : Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)
  Script de test et informations relatives à cette vulnérabilité : 11886
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2003-0660
- Correctif manquant : MS03-023
  Résumé : Buffer Overrun In HTML Converter Could Allow Code Execution (823559)

Script de test et informations relatives à cette vulnérabilité : 11878
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
Références : PCI DSS 6.1 , CVE-2003-0469

- Correctif manquant : MS02-006
  Résumé : Checks for MS HOTFIX for snmp buffer overruns
  Script de test et informations relatives à cette vulnérabilité : 10865
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2002-0053
- Correctif manquant : MS02-042
  Résumé : Windows Network Manager Privilege Elevation (Q326886)
  Script de test et informations relatives à cette vulnérabilité : 11091
  Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2002-0720
- Résumé : Microsoft Windows GP Trap Handler Privilege Escalation Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 800442
  Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2010-0232
- Correctif manquant : MS02-017
  Résumé : MUP overlong request kernel overflow Patch (Q311967)
  Script de test et informations relatives à cette vulnérabilité : 10944
  Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2002-0151
- Correctif manquant : MS03-045
  Résumé : Buffer Overrun in the ListBox and in the ComboBox (824141)
  Script de test et informations relatives à cette vulnérabilité : 11885
  Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2003-0659
- Correctif manquant : MS02-024
  Résumé : Windows Debugger flaw can Lead to Elevated Privileges (Q320206)
  Script de test et informations relatives à cette vulnérabilité : 10964
  Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2002-0367

Configuration / Communauté SNMP publique — Majeur

Description : Un service SNMP en version 1 ou 2 (sans mot de passe) et avec un nom de communauté commun (cf. ci-dessous) est accessible et fournit de nombreuses informations précieuses sur le système.

Résolution : Migrer vers SNMP v3 pour ajouter une authentification. A défaut, changer le nom de la communauté ou restreindre les machines habilitées à accéder au service SNMP.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 8.5 (Impact : 7.8, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:P/).

Informations : Communautés [public, private].
Voici un échantillon d'informations utiles pouvant être collectées par SNMP :
- Matériel et logiciel (Created directory: /var/net-snmp, Created directory: /var/net-snmp/mib_indexes, Hardware: x86 Family 6 Model 10 Stepping 7 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free))
- Nom de la machine (SQL2K)
- Comptes utilisateur (Guest, ToBeFound, Administrator, IUSR_VULNITSMB, IWAM_VULNITSMB, TsInternetUser)
- Interfaces réseau (127.0.0.1 / 255.0.0.0, 192.168.1.45 / 255.255.255.0)
- Programmes installés (Microsoft SQL Server 2000 (SQL2KVINCENT), WebFldrs)
- Connexions IIS actives (0)
- Partages réseau (TESTSMB, pourtous)
- Emplacement (Paris)
- Contact (vmaury@vulnit.com)

ainsi que d'autres informations utiles comme les processus, le stockage, les tables de

routage, connexions TCP et UDP, etc.

Configuration / Informations par RPC	Majeur

Description : Un service RPC fournit à tout un chacun (disposant ou non d'un compte sur le domaine) de nombreuses informations précieuses sur le système.

Résolution : Ce service requiert un compte (local ou domaine) à partir de votre système d'exploitation.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 8.5 (Impact : 7.8, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:P/).

Informations : Voici un échantillon d'informations utiles pouvant être collectées par RPC :<ul class='vulnList'>
Nom de domaine (VULNITLAB)
Comtes administrateur local (SQL2K\\Administrator (1), *unknown**unknown* (8), SQL2K\\ToBeFound (1))
ainsi que d'autres informations utiles sur les droits des comptes énumérés, politiques de sécurité, imprimantes, etc.

Configuration / Liste d'utilisateurs accessible	Élevé

Description : La configuration et la version du serveur permettent d'obtenir la liste de ses utilisateurs.

Résolution : Migrer vers un système d'exploitations plus récent.

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

Informations : [Administrator, Guest, IUSR_VULNITSMB, IWAM_VULNITSMB, ToBeFound, TsInternetUser]

Contrôle d'accès / Relai mail ouvert	Élevé

Description : Ce service mail ne contrôle pas l'adresse émetteur, ce qui pourrait permettre l'usurpation d'identité. De plus, ce serveur mail (SMTP) peut servir de relai à n'importe quel émetteur, et en particulier pour relayer des spams.

Résolution : Appliquer les patchs correctifs. Configurer le serveur pour contrôle l'émetteur du message.

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:C/A:N/).

Références : PCI DSS 2.2.2

Informations : L'envoi de mails dont l'identité est usurpée semble possible. Toutefois, seul l'envoi effectif de mail (en précisant une adresse destinataire) peut permettre de valider cette vulnérabilité.

Configuration / Liste d'instances accessible	Élevé

Description : La configuration et la version du serveur Microsoft SQL permettent d'obtenir la liste des instances de bases de données.

Résolution : Arrêter le service 'SQL Server Browser', ou à défaut, filtrer l'accès au port 1434/UDP aux seuls clients habilités.

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).

Informations : SQL2KVINCENT (8.00.194)

Patch mgt / Application des correctifs Web	Élevé

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Élevé

Méthodologie : boîte noire

- Résumé : IIS XSS via 404 error
  Script de test et informations relatives à cette vulnérabilité : 10936
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2002-0148 , CVE-2002-0150

Configuration / Service Discard	Moyen

Description : Le service Discard est activé sur ce serveur. Ce service est inutilisé de nos jours et devrait être coupé.

Résolution : Désactiver le service Discard, via /etc/inetd.conf sur Unix, ou via la clé de registre "EnableTcpDiscard" sur Windows.

Priorité : Moyen

Méthodologie : boîte noire

Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).

Références : PCI DSS 2.2.4

192.168.56.30

Patch mgt / Application des correctifs Web — Critique

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Critique

Méthodologie : boîte noire

- Paquet affecté : -WORDPRESS
  Résumé : WordPress 'wp-admin' Multiple Vulnerabilities - Aug09
  Script de test et informations relatives à cette vulnérabilité : 900915
  Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2009-2853 , CVE-2009-2854
- Paquet affecté : -WORDPRESS
  Résumé : WordPress cat Parameter Directory Traversal Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 800124
  Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-4769
- Résumé : PHP version smaller than 5.3.3
  Script de test et informations relatives à cette vulnérabilité : 110182
  Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2007-1581 , CVE-2010-0397 , CVE-2010-1860 , CVE-2010-1862 , CVE-2010-1864 , CVE-2010-1917 , CVE-2010-2097 , CVE-2010-2100 , CVE-2010-2101 , CVE-2010-2190 , CVE-2010-2191 , CVE-2010-2225 , CVE-2010-2484 , CVE-2010-2531 , CVE-2010-3062 , CVE-2010-3063 , CVE-2010-3064 , CVE-2010-3065
- Paquet affecté : -WORDPRESS
  Résumé : WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 900183
  Risque : 8.5 (Impact : 10.0, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).
  Références : PCI DSS 6.1 , CVE-2008-5695
- Résumé : GhostScripter Amazon Shop Multiple Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 100024
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1
- Paquet affecté : -TIKIWIKI
  Résumé : TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 100537
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-1133 , CVE-2010-1134 , CVE-2010-1135 , CVE-2010-1136
- Paquet affecté : -JOOMLA
  Résumé : Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 103114
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1
- Paquet affecté : -PHP
  Résumé : PHP version 5.3< 5.3.6
  Script de test et informations relatives à cette vulnérabilité : 110013
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2011-0421 , CVE-2011-0708 , CVE-2011-1092 , CVE-2011-1153 , CVE-2011-1464 , CVE-2011-1466 , CVE-2011-1467 , CVE-2011-1468 , CVE-2011-1469 , CVE-2011-1470
- Paquet affecté : - OF WORDPRESS
  Résumé : WordPress Multiple Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 900219
  Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2008-3747
- Paquet affecté : -WORDPRESS
  Résumé : WordPress 'wp-admin/includes/file.php' Arbitrary File Upload Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100345
  Risque : 6.8 (Impact : 6.4, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).

Références : PCI DSS 6.1
- Résumé : PHP MicroCMS Local File Include and SQL Injection Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 100808
  Risque : 6.8 (Impact : 6.4, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-3480
- Résumé : PHP version smaller than 5.3.4
  Script de test et informations relatives à cette vulnérabilité : 110181
  Risque : 6.8 (Impact : 6.4, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2006-7243 , CVE-2010-2094 , CVE-2010-2950 , CVE-2010-3436 , CVE-2010-3709 , CVE-2010-3710 , CVE-2010-3870 , CVE-2010-4150 , CVE-2010-4156 , CVE-2010-4409 , CVE-2010-4697 , CVE-2010-4698 , CVE-2010-4699 , CVE-2010-4700 , CVE-2011-0753 , CVE-2011-0754 , CVE-2011-0755
- Paquet affecté : -TOMCAT
  Résumé : Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 100712
  Risque : 6.4 (Impact : 4.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-2227
- Paquet affecté : -WORDPRESS
  Résumé : WordPress Multiple Vulnerabilities - Nov09
  Script de test et informations relatives à cette vulnérabilité : 900975
  Risque : 6.0 (Impact : 6.4, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:P/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2009-3890 , CVE-2009-3891
- Résumé : http TRACE XSS attack
  Script de test et informations relatives à cette vulnérabilité : 11213
  Risque : 5.8 (Impact : 4.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2003-1567 , CVE-2004-2320
- Paquet affecté : -WORDPRESS
  Résumé : WordPress Password Protection Security Bypass Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100549
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1
- Résumé : AWStats 'awstats.pl' Multiple Path Disclosure Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100070
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2006-3682
- Résumé : WonderCMS 'page' Parameter Cross Site Scripting And Information Disclosure Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 100908
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1
- Résumé : Imageview 'page' Parameter Local File Include Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 103100
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1
- Résumé : awiki Multiple Local File Include Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 103210
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1
- Résumé : QWikiwiki directory traversal vulnerability
  Script de test et informations relatives à cette vulnérabilité : 16100
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2005-0283
- Résumé : OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 103132
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1
- Paquet affecté : -TOMCAT
  Résumé : Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 103032
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-4172
- Résumé : WordPress Comment Author URI Cross-Site Scripting Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100239
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2009-2851
- Résumé : Apache Web Server ETag Header Information Disclosure Weakness
  Script de test et informations relatives à cette vulnérabilité : 103122

Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).
Références : PCI DSS 6.1 , CVE-2003-1418

- Paquet affecté : -WORDPRESS MU
  Résumé : WordPress MU Cross-Site Scripting Vulnerability - Apr09
  Script de test et informations relatives à cette vulnérabilité : 800376
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2009-1030
- Résumé : phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 801660
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-4480
- Paquet affecté : -WORDPRESS
  Résumé : WordPress wp-trackback.php Denial of Service Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 900968
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2009-3622
- Paquet affecté : -JOOMLA!
  Résumé : Joomla! Multiple Cross-site Scripting Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 901168
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-3712
- Résumé : Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 902830
  Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2012-0053
- Paquet affecté : -WORDPRESS
  Résumé : WordPress _REQUEST array Cross Site Request Forgery (CSRF) Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 800140
  Risque : 4.0 (Impact : 4.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:N/I:P/A:P/).
  Références : PCI DSS 6.1 , CVE-2008-5113
- Paquet affecté : -WORDPRESS
  Résumé : WordPress Trashed Posts Information Disclosure Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100505
  Risque : 4.0 (Impact : 2.9, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-0682
- Paquet affecté : -APACHE TOMCAT
  Résumé : Apache Tomcat Security bypass vulnerability
  Script de test et informations relatives à cette vulnérabilité : 901114
  Risque : 2.6 (Impact : 2.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-1157
- Résumé : Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100130
  Risque : 2.6 (Impact : 2.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:N/I:P/A:N/).
  Références : PCI DSS 6.1 , CVE-2009-0796
- Paquet affecté : -TOMCAT
  Résumé : Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 100598
  Risque : 2.6 (Impact : 2.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1 , CVE-2010-1157

Configuration / [device] L'appareil a des droits publics. — Majeur

Description : Les devices ayant des droits inapropriés (world) peuvent être accédés par n'importe quel utilisateur système. Cela peut ouvrir des brèches de sécurité si ce sont des devices partagés ou des binaires maintenus (des disques par exemple).

Résolution : L'administrateur devrait mettre correctement les accès au devices (en utilisant la configuration de groupe pour fournir un accès au device pour plusieurs utilisateurs, par exemple).

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.7 (Impact : 9.5, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:P/I:C/A:C/).

Informations : [/dev/fuse, /dev/rfkill]

Configuration / [account] Mauvais droits sur le dossier parent du home.	Majeur

Description : Le dossier home du compte affiché a le droit d'écriture de groupe, droit d'écriture pour tous – ou les deux – activé. Cela permet d'ajouter aux autres comptes de nouveaux fichiers (et potentiellement de supprimez des fichiers).

Résolution : Les droits en écriture devrait être retirés.

Priorité : Majeur

Méthodologie : boîte blanche

Risque : 8.5 (Impact : 9.2, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:C/I:C/A:N/).

Informations : [Login ID polkituser's home directory (/var/run/PolicyKit) has group `polkituser' write access]

Configuration / Liste d'utilisateurs accessible	Élevé

Description : La configuration et la version du serveur permettent d'obtenir la liste de ses utilisateurs.

Résolution : Migrer vers un système d'exploitations plus récent.

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

Informations : [nobody, None, user, root]

Patch mgt / Application des correctifs Unix	Élevé

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Élevé

Méthodologie : boîte noire

- Résumé : Apache httpd Web Server Range Header Denial of Service Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 901203
  Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
  Références : PCI DSS 6.1 , CVE-2011-3192
- Résumé : Samba Multiple Remote Denial of Service Vulnerabilities
  Script de test et informations relatives à cette vulnérabilité : 100644
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2010-1635

Configuration / Configuration Web	Moyen

Description : La configuration actuelle de ce site web présente des défauts.

Résolution : Corriger la configuration de ce site web.

Priorité : Moyen

Méthodologie : boîte noire

- Résumé : Apache Tomcat servlet/JSP container default files
  Script de test et informations relatives à cette vulnérabilité : 12085
  Risque : 6.8 (Impact : 6.4, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
  Références : PCI DSS 6.1

Configuration / [local network] Processus en cours d'écoute.	Moyen

Description : Listening process.

Résolution : Les processus installés en écoute sur les interfaces Internet doivent être étroitement controllés puisqu'ils sont les “portes ouvertes” vers l'extérieur.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.8 (Impact : 6.9, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:N/I:N/A:C/).

Informations :
- Process: apache2 - Socket: 80 - Type: TCP - Addr: every
- Process: nmbd - Socket: 137 - Type: UDP - Addr: every
- Process: nmbd - Socket: 138 - Type: UDP - Addr: every
- Process: smbd - Socket: 139 - Type: TCP - Addr: every
- Process: smbd - Socket: 445 - Type: TCP - Addr: every
- Process: sshd - Socket: 22 - Type: TCP - Addr: every

Configuration / [network] Il n'y a pas de fichier FTPUSERS.	Moyen

Description : Il n'y a pas de fichier de configuration ftpusers. Sur certains systèmes cela peut autoriser certains utilisateurs administratifs (faible UID) à accéder au serveur FTP local si il est activé (d'autres systèmes peuvent rendre son utilisation obsolète).

Résolution : Il est recommandé d'ajouter les utilisateurs administratifs dans /etc/ftpusers si vous avez un serveur FTP installé.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.8 (Impact : 6.9, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:C/I:N/A:N/).

Informations : [/etc/ftpusers]

Configuration / [ssh] La directive PasswordAuthentication est mise à une valeur	Moyen

désapprouvée.	

Description : La directive PasswordAuthentication détermine si les mots de passes sont une authentification suffisante.

Résolution : Définissez la directive PasswordAuthentication à une valeur approuvé.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.8 (Impact : 6.9, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:N/I:C/A:N/).

Informations :
- File: /etc/ssh/sshd_config - Unapproved value: yes

Configuration / [root] Login root distant autorisé dans SSHD_CONFIG.	Moyen

Description : Le fichier indiqué permet la connexion root pour telnet et d'autres services à distance (ie: autre que la console système).

Résolution : Pour /etc/default/login, soyez certain que la ligne “CONSOLE=/dev/console” existe. Pour /etc/securetty, assurez-vous qu'il n'y a pas d'entrées ttyp.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.8 (Impact : 10.0, Exploitabilité : 3.1) CVSS : (AV:L/AC:S/AU:S/C:C/I:C/A:C/).

Informations :
- SSHD_CONFIG: /etc/ssh/sshd_config

Configuration / [inet] Le port pour le service est aussi assigné à un autre service.	Moyen

Description : Le numéro de port indiqué est assigné à un autre service. Cela indique soit une mauvaise configuration dans la base de données des services, soit un signe possible d'une intrusion.

Résolution : Cela devrait être vérifié et corrigé. Si la raison pour laquelle il en est ainsi n'est pas apparente, alors le système devrait être vérifié pour d'autres signes d'intrusion.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 6.4 (Impact : 4.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:S/AU:N/C:N/I:P/A:P/).

Informations :
- Service 1: sieve - Service 2: cisco-sccp
- Service 1: ndtp - Service 2: pipe_server
- Service 1: ndtp - Service 2: search
- Service 1: postgres - Service 2: postgresql
- Service 1: postgres - Service 2: postgresql
- Service 1: sane - Service 2: sane-port
- Service 1: webcache - Service 2: http-alt
- Service 1: webcache - Service 2: http-alt

Configuration / [pass] Le compte est désactivé, mais a un shell valide.	**Moyen**

Description : Le compte affiché est désactivé d'une certaine façon ('*' dans le champ mot de passe, etc), mais le shell de connexion pour le compte est un shell valide (provenant de /etc/shells ou l'équivalent). Un shell valide peut potentiellement permettre de continuer à utiliser le compte.

Résolution : Le shell de connexion devrait être changé pour quelquechose n'existant pas, ou un binaire comme /bin/false.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 5.9 (Impact : 9.2, Exploitabilité : 2.5) CVSS : (AV:L/AC:S/AU:M/C:C/I:C/A:N/).

Informations : [backup, bin, daemon, games, gnats, irc, libuuid, list, lp, mail, man, news, nobody, postgres, proxy, root, sys, user, uucp, www-data]

Patch mgt / Application des correctifs Réseau	**Moyen**

Description : Les correctifs (patchs) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

Résolution : Appliquer les correctifs mis à disposition par l'éditeur.

Priorité : Moyen

Méthodologie : boîte noire

- Résumé : TCP Sequence Number Approximation Reset Denial of Service Vulnerability
  Script de test et informations relatives à cette vulnérabilité : 902815
  Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  Références : PCI DSS 6.1 , CVE-2004-0230

Configuration / [cron] L'utilisation de cron ne semble pas restreinte.	**Moyen**

Description : Cron autorise les utilisateurs a demander l'exécution de tâches au système à un moment possiblement récurrent. Cela peut être très utile, mais peut être une source potentielle sérieuse d'abus par soit les utilisateurs soit des crackers. L'utilisation de cron par les utilisateurs peut être restreinte en créant un fichier /etc/cron.allow (contenant uniquement les administrateurs système) ou un fichier /etc/cron.deny (listant les utilisateurs n'ayant pas l'autorisation d'accès). En fonction de la configuration si aucun n'existe, soit root sera le seul a pouvoir configurer des tâches cron, ou tous les utilisateurs pourront le faire. Pour de nombreux systèmes la configuration par défaut est d'autoriser l'accès à tous les utilisateurs.

Résolution : (Re)créer un fichier /etc/cron.allow ou etc.cron.deny

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 4.9 (Impact : 6.9, Exploitabilité : 3.9) CVSS : (AV:L/AC:S/AU:N/C:N/I:C/A:N/).

Configuration / [cron] La crontab root ne semble pas exister.	**Moyen**

Description : Il n'y a pas de crontab pour le compte superutilisateur. Ce n'est pas une erreur en soi, étant donné que de nombreux systèmes peuvent être livrés sans et utiliser d'autres méthodes (fichiers /etc/cron*) pour faire tourner des programmes en tant que root. Néanmoins, si il n'y a pas de méthode pour le compte root de faire tourner des scripts, certains scripts de vérification du système peuvent ne pas être exécutés du tout.

Résolution : Créez un root crontab.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 4.9 (Impact : 6.9, Exploitabilité : 3.9) CVSS : (AV:L/AC:S/AU:N/C:N/I:N/A:C/).

Configuration / [account] Le home de l'utilisateur n'est pas accessible.	**Moyen**

Description : Le compte affiché a un dossier home qui n'est pas accessible.

Résolution : Cela devrait être vérifié pour voir si celà est dû a des problèmes de réseau pour les dossier home à distance. Sans un dossier home valide, le compte aura '/' comme dossier home.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 4.5 (Impact : 6.9, Exploitabilité : 3.1) CVSS : (AV:L/AC:S/AU:S/C:C/I:N/A:N/).

Informations :
- User: nobody - Home: /nonexistent

Configuration / [pass] L'intégrité des mots de passe est douteuse.	**Moyen**

Description : Les fichiers de mots de passe ont des problèmes d'intégrité tel que trouvé par 'pwck -r'. Cela peut mener a des programmes de manipulation des mots de passe en boucle pour l'authentificationou des problèmes de connexion si non corrigé.

Résolution : Vérifiez l'intégrité des mots de passe

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 4.3 (Impact : 6.9, Exploitabilité : 2.5) CVSS : (AV:L/AC:S/AU:M/C:N/I:C/A:N/).

Informations :
- pwcd -r: /usr/sbin/pwck -r

Configuration / [local network] Processus en cours d'écoute.	**Moyen**

Description : Des processus n'ayant pas été lancés par root écoutent sur des interfaces ouvertes vers l'extérieur. Ces processus peuvent avoir été lancés par root et avoir changé leurs uid, ou être des processus non autorisés.

Résolution : Confirmez si leur présence est nécessaire.
Remarquez que parfois des services ouvrent des listeners UDP sporadic pour recevoir des requêtes DNS. Si vous recevez des rapports sur des services UDP qui sont plus tard fermés, ceci peut être un faux-positif.

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 4.0 (Impact : 2.9, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:N/I:P/A:N/).

Informations :
- Process: apache2 (run by 80) - Socket: TCP - Type: every - Addr: www-data

Configuration / Configuration Réseau	**Faible**

Description : La configuration actuelle de cet équipement réseau présente des défauts.

Résolution : Corriger la configuration de cet équipement réseau.

Priorité : Faible

Méthodologie : boîte noire

- Résumé : TCP timestamps
  Script de test et informations relatives à cette vulnérabilité : 80091
  Risque : 2.6 (Impact : 2.9, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:N/A:N/).
  Références : PCI DSS 6.1

Configuration / [account] Le compte semble être inactif.	**Faible**

Description : Le compte affiché semble ne pas être utilisé. Les fichiers dans le dossier home de cet utilisateur n'ont pas été modifiés depuis un certain temps.

Résolution : Après investigation, le compte devrait peut-être être désactivé.

Priorité : Faible

Méthodologie : boîte blanche

Risque : 1.7 (Impact : 2.9, Exploitabilité : 3.1) CVSS : (AV:L/AC:S/AU:S/C:N/I:P/A:N/).

Informations : [landscape, libuuid, tomcat6, user]

Configuration / [path] Le fichier n'exporte pas de paramètre initial pour PATH.	**Faible**

Description : Le fichier n'exporte pas de paramètre initial pour PATH.

Résolution : Un paramètre pour la variable PATH devrait être configuré dans les lieux par défaut pour les programmes shell de connexion (/etc/profile, /etc/csh.login, etc.).

Priorité : Faible

Méthodologie : boîte blanche

Risque : 1.7 (Impact : 2.9, Exploitabilité : 3.1) CVSS : (AV:L/AC:S/AU:S/C:N/I:P/A:N/).

Informations : [/etc/profile]

Configuration / [pass] Le compte n'a pas un shell valide.	**Faible**

Description : Le compte affiché n'a pas un programme ou shell de connexion valide. Ceux-ci sont définis dans /etc/shells.

Résolution : Envisager la suppression des comptes

Priorité : Faible

Méthodologie : boîte blanche

Risque : 1.4 (Impact : 2.9, Exploitabilité : 2.5) CVSS : (AV:L/AC:S/AU:M/C:P/I:N/A:N/).

Informations :
- Login: sshd - Shell: /usr/sbin/nologin
- Login: sync - Shell: /bin/sync

Annexes

Annexe A : Glossaire

- **Cible** - terme générique qui caractérise un serveur, poste de travail, imprimante, routeur ou n'importe quel élément accessible du réseau.
- **Correctif** - *patch* en anglais. C'est une mise à jour corrigeant une ou plusieurs vulnérabilités. Elle s'applique à un système d'exploitation, une base de données, un programme ou un paquet (sous Unix).
- **CVSS** - Common Vulnerability Scoring System. C'est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.
  La métrique de base (*Base metric*) est explicitée par le vecteur de 6 lettres indiqué pour expliciter chaque risque.
- **DBMS** - *DataBase Management System*. Système de gestion de base de données en français.
- **Exploitabilité** - facilité à exploiter une vulnérabilité. Plus l'exploitabilité est élevée, plus les compétences requises pour exploiter la faille sont faibles et donc plus une menace a de chance de survenir.
- **Fonction** - la fonction du contrôle détermine la cause d'une vulnérabilité. Par exemple, une injection SQL a pour cause une erreur de développement, un mot de passe trivial découle d'un contrôle d'accès mal paramétré. La configuration d'un service peut également entraîner des fuites d'informations.
- **Impact** - effet potentiel sur la disponibilité du service, la confidentialité ou l'intégrité des informations stockées sur la machine concernée.
- **Nom DNS** - (*Domaine Name Server*). Nom obtenu par résolution inverse auprès du ou des serveurs DNS.
- **Nom Netbios** - Nom d'une machine appartenant à un domaine ou un groupe de travail.
- **Objet** - ce sur quoi porte la vulnérabilité : systèmes d'exploitation (comprenant les applications installées sur ces systèmes), bases de données, sites/serveurs web ou réseau.
- **Priorité** - les 3 niveaux (Élevé, Majeur, Critique) suggérés dans le rapport permettent de traiter en priorité les vulnérabilités de risque maximal, dites critiques.
  Note : toutes les vulnérabilités remontées dans ce rapport sont de risque élevé (note CVSS supérieure à 7) et doivent donc toutes être considérées.
- **Risque** - risque potentiel d'une menace exploitant la vulnérabilité. Le risque final d'une vulnérabilité prend également en compte le risque intrinsèque de la machine ciblée (c'est-à-dire la valeur des informations qui y sont stockées ou l'importance opérationnelle des services qu'elle fournit) et les contrôles pouvant venir diminuer ce risque (traces d'audit, plan de secours, etc).
  Le calcul du risque est explicité dans ce document (partie Métrique de base).
- **Vulnérabilité** - faille de sécurité pouvant compromettre la disponibilité du service, la confidentialité ou l'intégrité des informations stockées sur la machine concernée.

Annexe B : Outils d'audit

- **Aircrack** est une suite d'outils d'audit wifi permettant d'analyser la sécurité de points d'accès wifi. Auteur et mainteneur : Thomas d'Otreppe.
- **db2getprofile** (de la suite db2utils) récupère le profil d'accès aux bases de données DB2 et fournit en particulier la liste des instances et bases de données. Auteur et mainteneur : Patrik Karlsson.
- **dhcping** est un scanner de serveurs DHCP et BOOTP. Auteur et mainteneur : Edwin Groothuis.
- **dig** - fourni avec le package dnsutils - permet entre autres d'interroger un serveur DNS pour obtenir la liste des machines d'un domaine par transfert de zone. Auteur et mainteneur : Internet Systems Consortium, Inc (ISC).
- **fimap** est un outil open source de tests de pénétration qui automatise le processus de détection de failles d'inclusion de fichiers. Auteur et mainteneur : Iman Karim.
- **flasm** désassemble les menus SWF pour y relever les liens vers les autres pages du site. Auteur et mainteneur : Ben Schleimer.
- **git** est un logiciel de gestion de versions décentralisé. Auteur et mainteneur : Linus Torvalds.
- **Medusa** permet de tester des identifiants de connexion sur de nombreux services (FTP, SSH, SNMP, SMTP...). Auteur et mainteneur : JoMo-Kun.
- **mit-krb5** implémente sous unix le protocole kerberos utilisé pour l'authentification au domaine (dans le cas des domaines gérés par un active directory à partir de Windows 2003). Auteur et mainteneur : Massachusetts Institute of Technology.
- **MSSQLScan** permet d'obtenir quelques informations sur les bases de données Microsoft SQL Server. Auteur et mainteneur : Patrik Karlsson.
- **nbtscan** reprend les fonctionnalités de la commande 'nbtstat' de Windows en fournissant une liste de tous les services Netbios ouverts. Auteur et mainteneur : Stephen Friedl.
- **Nmap** est un célèbre scanner de ports utilisé pour détecter quels sont les services ouverts sur les machines. Auteur et mainteneur : Gordon Lyon.
- **OpenVAS** intègre plusieurs milliers de tests sur l'application des correctifs (*patch management*) OS, applicatifs, DBMS, etc. Auteur et mainteneur : OpenVAS team.
- **rpcclient** permet d'accéder aux "tubes nommés" et d'exécuter des commandes MS RPC. Il fait partie de la suite Samba. Auteur et mainteneur : Samba team.
- **SidGuesser** permet de découvrir les instances Oracle lorsqu'elles ne sont pas transmises par le listener (attaque par dictionnaire). Auteur et mainteneur : Patrik Karlsson.
- **snmpwalk** fait partie du package net-snmp et permet de parcourir les informations fournies par le protocole SNMP. Auteur et mainteneur : Net-SNMP.
- **SMBAT**(SaMBa Auditing Tools) comprend l'outil smbdumpusers permettant de lister les utilisateurs de Windows NT/2000. Auteur et mainteneur : Patrik Karlsson.
- **samba** est une suite de programmes permettant d'interopérer avec les services Windows. Auteur et mainteneur : Samba team.
- **sqlmap** est un outil open source de tests de pénétration qui automatise le processus de détection de failles d'injection SQL. Auteur et mainteneur : Bernardo Damele.
- **sslscan** détermine quels algorithmes de chiffrement un serveur SSL propose (typiquement dans le cas d'un site https). Auteur et mainteneur : Ian Ventura-Whiting.
- **Tiger** est un outil d'audit et de détection d'intrusion pour Unix. Auteur et mainteneur : Tiger.
- **tnscmd10g** permet de recenser les instances des bases de données Oracle (versions 10g et 11g incluses). Auteur : James W. Abendschan, Mainteneur : Saez Scheihing.
- **WhatWeb** identifie les systèmes de gestion de contenu (CMS), plateformes de blogs, stats / packages d'analyse, et les bibliothèques javascript. Auteur et mainteneur : Brendan Coles.
- **wdiff** est une interface de comparaison de fichiers sur une base de mot par mot. Auteur et mainteneur : Denver Gingerich.

Annexe C : Génération du rapport

- **La librairie eZ Components** a permis de générer en PHP l'ensemble des graphiques contenus dans ce rapport. Auteur et mainteneur : eZ Systems.
- **wkhtmltopdf** (lire : WebKit HTML to PDF) combine la force du moteur de rendu XHTML/CSS WebKit (utilisé par Chrome et Safari par exemple) et sa librairie de rendu PDF.

- **PostgreSQL** est une base de données relationnelle. Auteur et mainteneur : PostgreSQL Global Development Group.

Auteur et mainteneur : Jakob Truelsen.

Légal

En respect de la LCEN (Loi pour la Confiance dans l'Economie Numérique, article 323-3-1 du 21 juin 2004), la solution DenyAll est exclusivement mise à disposition d'entreprises légitimes et d'utilisateurs dont la fonction justifie la réalisation d'audits de sécurité.
En acceptant la licence d'utilisation de DenyAll, l'utilisateur s'engage à respecter la loi Godfrain du 6 janvier 1988 punissant l'intrusion non autorisée dans un système informatique.

Copyright