Audit report

27 July 2015, 11:59:39 - UTC

Tool version	5.6
Number of scanned machines	4
Number of identified vulnerabilities	151

Table of contents

Introduction

The audit tool DenyAll Vulnerability Manager Enterprise Edition enhances the identification of potential IT security vulnerabilities and the risk they could generate if they were exploited by an evil attacker.

The first part of this report brings a brief and executive summary of the security vulnerabilities identified. The second part lists all these vulnerabilities coupled with an assessment of their potential risks and a disclosure to help you understand and remediate them. Finally, the first appendix lists all the servers and services discovered during the scan.

Methodology

This report is not meant to be exhaustive and thus, does not replace the analysis an expert in pentesting could make. Moreover, all the information contained in this report should be validated by the administrator of the system targeted by the audit, in order to avoid any vulnerability mistakenly identified by the tool ("false positive").

Risk assessment

The risk assessment used in this report for rating each vulnerability relies on the Common Vulnerability Scoring System (CVSS) which considers two factors:

- the potential impact of an attack exploiting this vulnerability, in terms of availability of the application, confidentiality and integrity of the information,
- the exploitability of the vulnerability, as an easy-to-exploit vulnerability increases the number of potential attackers and thus, the likelihood of an attack.

The CVSS ratings (base rating, impact and exploitability) spread between 0 and 10.

Priorization of vulnerabilities

The priority suggested for each vulnerability falls into five levels: critical priority (CVSS base score equals 10), major (base score between 8 and 10), high (base score between 7 and 8), major (base score between 4 and 7) and low (base score lower than 4).

In order to determine the real risk induced by each vulnerability, the potential impact must be weighted by the asset value (for instance, the operational criticality of an application or the value of the information that could be compromised), and the exploitability, by the company exposure (for instance, financial activities motivate more attacks than others).

Finally, these risks may be mitigated by specific controls, either perventive, dissuasive or palliative.

Management Report

Summary

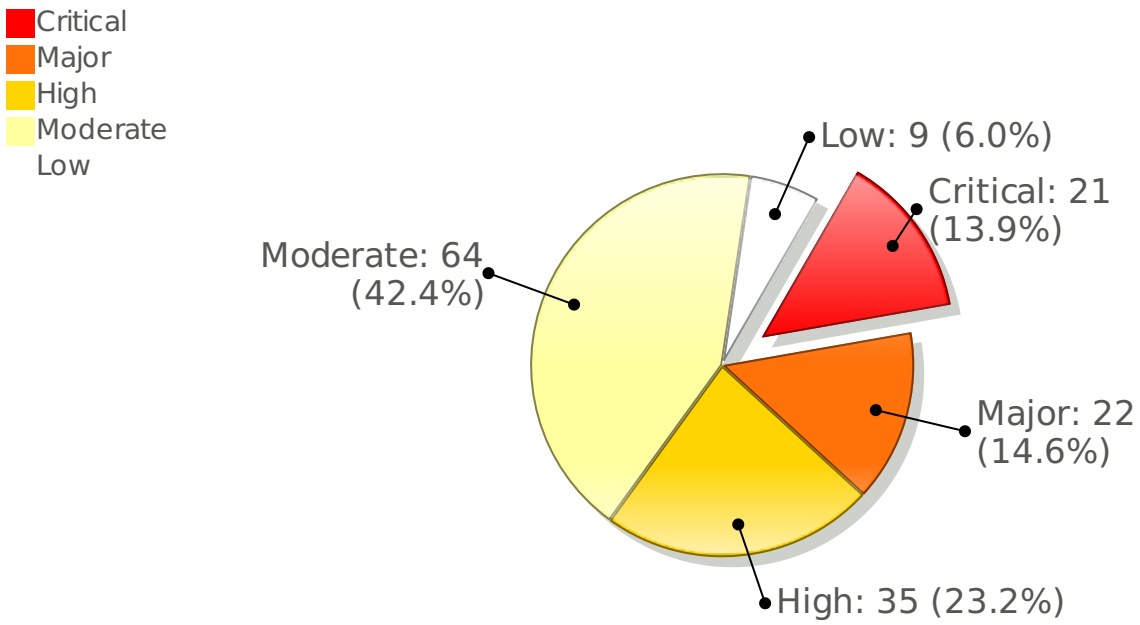
Among the 4 tested servers, 4 have at least one vulnerability. **4** of them require all your attention because **critical priority vulnerabilities have been detected on them**.

These vulnerabilities are graphically presented below and detailed in the technical report.

	Risques					
	Critical	Major	High	Moderate	Low	**TOTAL**
DBMS	8	6	7	12	1	34
Network	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

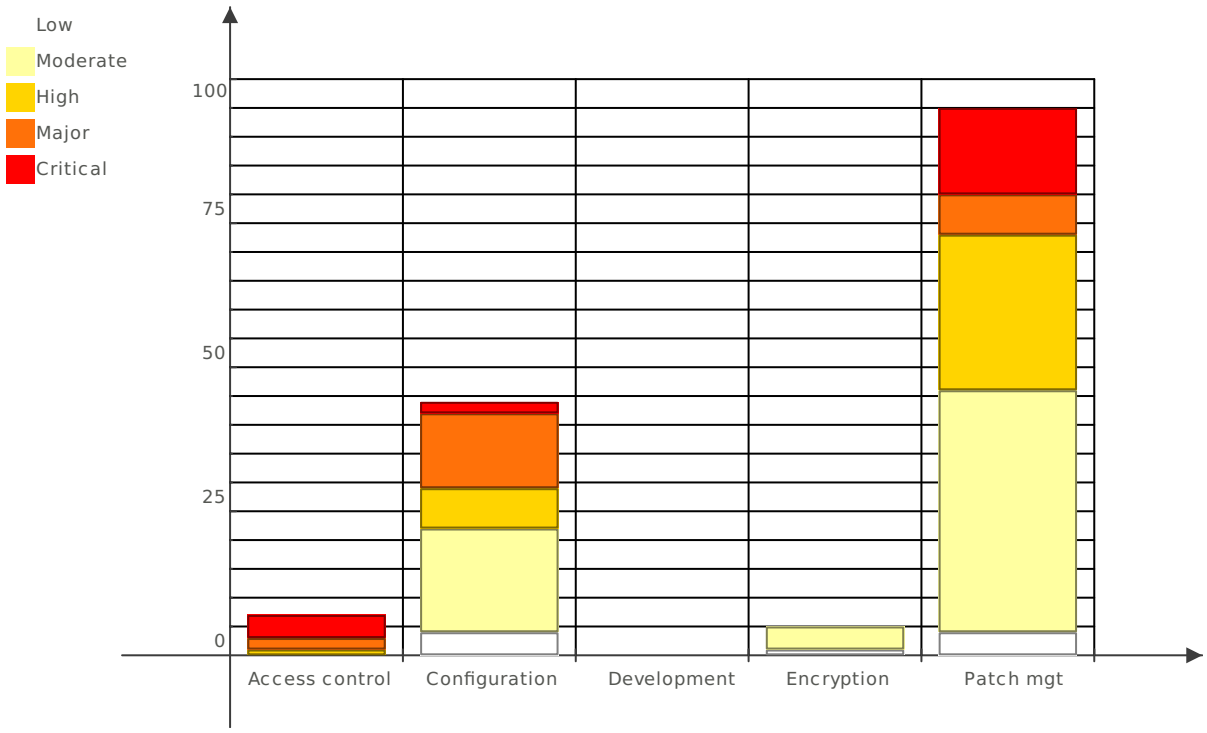
Vulnerabilities ordered by priority

This chart shows the number of identified vulnerabilities ordered by priority.

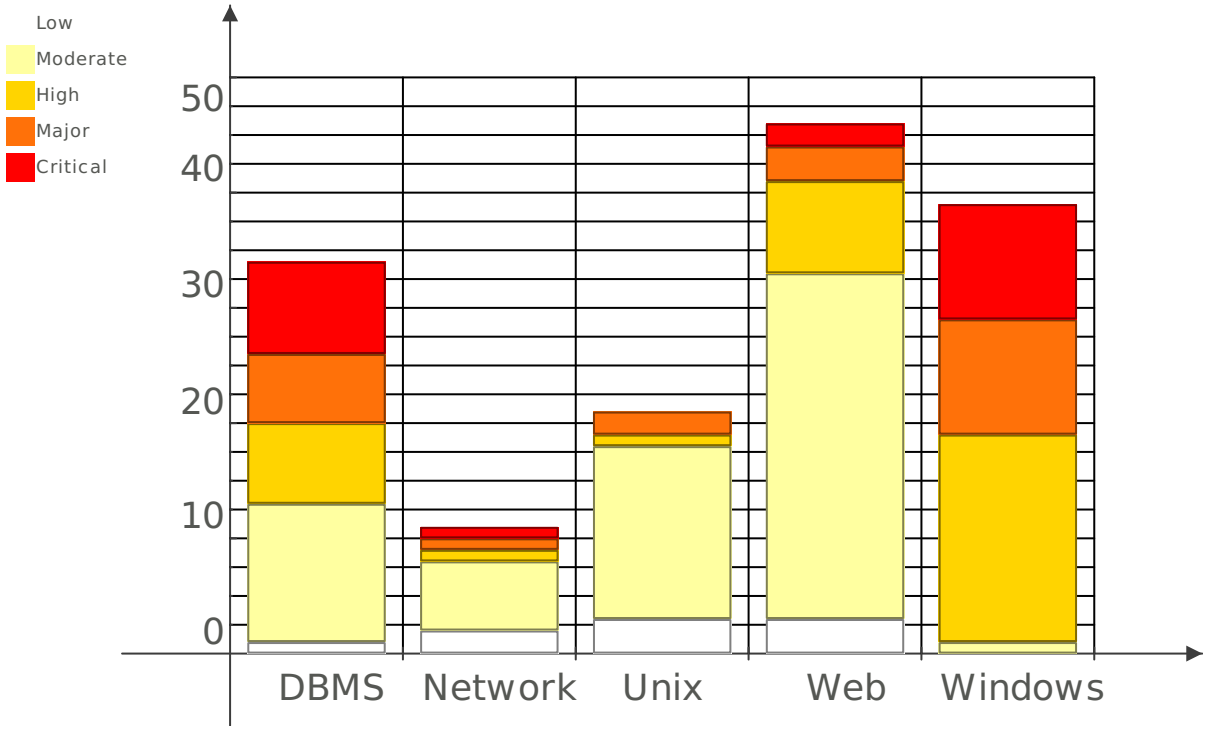


Vulnerabilities ordered by function and object

This chart shows the number of vulnerabilities ordered by control function.

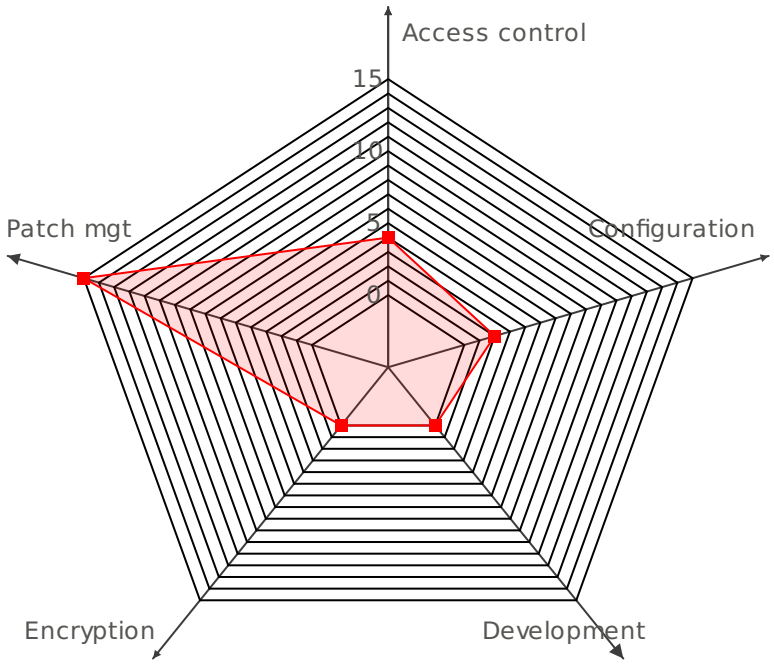


This chart shows the number of vulnerabilities ordered by control object.

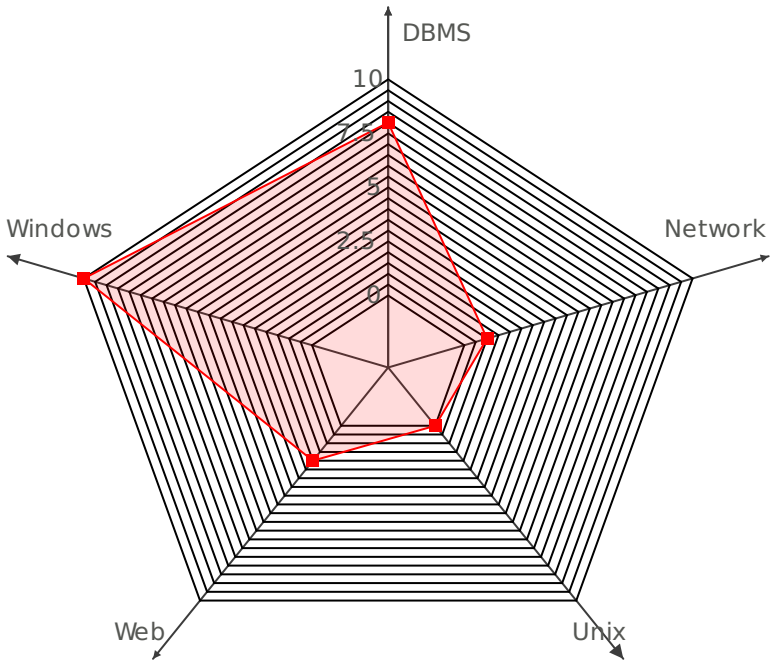


Critical priority vulnerabilities, by function and object

This chart shows the number of critical priority vulnerabilities ordered by control function.

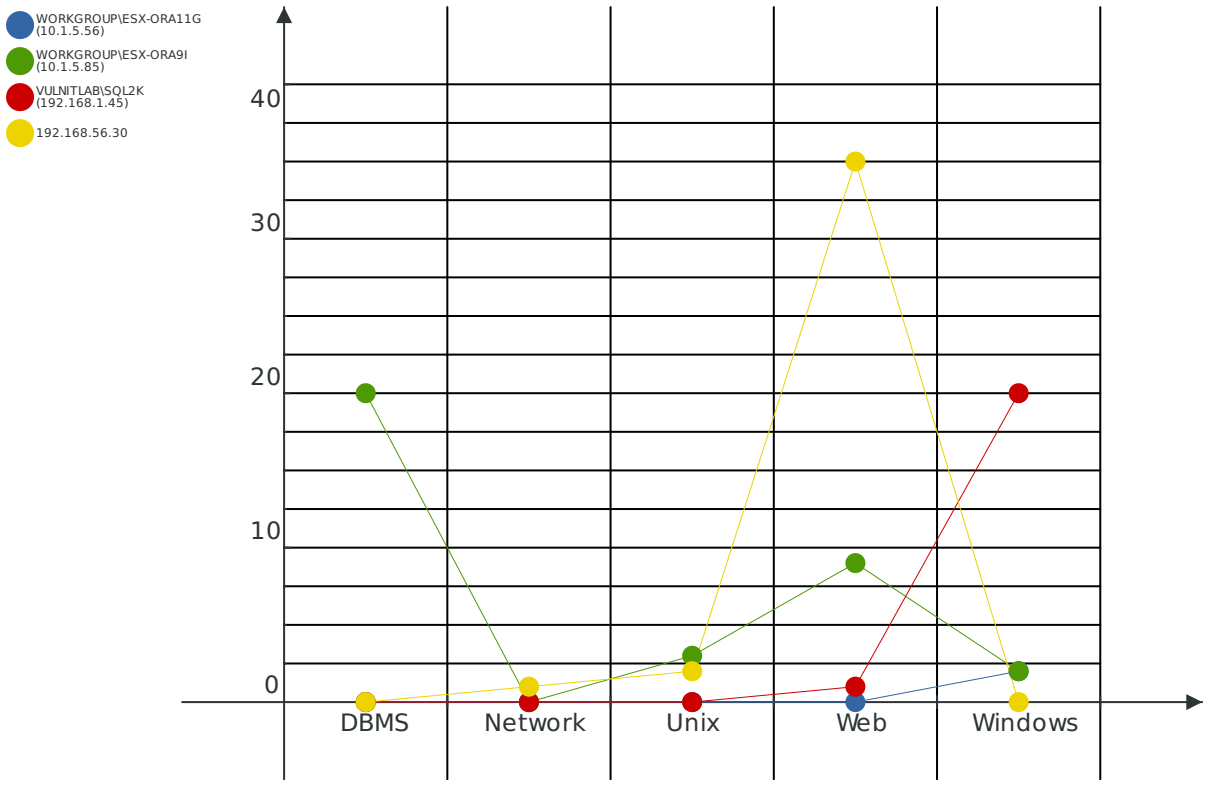


This chart shows the number of critical priority vulnerabilities classified by control object.



Number of missing patches, ordered by IP and objet

This chart presents the number of missing patches for each target ordered by control object.



Technical report

Inventory

WORKGROUP\ESX-ORA11G (10.1.5.56)

Informations on remote machine:

- DNS : esx-ora11g
- NetBios : WORKGROUP\ESX-ORA11G
- Free name : WORKGROUP\ESX-ORA11G

Last scanned: 2013-08-13 08:41:35

Validated administrator account: no

Target tested: yes

Number of vulnerabilites:

- Critical: 4
- Major: 10
- High: 2
- Moderate: 5
- Low: 0

Open ports: 7

Services:

- 135/tcp : RPC - Microsoft EPMAP - not tested
- 137/udp : Netbios name service - not tested
- 139/tcp : NETBIOS Services - not tested
- 445/tcp : SMB - Microsoft File Sharing - not tested
- 1025/tcp : RPC - Microsoft EPMAP - not tested
- 1031/tcp : BBN IAD - not tested
- 1521/tcp : Oracle - not tested

WORKGROUP\ESX-ORA9I (10.1.5.85)

Informations on remote machine:

- DNS : esx-ora9i
- NetBios : WORKGROUP\ESX-ORA9I
- Free name : WORKGROUP\ESX-ORA9I

Last scanned: 2013-08-13 08:41:35

Validated administrator account: no

Target tested: yes

Number of vulnerabilites:

- Critical: 8
- Major: 4
- High: 8
- Moderate: 21
- Low: 2

Open ports: 11

Services:

- 80/tcp : HTTP - World Wide Web - not tested
- 135/tcp : RPC - Microsoft EPMAP - not tested
- 137/udp : Netbios name service - not tested
- 139/tcp : NETBIOS Services - not tested
- 443/tcp : HTTPS - Secure HTTP - not tested
- 445/tcp : SMB - Microsoft File Sharing - not tested
- 1025/tcp : RPC - Microsoft EPMAP - not tested
- 1032/tcp : BBN IAD - not tested
- 1521/tcp : Oracle - not tested
- 2100/tcp : FTP - File Transfer Protocol - not tested
- 8080/tcp : HTTP - World Wide Web - not tested

VULNITLAB\SQL2K (192.168.1.45)

Informations on remote machine:

- DNS : sql2k
- NetBios : VULNITLAB\SQL2K
- Free name : VULNITLAB\SQL2K

Last scanned: 2013-08-13 09:42:21

Validated administrator account: no

Target tested: yes

Number of vulnerabilites:

- Critical: 8
- Major: 3
- High: 18
- Moderate: 1
- Low: 0

Open ports: 23

Services:

- 7/tcp : echo - not tested
- 9/tcp : discard server - not tested
- 13/tcp : daytime - not tested
- 17/tcp : Quote of the Day - not tested
- 19/tcp : ttytst source Character Generator - not tested
- 25/tcp : SMTP - Simple Mail Transfer Protocol - not tested
- 42/tcp : WINS - Windows Internet Naming Service - not tested
- 53/tcp : DNS - Domain Name Server - not tested
- 80/tcp : HTTP - World Wide Web - not tested
- 135/tcp : RPC - Microsoft EPMAP - not tested
- 139/tcp : NETBIOS Services - not tested
- 161/udp : SNMP - not tested
- 443/tcp : HTTPS - Secure HTTP - not tested
- 445/tcp : SMB - Microsoft File Sharing - not tested
- 515/tcp : Spooler - LPD - not tested
- 548/tcp : AFP - Apple Filing Protocol - not tested
- 1029/tcp : ms-lsa - not tested
- 1032/tcp : BBN IAD - not tested
- 1033/tcp : netinfo-local - not tested
- 1036/tcp : pcg-radar - not tested
- 1040/tcp : netarx - not tested
- 1433/tcp : MSSQL - Microsoft SQL Server - not tested
- 3372/tcp : MDTC - Microsoft Distributed Transaction Coordinator - not tested

192.168.56.30

Informations on remote machine:

- DNS : unknown
- NetBios : unknown

Last scanned:

Validated administrator account: yes

Target tested: no

Number of vulnerabilites:

- Critical: 1
- Major: 5
- High: 7
- Moderate: 37
- Low: 7

Open ports: 7

Services:

- 22/tcp : SSH - Secure Shell Login [OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)] - not tested
- 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)] - not tested
- 139/tcp : NETBIOS Services [Samba smbd 3.X (workgroup: WORKGROUP)] - not tested
- 143/tcp : IMAP - Internet Mail Access Protocol [Courier Imapd (released 2008)] - not tested
- 445/tcp : NETBIOS Services [Samba smbd 3.X (workgroup: WORKGROUP)] - not tested
- 5001/tcp : commplex-link [Oracle VM Manager] - not tested
- 8080/tcp : HTTP - World Wide Web - not tested

Summary

- WORKGROUP\ESX-ORA11G (10.1.5.56) - Patch mgt / Windows patch management - Critical
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Role does not have a password verification function - Critical
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Access control / Trivial SYSDBA account - Critical
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Well-known instance name - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / No firewall found - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Software disabled - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Access control / Trivial account - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Windows configuration - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Guest account enabled - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Minimum password length too low - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Passwords complexity requirements disable - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Password never expires - Major
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Password history too low - Major

- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Unused accounts should be locked - High
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Machine not in domain - High
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Limit of ROLES should be enabled - Moderate
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / AUDIT_SYS_OPERATIONS should be set to TRUE - Moderate
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / GLOBAL_NAMES should be set to TRUE - Moderate
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / os_authent_prefix should be null string - Moderate
- WORKGROUP\ESX-ORA11G (10.1.5.56) - Configuration / Minimum password age too low - Moderate
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Database patch management - Critical
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Web patch management - Critical
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Windows patch management - Critical
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Access control / Trivial SYSDBA account - Critical
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Access control / Trivial account - Major
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Configuration / Instance list available - High
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Configuration / Windows configuration - High
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Encryption / Weak SSL encryption - Moderate
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Patch mgt / Unix patch management - Moderate
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Encryption / SSLv2 - Moderate
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Encryption / Invalid SSL certificate - Moderate
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Encryption / SSLv3.0/TLSv1.0 Weak CBC Mode - Moderate
- WORKGROUP\ESX-ORA9I (10.1.5.85) - Encryption / SSL Renegotiation - Low
- VULNITLAB\SQL2K (192.168.1.45) - Access control / Open share folder - Critical
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / SNMP community (write) - Critical
- VULNITLAB\SQL2K (192.168.1.45) - Access control / Trivial account - Critical
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Windows patch management - Critical
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / SNMP community (read) - Major
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / RPC information leakage - Major
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Users list available - High
- VULNITLAB\SQL2K (192.168.1.45) - Access control / Open mail relay - High
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Instance list available - High
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Web patch management - High
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Discard service - Moderate
- 192.168.56.30 - Patch mgt / Web patch management - Critical
- 192.168.56.30 - Configuration / [device] Device has world permissions - Major
- 192.168.56.30 - Configuration / [account] Bad permissions on the parent home directory. - Major
- 192.168.56.30 - Configuration / Users list available - High
- 192.168.56.30 - Patch mgt / Unix patch management - High
- 192.168.56.30 - Configuration / Web configuration - Moderate
- 192.168.56.30 - Configuration / [local network] Listening processes. - Moderate
- 192.168.56.30 - Configuration / [network] There is no FTPUSERS file. - Moderate
- 192.168.56.30 - Configuration / [ssh] The PasswordAuthentication directive is set to an unapproved value. - Moderate
- 192.168.56.30 - Configuration / [root] Remote root login allowed in SSHD_CONFIG -

Moderate
- 192.168.56.30 - Configuration / [inet] The port for service is also assigned to another service. - Moderate
- 192.168.56.30 - Configuration / [pass] Login is disabled, but has a valid shell. - Moderate
- 192.168.56.30 - Patch mgt / Network patch management - Moderate
- 192.168.56.30 - Configuration / [cron] Use of cron is not restricted. - Moderate
- 192.168.56.30 - Configuration / [cron] Root crontab does not exist. - Moderate
- 192.168.56.30 - Configuration / [account] User's home directory is not accessible. - Moderate
- 192.168.56.30 - Configuration / [pass] Integrity of password files questionable. - Moderate
- 192.168.56.30 - Configuration / [local network] Listening processes. - Moderate
- 192.168.56.30 - Configuration / Network configuration - Low
- 192.168.56.30 - Configuration / [account] Login ID appears to be a dormant account. - Low
- 192.168.56.30 - Configuration / [path] File does not export an initial setting for PATH. - Low
- 192.168.56.30 - Configuration / [pass] Login ID does not have a valid shell. - Low

WORKGROUP\ESX-ORA11G (10.1.5.56)

Patch mgt / Windows patch management — Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Missing patch: MS10-012
  Summary: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
  Test script and information relative to this vulnerability: 902269
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0022 , CVE-2010-0231
- Missing patch: MS09-001
  Summary: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
  Test script and information relative to this vulnerability: 900233
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-4114 , CVE-2008-4834 , CVE-2008-4835

Configuration / Role does not have a password verification function — Critical

Description: Passwords should be at least 10 characters or more and alphanumeric. This should be ensured using a password verification function.

Remediation: Create the function, then:
ALTER PROFILE profile_name LIMIT PASSWORD_VERIFICATION_FUNCTION new_value

Priority: Critical

Methodology: white box

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

Informations:
- DEFAULT

Access control / Trivial SYSDBA account — Critical

Description: This Oracle database can be accessed using a trivial account having SYSDBA privileges (i.e. well known password, see the list of instances and accounts below).

Remediation: Change the passwords of these accounts or lock them.

Priority: Critical

Methodology: black box

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

Informations: SID : ORA11G (SYS/Compl3x3)

Configuration / Well-known instance name — Major

Description: The instance name of this database is well known (i.e. this name is often used in Oracle naming conventions).

Remediation: Change the name of this instance.

Priority: Major

Methodology: black box

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

Informations: [ORA11G]

Configuration / No firewall found — Major

Description: No firewall have been found on the machine

Remediation: Install a firewall

Priority: Major

Methodology: white box

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

References: PCI DSS 1.4

Configuration / Software disabled — Major

Description: Security software is disabled

Remediation: Enable the product

Priority: Major

Methodology: white box

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

Informations: WindowsFirewall - Domain profile, WindowsFirewall - Standard profile

Access control / Trivial account — Major

Description: This Oracle database can be accessed using a trivial account (i.e. well known password, see the list of instances and accounts below).

Remediation: Change the passwords of these accounts or lock them.

Priority: Major

Methodology: black box

Risk: 9.3 (Impact: 10.0, Exploitability: 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 / Windows configuration — Major

Description: The current configuration of this Windows server shows the weaknesses identified below.

Remediation: Improve the configuration of this Windows server.

Priority: Major

Methodology: black box

- Summary: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
  Test script and information relative to this vulnerability: 801991
  Risk: 8.8 (Impact: 8.3, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-1999-0519

Configuration / Guest account enabled — Major

Description: Guest account is enabled

Remediation: Disable domain and local guest accounts

Priority: Major

Methodology: white box

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

Informations: Invité

Configuration / Minimum password length too low — Major

Description: A password too short increases probability of a successful brute-force attack

Remediation: Increase minimum password length (at least 6 characters)

Priority: Major

Methodology: white box

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

References: PCI DSS 8.5.10

Configuration / Passwords complexity requirements disable — Major

Description: Passwords complexity requirements prevents users to define easy passwords

Remediation: Enable passwords complexity requirements

Priority: Major

Methodology: white box

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

References: PCI DSS 8.5.11

Configuration / Password never expires	Major

Description: The password never expires, which increases probability of a successful brute-force attack

Remediation: Remove the option which allows non-expiring password

Priority: Major

Methodology: white box

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

References: PCI DSS 8.5.9

Informations: Administrateur

Configuration / Password history too low	Major

Description: Password history prevent users to reuse old passwords

Remediation: Increase the password history value (at least 4)

Priority: Major

Methodology: white box

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

References: PCI DSS 8.5.12

Configuration / Unused accounts should be locked	High

Description: Unused accounts may be a potential attack vector, so you should lock them.

Remediation: ALTER USER <user> ACCOUNT LOCK;

Priority: High

Methodology: white box

Risk: 7.9 (Impact: 8.3, Exploitability: 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 not in domain	**High**

Description: Machine is not member of a Windows domain

Remediation: Add the machine to the domain

Priority: High

Methodology: white box

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

Informations: DenyAll.local, WORKGROUP, DENYALL

Configuration / Limit of ROLES should be enabled	**Moderate**

Description: Limited number of ROLES enabled.

The CIS benchmark recommendation is 30 but with SYS getting around 20 right out of the box, 50 is a more realistic target.

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

Priority: Moderate

Methodology: white box

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

Informations:
- Current value: NONE

Configuration / AUDIT_SYS_OPERATIONS should be set to TRUE	**Moderate**

Description: CIS recommendation. Default is FALSE. Set to TRUE to audit all activity

performed as SYSDBA or SYSOPER.

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

Priority: Moderate

Methodology: white box

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

Informations:
- Current value: 0

Configuration / GLOBAL_NAMES should be set to TRUE	Moderate

Description: Setting GLOBAL_NAMES=TRUE ensures that the name of a database link matches the name of the remote database.

This is a CIS benchmark recommendation. Be careful with applications that have more than 1 link to the same remote DB (Oracle E-Business Suite, for instance) since you'll need to specify unique names that therefore cannot all match the remote DB name.

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

Priority: Moderate

Methodology: white box

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

Informations:
- Current value: None

Configuration / os_authent_prefix should be null string	Moderate

Description: CIS recommendation is to set os_authent_prefix to the null string. The default is OPS$.

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

Priority: Moderate

Methodology: white box

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

Informations:
- Current value: ora11g

Configuration / Minimum password age too low	Moderate

Description: Minimum password age too low allow a user to change his password many times to redefine it to its actual value, bypasssing the history policy

Remediation: Increase the minimum password age (recommended: 1 day)

Priority: Moderate

Methodology: white box

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

References: PCI DSS 8.5.9

WORKGROUP\ESX-ORA9I (10.1.5.85)

Patch mgt / Database patch management — Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server Multiple Unspecified Vulnerabilities - Jan 08
  Test script and information relative to this vulnerability: 802528
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: 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
- Affected package: -ORACLE DATABASE AND APPLICATION SERVER
  Summary: Oracle Database Server and Application Server Ultra Search Component Unspecified Vulnerability
  Test script and information relative to this vulnerability: 802524
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-0347
- Affected package: -ORACLE DATABASE AND APPLICATION SERVER
  Summary: Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities
  Test script and information relative to this vulnerability: 802526
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: 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
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server Multiple Unspecified Vulnerabilities
  Test script and information relative to this vulnerability: 802527
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: 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
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server Multiple Unspecified Vulnerabilities - April 06
  Test script and information relative to this vulnerability: 802538
  Risk: 9.1 (Impact: 10.0, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2006-1868 , CVE-2006-1871 , CVE-2006-1872 , CVE-2006-1873 , CVE-2006-1874
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server Multiple Vulnerabilities - Oct 06
  Test script and information relative to this vulnerability: 802520
  Risk: 9.1 (Impact: 10.0, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
  References: 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
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server MDSYS.MD Buffer Overflows and Denial of Service Vulnerabilities
  Test script and information relative to this vulnerability: 802523
  Risk: 8.5 (Impact: 9.2, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:N/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2007-0272
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server 'RDBMS' component Denial of Service Vulnerability
  Test script and information relative to this vulnerability: 802539
  Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
  References: PCI DSS 6.1 , CVE-2007-5506
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server Upgrade and Downgrade Component Multiple Vulnerabilities

Test script and information relative to this vulnerability: 802519
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
References: PCI DSS 6.1 , CVE-2007-2113 , CVE-2007-2118

- Summary: Oracle 9iAS SOAP Default Configuration Vulnerability
  Test script and information relative to this vulnerability: 11227
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2001-1371
- Affected package: -ORACLE DATABASE AND APPLICATION SERVER
  Summary: Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities
  Test script and information relative to this vulnerability: 802525
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2006-0435
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database Server Multiple Components Multiple Vulnerabilities
  Test script and information relative to this vulnerability: 802522
  Risk: 6.5 (Impact: 6.4, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2007-3855
- Summary: Oracle 9iAS default error information disclosure
  Test script and information relative to this vulnerability: 11226
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2001-1372
- Summary: Oracle 9iAS access to SOAP documentation
  Test script and information relative to this vulnerability: 11223
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1
- Summary: Oracle 9iAS Jsp Source File Reading
  Test script and information relative to this vulnerability: 10852
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2002-0562
- Summary: Oracle 9iAS Java Process Manager
  Test script and information relative to this vulnerability: 10851
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2002-0563
- Summary: Oracle 9iAS Dynamic Monitoring Services
  Test script and information relative to this vulnerability: 10848
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2002-0563
- Summary: Oracle 9iAS iSQLplus XSS
  Test script and information relative to this vulnerability: 12112
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1
- Affected package: -ORACLE DATABASE
  Summary: Oracle Database 'XML DB component' Unspecified vulnerability
  Test script and information relative to this vulnerability: 902043
  Risk: 4.0 (Impact: 2.9, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2010-0851
- Summary: Oracle 9iAS SOAP configuration file retrieval
  Test script and information relative to this vulnerability: 11224
  Risk: 2.1 (Impact: 2.9, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2002-0568

Patch mgt / Web patch management — Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Affected package: -OPENSSL
  Summary: OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability
  Test script and information relative to this vulnerability: 100527

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: PCI DSS 6.1 , CVE-2009-3245

- Affected package: -OPENSSL
  Summary: OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability
  Test script and information relative to this vulnerability: 100668
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2010-0742
- Summary: mod_ssl hook functions format string vulnerability
  Test script and information relative to this vulnerability: 13651
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2004-0700
- Summary: http TRACE XSS attack
  Test script and information relative to this vulnerability: 11213
  Risk: 5.8 (Impact: 4.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2003-1567 , CVE-2004-2320
- Summary: Allaire JRun directory browsing vulnerability
  Test script and information relative to this vulnerability: 10814
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2001-1510
- Summary: JServ Cross Site Scripting
  Test script and information relative to this vulnerability: 10957
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1
- Summary: Web Server Cross Site Scripting
  Test script and information relative to this vulnerability: 10815
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1
- Summary: Apache Web Server ETag Header Information Disclosure Weakness
  Test script and information relative to this vulnerability: 103122
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2003-1418
- Summary: FastCGI samples Cross Site Scripting
  Test script and information relative to this vulnerability: 10838
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1

Patch mgt / Windows patch management — Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Missing patch: MS09-001
  Summary: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
  Test script and information relative to this vulnerability: 900233
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-4114 , CVE-2008-4834 , CVE-2008-4835
- Missing patch: MS10-012
  Summary: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
  Test script and information relative to this vulnerability: 902269
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0022 , CVE-2010-0231

Access control / Trivial SYSDBA account — Critical

Description: This Oracle database can be accessed using a trivial account having SYSDBA

privileges (i.e. well known password, see the list of instances and accounts below).

Remediation: Change the passwords of these accounts or lock them.

Priority: Critical

Methodology: black box

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

Informations: SID : ORA9I (SYS/ORACLE)

Access control / Trivial account	Major

Description: This Oracle database can be accessed using a trivial account (i.e. well known password, see the list of instances and accounts below).

Remediation: Change the passwords of these accounts or lock them.

Priority: Major

Methodology: black box

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

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

Configuration / Instance list available	High

Description: The Oracle database configuration enables to obtain the list of all the database instances.

Remediation: Migrate to a newer version (Oracle 10g minimum) and make sure the listener.ora file does not contain the line "LOCAL_OS_AUTHENTICATION_LISTENER = OFF".

Priority: High

Methodology: black box

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

Informations: [ORA9I]

Configuration / Windows configuration	High

Description: The current configuration of this Windows server shows the weaknesses identified below.

Remediation: Improve the configuration of this Windows server.

Priority: High

Methodology: black box

- Summary: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
  Test script and information relative to this vulnerability: 801991
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-1999-0519

Encryption / Weak SSL encryption — Moderate

Description: The SSL server allows connections using weak ciphers (which key length is less than 128 bits), which could enable decoding connection credentials and data transfered in a timely manner.

Remediation: Restrict the list of encryption ciphers to only allow those which key length is 128 bits (at least).

Priority: Moderate

Methodology: black box

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

References: 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 / Unix patch management — Moderate

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Moderate

Methodology: black box

- Affected package: -OPENSSL
  Summary: OpenSSL 'ssl3_get_record()' Remote Denial of Service Vulnerability
  Test script and information relative to this vulnerability: 100587
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2010-0740
- Summary: Apache Connection Blocking Denial of Service
  Test script and information relative to this vulnerability: 12280
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2004-0174
- Affected package: -OPENSSL
  Summary: OpenSSL 'dtls1_retrieve_buffered_fragment()' Remote Denial of Service Vulnerability
  Test script and information relative to this vulnerability: 100588
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2010-0433

Encryption / SSLv2 — Moderate

Description: The HTTPS server supports SSLv2 or SSLv3 which is vulnerable to a Man In The Middle attack

Remediation: Disable SSLv2 support on the server

Priority: Moderate

Methodology: black box

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

References: PCI DSS 2.2.2

Informations: SSLv2 supported

Encryption / Invalid SSL certificate	Moderate

Description: Invalid or not trusted certificate

Remediation: Install a valid certificate issued by a trusted certificate authority

Priority: Moderate

Methodology: black box

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

References: PCI DSS 2.2.2

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

Encryption / SSLv3.0/TLSv1.0 Weak CBC Mode	Moderate

Description: The SSL protocol, as used in certain configurations encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses the HTML5 WebSocket API, the Java URLConnection API, or the Silverlight WebClient API, aka a "BEAST" attack.
Theory about this attack is available in Gregory V. Bard publications:
- http://eprint.iacr.org/2004/111.pdf
- http://eprint.iacr.org/2006/136.pdf
A more technical presentation of the attack has been published by Rizzo et Duong:
http://www.educatedguesswork.org/2011/09/security_impact_of_the_rizzodu.html

Remediation: The best way to fix this design flaw is to migrate to TLSv1.1 or TLSv1.2 that fixes it.
But not all clients and serveurs can work with those TLS versions. So there a way to mitigate this flaw that consist to prioritize the RC4 ciphers of SSLv3/TLSv1 and disable the CBC modes.The way to do this depends on the involved server software.

For an Apache web server, you can prioritize the most some TLSv1.2 cipher suite, then RC4 for clients that can only handle TLSv1 this way:
> SSLHonorCipherOrder On
> SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH

The same thing for a Postfix server:
> tls_preempt_cipherlist = yes
> tls_high_cipherlist = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH

Priority: Moderate

Methodology: black box

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

References: 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)

Encryption / SSL Renegotiation	**Low**

Description: The HTTPS server supports unsecure renegotiation which is vulnerable to a Man In The Middle attack

Remediation: Unsecured renegotiation must be disabled

Priority: Low

Methodology: black box

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

References: PCI DSS 2.2.2

Informations: SSL insecure renegotiation supported

VULNITLAB\SQL2K (192.168.1.45)

Access control / Open share folder — Critical

Description: The current configuration allows anyone to access the Windows shares listed below and to the files they contain.

Remediation: Restrict access to this Windows share to the authorized users only.

Priority: Critical

Methodology: black box

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

Informations: [TESTSMB]

Configuration / SNMP community (write) — Critical

Description: A well-known SNMP community (see below) has write access on this server, which allows to remotely administrate the server (in particular, stop this server).

Remediation: Consider migrating to SNMP v3 in order to add authentication. Otherwise, change the community name or restrict the access to a list of allowed users.

Priority: Critical

Methodology: black box

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

Informations: [private]

Access control / Trivial account — Critical

Description: This Microsoft SQL Server database can be accessed using a trivial administrator account (i.e. no password, or same password as login).

Remediation: Change administrator account password, or lock this account.

Priority: Critical

Methodology: black box

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

Informations: SID : SQL2KVINCENT ([sa])

Patch mgt / Windows patch management — Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Missing patch: MS10-012
  Summary: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
  Test script and information relative to this vulnerability: 902269
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0022 , CVE-2010-0231
- Missing patch: MS09-048
  Summary: Microsoft Windows TCP/IP Remote Code Execution Vulnerability (967723)
  Test script and information relative to this vulnerability: 900838
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-4609 , CVE-2009-1925 , CVE-2009-1926
- Missing patch: MS09-001
  Summary: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
  Test script and information relative to this vulnerability: 900233
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-4114 , CVE-2008-4834 , CVE-2008-4835
- Summary: IIS .IDA ISAPI filter applied
  Test script and information relative to this vulnerability: 10695
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2001-0500
- Missing patch: MS03-039
  Summary: Microsoft RPC Interface Buffer Overrun (KB824146)
  Test script and information relative to this vulnerability: 102015
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2003-0528 , CVE-2003-0605 , CVE-2003-0715
- Missing patch: MS09-055
  Summary: Microsoft Windows ATL COM Initialization Code Execution Vulnerability (973525)
  Test script and information relative to this vulnerability: 900880
  Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2009-2493
- Summary: Microsoft RPC Interface Buffer Overrun (823980)
  Test script and information relative to this vulnerability: 11808
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2003-0352
- Missing patch: MS03-007
  Summary: Unchecked Buffer in ntdll.dll (Q815021)
  Test script and information relative to this vulnerability: 11413
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2003-0109
- Missing patch: MS02-050
  Summary: Certificate Validation Flaw Could Enable Identity Spoofing (Q328145)
  Test script and information relative to this vulnerability: 11145
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2002-0862 , CVE-2002-1183
- Missing patch: MS02-055
  Summary: Unchecked Buffer in Windows Help(Q323255)
  Test script and information relative to this vulnerability: 11147
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2002-0693 , CVE-2002-0694
- Missing patch: MS03-043
  Summary: Buffer Overrun in Messenger Service (828035)
  Test script and information relative to this vulnerability: 11888
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2003-0717
- Missing patch: MS02-063
  Summary: Unchecked Buffer in PPTP Implementation Could Enable DOS Attacks (Q329834)
  Test script and information relative to this vulnerability: 11178
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2002-1214
- Missing patch: MS03-041
  Summary: Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)
  Test script and information relative to this vulnerability: 11886
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2003-0660
- Missing patch: MS03-023
  Summary: Buffer Overrun In HTML Converter Could Allow Code Execution (823559)
  Test script and information relative to this vulnerability: 11878
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).

References: PCI DSS 6.1 , CVE-2003-0469
- Missing patch: MS02-006
  Summary: Checks for MS HOTFIX for snmp buffer overruns
  Test script and information relative to this vulnerability: 10865
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2002-0053
- Missing patch: MS02-042
  Summary: Windows Network Manager Privilege Elevation (Q326886)
  Test script and information relative to this vulnerability: 11091
  Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2002-0720
- Summary: Microsoft Windows GP Trap Handler Privilege Escalation Vulnerability
  Test script and information relative to this vulnerability: 800442
  Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2010-0232
- Missing patch: MS02-017
  Summary: MUP overlong request kernel overflow Patch (Q311967)
  Test script and information relative to this vulnerability: 10944
  Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2002-0151
- Missing patch: MS03-045
  Summary: Buffer Overrun in the ListBox and in the ComboBox (824141)
  Test script and information relative to this vulnerability: 11885
  Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2003-0659
- Missing patch: MS02-024
  Summary: Windows Debugger flaw can Lead to Elevated Privileges (Q320206)
  Test script and information relative to this vulnerability: 10964
  Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2002-0367

Configuration / SNMP community (read) — Major

Description: An SNMP service in version 1 or 2 (without authentication) uses a well-known community name (see below) to provide many useful information on the system.

Remediation: Consider migrating to SNMP v3 in order to add authentication. Otherwise, change the community name or restrict the access to a list of allowed users.

Priority: Major

Methodology: black box

Risk: 8.5 (Impact: 7.8, Exploitability: 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 / RPC information leakage	Major

Description: A RPC service provides to anyone many critical information on the system (with no need to be authenticated on the domain).

Remediation: Migrate to a more recent operating system.

Priority: Major

Methodology: black box

Risk: 8.5 (Impact: 7.8, Exploitability: 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 / Users list available	High

Description: The server version and configuration enables to obtain the list of its users.

Remediation: Migrate to a more recent operating system.

Priority: High

Methodology: black box

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

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

Access control / Open mail relay	High

Description: This mail service allows anyone to send e-mail through it, which could enable mascerading (identity theft). Moreover, this mail server may be used by anonymous originators, in particular to relay spams.

Remediation: Apply the corrective patchs if needed. Configure this server to accept and forward only the authorized messages (from authenticated senders).

Priority: High

Methodology: black box

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

References: 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 / Instance list available	High

Description: The Microsoft SQL Server version and configuration enable to obtain the list

of all the database instances.

Remediation: Stop the 'SQL Server Browser' service. Otherwise, restrict access to the 1434/UDP port to authorized users only.

Priority: High

Methodology: black box

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

Informations: SQL2KVINCENT (8.00.194)

Patch mgt / Web patch management	**High**

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: High

Methodology: black box

- Summary: IIS XSS via 404 error
  Test script and information relative to this vulnerability: 10936
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2002-0148 , CVE-2002-0150

Configuration / Discard service	**Moderate**

Description: The Discard service is open on this server. This service is unused today and should be closed.

Remediation: Close the Discard service, via /etc/inetd.conf on Unix, or via the registry ("EnableTcpDiscard" key) on Windows.

Priority: Moderate

Methodology: black box

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

References: PCI DSS 2.2.4

192.168.56.30

Patch mgt / Web patch management — Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Affected package: -WORDPRESS
  Summary: WordPress 'wp-admin' Multiple Vulnerabilities - Aug09
  Test script and information relative to this vulnerability: 900915
  Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2009-2853 , CVE-2009-2854
- Affected package: -WORDPRESS
  Summary: WordPress cat Parameter Directory Traversal Vulnerability
  Test script and information relative to this vulnerability: 800124
  Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-4769
- Summary: PHP version smaller than 5.3.3
  Test script and information relative to this vulnerability: 110182
  Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
  References: 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
- Affected package: -WORDPRESS
  Summary: WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability
  Test script and information relative to this vulnerability: 900183
  Risk: 8.5 (Impact: 10.0, Exploitability: 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).
  References: PCI DSS 6.1 , CVE-2008-5695
- Summary: GhostScripter Amazon Shop Multiple Vulnerabilities
  Test script and information relative to this vulnerability: 100024
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1
- Affected package: -TIKIWIKI
  Summary: TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities
  Test script and information relative to this vulnerability: 100537
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2010-1133 , CVE-2010-1134 , CVE-2010-1135 , CVE-2010-1136
- Affected package: -JOOMLA
  Summary: Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities
  Test script and information relative to this vulnerability: 103114
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1
- Affected package: -PHP
  Summary: PHP version 5.3< 5.3.6
  Test script and information relative to this vulnerability: 110013
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: 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
- Affected package: - OF WORDPRESS
  Summary: WordPress Multiple Vulnerabilities
  Test script and information relative to this vulnerability: 900219
  Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2008-3747
- Affected package: -WORDPRESS
  Summary: WordPress 'wp-admin/includes/file.php' Arbitrary File Upload Vulnerability
  Test script and information relative to this vulnerability: 100345
  Risk: 6.8 (Impact: 6.4, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1
- Summary: PHP MicroCMS Local File Include and SQL Injection Vulnerabilities

Test script and information relative to this vulnerability: 100808
Risk: 6.8 (Impact: 6.4, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
References: PCI DSS 6.1 , CVE-2010-3480

- Summary: PHP version smaller than 5.3.4
  Test script and information relative to this vulnerability: 110181
  Risk: 6.8 (Impact: 6.4, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
  References: 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
- Affected package: -TOMCAT
  Summary: Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities
  Test script and information relative to this vulnerability: 100712
  Risk: 6.4 (Impact: 4.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2010-2227
- Affected package: -WORDPRESS
  Summary: WordPress Multiple Vulnerabilities - Nov09
  Test script and information relative to this vulnerability: 900975
  Risk: 6.0 (Impact: 6.4, Exploitability: 6.8) CVSS : (AV:N/AC:M/AU:S/C:P/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2009-3890 , CVE-2009-3891
- Summary: http TRACE XSS attack
  Test script and information relative to this vulnerability: 11213
  Risk: 5.8 (Impact: 4.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2003-1567 , CVE-2004-2320
- Affected package: -WORDPRESS
  Summary: WordPress Password Protection Security Bypass Vulnerability
  Test script and information relative to this vulnerability: 100549
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1
- Summary: AWStats 'awstats.pl' Multiple Path Disclosure Vulnerability
  Test script and information relative to this vulnerability: 100070
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2006-3682
- Summary: WonderCMS 'page' Parameter Cross Site Scripting And Information Disclosure Vulnerabilities
  Test script and information relative to this vulnerability: 100908
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1
- Summary: Imageview 'page' Parameter Local File Include Vulnerability
  Test script and information relative to this vulnerability: 103100
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1
- Summary: awiki Multiple Local File Include Vulnerabilities
  Test script and information relative to this vulnerability: 103210
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1
- Summary: QWikiwiki directory traversal vulnerability
  Test script and information relative to this vulnerability: 16100
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2005-0283
- Summary: OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability
  Test script and information relative to this vulnerability: 103132
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1
- Affected package: -TOMCAT
  Summary: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities
  Test script and information relative to this vulnerability: 103032
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2010-4172
- Summary: WordPress Comment Author URI Cross-Site Scripting Vulnerability
  Test script and information relative to this vulnerability: 100239
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2009-2851
- Summary: Apache Web Server ETag Header Information Disclosure Weakness
  Test script and information relative to this vulnerability: 103122
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2003-1418

- Affected package: -WORDPRESS MU
  Summary: WordPress MU Cross-Site Scripting Vulnerability - Apr09
  Test script and information relative to this vulnerability: 800376
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2009-1030
- Summary: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
  Test script and information relative to this vulnerability: 801660
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2010-4480
- Affected package: -WORDPRESS
  Summary: WordPress wp-trackback.php Denial of Service Vulnerability
  Test script and information relative to this vulnerability: 900968
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2009-3622
- Affected package: -JOOMLA!
  Summary: Joomla! Multiple Cross-site Scripting Vulnerabilities
  Test script and information relative to this vulnerability: 901168
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2010-3712
- Summary: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
  Test script and information relative to this vulnerability: 902830
  Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2012-0053
- Affected package: -WORDPRESS
  Summary: WordPress _REQUEST array Cross Site Request Forgery (CSRF) Vulnerability
  Test script and information relative to this vulnerability: 800140
  Risk: 4.0 (Impact: 4.9, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:N/I:P/A:P/).
  References: PCI DSS 6.1 , CVE-2008-5113
- Affected package: -WORDPRESS
  Summary: WordPress Trashed Posts Information Disclosure Vulnerability
  Test script and information relative to this vulnerability: 100505
  Risk: 4.0 (Impact: 2.9, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2010-0682
- Affected package: -APACHE TOMCAT
  Summary: Apache Tomcat Security bypass vulnerability
  Test script and information relative to this vulnerability: 901114
  Risk: 2.6 (Impact: 2.9, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2010-1157
- Summary: Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vulnerability
  Test script and information relative to this vulnerability: 100130
  Risk: 2.6 (Impact: 2.9, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:N/I:P/A:N/).
  References: PCI DSS 6.1 , CVE-2009-0796
- Affected package: -TOMCAT
  Summary: Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability
  Test script and information relative to this vulnerability: 100598
  Risk: 2.6 (Impact: 2.9, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1 , CVE-2010-1157

Configuration / [device] Device has world permissions — Major

Description: Devices that have improper (world) permissions might be accessed by any system user. This might open security holes if these are shared devices or hold binaries (disks for example).

Remediation: The administrator should properly set device access (using group configuration to provide access to a device to multiple users, for example).

Priority: Major

Methodology: white box

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

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

Configuration / [account] Bad permissions on the parent home directory.	Major

Description: The home directory of the listed login ID has group write permission, world write permission or both enabled. This allows new files to be added (and existing files potentially removed) by others.

Remediation: The write permissions should be removed.

Priority: Major

Methodology: white box

Risk: 8.5 (Impact: 9.2, Exploitability: 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 / Users list available	High

Description: The server version and configuration enables to obtain the list of its users.

Remediation: Migrate to a more recent operating system.

Priority: High

Methodology: black box

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

Informations: [nobody, None, user, root]

Patch mgt / Unix patch management	High

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: High

Methodology: black box

- Summary: Apache httpd Web Server Range Header Denial of Service Vulnerability
  Test script and information relative to this vulnerability: 901203
  Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
  References: PCI DSS 6.1 , CVE-2011-3192
- Summary: Samba Multiple Remote Denial of Service Vulnerabilities
  Test script and information relative to this vulnerability: 100644
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2010-1635

Configuration / Web configuration	Moderate

Description: The current configuration of this web server shows the weaknesses

identified below.

Remediation: Improve the configuration of this web server.

Priority: Moderate

Methodology: black box

- Summary: Apache Tomcat servlet/JSP container default files
  Test script and information relative to this vulnerability: 12085
  Risk: 6.8 (Impact: 6.4, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).
  References: PCI DSS 6.1

Configuration / [local network] Listening processes.	Moderate

Description: Processus en cours d'écoute.

Remediation: Installed processes listening on Internet interfaces must be tightly controlled since they are the "open doors" to the outside.

Priority: Moderate

Methodology: white box

Risk: 6.8 (Impact: 6.9, Exploitability: 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] There is no FTPUSERS file.	Moderate

Description: There is no ftpusers configuration file. In some systems this might enable all administrative users (low UID) to access the local FTP server if it is enabled (some other systems might deprecate its use).

Remediation: It is recommended that administrative users are added into /etc/ftpusers if you have a FTP server installed.

Priority: Moderate

Methodology: white box

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

Informations: [/etc/ftpusers]

Configuration / [ssh] The PasswordAuthentication directive is set to an unapproved value.	Moderate

Description: The PasswordAuthentication directive determines if passwords are a sufficient authentication.

Remediation: Set the PasswordAuthentication directive to an approved value.

Priority: Moderate

Methodology: white box

Risk: 6.8 (Impact: 6.9, Exploitability: 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] Remote root login allowed in SSHD_CONFIG	**Moderate**

Description: The indicated file allows remote (i.e., other than system console). root logins for telnet and other services.

Remediation: For /etc/default/login, be sure that the line "CONSOLE=/dev/console" exists. For /etc/securetty, be sure that there are no ttyp entries.

Priority: Moderate

Methodology: white box

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

Informations:
- SSHD_CONFIG: /etc/ssh/sshd_config

Configuration / [inet] The port for service is also assigned to another service.	**Moderate**

Description: The indicated port number is assigned to another service. This indicates either a misconfiguration in the services database, or a possible sign of an intrusion.

Remediation: This should be checked and corrected. If it is not apparent why it is like this, the system should be checked for other signs of intrusion.

Priority: Moderate

Methodology: white box

Risk: 6.4 (Impact: 4.9, Exploitability: 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] Login is disabled, but has a valid shell.	**Moderate**

Description: The listed login ID is disabled in some manner ('*' in passwd field, etc), but the login shell for the login ID is a valid shell (from /etc/shells or the system equivalent). A

valid shell can potentially enable thelogin ID to continue to be used.

Remediation: The login shell should be changed to something that doesn't exist, or to something like /bin/false.

Priority: Moderate

Methodology: white box

Risk: 5.9 (Impact: 9.2, Exploitability: 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 / Network patch management	Moderate

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Moderate

Methodology: black box

- Summary: TCP Sequence Number Approximation Reset Denial of Service Vulnerability
  Test script and information relative to this vulnerability: 902815
  Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:P/).
  References: PCI DSS 6.1 , CVE-2004-0230

Configuration / [cron] Use of cron is not restricted.	Moderate

Description: Cron allows users to submit jobs for the system to do at a particular, possibly recurring time. It can be very useful, but also has a very real potential for abuse by either users or system crackers. Users can be restricted to use cron by creating a /etc/cron.allow (holding only system administrators) or a /etc/cron.deny file (listing which users are not allowed access). Depending on the site configuration if none exist either only root will be able to setup cron tasks or all users will be permitted. In many systems the default is to allow access to all users.

Remediation: Create and complete a /etc/cron.allow or /etc/cron.deny file.

Priority: Moderate

Methodology: white box

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

Configuration / [cron] Root crontab does not exist.	Moderate

Description: There is no crontab for the superuser account this is not in itself an error since many systems might ship without one and use other methods (/etc/cron* files) to run programs as root. However, if there is no method for root to run scripts some system checking scripts (like tiger) might not get executed at all.

Remediation: Create a root crontab.

Priority: Moderate

Methodology: white box

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

Configuration / [account] User's home directory is not accessible.	**Moderate**

Description: The listed login ID has a home directory which is not accessible.

Remediation: This should be checked to see if this is due to networking problem for remote home directories. Without a valid home directory, the user will end up with / as the home directory.

Priority: Moderate

Methodology: white box

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

Informations:
- User: nobody - Home: /nonexistent

Configuration / [pass] Integrity of password files questionable.	**Moderate**

Description: The password files have integrity issues as found by 'pwck -r'. This can lead to looping of password manipulation programs and to authentication or login issues if not corrected.

Remediation: Check the integrity of passwords

Priority: Moderate

Methodology: white box

Risk: 4.3 (Impact: 6.9, Exploitability: 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] Listening processes.	**Moderate**

Description: Processes that have not been run by root are listening on interfaces open to the outside. This processes might have been run by root and changed uids or might be rogue processes.

Remediation: Confirm if their presence is necessary.
Notice that sometimes services open sporadic UDP listeners to receive DNS requests, if you receive reports on open UDP services that later on are closed this might be a false positive.

Priority: Moderate

Methodology: white box

Risk: 4.0 (Impact: 2.9, Exploitability: 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 / Network configuration	Low

Description: The current configuration of this network device shows the weaknesses identified below.

Remediation: Improve the configuration of this ne'twork device.

Priority: Low

Methodology: black box

- Summary: TCP timestamps
  Test script and information relative to this vulnerability: 80091
  Risk: 2.6 (Impact: 2.9, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:N/A:N/).
  References: PCI DSS 6.1

Configuration / [account] Login ID appears to be a dormant account.	Low

Description: The listed login ID appears to be dormant. Files in the home directory of this user have not been modified in the specified period of time.

Remediation: After investigation the account may need to be disabled

Priority: Low

Methodology: white box

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

Informations: [landscape, libuuid, tomcat6, user]

Configuration / [path] File does not export an initial setting for PATH.	Low

Description: File does not export an initial setting for PATH.

Remediation: An initial setting of the PATH variable should be setup in the default locations for shell login programs (/etc/profile, /etc/csh.login, etc.).

Priority: Low

Methodology: white box

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

Informations: [/etc/profile]

Configuration / [pass] Login ID does not have a valid shell.	Low

Description: The listed login ID does not have a valid login program or shell. Usually these are defined in /etc/shells.

Remediation: Consider deleting the accounts

Priority: Low

Methodology: white box

Risk: 1.4 (Impact: 2.9, Exploitability: 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

Appendices

Appendix A: Glossary

- **Target** - generic term which means server, desktop, workstation, printer, router or any other device accessible on the network.
- **Patch** - update fixing one or more vulnerabilities. Patches concern operating systems, databases, softwares, or packets (Unix).
- **CVSS** - Common Vulnerability Scoring System. This is an assessment standard of the severity of computer system security vulnerabilities. The Base metric is displayed as a 6-letter vector following each risk.
- **DBMS** - DataBase Management System.
- **Exploitability** - easiness to exploit a vulnerability. A higher exploitability indicates that the vulnerability requires less skills to be exploited, so a threat may more likely occur.
- **Function** - the control function determines the roots of a vulnerability. For instance, an SQL injection is caused by a development mistake. A trivial password comes from a wrong access control parameterization. The configuration of a service may also lead to information leakage.
- **Impact** - potential effect on the service availability, the confidentiality or the integrity of the data stored on a target.
- **DNS name** - Domaine Name Server. A name obtained by reverse resolution from the DNS server.
- **Netbios name** - Name of a target belonging to a Windows domain or workgroup.
- **Object** - the system concerned by the vulnerability: operating system (including the applications installed on the OS), DBMS, web servers/sites or network.
- **Priority** - The 3 levels (Critical, Major and High) suggested in this report facilitate the identification of the most critical vulnerabilities in order to address them first.
  Note: all the vulnerabilities mentioned in this report are high-risk issues (CVSS greater than 7) and thus, should all be addressed.
- **Risk** - potentiel risk of a threat exploiting the vulnerability. The final risk of a vulnerability should also consider the value of the targeted asset (i.e. the criticity of the information stored in this target or the operational dependancy to the services provided by this target) and the controls that could mitigate the risk (audit logs, contingency plan, etc).
  The risk computation is explained in this document (in the Base metric chapter).
- **Vulnerability** - weakness which allows an attacker to reduce a system's information assurance (in terms of service availability, integrity or confidentiality of the information stored on the targeted device).

Appendix B: Auditing tools

- **Aircrack** is a set of auditing tools allowing to analyse the security of wifi access points. Author and maintainer: Thomas d'Otreppe.
- **db2getprofile** (part of the db2utils suite) gets the access profile to DB2 database and particularly lists the instances and databases. Author and maintainer: Patrik Karlsson.
- **dhcping** is a DHCP and BOOTP scanner. Author et maintainer: Edwin Groothuis.
- **dig** - provided within the dnsutils package - allows to request a DNS server to get the list of the nameservers by DNS zone transfer. Author and maintainer: Internet Systems Consortium, Inc (ISC).
- **fimap** is an open source penetration testing tool that automates the process of detecting file inclusion flaws. Author and maintainer: Iman Karim.
- **flasm** disassembles SWF menus in order to extract the links redirecting to other webpages. Author and maintainer: Ben Schleimer.
- **git** is a distributed version control system Author and maintainer: Linus Torvalds.
- **Medusa** allows to test connexion ID on lots of services (FTP, SSH, SNMP, SMTP...). Author and maintainer: JoMo-Kun.
- **mit-krb5** implements under unix the kerberos protocol used for the domain authentication (when the domain is managed by an Active Directory starting from Windows 2003). Author and maintainer: Massachusetts Institute of Technology.
- **MSSQLScan** allows to get some informations on Microsoft SQL Server database. Author and maintainer: Patrik Karlsson.
- **nbtscan** includes the same features as windows 'nststat' command (listing all open Netbios services). Author and maintainer: Stephen Friedl.
- **Nmap**, the famous ports scanner used to detect running services on targets. Author and maintainer: Gordon Lyon.
- **OpenVAS** integrates several thousands of tests upon patch management: OS, applications, DBMS, etc. Author and maintainer: OpenVAS team.
- **rpcclient** allows to acces to "named pipe" and to execute MS RPC commands. It's part of the Samba suite. Author and maintainer: Samba team.
- **SidGuesser** allows to discover Oracle instances when they are transmitted by listener (attacking using a dictionary). Author and maintainer: Patrik Karlsson.
- **snmpwalk** provided within the net-snmp package allows to browse informations given by SNMP protocol. Author and maintainer: Net-SNMP.
- **SMBAT**(SaMBa Auditing Tools) includes smbdumpusers tool allowing to list the users of Windows NT/2000. Author and maintainer: Patrik Karlsson.
- **samba** is the standard Windows interoperability suite of programs for Linux and Unix. Author and maintainer: Samba team.
- **sqlmap** is an open source penetration testing tool that automates the process of detecting SQL injection flaws. Author and maintainer: Bernardo Damele.
- **sslscan** determines which cryptographic algorithms is in use on a SSL server (basically in the case of an https webapplication). Author and maintainer: Ian Ventura-Whiting.
- **Tiger** is a Unix security audit and intrusion detection tool. Author and maintainer: Tiger.
- **tnscmd10g** allows to list the instances of the Oracle database (including 10g and 11g versions). Author: James W. Abendschan, Maintainer: Saez Scheihing.
- **WhatWeb** identifies content management systems (CMS), blogging platforms, stats/analytics packages, javascript libraries, servers and more. Author and maintainer: Brendan Coles.
- **wdiff** is a front end to diff for comparing files on a word per word basis. Author and maintainer: Denver Gingerich.

Appendix C: Report generation

- **The eZ Components library** allows to generate all the figures inside this report. Author and maintainer: eZ Systems.
- **PostgreSQL** is a relational database management system (RDBMS). Author and maintainer: PostgreSQL Global Development Group.
- **wkhtmltopdf** (read: WebKit HTML to PDF) combines the strength of the XHTML/CSS Webkit engine (used by Chrome and Safari for example) and its PDF library. Author and maintainer: Jakob Truelsen.

Legal notice

In accordance with the LCEN Act of 22 June 2004, the DenyAll product is exclusively made available for legitimate users and businesses whom their mission is to perform security audits.
By accepting the DenyAll agreement license, the user agrees to abide by the Godfrain act of January 6, 1988 punishing unauthorized intrusions into a computer system.

Copyright statement