DBMS Configuration Security Assessment Results

Afonso Neto, Marco Vieira

Detailed results for all the tests in the 4 cases

TEST Result	Key
Passed	P
Failed	F
Unknown	U

#	TEST	Fail	Result in Case 1	Result in Case 2	Result in Case 3	Result in Case 4
	ENVIRONMENT					
1	If the machine is turned off, does any service other than the database become unavailable? Is there any process running on the machine which is not demanded by the DBMS, the OS or the machine maintenance/security?	Yes	P	P	F	F
2	Is the DB machine a Windows Domain Server Controller?	Yes	P	P	P	P
3	Is there a firewall on the network border? Is there a firewall running on the DBMS machine? Are both firewalls properly configured by experienced staff with solid network knowledge?	No	P	F	P	F
4	Is it possible to an unauthorized person to physically access the machine without supervision at any given time?	Yes	P	P	F	P
5	List the protocols available in the network stack in the OS of the DBMS machine. For each protocol, is there a clear justification for its availability?	No	P	F	F	F
6	List the DBMS processes in the OS. For each process, is the user running it used to run any other process at any time?	Yes	F	F	F	F
7	Locate the DBMS processes user. Does that user have administration rights? Does it can run applications not DB related? Does it have read rights on any file not necessary to the DBMS processes?	Yes	F	F	F	F
8	Locate the DBMS processes user. Can you login in the OS with it? (assume you know its password)	Yes	P	P	P	P
	INSTALLATION SETUP					
9	Locate the log files of the DBMS and identify their file system partition. Are there any other files in this partition besides the logs?	Yes	F	F	P	F
10	Locate the log files of the DBMS and identify their file system partition. Does that partition have exclusive read/write rights for the DBMS user?	No	F	F	F	F
11	Locate the data files of the DBMS and identify their file system partition. Are there any other files in this partition besides the data files?	Yes	P	F	P	F

12	Locate the data files of the DBMS and identify their file system partition. Does that partition have exclusive read/write rights for the DBMS user?	No	F	F	F	F
13	List all OS users which work only with the DB. List all OS regular users (not DB users). List all DBMS applications and OS applications that are necessary for the OS users that work with the DB. Does any regular user can access any DBMS application listed? Does any DB user can access any application not in one of the lists?	Yes	F	F	F	F
14	List all DBMS databases. Install a fresh copy of the DBMS in a test machine without any customization and then list its DBMS databases. Is there any database in both lists which isn't required for the DBMS?	Yes	F	P	P	P
15	List all DBMS accounts. Install a fresh copy of the DBMS in a temporary machine without any customization and then list its DBMS accounts. Is there any account in both lists?	Yes	F	P	P	P
16	List any identification names a remote user must know to connect to the DBMS. Install a fresh copy of the DBMS in a temporary machine without any customization and then list the identification names a remote user must know to connect to this DBMS instance. Is there any name in both lists?	Yes	F	P	P	P
17	List any TCP/UDP ports a remote user must know to connect to the DBMS. Install a fresh copy of the DBMS in a temporary machine without any customization and then list the TCP/UDP ports a remote user must know to connect to this DBMS instance. Is there any port in both lists?	Yes	F	F	P	F
18	List all SSL certificates used with the DBMS. For each one, was it created by experienced staff with that specific purpose?	No	P	P	F	P
19	Is there any kind of development or testing being done in the production server?	Yes	F	F	F	F
20	Does any developer have a valid DBMS account or OS account in the production server?	Yes	P	F	P	F
21	List the sub-net mask of the IP address of the production and the development servers. Are they the same? Are both servers reachable from one other through a path with only layer 2 network equipments (hubs, switches, etc…)?	Yes	F	P	F	F
22	List all files installed with the DBMS application. For each file, is its owner correctly set as the DBMS user?	No	P	U	F	F
23	List all files installed with the DBMS application. For each file, are its rights correctly configured according to its purposes?	No	F	F	F	F
OPERATIONAL PROCEDURES						

24	Check your DBMS version. Check the latest DBMS version available from the vendor which is an update to your version. Are they different? Is there any recommendation from the vendor against the use of the version you are using?	Yes	F	P	P	F
25	Is a carefully thought out, documented backup procedure regularly executed? If the person in charge suddenly quit, is it easy for anyone else to resume its task?	No	P	P	F	P
26	Is the backup data regularly tested after it is generated? Is a recovery procedure regularly fully simulated? Is the backup data stored in a secure place other than the DB server?	No	F	F	F	F
SYSTEM LEVEL CONFIGURATION						
27	During a connection procedure, does the server assign a full range random local port for the remote user to connect?	Yes	P	U	U	U
28	Establish a connection from any remote user to the server, capture the underlying network traffic and ask for a security expert to analyze it. Is the connection being secured with a recognized encryption protocol like TLS?	No	F	F	F	F
29	Does the user connection require the knowledge of a server certificate?	No	F	F	F	F
30	List all configuration files/parameters of the DBMS. Is a host name used on any parameter?	Yes	P	P	P	P
31	For each registered DBMS user, was it created for a specific application/purpose/person? Is the authentication procedure used in the applications recognizably secure? Does it use a standard algorithm or protocol?	No	P	F	P	F
32	Establish a connection with the DBMS and let it stay idle. Is the connection severed in a reasonable amount of time?	No	F	F	F	F
33	Is any specific information other than a username and password obtained from the client host during the authentication procedure?	Yes	P	P	P	P
34	List all authentication methods used with the DBMS. For each one, does it depend only on the host?	Yes	P	P	P	P
35	Was a clear policy defined (and documented) about how passwords would be changed, when they must be changed, how they should be retrieved if lost and what rules they must obey? Does it comply with standard recommendations from security experts?	No	P	F	F	F
36	Try authenticating several times with a wrong password. Is there a try when the account becomes permanently locked?	No	P	F	F	F

37	Advance the server clock an unreasonable number of months. Authenticate to the server. Are you forced or recommended to change the current password?	No	F	F	F	F
38	Try changing your password to the same password. Did you succeed?	Yes	F	F	F	F
39	Locate the table or file where the passwords are stored and ask for a security expert to analyze it. Are the passwords stored as some recognizably standard hash algorithm?	No	P	P	P	P
40	Is logging turned on? Is the log level set to report at least database errors and client connections? Is there a clearly justified reason for it not to be set to a higher level?	No	P	F	P	F
41	Are the logs periodically checked? Are the logs also included in the backup procedures? Is the space of the partition where the logs are written monitored?	No	P	F	P	F
42	Are the following operations traceable: creation and destruction of users, objects and sessions, failed and successful logins, rights assignments and data changes on critical tables?	No	F	F	F	F
43	Is the trace data stored in a different area than the database? Does that area have its read/rights permissions correctly set? Is the space of the partition where it is stored monitored?	No	F	F	F	F
44	For each configuration file, analyze its permissions. Is it readable only by authorized users?	No	P	P	F	F
45	For each system variable, does it contain sensitive information (any which should be private) and can be seen by all OS users?	Yes	P	P	P	P
46	Are core_dump or trace files being generated for failed processes and are they generally visible in the OS?	Yes	F	P	P	P
47	Does the editor used to update configuration files generate backups of the edited files and do they remain available for reading afterwards?	Yes	P	P	P	P
48	For each function and extended functionality available, does it allow a user to access a file on the file system?	Yes	P	P	P	P
49	For each function and extended functionality available, does it allow a user to do any kind of network operation?	Yes	P	P	F	P
50	For each function and extended functionality available, is its availability clearly required? Is it impossible to do the same task without it?	No	U	P	F	F
51	For each function and extended functionality available, does it allow a user to gather any information about the OS?	Yes	U	P	F	U
APPLICATION LEVEL CONFIGURATION AND USAGE						

52	Make a list of all system tables (not created for use with applications). For each one, check if there is any user with some permission (read or write) over it. Are those permissions clearly justified and necessary?	No	P	F	P	F
53	Make a list of all system databases. For each element on the list, check if there is any user with some permission over it. Is this permission clearly justified and necessary?	No	P	F	P	P
54	For each non-DBA user, list all its permissions. For each permission, does it have a clear justification? Is it impossible for the user to work without it?	No	P	F	F	P
55	For each non-DBA user, list all its permissions. For each permission, is it of type ANY or ALL, which would automatically propagate to other objects of the same type?	Yes	P	P	F	P
56	For each non-DBA user, list all its permissions. For each permission, does it allow that user to grant it to another user?	Yes	P	P	F	P
57	For each non-DBA user, list all its permissions. For each permission, does it allow that user to change some system configuration which is either critical or valid to the whole DB?	Yes	P	P	P	P
58	For each non-DBA user, list all its permissions. For each permission, does the user inherit it from a group or role he is assigned to?	No	F	F	F	F
59	List all documents and files that contain any schema information. For each one, is it stored in the DB server?	Yes	P	F	P	P