The Database Exposure Survey 2007

David Litchfield [davidl@ngssoftware.com]
12th November 2007

An NGSSoftware Insight Security Research (NISR) Publication

http://www.ngssoftware.com

Introduction

This survey seeks to answer how many database servers exist on the internet and are listening on their default TCP ports and are *not* protected by a firewall. This is achieved by sampling a number of random hosts on the Internet and projecting the results to cover the Internet address space. The answer will help us to determine our risk of exposure to a potential future database worm or indeed the potential for database security breaches by hackers and criminals. The last time this survey was performed was in December 2005 and this survey, as well as looking at its own findings, will compare and contrast with the findings from 2005 [1].

Executive Summary of Results

The survey found that there are approximately 368,000 Microsoft SQL Servers directly accessible on the Internet and around 124,000 Oracle database servers directly accessible on the Internet. Between the two vendors, there are 492,000 database servers out there on the Internet *not* protected by a firewall. Whilst the number of Oracle servers has very slightly dropped since 2005 when it was estimated there were 140,000, the number of SQL Servers has risen dramatically from 210,000 in 2005. Of the SQL Servers found 82% were running SQL Server 2000 and of those only 46% were running Service Pack 4, the most recent, and the remainder were running Service Pack 3a or less. Indeed 4% were found to be completely unpatched and are vulnerable to the flaw exploited by the Slammer worm as well as an authentication flaw known as the "Hello bug". With regards to the Oracle servers, 13 were running de-supported versions of Oracle that no longer receive patches and are known to be vulnerable to critical vulnerabilities – in other words those that can be exploited by an attacker without a username and password and gain full control of the target. Given that it's not possible to tell whether an Oracle server has been patched or not by looking at its version number it's difficult to draw accurate conclusions about the state of vulnerability with regards to the other servers. The findings also suggest that people don't deploy hotfixes but wait for Service Packs. In SQL Server 2000 for example, only 8 of 129 systems found had interim fixes – the rest were running either RTM, Service Pack 3/3a or Service Pack 4.

In the author's opinion, these findings represent a significant risk: whilst it's not possible to say how many of these systems are engaged in a commercial function, with just under half a million servers accessible there is clearly potential for external hackers and criminals to gain access to these systems and to sensitive information. It is well known that Oracle prior to 10g installs with a number of user accounts with default passwords including DBA accounts and earlier versions of SQL Server would install with the superuser account (sa) with a blank password. How many of these unprotected database servers have these defaults in place?

How the survey was performed

The survey in 2005 selected 8000 addresses at random and checked the next 60 addresses for the presence of a database server meaning 480,000 addresses were checked. This survey used a different methodology. A check was made against 1,160,000 random IP addresses. Each IP address was probed on TCP port 1433 (SQL Server) and 1521 (Oracle) and if the port was open a version check was made. Only those systems that responded correctly to a version check were counted in order to remove false positives. The IP address range is 2^32 bits but of these only addresses below 224.0.0.0 are "in use" – 224.0.0.0 and above are multicast addresses. This means that there are 3,753,869,056 possible addresses. Of these ranges 10.x.x.x, 172.16.x.x and 192.168.x.x are considered as private addresses and 127.x.x.x represents the local system. This reduces the possible address space to 3,720,183,560. Of these 3,720,183,560 addresses, only 73% have been allocated [2a] leaving 2,715,733,999 possible hosts. [Note - whilst the IANA have also reserved address ranges such as 192.0.2.0/24 (TEST-NET) [2b] these were not deducted.] The IP addresses of those systems that were checked were generated randomly by the C rand() function on Windows – this is a linear congruential random number generator. In terms of coverage this means a good spread of addresses over the survey were checked:

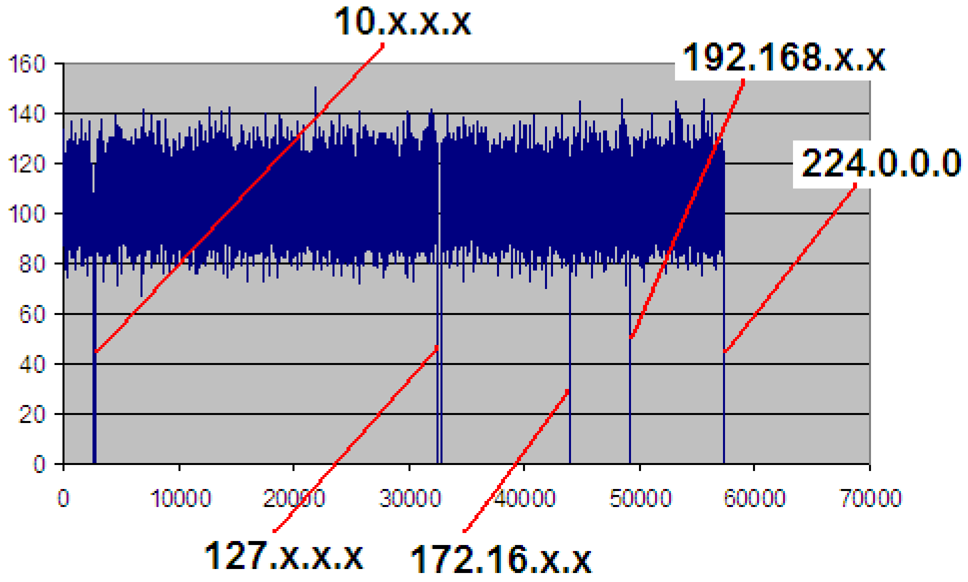

Figure 1 - Coverage

The graph in Figure 1 shows the number of addresses generated for each 16bit block (65,535 addresses). As can be seen, all except the private ranges (10.x.x.x, 172.16.x.x, 192.168.x.x and 127.x.x.x) and non-multicast addresses (< 224.0.0.0) were checked.

Before looking at the results the sample size should be discussed. Can an accurate picture be drawn by looking at only just over a million IP addresses? I think accurate enough though others will and of course may disagree. Certainly, one or two more or less would influence the results fairly substantially. After discussions with colleagues the 2008 sample size will be bigger.

Results

A check was made against 1,160,000 addresses. 157 SQL Servers were found and 53 Oracle servers were found. This means that 1 in 7388 hosts are running SQL Server (1,160,000 / 157) and that 1 in 21886 hosts are running Oracle (1,160,000 / 53). With 1 SQL Server for every 7388 hosts, when extrapolated to cover the IP address range in use (2,715,733,999), there are a projected 367,587 SQL Servers (2715733999 / 7388) accessible on the Internet. There is 1 Oracle server per 21886 hosts and therefore there are 2715733999 / 21886 = 124,085 Oracle servers accessible on the Internet. Let's examine the breakdown of these systems:

Results for SQL Server
Of the 157 systems found after checking 1,160,000 IP addresses at random, 129 were running SQL Server 2000 and 28 were running SQL Server 2005.

SQL Server 2000 version	Number found
8.0.194	5
8.0.311	3
8.0.760	25
8.0.766	31
8.0.818	6
8.0.2039	59

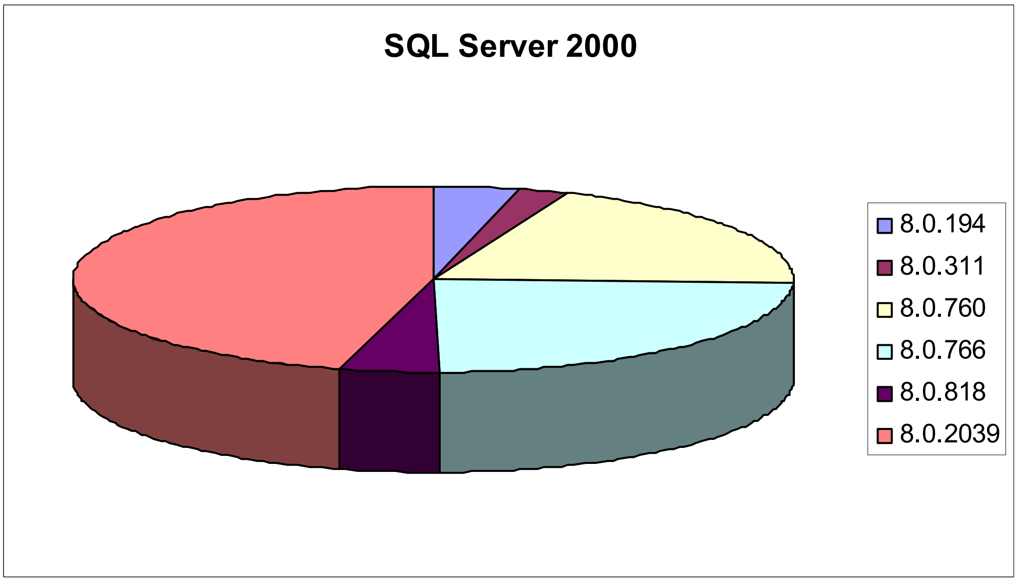

Figure 2 – Breakdown of SQL Server 2000 versions.

Here we can see that 56 of the 129 SQL Server 2000 systems (43%) are still on Sp3/SP3a which is down 30% from 2005. 59 of 129 (46%) are running SP4, up by 26% from 2005. This is good. Unfortunately 8 systems were running SQL Server 2000 RTM and RTMa – RTMa does however have the patch for the flaw exploited by the Slammer worm.

Only 8 systems had an interim patch or hotfix. All the others were either RTM, SP3/3a or Service Pack 4. This suggests that people don't install hotfixes but rather, they wait for Service Packs.

SQL Server 2005 version	Number found
9.0.1399	12
9.0.1406	2
9.0.2047	4
9.0.3042	4
9.0.3054	6

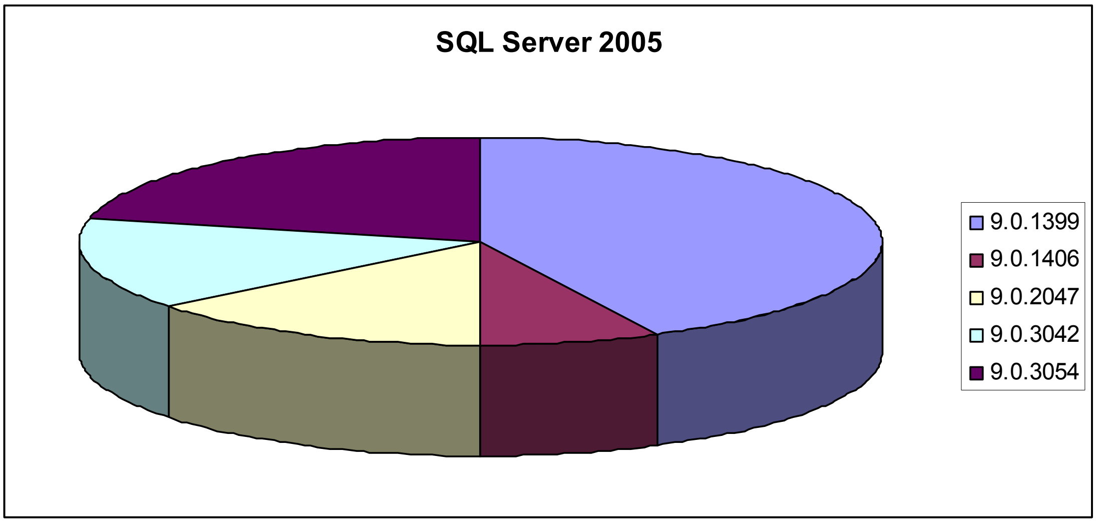

Figure 3 – SQL Server 2005 versions

SQL Server 2007 Findings Compared with 2005

The 2005 survey findings suggested that there were around 210,000 unprotected SQL Servers. Two years later, this survey has found that there are now around 368,000. This is a significant increase. It is not known whether this is due to a growth in SQL Server installs or MSDE installs. Either way, with regards to a potential database worm such as Slammer, Spida or Voyager Alpha Force, with a large increase in population the risk also increases. What helps here is the fact that no major flaw has been found in SQL Server since 2003. If the growth in numbers since 2005 is due to an increase in SQL Servers however, then this does not bode well for the consumer public as this would represent an increase in risk of potential database security breaches and therefore identity theft and fraud. Whether the growth is through SQL Server or MSDE as far as the potential for a worm is concerned

Results for Oracle

The 2005 survey found that there were approximately 140,000 Oracle database servers accessible on the Internet not protected by a firewall. This survey projects there to be around 124,000. This drop could be due to the change in scanning methodology but perhaps not because one would expect to see a similar drop in SQL Server numbers if this were true.

Let’s look at those systems that were found.

Oracle Version	**Number found**
8.0.5.0.0	5
8.0.6.0.0	1
8.1.7.0.0	4
8.1.7.4.0	2
9.0.1.1.1	1
9.2.0.1.0	16
9.2.0.3.0	6
9.2.0.4.0	3
9.2.0.6.0	4

9.2.0.8.0	1
10.2.0.1.0	5
10.2.0.2.0	1
10.2.0.3.0	4

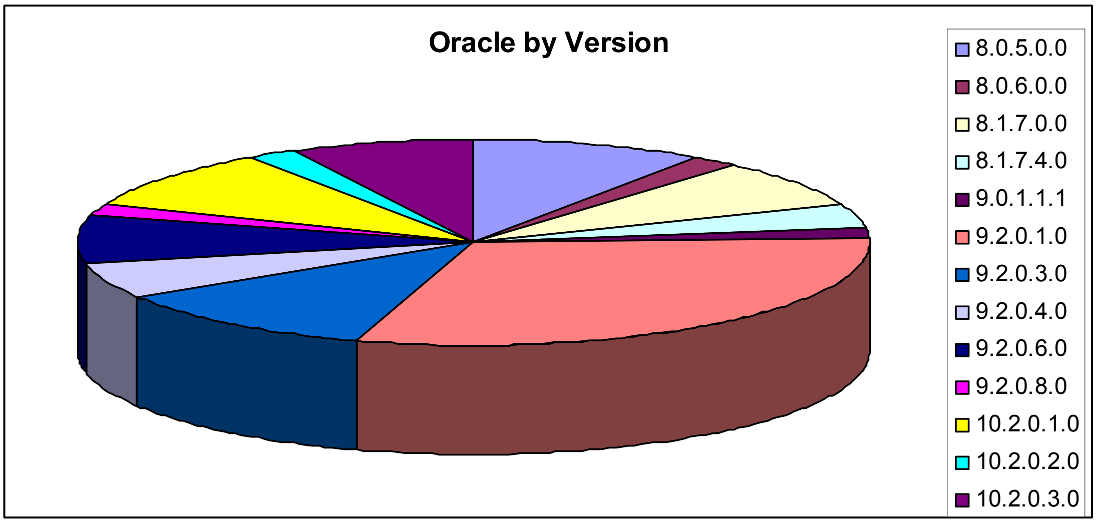

Figure 4 – Oracle versions

We can see that a large number, 13, of these servers are running old versions that are known to be vulnerable to the long username buffer overflow that can be exploited without a user ID and password. 35, 66%, are running versions known to have buffer overflows in extproc [3],[4]. These long username and extproc overflows can be exploited by attackers without a username and password.

Breakdown of Oracle per Operating System

The breakdown of Oracle per operating system is quite interesting. It shows a large number of those with unprotected Oracle servers are running on Windows. Does this support the myth that Windows users don't know what to do when it comes to security? Probably not as the sum of the number of Solaris and Linux systems found is close enough that no one camp can be deemed to be worse than the other.

OS	Number found
Windows	30
Solaris	7
Linux	16

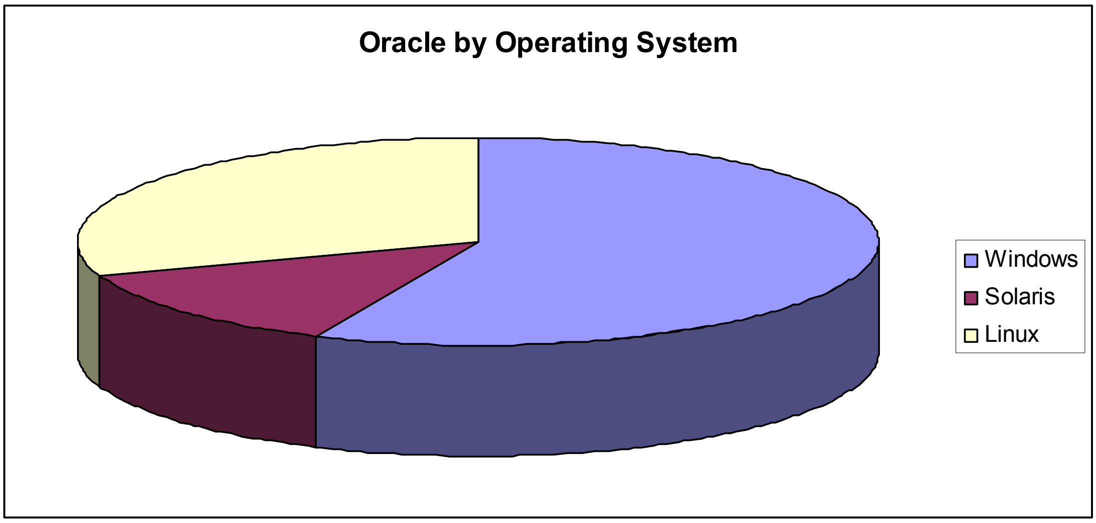

Figure 4 - Oracle by Operating System

What to do next

It may be the case that many database administrators don't even know that their systems are accessible over the Internet. It is not uncommon to find a hole has been opened in the firewall to allow testing for some application and the hole has not been closed after the testing has completed. These steps can be taken to minimize associated risks:

- If you think your database servers can't be access from the Internet, then test this to make sure your understanding is correct. This can be done by attempting to telnet into your database server's listening TCP port for example or by using a TCP port scanner.
- If you must allow access to third parties to your database servers then don't allow access to all and sundry. Configure your firewall to only allow connections from set IP addresses or address ranges.
- Ensure the passwords for default user accounts have been changed. Lock all accounts that aren't actively used. Use strong, difficult to guess passwords for those accounts that are used.
- Keep up to date with patches! This seems like a no-brainer but the evidence suggests otherwise.
- Regularly perform vulnerability assessments with a database specific vulnerability assessment scanner. Examples of such tools include NGSSQuirreL, Appdetective and Shadow DB Scanner.
- Regularly review logs to look for attempts by hackers to penetrate your systems.

Conclusion

With an estimated 368,000 Microsoft SQL Servers and 124,000 Oracle database servers, the results of this survey suggest that there are far too many database servers out there on the Internet open to attack. The number of systems found not to be fully patched and the massive increase in SQL Server numbers shows that the world's database security posture is getting worse not better. As a final note we must remember that these numbers represent the projected number of systems listening on their default TCP ports. No doubt there will be more listening on non-default ports such as 2433 or 1526. Whilst this survey did not look for such systems we can be sure hackers and criminals will.

[1] http://www.databasesecurity.com/dbsec/database-exposure-survey-2005.pdf
[2a] http://www.isi.edu/ant/address/
[2b] http://tools.ietf.org/html/rfc3330
[3] http://www.nextgenss.com/advisories/ora-extproc.txt
[4] http://www.ngssoftware.com/advisories/oracle23122004/