

פרוייקט בהאקינג ואבטחת מידע

Administrative

- Course Number: The project will be performed under the course 236340 (Project in Computer Communications)
- Projects will be introduced on 15/03/2007 10:30 room 601
- Project requests should arrive until 22/03/2007, by e-mail to shulman@imperva.com.
- Number of projects is limited
- Further information and contact:
 - Mr. Amichai Shulman: 054-5885083
 - Prof. Eli Biham

Project 1: Hacking Database Network Protocols

General Description

Database servers today are the most critical assets of an organization. In recent years, these servers have become the target of hackers employing three types of attack techniques: low level network attacks against the operating system that hosts the database server, SQL injection attacks through application servers and direct SQL based attacks. All techniques have been widely explored and studied and commercial tools are available to protect databases against such techniques. As a consequence hackers have started to explore a new technique – network level attacks against the protocol used by the database server.

All commercial database vendors (Oracle, Microsoft, IBM, Sybase) use propriety and obscure protocols to communicate between client and database server. These protocols have been proven to contain security related vulnerabilities, some of which became public recently.

Requirements

Students will be focusing on one of two issues:

Response Message Tampering

All of the research regarding vulnerabilities is concerned today with request tampering. However, there is also an incentive for looking at response tampering, in conjunction with the use of database links.

In this project, students will be given protocol documentation for a specific database and will be asked to explore it, in lab conditions, for potential security vulnerabilities by applying response tampering techniques.

- Each group of students will have to suggest a list of potential vulnerabilities according to the protocol documentation
- The students are then required to actually test their suggestions against an actual system trying to hack into it.

- In the process of trying to hack into the systems the students will be required to find the necessary hacking tools, modify existing tools or even create their own hacking tools

Open Source Protocol Attacks

While all research regarding commercial database products involves a black-box approach, an alternative method can be applied to open source databases such as MySQL. Students will be required to explore an open source database communication protocol for security vulnerabilities:

- Install MySQL database server and source files
- Identify modules relevant for communication protocol vulnerabilities
- Review the relevant source code for security vulnerabilities based on a predefined plan.
- Demonstrate detected vulnerabilities

Goals

Get an understanding with the process of assessing the security and robustness of network protocols.

Get the chance for a sneak preview into the world of hackers and crackers, their methodology and tools.

Prerequisites

Knowledge of TCP/IP

Understanding of network protocols

Acquaintance with commercial database software (Oracle, Microsoft SQL Server, etc.) or open source database software (MySQL, Postgress).

Programming knowledge (preferably Java).

Project 2: Automatic Vulnerability Discovery

General Description

Database servers today are the most critical assets of an organization. In recent years, these servers have become the target of hackers employing three types of attack techniques: low level network attacks against the operating system that hosts the database server, SQL injection attacks through application servers and direct SQL based attacks.

The latter two attack types can be leveraged by exploiting specific database vulnerabilities that allow for privilege elevation. Recent studies by security researchers have shown that many such vulnerabilities are lurking within built in stored procedures and functions. In particular, SQL injection vulnerabilities within stored procedures provide a method for executing arbitrary SQL statements in the context of a privileged user, and buffer overflow vulnerabilities provide a method for executing arbitrary code on the database server's machine.

Requirements

In this project, students will be required to extend an automated assessment tool for database stored procedure. The tool, created by other students, is designed to test all susceptible stored procedures within a database for the potential existence of buffer overflow or SQL injection vulnerabilities.

- The students will extend the tool to support an additional database server platform (Oracle, MS-SQL, Sybase)
- The students will implement an improvement to the detection method used by the existing tool.
- Students may be required to fully exploit a sample vulnerability they discover.

Goals

Get acquainted with the process of assessing the security and robustness database servers. Get the chance for a sneak preview into the world of hackers and crackers, their methodology and tools.

Prerequisites

Understanding relational databases

Knowledge of the SQL language

Acquaintance with commercial database software (Oracle, Microsoft SQL Server, etc.)

Java Language Programming

Project 3: Vulnerability Detection in Oracle Database Packages

General Description

The Oracle database server is delivered with numerous internal software modules called “Packages”. While packages are written in a language that draws from the standard SQL language, they are stored within the server in an obfuscated manner called “wrapped” format.

The built-in packages in the Oracle server have been notoriously susceptible to various types of security vulnerabilities such as buffer overflow and SQL injection. Some work have been done recently by researchers in order to overcome the obfuscation technique and access the original code of the packages.

Requirements

The students are required to explore methods for retrieving (at least partially) the original source code (or an equivalent byte code) of the “wrapped” packages in Oracle 10gR2 database.

Based on the information extracted in the previous process students will suggest a method for automatically detecting vulnerable packages.

Goals

Get an understanding of coding techniques that result in security vulnerabilities.

Get the chance for a sneak preview into the world of hackers and crackers, their methodology and tools.

Requirements

Acquaintance with database servers (and preferably Oracle)

Strong background in programming and debugging applications

Project 4: Automated Database Security Scanner

General Description

Database servers today are the most critical assets of an organization. In recent years, these servers have become the target of hackers employing many types of attacks. One of the tools that help database owner to cope with the growing risk is a security scanner. This tool reveals potential security vulnerabilities and configuration problems that may be abused by an attacker. An implementation of such a tool requires an engine that can query the database for configuration information, privileges information and so on, coupled with an adequate set of such queries and a proper reporting mechanism.

While a number of vendors sell commercial products that implement the above functionality there is also a public domain tool that does the same. This tool though public domain, only implements testing scenarios for commercial database servers (Oracle, DB2, Sybase, etc.).

Requirements

Extend a public domain tool for security database scanning to support the exploration of operating system related issues of database servers

The students will be required to meet the following requirements:

- Add the code required for interacting with the operating system
- Survey the Internet for security resources regarding MySQL security configuration and formulate scanning rules to be implemented
- Implement the security rules within the tool.
- Test the tool using various actual MySQL database servers.

Goals

Get acquainted with the process of assessing the security and robustness database servers. Learn about the important security attributes of a database server in general and MySQL in particular.

Prerequisites

Understanding relational databases

Knowledge of Windows and Linux scripting

Some Java programming skills