Glossary

active reconnaissance The use of active investigation methods for gathering information about a system or an infrastructure directly.

adware A general term for software that uses typical malware intrusion techniques to obtain marketing data or advertise a product or service.

alternate key A field with values that are not chosen as a primary key, but can be used in cases where the primary key is not available.

attribute A characteristic or variable that describes or further identifies an entity.

audit scope The area or system on which the security audit will focus. Defining the scope of the audit is one of the most important steps of the auditing process.

authentication The process of confirming the identity of those individuals or applications that request access to a secure environment.

authorization The process of ensuring that those individuals or applications that request access to an environment or an object within that environment have the permission to do so.

automated audit An audit conducted using tools that are either installed onto a machine or embedded within an application for the purpose of recording the typical behavior of a system.

availability The efforts taken through policy, procedures, and design in order to create and maintain the accessibility of resources within a database environment.

back door A method created during the programming of a worm in which access is gained into a system by avoiding normal security, which gives the creator of the worm undetected access into the system.

backup An intentional copy of data, program files, and system configurations that is used to archive and store information in the event of network failure or malware attacks.

backup management plan A process developed to ensure the safety of the data on a network.

binary code installations Binary files that are packaged and ready to be installed without the need for compiling the code to enable it to be run as an executable file on a particular machine.

binary file A file that contains code that can be read by machines and run as an executable file.

black box testing An assessment that is conducted with no prior knowledge of the system or infrastructure that is being tested.

black hat Someone who breaks into computer networks without authorization and with malicious intent.

bond parameters Placeholders to bind user input.

boot sector An area of the hard disk that contains records necessary to the boot process of a computer.

boot sector virus Malware that infiltrates a system by loading itself onto the boot sector of a hard disk via an infected floppy disk left in a floppy disk drive.

bot (software robot) A form of malware that has the ability to perform a large array of automated tasks for an intruder at a remote location, ranging in severity from spamming a system to initiating DoS attacks on systems.

botmaster An individual who controls a network of bots and who accumulates a number of bots and then rents these botnets to other intruders and cybercriminals for the purpose of spamming, phishing, and other more serious types of cybercrime.

botnet A network of bots.

buffer manager A portion of the SQL Server responsible for accessing data pages and updating the database.

buffer pool (buffer cache) The area where data pages from a database are stored to minimize the need to read and write from the database file located on the hard disk.

caching The process of saving a duplicate of the requested data to another area of a system in hopes of saving resources and speeding up the future requests for that same data.

candidate key A field with values that meet the requirements for a primary key.

Client Access License (CAL) A unique license that allows users or devices access to gain a licensed Microsoft SQL Server 2008 server.

cold site A facility that provides the basic necessities for rebuilding a network. A contract that involves a cold site would promise the use of a facility that provides water, power, and air conditioning or heat.

column (field) The component of a table that maintains a general category of information with similar data types.

commit To make a change within a DBMS that is permanent and visible to other users.

compile The act of converting source code that is written in one language into a different programming language or machine language.

composite key A group of two or more fields where their values can be combined to be used as a primary key.

computer security A set of established procedures, standards, policies, and tools that is used to protect a computer from theft, misuse, and unwanted intrusions, activities, and attacks.

computer virus A form of malware intended to spread from one computer to another without detection.

concurrency The simultaneous access of resources and data.

confidentiality The efforts taken through policy, procedure, and design to create and maintain the privacy and discretion of information and systems.

control file A file within a database that contains the location and important credentialing information of other files.

cracker An individual who breaks into networks without authorization with hopes to destroy and/or steal information.

credential A piece of information that is used to verify identity, such as a person's username and password, an application's secure ID, or a host's network name and address.

database A collection of data stored on a computer using an application called a database management system.

database connection manager The component of the database architecture that manages connections to the MySQL server.

database link A link made between two databases that when created results in one logical data storage unit. Links are created in Oracle to apply common policies and to create associations between databases.

database management system (DBMS) An application that allows users to search stored data in order to locate specific information.

database model A representation of the way data is stored.

database security A set of established procedures, standards, policies, and tools that is used to protect data from theft, misuse, and unwanted intrusions, activities, and attacks.

datafile A file that contains the actual data for the database and holds the information for all logical structures (tables, records, and so forth) within the database.

data sending Trojan Malware that obtains sensitive data from your computer and transmits it back to a cracker.

deadlock A situation when two transactions cannot proceed because each user has data that the other needs.

denial of service (DoS) attack A concerted effort made by malware to keep system resources, such as Internet sites, from functioning correctly.

destructive Trojan Malware that is installed on a computer with the intent to destroy a system as a whole by randomly deleting files and folders and corrupting the registry.

differential backup An intentional copy of data, program files, and system configurations that only saves the data that has changed since the last backup was complete.

digital certificate A password-protected and encrypted file that holds the identity of a user or object.

digital signature Code that uses cryptography to verify the authenticity of a source of information.

disaster plan A plan developed to ensure the quick reinstatement of a network that has fallen victim to a human or naturally caused disaster.

DNS poisoning An intrusion where a cracker gains control over the DNS server and changes the domain name's respective IP address, redirecting requests to sites that the cracker has built and maintains.

dynamic analysis An attempt to find errors or vulnerabilities in the source code of a program dynamically while it is being executed.

dynamic SQL statement A SQL statement that is generated on the fly by an application (such as a Web application), using a string of characters derived from a user's input parameters into a form within the application itself.

encryption The transformation of data by using sophisticated algorithms in an attempt to make the data unrecognizable.

entity A person, place, or thing stored within the table of a database and for which attributes and relationships exist.

exploitation The act of using system vulnerabilities and carefully crafted SQL queries to gather information and subsequently peel away at the infrastructure's security defense for the purpose of gaining access or control of a system.

external audit An audit conducted using a third-party group or a number of individuals from a source outside the organization itself.

external testing An assessment that is conducted outside the organization's security border; this type of testing will display attacks and liabilities that can be exploited externally from competitors, external users, and hackers. Initial tasks most commonly completed during external testing involve information gathering. An external intruder must gain information from a system or an infrastructure to break into it.

fiber A subcomponent of a thread, which is handled by the server to accomplish a task.

filegroup A collection of one or more physical data files within a SQL Server database.

file-infected virus A form of malware that will attach itself to an executable file that requires a user to run before it can propagate and corrupt the system.

File Transfer Protocol (FTP) Trojan Malware that allows the attacker to use someone else's computer as an FTP server.

flat model A two-dimensional list of data entries, where all data within a field are understood to be similar, and all data within a record are understood to be related to one another.

foreign key A field within a table that contains a label used to build a relationship between two tables.

formal audit An audit most often conducted to satisfy specific industry standards that are required by law for certain types of organizations.

full backup An intentional copy of data, program files, and system configurations that stores all information, regardless of its critical nature, age, and prior backup activity.

grey hat An individual or groups of individuals who waver between the classification of a hacker and a cracker, and who either act in goodwill or in malice.

hacker Someone who has mastered the hardware and software of modern computer systems and enjoys the exploration and analysis of network security with no intent to intrude or cause harm.

hactivist Hackers and crackers who use their extensive experience and skill to use networks to share their ideologies regarding controversial social, political, and economic topics.

Health Insurance Portability and Accountability Act (HIPAA) Strict laws for health institutions throughout the United States that ensure the security and privacy of patient records by dictating the way in which files are accessed, stored, and transmitted on a network.

hierarchical database structure A treelike storage schema that represents records and relationships through the use of tiers and parent-child relationships.

hijacking A process in which Web sites are hacked into and rewritten to react differently to users than how the original Web site designer intended.

honeypot A fake environment that includes false data to mislead intruders who are attempting to gather information about the database.

hot site An exact replica of an organization's network, or a mirror site, that promises the vendor will assume all responsibility for ensuring that the network is readily available in the event of a disaster.

Hypertext Transfer Protocol (HTTP) The portion of an Internet address that informs the browser what protocol is used to send the request for a particular Web site.

incremental backup An intentional copy of data, program files, and system configurations that is conducted on only the data that has changed since the last full or incremental backup.

inference A way that unauthorized users can obtain sensitive information by making assumptions based on the database's reactions or query responses to nonsensitive queries.

informal audit An audit conducted as a way to provide organizations evidence that their security policies and practices are effective and working properly.

information reconnaissance The process of gathering information either directly (e.g., actively) or indirectly (e.g., passively) from a system or the system's environment.

instance A broad term that refers to the background processes and structured memory used during interaction with the database.

integrated services A valuable tool in data warehouses where different types of data need to be joined together for reporting and extrapolation.

integrity Efforts taken through policy, procedure, and design in order to create and maintain reliable, consistent, and complete information and systems.

internal audit An audit conducted using a committee of individuals who are employees of the company itself.

internal security controls The systematic measures and checks put into place to ensure that networks remain sound and secure.

internal testing An assessment that is conducted within the organization's security border that will display vulnerabilities that exist among internal users such as employees and contractors. It also identifies attacks and the damage that can be caused within the network itself. A task conducted during an internal security assessment might include an evaluator logging in to a user's computer in an attempt to raise the user's privileges on a particular system.

Kerberos An authentication protocol that was built by MIT to provide secure means for authentication using symmetric-key cryptology to verify the identity of a client to a server and a server to a client.

key A single field or group of fields used to identify an entry in a table.

key logger Malware constructed to log every keyboard stroke that a user types on the keyboard.

lock A mechanism within a DBMS that controls concurrency by preventing users from taking hold of data until changes being made are completed or committed.

log file A file that stores information about the transactions in the database to be used for recovery and backup.

logic bomb Malware that can lie dormant until a specific predetermined variable is met, whose variables typically depend on the environment in which it resides.

login An object that is mapped to a user account within each database and is associated to users by the security identifier or SID.

macro A small program that enables users to automate a large number of repeated processes within a document.

macro virus Malware that can either be attached to a macro, or can replace a macro within a document, and that runs automatically when the document containing the infected macro is opened or closed.

malicious software A programming code written and used by unauthorized intruders to perform a certain task on a computer.

malware An abbreviation for the term malicious software.

memory target The reserved space for the buffer cache.

misleading applications Applications that deceive users into believing that their computer's security has been breached, therefore tricking the user into downloading and purchasing rogue antivirus tools to remove the bogus breach.

Mixed Mode Authentication A form of authentication that allows both Windows authentication and SQL Server authentication to be used. The database will accept both Windows and server logins.

multipartite virus A form of malware that combines the characteristics of a boot sector virus with those of a file-infected virus.

network database model A treelike structure that stores information in the form of a hierarchy, using tiers and parent-child-like entities to represent relationships.

network port scanner Automated tools that are designed to traverse the network in an attempt to locate available vulnerable ports and identify the services that they use.

network security A set of established procedures, standards, policies, and tools that are used to protect data from theft, misuse, and unwanted intrusions, activities, and attacks.

network sniffers The utilities that monitor the network looking for a number of combined types of vulnerability. Network sniffers can identify missing software patches, application types, application version numbers, open ports, operating systems, and firewalls, to name a few.

nonresident virus The general term for malware that requires users to initiate it by downloading a program or opening up an e-mail attachment.

online analytical processing (OLAP), (decision support systems [DSS]) Databases that store large volumes of historical data for report generating and analyzing.

online transaction processing (OLTP) database A database that is created for real-time storage and manipulation of data within an organization.

open source A term that refers to software that has been written to be distributed for use and downloaded free of charge.

operational information security A term that refers to the secure operation of an organization through the development and reliability of an environment's policies and procedures that focus on security policies, change management, update management, and disaster recovery plans.

optimization The process of locating the quickest and most efficient way to retrieve the data being requested by a user.

OS upgrade The process of installing a new version of an operating system onto a host or a server.

page A fixed unit of storage that is transferred or swapped from one storage device to another.

pagefile The dedicated swap space for a page.

parallel processing When more than one server processes one query at the same time.

parsing The act of analyzing a construction of a query for correct syntax and semantics.

passive reconnaissance The use of passive investigation methods to gather information about a system or an infrastructure indirectly.

password hash A cryptology-encoded string version of a user or system password.

password scanners Essentially, network sniffers that traverse the network searching for passwords from remote authentication systems. Password scanners capture passwords as they are sent remotely across the network and record them for the attacker to maintain.

patch A small program that is used to fix or update software programs or hardware devices.

payload The component of a worm that holds all of the instructions on how to affect each computer that it encounters.

personal identifiable information (PII) Personal information that identifies a person.

phishing The attempt to obtain PII from people through the use of spoofed e-mail addresses and URLs.

point of sales (POS) system A system that is meant to handle cash register or sales transactions.

polyinstantiation A strategy that allows the database to contain multiple instances of a record, all pointing to the same primary key, but contain and display different values to users of different security classifications.

polymorphism The incidence of changing forms, or self-modification.

primary data file The main data file for a SQL Server database which is the file of origin for the entire database and references all other secondary data files.

primary filegroup The collection of files that contains all of the SQL Server system files, including the primary data files.

primary key A field that contains a unique label by which we can identify a record or row in a table.

principle of least privilege A security standard by which each user added to a system is given the minimum set of privileges that he or she requires to conduct legitimate business within that system.

privilege The ability to access a specific database resource or to perform a specific action within a database.

process A set of instructions that is executed by the operating system intended to complete a task.

Process Global Area (PGA) The central area where information is stored for background and server processes. It allocates space for each individual background process.

programming language A type of synthetic language developed with a specific syntax and semantic rules that allows individuals to create statements or functions to interface and control the behavior or functionality of a machine.

proxy Trojan Malware that enables a cracker to use someone else's computer to access the Internet in order to keep his or her identity hidden.

query A search initiated by a user in an attempt to retrieve certain information from a database.

query cache A memory component that plays a role in ensuring that query processing is successful.

query engine A component of the architecture that optimizes and manages queries and SQL statements.

query management The steps taken by a database management application to process a user query.

read consistency A term that refers to the accuracy and reliability of data within a database.

redo log A file within a database that contains information regarding all changes made to the data within the database.

relational database A storage model in which common entities are stored within separate tables that use unique key identifiers to build relationships between these entities.

relationship A term that defines the association between two entities and binds them.

remote access and administration Trojan (RAT) Malware that provides remote access capability to the cracker from whom the virus originated, who in turn is provided complete control of and access to someone else's computer from a remote location.

replication The act of sending copies of one database to another database within a network.

report A document that contains a formatted result of a user's query.

resident virus Malware that installs itself or takes residence directly in the main system memory of a computer.

response file A file that holds the specification of a typical Oracle installation for the purpose of creating silent installations.

rogue access point A wireless access point (e.g., wireless router) that is installed within a company's wireless range without authorization, exposing the entire network and leaving it open for anyone and everyone to navigate.

role A set of related privileges that are combined to provide a centralized unit from which to manage similar users or objects of a database.

row (record, tuple) The component of a table that holds distinct units of data identified using unique strings of numbers or characters.

script kiddie Amateur cracker who uses programs and scripts written by other people to infringe upon a computer network system's integrity.

secondary (alternative) key A field with values that contains nonunique data and that can refer to several records at one time.

secondary data file An optional data file found within a SQL Server database that is not a primary data file.

security audit The procedures by which all of an environment's security controls and systems are thoroughly reviewed to identify and report weaknesses within an organization.

security policy A document that defines the overall goal of security and identifies the scope of what to secure, as well as the roles and responsibilities of the people within the organization.

security scope This defines the perimeter of the overall security assessment, the physical and logical area included within the assessment.

security testing The process of identifying the feasibility and impact of an attack or intrusion of a system by simulating active exploitation and executing potential attacks within that environment.

service ticket A unique key that is used to validate a person's identification (similar to a driver's license), for the purpose of gaining access into a secured environment.

shared site agreement An arrangement between companies with similar, if not identical, data centers.

signature A pattern of characters that is identified for a specific family of viruses.

silent installation An installation of an application that completes without prompting a user for setting specifications.

social engineer An individual who uses human interaction to manipulate people into gaining access to systems, unauthorized areas, and confidential information.

software upgrade A combination of a number of software or hardware packages that creates a new version of software.

sort (control) key A field in which values are used to sequence data.

source code A group of statements or functions written using a specific programming language and that are combined to create a specific type of application or utility.

source code installation Allows a user to download the actual MySQL source code, change it, and compile it into a binary file for installation execution.

spoofing A process that involves hackers building Web sites to look identical to other popular sites in hopes of drawing in a user.

spyware A general term for any software that intentionally monitors and records a user's computer and/or Internet activities.

SQL injections Methods by which intruders use bits of SQL code and SQL queries to gain database access.

startup page The Web site that is displayed when the Web browser is started.

static analysis An effort to find problems while the program is inactive.

static SQL statement A statement that is built by the user; the full text of the statement is known at compilation.

storage engine A component of the MySQL database architecture that reads and writes data to and from the database and offers services to enable customization of an environment.

storage management A term that refers to the process of storing and retrieving data throughout the database.

System Global Area (SGA) The central area where all shared data and processes are stored, including information shared by users and database processes.

table One of the most basic units of storage within a database, typically representing unique and specific data objects.

Tabular Data Stream (TDS) A Microsoft-defined protocol that describes the specifications as to how the SQL Server and a client can communicate.

thread A process that runs independently from another process. It utilizes a portion of the CPU and contains tasks or executions that share the same resources, yet run independently from one another.

time bomb (time-delayed virus) Malware that can lie dormant until a specific variable is met, such as times, days, or specific days that are predetermined and written within its code.

transaction The group of statements or operations processed by a database to execute a user's request to update or change the database.

transaction manager A component of the MySQL database architecture that is responsible for avoiding and resolving deadlocks and corrupted data.

transmission packet Sensitive information about users or businesses compiled by spyware that is sent back to its original creators for use as they see fit.

Trojan (Trojan horse) Malware that disguises itself and its harmful code and often hides within enticing programs such as software updates, games, and movies.

update A change to a system that is added to software or firmware that is already installed on a network.

update management policy A document that includes procedures for patch updates, software upgrades, OS upgrades, and firmware changes.

upgrade Replacements for older versions of software or firmware.

user-defined filegroup A collection of files created by a user.

user profile A set of rules that limits a user's access to database resources, and can be used to set password restrictions as well.

virtual address space The complete virtual memory area allotted to a program.

virtual memory A technique for extending the availability of memory by which units of storage located on different memory devices are used to store data from one entity in such a way that it appears as though the data has been stored in one continuous block of the same memory.

warm site A facility that contains the basic environmental concerns, as well as computers, connection firmware, and software devices necessary to rebuild a network system.

Web applications Programs that are available on a network and provide a way for users to interact with remote systems or databases.

Web browser An application that acts as a user interface of the Internet, allowing users to interact and view Web pages on the World Wide Web.

Web page A document containing a specific programming language (e.g., HTML or JAVA) that is designed to be viewable on the World Wide Web.

white box testing (targeted testing) An assessment that is conducted by an intruder who already has information about the system or the infrastructure. It is also known as targeted testing because prior knowledge exists and known weaknesses within the infrastructure allow for intruders to focus on specific areas of the infrastructure. The goal is to assess the damage that can be done by users who understand the infrastructure that they are attempting to intrude; the results will provide a more comprehensive, thorough picture of specific system weakness than that found in black box testing.

white hat An ethical hacker; hackers who use their extensive experience and knowledge to test systems and provide security consultation to others.

Windows Authentication mode A form of authentication that allows only Windows authentication to be used for accessing the database; those users logging in to the database must have a Windows login to access it.

Wired Equivalent Privacy (WEP) crackers Software applications that are used to decrypt WEP keys.

wireless scanners Utilities that identify vulnerabilities within a wireless network, including missing encryption keys and poor security measures.

word blocking The act of blocking keywords that are not allowed to be used as input within a Web application or a Web URL.

word filtering A balance of blocking those known keywords that are not allowed to be used as input within a Web application or Web URL, and identifying those keywords that are allowed to be used as input within a Web application or Web URL.

worker process A pool of either threads or fibers that SQL Server keeps for all user connections.

worm Self-replicating malware that is able to harness the power of networks and use this power in its attacks against them.

Index

A

- ABConsulting, 272
- access control, auditing, 252
- access points, rogue, 271
- account administration, auditing, 251–252
- Account Provisioning page, 135
- Active Data Guard application, Oracle, 155
- active reconnaissance, 268–269, 276
- activity, auditing, 253
- Add node to a SQL Server failover cluster link, 127
- Add Port option, 86
- administrator account, 205
- Advanced Cluster Completion link, 128
- Advanced Cluster Preparation link, 128
- Advanced Compression application, Oracle, 154
- advanced page, installing Microsoft SQL Server, 128
- Advanced Replication tool, 153
- Advanced Security Option, 154
- Advanced Security service, 179
- Advanced settings, Windows, 86
- adware, 20, 35
- alert of events, 196
- Allow program through Windows Firewall option, 86
- Allow the connection it is secure option, 87
- alpha phase, 81
- alternate key, 47, 71, 73
- amazon.com, 203
- Analysis Services Configuration window, 135, 136
- Analysis Services (SSAS), 123
- architecture, of Microsoft SQL Server, 65–66
- Archive storage engine, 64
- assessment phase of security architecture, 25
- attachments, e-mail, 15–16
- attributes, 50, 71
- audit scope, 245, 257
- auditing, 241–259
  - access control, 252
  - account administration, 251–252
  - activity, 253
  - data privileges, 252
  - encryption, 253
  - overview, 244–245
  - passwords, 252
  - planning for, 249–251
  - process of, 245–249
  - reporting on, 253–254
  - server maintenance, 251
  - types of, 243–244
  - vendor-specific information, 254–257
    - Microsoft SQL Server, 254
    - MySQL, 256–257
    - Oracle, 254–255
- authentication, 175–183
  - database authentication, 176
  - for Microsoft SQL Server, 178
  - for MySQL, 178–179
  - network authentication, 176–178
  - operating system authentication, 176
  - for Oracle, 179
  - password policies, 179–183
    - database-enforced, 180
    - for Microsoft SQL Server, 182
    - for MySQL, 182
    - for Oracle, 182–183
    - written, 180–182
  - third-party authentication, 176–178
- authorization, 183–192
  - adding and removing users, 185–186
  - default user accounts
    - for Microsoft SQL Server, 184
    - for MySQL, 185
    - for Oracle, 185
  - roles, 189–192
    - in Microsoft SQL Server, 190–191
    - in MySQL, 191
    - in Oracle, 192
  - user account management, 184
  - user privileges, 186–189
    - in Microsoft SQL Server, 186–187
    - in MySQL, 187–188
    - in Oracle, 188–189
- automated audits, 244, 257
- availability, 6–7, 35

B

- back door, 22, 35
- backup management plan, 31–32, 35
- beta phase, 80
- binary code installations, 79
- binary file, 79
- Bitmap Indexes feature, 153
- black box testing, 264, 276
- black hat, 8, 35
- Black Hole Engine, 65
- blind injections, 210
- bloggers, 83, 126, 157
- bond parameters, defending against SQL injection, 236
- boot sector, 20, 35
- bot (software robot), 35
- botmaster, 24, 35
- botnet, 24, 35
- browser plug-ins, 207
- brute force attacks, exploiting privileges using, 234
- buffer cache, 68, 69
- buffer management, for Microsoft SQL Server, 69
- buffer manager, 69, 71
- buffer pool, 69, 71
- bug alerts, 84
- BUILT-IN\Administration account, 184
- Business Intelligence Development Studio, 124

C

- C Include Files/Lib Files, 89
- caching, 58, 71
- CAL (Client Access License), 124, 143
- CallsRus, 191
- candidate key, 47, 71

case sensitivity, 232
Case statement, 232
CD-RW (compact disc-rewritable), 32
Change Management Pack application, Oracle, 155
checkpoint (CKPT), 57
CLDCLL_SALES_ROLE role, 189
Client Access License (CAL), 124, 143
Client Tools Connectivity, 124
clients, 199, 200
close ports, 167
CMAN (Oracle Connection Manager), 154
code, locating vulnerabilities for SQL injection, 212
cold site, 33, 35
column field, 71
Column_Name, 227
columns, 45, 230–231
Comma-separated values (CSV), 64
commit, 56, 71
common words, breaking down, 232
Community site, Oracle, 157
Compact 3.5, 121
compact disc-rewritable (CD-RW), 32
compiling, 79
Complete installation type, 89
Complete Package, MySQL, 85
Complete window, 137
complexity, 169, 180
components, of databases, 45–48
  keys, 45–47
  queries, 48
  tables, 45
composite key, 47, 71
computer security, 5, 35. *See also* security
computer users, as threats, 9–10
computer viruses. *See* viruses
concurrency, 56, 72
conditions, extracting data with SQL injection using, 228–229
confidentiality, 6, 36
Configuration Assistant window, 163
Configuration Management Pack application, Oracle, 155
configuration security options, 98
Configure the MySQL Server now check box, Configuration Wizard, 96, 98
connect to user, 179
connection context, 69
connections, encrypting, 108
control (sort) key, 73
control file, 58, 72
control key, 47
CPU, determining, 150
crackers, 7–8, 36
credentials, 175, 197
CSV (comma-separated values), 64
current user, 179
Custom installation screen, 89
Custom installation type, 89

D

data definition language (DDL), 62
data flow analysis, locating vulnerabilities for SQL injection, 214
data manipulation language (DML), 62
Data Mining application, Oracle, 154
Data Profiling and Quality application, Oracle, 154
Data Security Standard (DSS), 40
data structures, system-level, 68
data type errors, 227
database, 72
database administrator (DBA), 250
database authentication, 176
Database Configuration Assistant (DBCA), 149, 255
database connection manager, 61–62, 72
Database Engine Configuration window, 135, 136
Database Engine Services, 122
database link, 179, 197
database management system (DBMS), 44, 72, 248
database model, 48, 72
database response, 223
database security, 4–5, 36, 167
Database Vault application, 154
database-enforced password policies, 180
databases, 43–76
  components of, 45–48
    keys, 45–47
    queries, 48
    tables, 45
  defending against SQL injection
    by restricting databases, 236
    using security-consious design of, 236–237
  defined, 44
  environment policies, 27–35
    backup management plan, 31–32
    disaster plan, 33–35
    security policies, 27–28
    update and upgrade management, 28–31
  management systems for, 54–55
  Microsoft SQL Server, 65–71
    architecture and engines, 65–66
    installing, 113–144
    memory management for, 67–69
    physical structure of, 66
  models for, 48–53
    flat model, 48–49
    hierarchical model, 49–50
    network model, 50
    object-oriented databases, 51–52
    object-relational database, 53
    relational database, 50–51
  MySQL, 60–71
    database connection manager, 61–62
    installing, 77–111
    query engine, 62
    storage engine, 63–65
    storage management, 63
    transaction manager, 62–63
  Oracle, 57–60
    installing, 145–172
    instance and database, 57–58

memory structure of, 58–60
physical structure of, 58
query management in, 55–56
read consistency in, 55–56
relationships in, 53–54
restricting access to, 108
types of, 54
datafile, 58, 72
data-sending Trojan, 23, 36
DBA (database administrator), 250
DBCA (Database Configuration Assistant), 149, 255
DBMS (database management system), 44, 72, 248
DDL (data definition language), 62
deadlock, 56, 72
decision support system (DSS), 54
Dedicated MySQL Server Machine option, 100
Dedicated option, 100
default user accounts
for Microsoft SQL Server, 184
for MySQL, 185
for Oracle, 185
denial of service (DoS) attacks, 22, 36
denying privileges, 186
deployment phase of security architecture, 26–27
design phase of security architecture, 25–26
destructive Trojan, 23, 36
detailed configuration type, Configuration Wizard, 95, 98
Developer Edition, 121
Developer option, 99
Diagnostic Pack application, Oracle, 155
differential backup, 32, 36
digital certificate, 177, 197
digital signatures, 85, 110
digital versatile discs (DVD), 32
disaster plan, 33–35, 36
Disk Space Requirements Window, 133
disregard for company policy error, 9
distribution formats, for MySQL, 79–80
dll (dynamic link library), 67
DML (data manipulation language), 62
DNS (Domain Name Server), 14, 36
DoS (denial of service) attacks, 22, 36
downloading MySQL, 84–85
DSS (Data Security Standard), 40
DSS (decision support system), 54
DVD (digital versatile disc), 32
dynamic analysis, 212, 215
dynamic link library (dll), 67
dynamic SQL statement, 204, 215

E

Edition Upgrade link, 127
editions
of Microsoft SQL Server, 121–122
of MySQL, 80–82
of Oracle, 152–154
e-mail, 15–17
attachments, 15–16
embedded HTML in, 17
exploiting privileges using, 235
phishing with, 16
embedded HTML, in e-mail, 17
employees, defining roles of, 28
Enable TCP/IP Networking check box, 102
encoding, 232
encryption, 18, 36, 108, 168, 253
End User License Agreement, 87
engines, for Microsoft SQL Server, 65–66
Enterprise Edition, 121, 153, 154–155, 156
entities, 50, 72
Error and Usage Reporting window, 137
errors, vulnerabilities for SQL injection through, 208–211
Essentials Package, MySQL, 85
executable (exe), 67
expired passwords, 169, 180
exploitation, 221, 238. *See also* SQL injection
Express Edition (XE), 152, 155
external audits, 244, 257
external testing, 265, 276
extracting data with SQL injection, 225–232
advanced techniques for, 231–232
large-scale, 229–231
obtaining columns, 230–231
obtaining database names, 230
obtaining table names, 230
statement exploits, 225–232
using conditions, 228–229
using UNION, 226–227

F

failed attempts, 169, 180
Falcon Engine, 65
Fast Start Fault Recovery feature, 153
Feature Selection window, 130, 133
Federated storage engine, 64
fibers, 69, 72
fields, 45
file transfer protocol (FTP) Trojan, 23, 36
filegroups, 66, 72
file-infected viruses, 21, 36
Fine Grained Access Control feature, 153
firewalls, 167, 272
fixed database roles, 190–191
Fixed privileges, 186
fixed server roles, 190
flat model, 48–49, 72
Folder Name field, 89
foreign key, 46–47, 72
formal audits, 244, 257
Forums, Microsoft SQL, 126
free downloads, of Oracle, 157
FTP (file transfer protocol) Trojan, 23, 36
full backup, 32, 36

G

General Availability (GA), 80
General Public License (GPL), 79
glibc2.3 library, 94
GNU gunzip, 93
GNU tar, 93
GnuPG (Gnu Privacy Guard), 85
goals, for policies, 28

- GPL (General Public License), 79
- GRANT command, 188
- grantable privileges, 233
- granting privileges, 186
- graphical user interface (GUI), 124
- grey hat, 8, 36
- Guest user, 184
- GUI (graphical user interface), 124
- .gz format, 94

H

- –h option, 95
- hackers, 7–8, 36
- hactivist, 8, 36
- handling noncompliance, 28
- hard disk space, 149
- Hardware and Software Requirements link, 126
- hardware requirements
  - for Microsoft SQL Server, 115–119
  - for Oracle, 149–150
- Health Information Technology for Economic and Clinical Health (HITECH), 40
- Health Insurance Portability and Accountability Act (HIPAA), 6, 36
- help
  - for Microsoft SQL Server, 125–126
  - for MySQL, 83–84
  - for Oracle, 157–158
- hierarchical model, for databases, 49–50
- hijacking, 11, 36
- HIPAA (Health Insurance Portability and Accountability Act), 6, 36
- HITECH (Health Information Technology for Economic and Clinical Health), 40
- honeypot, 237, 238
- hot site, 33, 37
- How to Get Started with SQL Server 2008 Failover Clustering link, 127
- HTML (HyperText Markup Language), 11, 203
- HTTP (hypertext transfer protocol), 13, 37
- HTTP actions, 206–207
- HyperText Markup Language (HTML), 11, 203
- hypertext transfer protocol (HTTP), 13, 37

I

- ibdata1 file, 101
- IE (Internet Explorer), 14
- If statement, 232
- inappropriate disclosure, 9
- incremental backup, 32, 37
- inference, 193–197
  - examples of, 193–194
  - minimizing, 194–197
- informal audits, 243, 257
- information reconnaissance, 268–269, 276
- Information_schema, 233
- Information_Schema.Columns, 227
- Information_Schema.Tables, 227
- initiated delays, 228
- injection attack, SQL, 235
- injection defense, SQL, 235
- injections, SQL, 202, 215
- In-Memory Database Cache application, Oracle, 154
- InnoDB storage engine, 64
- InnoDB tablespace, 101
- Install As Windows Service option, Configuration Wizard, 96, 104
- Install Upgrade Advisor link, 127
- installation page, installing Microsoft SQL Server, 127
- Install-based configuration file link, 128
- Installed SQL Server features discovery report link, 127
- installing
  - Microsoft SQL Server, 126–128
    - advanced page, 128
    - installation page, 127
    - maintenance page, 127
    - options page, 128
    - resources page, 128
    - server installation center, 126–127
    - step-by-step instructions, 128–139
    - tools page, 127
  - MySQL
    - on UNIX, 93–96
    - on Windows, 85–86, 87–92
  - Oracle
    - on UNIX, 166
    - on Windows, 158–165
- instance, 57–58, 72
- Instance Configuration window, 133
- instant messages, as threats, 17
- Integrated Services (SSiS), 123, 143
- integrity, 6, 37
- internal audits, 244, 257
- internal security controls, 244, 257
- internal testing, 264, 276
- Internet, 10–15
  - Web browsers, 13–15
  - Web pages, 11–12
- Internet Explorer (IE), 14
- Internet Protocol (IP), 14
- Internet relay chat (IRC), 23
- intrusion, process of, 273
- IP (Internet Protocol), 14
- IP addresses, 108, 167
- IRC (Internet relay chat), 23

K

- KDC (Key Distribution Center), 177
- Kerberos, 176, 197
- Key Distribution Center (KDC), 177
- key logger, 270, 276
- keys, 45–47, 72
  - foreign key, 46–47
  - primary key, 46
- Knowledge Center, Oracle, 157

L

- Label Security application, 154
- Launch the MySQL Server automatically option, Configuration Wizard, 96, 104
- layers of security
  - computer security, 5
  - database security, 4–5
  - network security, 5

lexical analysis, locating vulnerabilities for SQL injection, 214–215
LGWR (log writer), 57
licensing options
  for Microsoft SQL Server, 124–125
  for Oracle, 155–156
Licensing Terms window, 132
locks, 56, 72
log cache, 69
log file, 66, 72
log writer (LGWR), 57
logic bombs, 19, 37
logic inference, 193–194
login, 175, 197
Look In list arrow, 89

M

m2 suffix, 81
macro, 20, 37
mailing lists, MySQL, 83
main memory, 150
maintenance page, installing Microsoft SQL Server, 127
malicious software, 11–12, 37
malware, 11–12, 18–24, 37
  Bots, 24
  computer viruses, 18–21
  Trojan viruses, 22–24
  worms, 21–22
management
  phase of security architecture, 27
  policies, updating, 28
  systems for databases, 54–55
  tools for Microsoft SQL Server, 123–124
  of user accounts, 184
Manual Setting, 102
many-to-many relationship, 54
Materialized View feature, 153
MD5 Checksum, 84
MDAC (Microsoft Data Access Components), 120
media type, choosing, 31
memory pool, for Microsoft SQL Server, 68–69
Memory storage engine, 64
memory structure
  of Microsoft SQL Server, 67–69
    buffer management, 69
    executable code, 67–68
    memory pool, 68–69
    threads and processes, 69–71
  of Oracle, 58–60
    PGA, 59–60
    processes, 60
    SGA, 59
memory target, 69, 72
Metalink account, 160
Metalink service, 157
Microsoft Data Access Components (MDAC), 120
Microsoft Online Books, 125
Microsoft SQL Forums, 126
Microsoft SQL release notes, 126
Microsoft SQL Server, 55, 65–71, 113–144
  architecture and engines, 65–66
  auditing, 254
  authentication for, overview, 178
  default user accounts for, 184
  editions of, 121–122
  features of
    licensing options, 124–125
    management tools, 123–124
    server tools, 122–123
  help for, 125–126
  installing, 126–128
    advanced page, 128
    installation page, 127
    maintenance page, 127
    options page, 128
    resources page, 128
    server installation center, 126–127
    step-by-step instructions, 128–139
    tools page, 127
  memory management for, 67–69
    buffer management, 69
    executable code, 67–68
    memory pool, 68–69
    threads and processes, 69–71
  password policies for, 182
  physical structure of, 66
  preinstallation preparation, 115
  requirements for, 115–119
  roles in, 190–191
  security suggestions for, 140–142
    after installation, 141–142
    during installation, 140–141
    prior to installation, 140
  software prerequisites, 120
  supported platforms, 119
  user privileges in, 186–187
Microsoft Windows Installer (MSI), 87
misleading applications, 15, 37
Mixed Mode Authentication, 135, 178, 197
models, for databases, 48–53
  flat model, 48–49
  hierarchical model, 49–50
  network model, 50
  object-oriented databases, 51–52
  object-relational database, 53
  relational database, 50–51
monitoring, defending against SQL injection with, 237–238
MSI (Microsoft Windows Installer), 87
Multifunctional option, 100
multipartite viruses, 21, 37
multiple layers of security
  computer security, 5
  database security, 4–5
  network security, 5
my.cnf file, 95, 106
my.ini file, 95, 98, 104
MyISAM storage engine, 64
MySQL, 55, 60–71, 77–111
  auditing, 256–257
  authentication for, overview, 178–179
  database connection manager, 61–62
  default user accounts for, 185
  downloading, 84–85
  editions of, 80–82
  forums for, 83
  help for, 83–84
  manual for, 83
  password policies for, 182
  preinstallation preparation, 79–84
  query engine, 62
  roles in, 191
  security suggestions for, 107–109

account access and user privileges, 108
network connection administration, 108–109
passwords, 108
storage engine, 63–65
storage management, 63
supported platforms, 83
transaction manager, 62–63
on UNIX
configuring, 106–107
installating tar.gz, 93–94
installing, 93–96
installing binary distributions, 93
installing RPM, 94–95
user privileges in, 187–188
on Windows
adding MySQL port in Windows 7, 86–87
adding MySQL port in Windows Vista, 86
configuring, 95–107
installing, 85–86, 87–92
mysql_install_db file, 106, 107
mysql.user table, 234

N

Name text field, 87
Native Mode type, 137
network and database administrators, as threats, 10
network authentication, 176–178
network connection administration, for MySQL, 108–109
network database model, 50, 72
network errors, 9
network model, for databases, 50
network port scanners, 270, 276
network resource requirements
for Microsoft SQL Server, 120
for Oracle, 152
network security, 5, 37
network sniffers, 268, 270, 276
New Inbound Rule Wizard dialog box, 87
New SQL Server failover cluster installation link, 127
new target, testing, 22
Noinstall Archive, MySQL, 86
noncompliance, handling, 28
non-platform-specific category, RPM package, 94
nonresident virus, 19, 37
Non-Transactional option, 100
Not Configured type, 137
nothing returned, 225
null, 227

O

objectives
of security, 5–7
availability, 6–7
confidentiality, 6
integrity, 6
of testing, 265
object-oriented databases, 51–52
object-relational database, 53
OFA (Optimal Flexible Architecture), 149
OLAP (online analytical processing), 54, 72, 123
OLTP (online transaction processing), 54, 72
one-to-many relationship, 53
one-to-one relationship, 53
online analytical processing (OLAP), 54, 72, 123
Online Index Rebuild feature, 153
Online Installation Help link, 127
online intruders, types of, 8
Online Release Notes link, 126
online transaction processing (OLTP), 54, 72
open source, 55, 72
opening unknown e-mails error, 9
OPENROWSET procedure, exploiting privileges using, 235
operating system (OS), 18, 167
authentication, 176
requirements
for Microsoft SQL Server, 119
for Oracle, 150
upgrades, 31, 37
operational information security, 27, 37
OPQ (Oracle Parallel Query), 153
Optimal Flexible Architecture (OFA), 149
optimization, 56, 73
options page, installing Microsoft SQL Server, 128
Oracle, 57–60, 145–172
auditing, 254–255
authentication for, overview, 179
default user accounts for, 185
editions of, 152–154
Enterprise Edition options, 154–155
free downloads of, 157
help for, 157–158
instance and database, 57–58
licensing options, 155–156
memory structure of, 58–60
PGA, 59–60
processes, 60
SGA, 59
OUI for, 158
password policies for, 182–183
physical structure of, 58
preinstallation preparation, 147–149
requirements for, 149–152
64-bit and 32-bit, 150–151
hardware requirements, 149–150
network resource requirements, 152
operating system requirements, 150
software requirements, 151
roles in, 192
security suggestions for, 166–170
checklist, 167–168
password policies and user accounts, 168–170
using Oracle security suite, 168
on UNIX, installing, 166
user privileges in, 188–189
on Windows, installing, 158–165
Oracle Active Data Guard application, 155
Oracle Advanced Compression application, 154

Oracle Change Management Pack application, 155
Oracle Community site, 157
Oracle Configuration Management Pack application, 155
Oracle Connection Manager (CMAN), 154
Oracle Data Guard feature, 153
Oracle Data Mining application, 154
Oracle Data Profiling and Quality application, 154
Oracle Database Standard Edition One (SEO), 152, 156
Oracle Database Standard Edition (SE), 153, 156
Oracle Diagnostic Pack application, 155
Oracle In-Memory Database Cache application, 154
Oracle Knowledge Center, 157
Oracle OLAP application, 155
Oracle Parallel Query (OPQ), 153
Oracle Partitioning application, 155
Oracle patches, 167
Oracle Provisioning and Patch Automation Pack application, 155
Oracle RAC One Nod application, 154
Oracle Real Application Clusters (RAC), 154
Oracle Real Application Testing application, 155
Oracle security suite, 168
Oracle Spatial application, 155
Oracle Streams feature, 154
Oracle Total Recall application, 155
Oracle Tuning Pack application, 155
Oracle University Installer (OUI), 158
Oracle University site, 157
orainstRoot.sh file, 166
OS. *See* operating system
OUI (Oracle University Installer), 158
OUI welcome screen, 160

P

pagefile, 67, 73
pages, 67, 73
Parallel Backup and Recovery feature, 154
Parallel DML feature, 153
Parallel Index Scans feature, 154
Parallel Indexing Rebuilding feature, 154
parallel processing, 56, 73
parsing, 56, 73
Partitioning application, Oracle, 155
passive reconnaissance, 268, 276
password discretion, 181
password error, 9
password hash, 233, 238
Password Management, 164, 166
password policies, 179–183
  database-enforced, 180
  for Microsoft SQL Server, 182
  for MySQL, 182
  for Oracle, 182–183
  written, 180–182
password scanners, 270, 277
passwords
  auditing, 252
  exploiting, 233–234
  reuse of, 180
  sharing, 181
  storing, 181
patch, 30, 37, 167
payload, 22, 37
Payment Card Industry (PCI), 40
Per Processor Licensing, 124
Per Server Plus Device CAL license, 124
Per Server Plus User CAL license, 124
performance monitor (PMON), 57
personal identifiable information (PII), 14, 37
PGA (Process Global Area), 57, 58, 59–60, 73
phases of security architecture
  assessment, 25
  deployment, 26–27
  design, 25–26
  management, 27
phishing, 16, 37
physical structure
  of Microsoft SQL Server, 66
  of Oracle, 58
PII (personal identifiable information), 14, 37
PKI (public key infrastructure), 177
planning
  for auditing, 249–251
  for testing, 266–267
platform-specific category, RPM package, 94
platforms, 83, 119, 223
PMON (performance monitor), 57
point of sales (POS) system, 54, 73
policies, for database environment, 27–35
  backup management plan, 31–32
  disaster plan, 33–35
  security policies, 27–28
  update and upgrade management, 28–31
polyinstantiation, 195, 198
polymorphism, 19, 37
poor habits, network error, 9
port addresses, 271
Port Number text field, 87
port redirection, 272
ports, 86–87, 108
POS (point of sales) system, 54, 73
primary data file, 66, 73
primary filegroup, 66, 73
primary key, 46, 73
principle of least privilege, 186, 198
privileges, 186–189
  auditing, 252
  exploiting, 232–235
    automated tools, 234–235
    brute force attacks, 234
    using e-mail, 235
    using OPENROWSET procedure, 235
  in Microsoft SQL Server, 186–187
  in MySQL, 187–188
  in Oracle, 188–189

procedure cache, 69
process, 60, 73
Process Global Area (PGA), 58, 59–60, 73
processes
  identifying, 28
  for Microsoft SQL Server, 69–71
  for Oracle, 60
processors, 156
procrastination, 9
Product Key window, 132
Program Global Area (PGA), 57
programming language, 79, 110
programs, 233
Provisioning and Patch Automation Pack application, Oracle, 155
proxy servers, 207
proxy Trojan, 23, 37
public key infrastructure (PKI), 177

Q

queries, components of databases, 48
query cache, 62, 73
query engine, 62, 73
query management, 55–56, 73
query responses, limiting, 196

R

RAC (Oracle Real Application Clusters), 154
RAC One Nod application, Oracle, 154
random access memory (RAM), 19, 150
RAT (Remote access and administration Trojan), 23, 38
RC (Release Candidate), 80
RDBMSs (Relational Database Management Systems), 51, 54
read consistency, 55–56, 73
Real Application Testing application, Oracle, 155
RECO (recovered), 57
records, 45
recovered (RECO), 57
redo log, 58, 73
relational database, 50–51, 73
Relational Database Management Systems (RDBMSs), 51, 54
relational engine, 66
relationships, 50, 53–54, 73
Release Candidate (RC), 80
release notes, Microsoft SQL, 126
Remote access and administration Trojan (RAT), 23, 38
remote access, disabling, 108
Remove node to a SQL Server failover cluster link, 127
removing user accounts, 185–186
Repair link, 127
replication, 122, 143
reporting
  on auditing, 253–254
  on testing, 274–276
Reporting Services Configuration window, 137
Reporting Services (SSRS), 122
reports, 48, 73
requirements
  for Microsoft SQL Server, 115–119
  for Oracle, 149–152
    64-bit and 32-bit, 150–151
    hardware requirements, 149–150
    network resource requirements, 152
    operating system requirements, 150
    software requirements, 151
residence, 19
resident virus, 19, 38
resources page, installing Microsoft SQL Server, 128
response file, 171
restricting access to databases, with IP addresses, 108
results returned, 224
reused passwords, 169
reverse Telnet, 272
revoking privileges, 186
rogue access point, 277
roles, 189–192
  in Microsoft SQL Server, 190–191
  in MySQL, 191
  in Oracle, 192
root commands, 94
root.sh file, 166
Row Level Security feature, 153
rows, 45
.rpm format, 94
run time, restricting, 167
./runInstaller.sh file, 166

S

SA account, 184
SALES_DEPTAPP_ROLE role, 189
sanitizing data, 236
Sarbanes-Oxley Act (SOX), 40
scope boundary, 267
script kiddie, 8, 38
scripting language, 222
SE (Oracle Database Standard Edition), 153, 156
Search for product updates link, 127
secondary (alternative) key, 73
secondary data file, 66, 73
secondary key, 47
security
  architecture of, 24–27
    assessment and analysis, 25
    deployment, 26–27
    design, 25–26
    management and support, 27
  objectives of, 5–7
    availability, 6–7
    confidentiality, 6
    integrity, 6
  reasons for, 3–7
  threats against, 7–17
    computer users, 9–10
    e-mails, 15–17
    hackers, 7–8
    instant messages, 17
    Internet, 10–15
    malware, 18–24
    misleading applications, 15
    network and database administrators, 10
    social engineers, 9
    tweets, 17

security audits, 243, 257, 263
Security Documentation link, 126
security patches, 167
security policies, 27, 38
security scope, 266, 277
security testing, 277
SELECT @@VERSION command, 224
SELECT statement, 227
self-encryption, 18
Send Windows and SQL Server Error Reports to Microsoft or your corporate report server option, 137
SEO (Oracle Database Standard Edition One), 152, 156
Server Books Online, SQL, 125
Server Configuration Manager, SQL, 123
Server Express Edition, SQL, 121
server maintenance, auditing, 251
Server Management Studio, SQL, 124
Server option, 100
Server Profiler, 124
server tools, for Microsoft SQL Server, 122–123
Service Accounts window, 133
service ticket, 177, 198
Setup Wizard exit screen, 99
setup.exe file, 87
SGA (System Global Area), 57, 58, 59, 74
shared site agreements, 33, 38
SharePoint Integrated Mode type, 137
SID (System Identifier), 164
signatures, 18, 38
silent installation, 158, 171
Single statement privileges, 186
SMON (system monitor), 57
social engineering, 269
social engineers, 9, 38
software requirements
  for Microsoft SQL Server, 120
  for Oracle, 151
software robot (bot), 35
software upgrades, 30, 38
sort (control) key, 73
sort key, 47
source code, 79, 110
source code installations, 79, 110
SOX (Sarbanes-Oxley Act), 40
Spatial application, Oracle, 155
spoofing, 12, 38
spyware, 19, 38
SQL (Structured Query Language), 48
SQL CAL, 124
SQL injection, 201–238
  defending against, 235–238
    diligent monitoring, 237–238
    restricting databases, 236
    sanitizing data, 236
    security-consious database design, 236–237
    using bond parameters, 236
  exploiting privileges and passwords, 232–235
    identifying privileges, 232–233
    obtaining passwords, 233–234
    obtaining privileges, 234–235
  extracting data with, 225–232
    advanced techniques for, 231–232
    large-scale, 229–231
    statement exploits, 225–232
    using conditions, 228–229
    using UNION, 226–227
  identifying vulnerabilities for, 205–215
    data flow analysis, 214
    direct testing, 212
    and HTTP actions, 206–207
    inferential testing for, 205–206
    lexical analysis, 214–215
    string-based matching, 213
    through errors, 208–211
    using code for locating, 212
  information gathering for, 221–225
    about database, 222
    identifying vendor, 222–224
    identifying version, 224–225
  overview, 202–205
SQL Server, 65
SQL Server Books Online, 125
SQL Server Configuration Manager, 123
SQL Server Express Edition, 121
SQL Server Management Studio, 124
sql_logins table, 234
SSAS (Analysis Services), 123
SSH encryption, 108
SSiS (Integrated Services), 123, 143
SSL encryption, 108
SSRS (Reporting Services), 122
Standard Character Set option, 102
standard configuration, Configuration Wizard, 95
Standard Configuration option, Configuration Wizard, 96
Standard Edition, 121
startup page, 14, 38
statement exploits, 225–232
static analysis, 212, 215
static SQL statement, 204, 215
statistical inference, 194
stealth, 18
storage engines, 63–65, 66, 74
storage management, 63, 74
storage units, swapping, 67
Streams feature, Oracle, 154
Strict Mode, 102
string-based matching, 213
Structured Query Language (SQL), 48
swapping units of storage, 67
sys.columns, 231
System Configuration Checker link, 126, 127, 130
System Global Area (SGA), 57, 58, 59, 74
System Identifier (SID), 164
system monitor (SMON), 57
system-level data structures, 68
system.mgmt_credentials2.table, 234
sysxlogins table, 234

T

table identification, 231
Table_Name, 227
tables
  components of databases, 45
  obtaining names for data extraction, with SQL injection, 230

- Tabular Data Stream (TDS), 65, 74
- TAF (Transparent Application Failover), 153
- .tar format, 94
- target testing, 265, 277
- TCP Protocol, 86
- TDE (transparent data encryption), 140
- TDS (Tabular Data Stream), 65, 74
- technical support, 157
- testing, 261–279
  - escalating privileges, 273–274
  - information reconnaissance, 268–269
  - objectives of, 265
  - obtaining access, 269–273
    - exploiting network hardware, 271–272
    - exploiting operating system, 272–273
    - exploiting Web applications, 273
    - using automated tools, 269–271
  - planning for, 266–267
  - reporting on, 274–276
  - types of, 264–265
- TFName, 213
- TGS (Ticket-granting service), 177
- TGT (ticket-granting ticket), 177
- third-party applications, 207
- third-party authentication, 176–178
- threads, for Microsoft SQL Server, 69–71
- threats, 7–17
  - computer users, 9–10
  - e-mails, 15–17
    - attachments, 15–16
    - embedded HTML in, 17
    - phishing with, 16
  - hackers, 7–8
  - instant messages, 17
  - Internet, 10–15
    - Web browsers, 13–15
    - Web pages, 11–12
  - misleading applications, 15
  - network and database administrators, 10
  - social engineers, 9
  - tweets, 17
- Ticket-granting service (TGS), 177
- ticket-granting ticket (TGT), 177
- time bomb (time-delayed virus), 19, 38
- time-based responses, 228
- tools page, installing Microsoft SQL Server, 127
- Total Recall application, Oracle, 155
- transaction commits, 56
- transaction manager, 62–63, 74
- Transactional Database Only option, 100
- Transactional option, 100
- transactions, 56, 74
- transmission packet, 19, 38
- Transparent Application Failover (TAF), 153
- transparent data encryption (TDE), 140
- Transportable Tablespaces feature, 153
- Trojan horse, 38
- Trojan viruses, 22–24
- Tuning Pack application, Oracle, 155
- tuples, 45
- tweets, as threats, 17
- Twitter.com, 17, 83, 126, 158
- Typical installation type, 89

U

- undo, transaction commits, 56
- Uniform Resource Locator (URL), 12
- UNION statement, 226–227
- units of storage, swapping, 67
- Universal Serial Bus (USB), 9
- University site, Oracle, 157
- UNIX, MySQL on
  - configuring, 106–107
  - installating tar.gz, 93–94
  - installing, 93–96
  - installing binary distributions, 93
  - installing RPM, 94–95
- update management policy, 38
- updates, 28–31, 38
- Upgrade Documentation link, 127
- Upgrade for SQL Server 2000 or SQL Server 2005 link, 127
- Upgrade Integration Services Package link, 127
- upgrades, 28–31, 38
- URL (Uniform Resource Locator), 12
- USB (Universal Serial Bus), 9
- user accounts
  - adding and removing, 185–186
  - default
    - for Microsoft SQL Server, 184
    - for MySQL, 185
    - for Oracle, 185
  - management of, 184
- user capability, limiting, 196
- user profile, 183, 198
- user-defined filegroup, 66, 74
- UserInput, 213
- users, as threats, 9–10

V

- –v option, 95
- /var/lib/mysql directory, 95
- versions, 224–225. *See also* editions
- virtual address space, 67, 74
- virtual memory, 67, 74
- Virtual Private Database (VPD), 153
- viruses, 18–21
  - categories of, 19–20
  - types of, 20–21
- VPD (Virtual Private Database), 153
- vulnerabilities for SQL injection, 205–215
  - data flow analysis, 214
  - direct testing, 212
  - and HTTP actions, 206–207
  - inferential testing for, 205–206
  - lexical analysis, 214–215
  - string-based matching, 213
  - through errors, 208–211
  - using code for locating, 212

W

- warm site, 33, 38
- WBDS (World Bank Database Society), 177
- Web applications, 203, 215

Web browsers, 13–15, 38
Web Edition, 121
Web pages, 11–12, 38
Web sites, 12, 125
WEP (Wired Equivalent Privacy) crackers, 271, 277
white box testing, 265, 277
white hat, 8, 38
Windows, MySQL on
  adding MySQL port in Windows 7, 86–87
  adding MySQL port in Windows Vista, 86
  configuring, 95–107
  installing, 85–86, 87–92
Windows Authentication mode, 135, 178, 198
Windows Firewall with Advanced Security dialog box, 86
Wired Equivalent Privacy (WEP) crackers, 271, 277
wireless scanners, 270, 277
word blocking, 236, 238
word filtering, 236, 238
worker process, 70, 74
Workgroup CAL, 124
Workgroup Edition, 121
World Bank Database Society (WBDS), 177
worms, 21–22, 38
written password policies, 180–182

X

XE (Express Edition), 152, 155

Y

yahoo.com, 14

Z

.zip format, 94