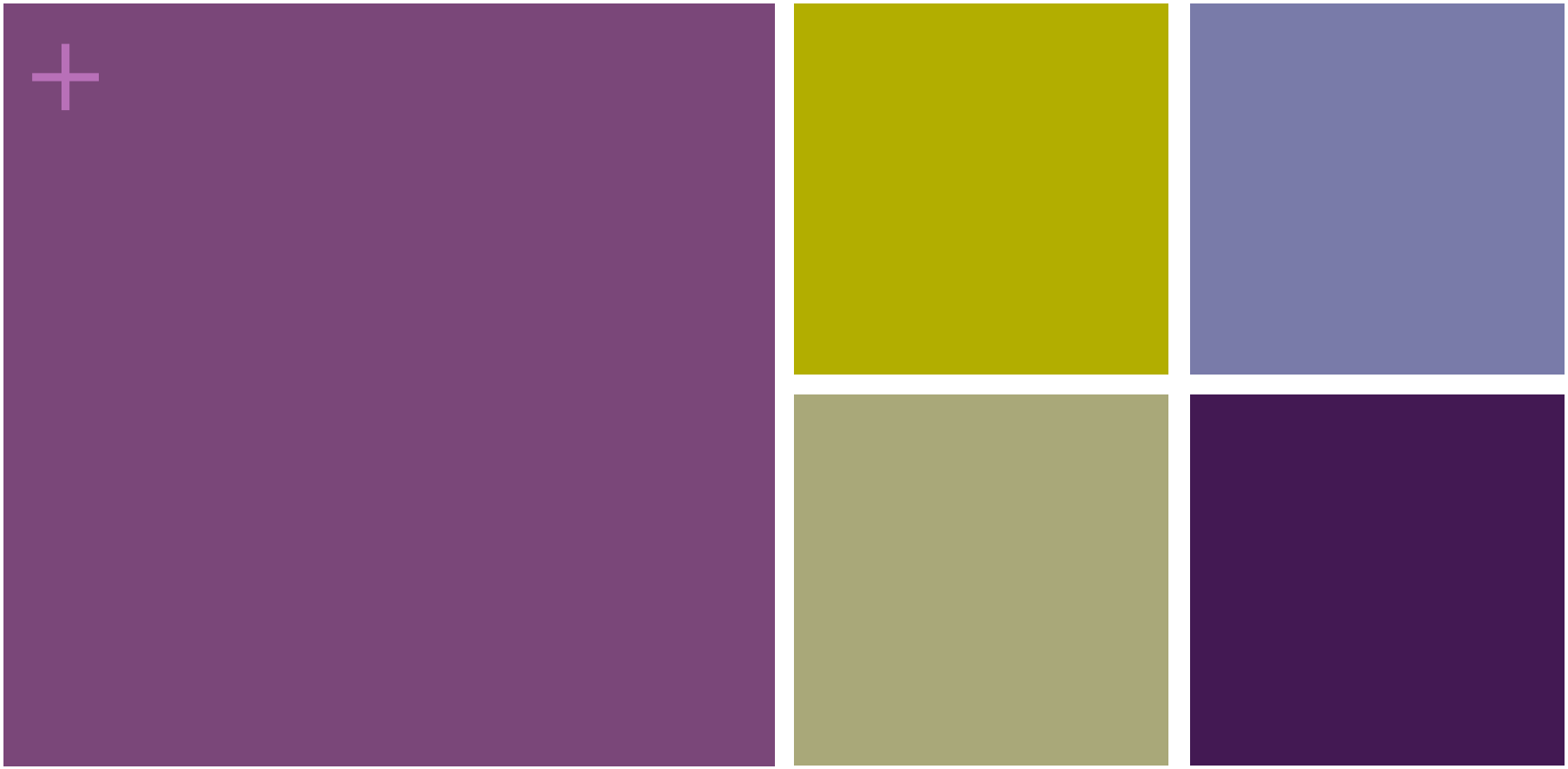

Database Security

Security Testing

Objectives

- Provide an overview of security testing fundamentals
- Identify the difference between security testing and security auditing
- Describe the methodology used to perform a security test
- Define common techniques that intruders use to gather information
- Describe common methods used to gain unauthorized access into a system
- Identify common strategies used to escalate one’ s privileges in a system

Security Testing

- Process of identifying the feasibility and impact of an attack or intrusion by:
  - Simulating active exploitation
  - Executing potential attacks within the environment
- Active evaluation of security measures
- Conducted from an attacker’ s perspective
- Typically outsourced to third-party
- Differences between auditing and security testing
  - Audits conducted to locate potential weaknesses within company’ s internal controls

Security Testing (cont’ d.)

- Differences between auditing and security testing
  - Security testing does not cover security policies, human resources, and legal or standards compliance
    - Security auditing covers these areas
  - Auditing compares documentation with the architecture
    - Ensures environment’ s accuracy and reliability
  - Security testing measures environment’ s strength and effectiveness

Security Testing (cont’ d.)

- Differences between auditing and security testing (cont’ d.)
  - Security testing can be conducted without prior knowledge of the environment
    - Auditing requires a great deal of infrastructure knowledge
  - Penetration testing is more costly and time consuming than auditing
    - Often conducted with a very narrow scope

Security Testing (cont’ d.)

- Characteristics of a security tester
  - Similar to those of a security auditor
  - Ability to think and act like an intruder
    - Attack attempts are creative

Security Testing Classification

- Successful testing is conducted from the attacker’s perspective
  - Includes both internal and external vantage points
- Different testing perspectives
  - Internal
    - Conducted within organization’s security border
  - External
    - Conducted outside organization’s network security border
  - Black box
    - Conducted with no prior knowledge of the system

Security Testing Classification (cont’ d.)

- Different testing perspectives (cont’ d.)
  - White box (target testing)
    - Conducted by an intruder with existing information about the system
- Skill sets required to conduct the tests
  - External and black box testers have broad, diverse skills
    - Knowledge of different network and security technologies
  - Internal or white box testers may have less expertise
    - Because they have awareness of the environment

The Goal of Security Testing

- Test the strength of implemented security measures
- Goals of a security test depend on:
  - Type of test conducted
  - Scale of testing
- Examples of common testing goals
  - Assess ability to block intruders from obtaining administrative rights to a critical database
  - Assess ability to block access to the physical location of the database

Testing Methodology

- Security testing is time- and resource-intensive
- Unstructured approach is ineffective
- Standardized testing methodology allows:
  - Prioritization to address resource constraints
  - Decreased assessment time by avoiding redundancy
  - Improved picture of security strength using enforced consistent testing
  - Efficient communication using standardized reports

Planning and Preparation Phase

- Defining the scope
  - Security scope defines perimeter of overall assessment
    - Physical and logical area being assessed
  - Examples of scope
    - Database servers, finance department, injections, escalated privileges
- Scope defined by:
  - Goal of particular security test

Planning and Preparation Phase (cont'd.)

- Example of white box testing scope definition
  - Goal: ensure privileges cannot be escalated by unauthorized users on database servers
  - Scope: hardware, software, and related tasks that assessor needs to use to test against that goal
  - Out of scope: all other hardware, software, and unrelated tasks
- Black box testing scope definition
  - Perimeter cannot be defined because tester has no information about systems

Planning and Preparation Phase (cont'd.)

- Black box testing scope definition (cont'd.)
  - Scopes often defined by analyzing level of access achieved by the attacker
  - Determine how much information would need to be obtained to access different levels of infrastructure
- Other tasks involved in developing a scope
  - Defining a contract or service-level agreement
  - Conducting a threat assessment
  - Scheduling an assessment
  - Listing resources needed to complete assessment

Planning and Preparation Phase (cont'd.)

- Gathering information
  - Done prior to assessment
    - To prioritize and identify goals
  - Done during assessment (information reconnaissance)
    - To identify information leaks within the infrastructure
- Examples of information obtained prior to the database security assessment
  - Infrastructure information found in network diagrams and database schematics

Planning and Preparation Phase (cont'd.)

- Examples of information obtained prior to the database security assessment (cont'd.)
  - A prioritized set of data storage server and information assets
  - Weak areas of the database infrastructure, those areas lacking sufficient defense
  - Areas that have the highest potential for attack (sensitive data)
  - Areas that offer entry points for intruders
  - Potential attack strategies based on infrastructure or recent and past trends of intruders

Planning and Preparation Phase (cont’d.)

- Information gathering process can change the original course of the assessment
- Examples of tools that aid information gathering
  - Port and vulnerability scanning tools
  - Surveillance cameras

Execution Phase

- Conducting the database security assessment
- Tasks depend on:
  - Area tested
  - Type of test
  - Scope of test
  - Test priority
- Techniques covered in this section
  - Apply to black box security assessment
  - Intruder’ s perspective

Execution Phase (cont’ d.)

- Information reconnaissance
  - Information gathering
    - Direct or indirect methods can be used
  - Greatest security defense is time
    - Allows time for security logs to capture their presence
- Types of information reconnaissance
  - Passive reconnaissance
    - Uses passive investigation methods
    - Gathers system information without direct interaction with the system

Execution Phase (cont'd.)

- Examples of tools used for passive reconnaissance
  - Network sniffer to capture network activity
    - Gives information about amount, frequency, and type of communication on a network
  - Database and SQL sniffers
    - Intended to help DBAs and developers monitor their own database systems
    - Can be used by unauthorized individuals to gather information about a database without communicating with it directly

Execution Phase (cont’ d.)

- Types of information reconnaissance (cont’ d.)
  - Active reconnaissance
    - Uses active investigation methods
- Examples of tools used for active reconnaissance
  - SQL injections used to make inferences about system or environment
  - Automated tools to send pings or packets to initiate a response
- Using active methods can lead to the detection of an intruder on the system

Execution Phase (cont’ d.)

- Scenario illustrating passive and active reconnaissance
  - Man decides to rob convenience store
  - Passive reconnaissance methods
    - Watching the store from car
    - Noting clerks’ habits and time schedules of changing register drawers and opening the safe
  - Active reconnaissance methods
    - Shopping the store and talking to clerks
    - Looks at positioning of the safe, phones, alert buttons

Execution Phase (cont’ d.)

- Obtaining access into a system infrastructure
  - Common initial milestone in security assessment process
- Common doors intruders use to obtain access
  - Physical server, wireless network
- Use of automated tools can aid:
  - Data capture
  - Password cracking
  - Finding vulnerabilities
  - Identifying hardware, software, and network devices

Execution Phase (cont’ d.)

- Network port scanners
  - Designed to traverse network and locate vulnerable ports
- Key logger
  - Hardware that records keystrokes of a user into a text file sent back to the attacker for a specific period of time and frequency
- Password scanners
  - Traverse network searching for passwords from remote authentication systems
    - Capture, record, and return passwords

Port address	Service	Comments
21	File Transfer Protocol (FTP)	Used for FTP file transfers, uploading and downloading files from a server
23	Telnet	Used for all Telnet sessions, connecting to a remote machine
25	Simple Mail Transfer Protocol	Used for sending outgoing mail
53	Domain Name Service (DNS)	Used to transfer domain name information
67	Dynamic Host Configuration Protocol (DHCP)	Used for allocating new leases and IP addressing information
80	Hypertext Transfer Protocol (HTTP)	Used for Internet traffic and requests
110	Post Office Protocol 3 (POP3)	Used to support incoming e-mail messages
161	Simple Network Management Protocol	Used to gather information about network device status
1433	SQL Server and SQL Server Replication	Used as the default connection to a Microsoft SQL Server database and for replication of Microsoft SQL servers
1434	SQL Server Monitoring	Used by Microsoft SQL Server for monitoring performance of the database servers
1521	Oracle	Used as the default connection to an Oracle database
3306	MySQL	Used as the default connection to a MySQL database

Table 10-1 Common port addresses

Execution Phase (cont’ d.)

- Network sniffers
  - Traverse network searching for packets of data from which information can be extracted
  - Can identify missing software patches, application types, operating systems, firewalls, and more
- Wireless scanners
  - Identify vulnerabilities within a wireless network
    - Missing encryption keys and poor security measures
  - Scanning can be active or passive

Execution Phase (cont'd.)

- Wired Equivalent Privacy (WEP) crackers
  - Software applications used to decrypt WEP keys
  - Provide attackers with entry into a wireless environment
- Exploiting network hardware
  - Rogue access points
    - Wireless access point installed without authorization
    - Allows intruders access to network
  - Firewall penetration
    - Older firewalls contain services and default accounts with known security vulnerabilities

Execution Phase (cont’ d.)

- Port redirection and reverse Telnet
  - A well-known access technique
  - Works by redirecting packets into unauthorized territory
- Exploiting the operating system
  - Operating systems released with limited testing
    - Rely on customers to report security vulnerabilities
  - Patches must be installed promptly to keep network secure

Execution Phase (cont’ d.)

- Exploiting Web applications
  - Web applications interact with servers
    - Legitimate way for intruders to gain access
  - Example
    - Network, database, and SQL sniffers used to identify database applications
    - Vulnerabilities identified through Internet search
    - Attacker exploits vulnerability to gain access
    - Attacker uses SQL statements to construct database schema and escalate user privileges

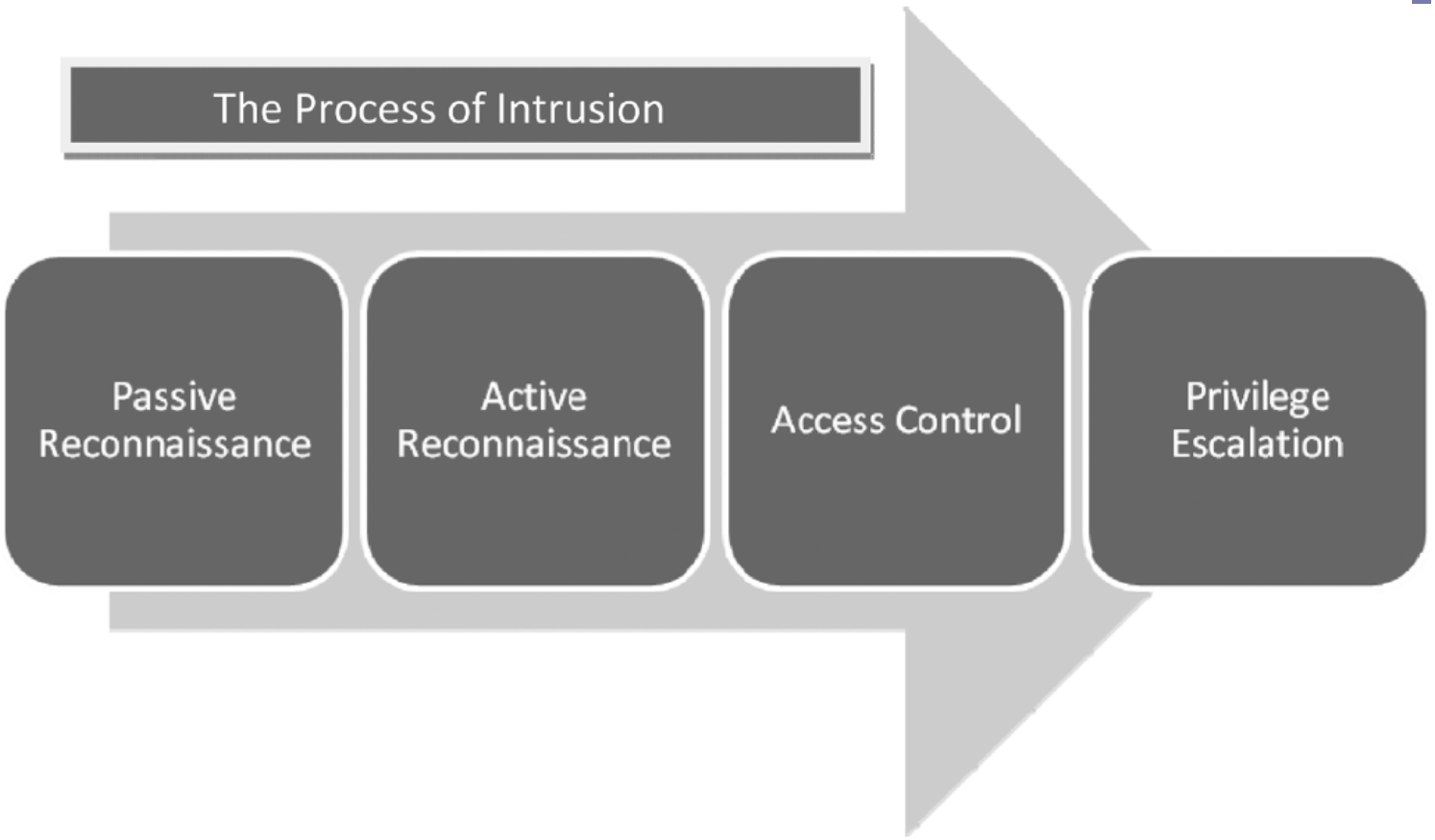

Figure 10-1 The process of intrusion

Escalating Privileges

- Methods for escalating privileges depend on:
  - How user is physically connecting to the database
  - User account that attacker is using to connect
- Common methods for escalating privileges
  - Manipulate guest accounts to increase account capabilities
  - Use password cracker to decrypt passwords obtained from the OS, network, or database
  - Use network sniffers to discover passwords traveling across the network

Escalating Privileges (cont’ d.)

- Common methods for escalating privileges (cont’ d.)
  - Manipulate Windows services written to be executed as the local system account
  - Use third-party tools designed to allow users to run code for escalating privileges
  - Use cross-site scripting techniques to run malicious code on the local machine using the Web browser
  - Use brute force strategies to increase user credentials and privileges

Escalating Privileges (cont’ d.)

- Common methods for escalating privileges (cont’ d.)
  - Use passive information-gathering techniques and the individual’ s current system privileges to learn more about the system’ s security structure

Reporting Phase

- Final step of the security assessment
  - Results are analyzed
  - Report is drawn up
    - Report format should be detailed
- Common components of a written security assessment report
  - Gathered background information
  - Defined perimeter and scope
  - Security assessment objective

Reporting Phase (cont’ d.)

- Common components of a written security assessment report (cont’ d.)
  - Key findings
  - Remediation recommendations, including deliverables, resources, and time frame
  - Methodology used for penetration testing
  - Remediation process including detailed steps
  - Schedule for a repeat security assessment for remediated areas

Summary

- Security testing
  - Process of penetrating the security of an environment to measure its strength and determine the feasibility of an attack
  - Often conducted on small group of assets within an organization
- Ideal security strategy includes both testing and auditing
- Types of security assessments include internal, external, black box, and white box

Summary (cont’ d.)

- Defining scope for a black box test is more difficult than a white box test because of lack of information about the infrastructure under test
- Planning for a white box test includes pretest information gathering, scope and perimeter definition, contract development, assessment scheduling, and threat prioritization
- Active and passive reconnaissance can be used to gather information about a system
- Several automated tools are available to aid an intruder in gaining access to a system