

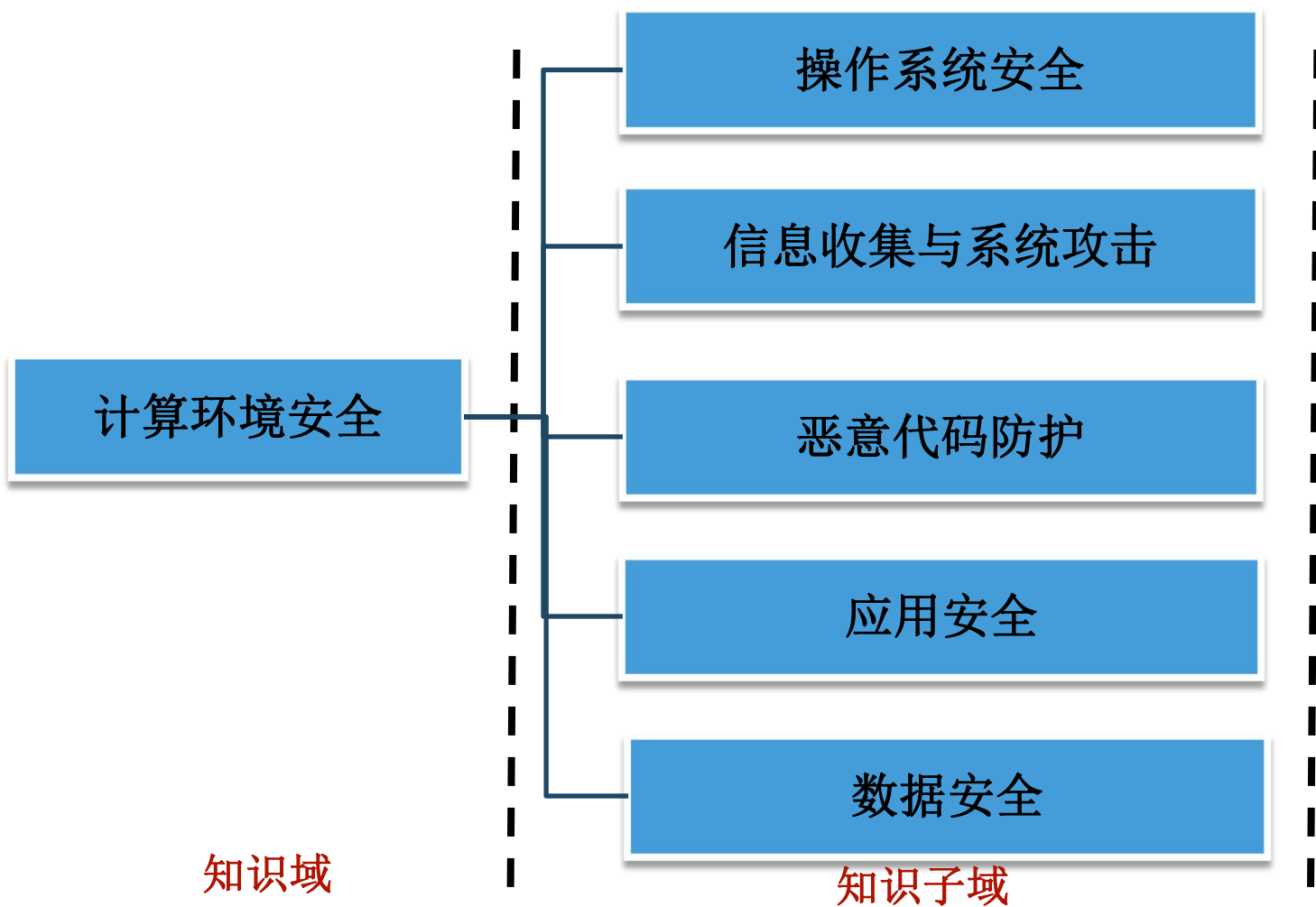
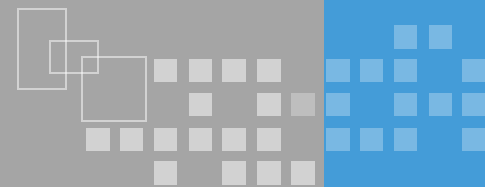


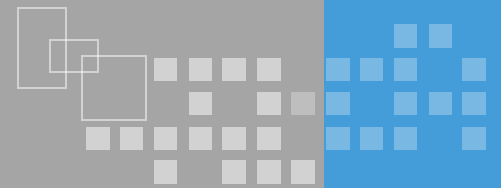
计算环境安全

版本：4.2

河南信安世纪 齐文振

课程内容



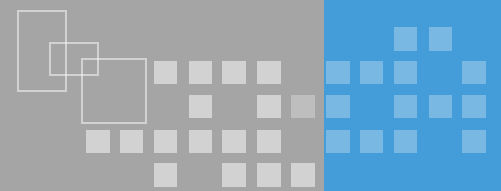


❖ 操作系统安全机制

- 了解操作系统标识与鉴别、访问控制、权限管理、信道保护、安全审计、内存存取、文件保护等安全机制；

❖ 操作系统安全配置

- 了解安全补丁、最小化部署、远程访问控制、账户及口令策略、安全审计及其他操作系统配置要点。

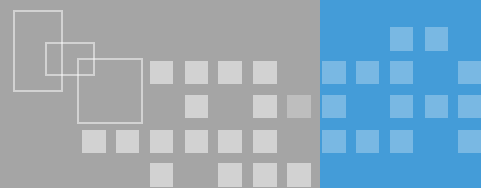


❖ 操作系统安全目标

- 标识系统中的用户和进行身份鉴别
- 依据系统安全策略对用户的操作进行访问控制，防止用户和外来入侵者对计算机资源的非法访问
- 监督系统运行的安全性
- 保证系统自身的安全和完整性

❖ 实现目标的安全机制

- 标识与鉴别、访问控制、最小特权管理、信道保护、安全审计、内存存取保护、文件系统保护等



❖ Windows系统的标识

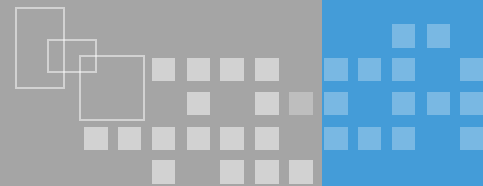
- 安全主体（账户、计算机、服务等）
- **安全标识符**（Security Identifier, SID）
 - 安全主体的代表（标识用户、组和计算机账户的唯一编码）
 - 范例：S-1-5-21-1736401710-1141508419-1540318053-500



相对标识符	说明
500	管理员
501	来宾
502	密钥分发中心服务的服务账户
512	域管理员
513	域用户
514	域来宾
515	域计算机
516	域控制器
544	内置管理员
545	内置用户
546	内置来宾

❖ Linux/Unix系统的标识

- 安全主体：用户标识号（User ID）



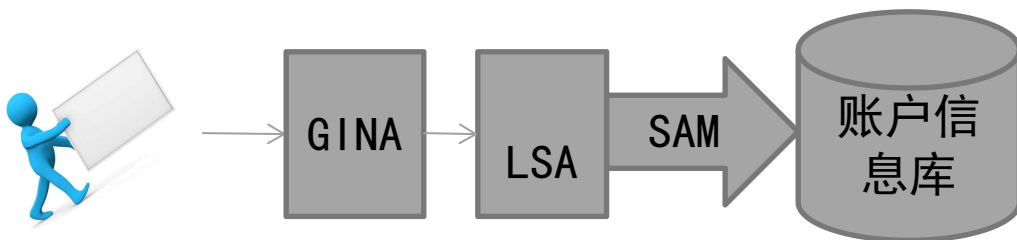
❖ Windows系统用户信息管理（SAM）

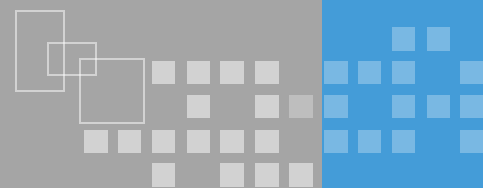
- 存储在注册表中，运行期锁定
- 操作权限`system`，依靠系统服务进行访问
- 示例：Windows密码散列值（LM-Hash）

Administrator: 500:C8825DB10F2590EAAAD3B435B51404EE
:683020925C5D8569C23AA724774CE6CC:::

❖ 身份鉴别

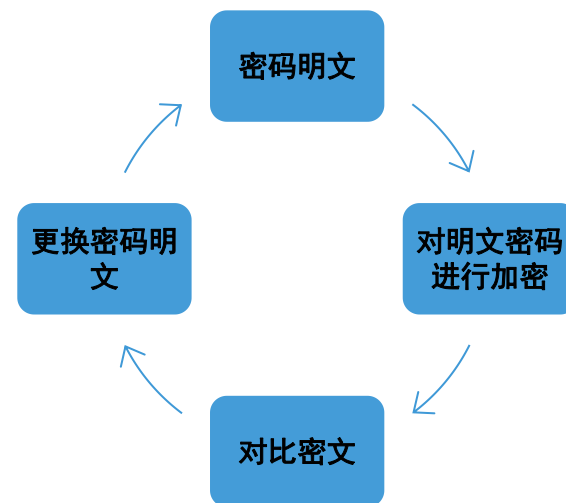
- 远程鉴别
 - SMB、LM、NTLM
- 本地鉴别





❖ Linux系统用户信息管理

- 用户帐号文件 (/etc/passwd)
 - 使用不可逆DES算法加密的用户密码散列（早期）
 - 文本格式、**全局可读**
- 影子文件 (/etc/shadow)
 - 存储存放用户密码散列、密码管理信息等
 - 文本格式，仅**对root可读可写**



#root:\$1\$acXMce89:13402:0:99999:7:::

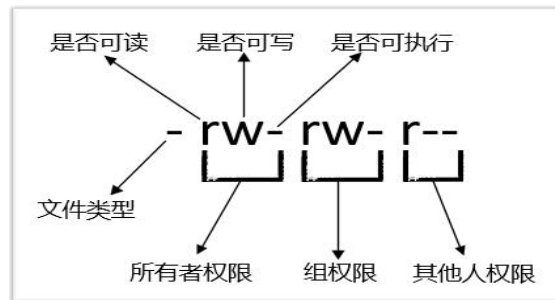
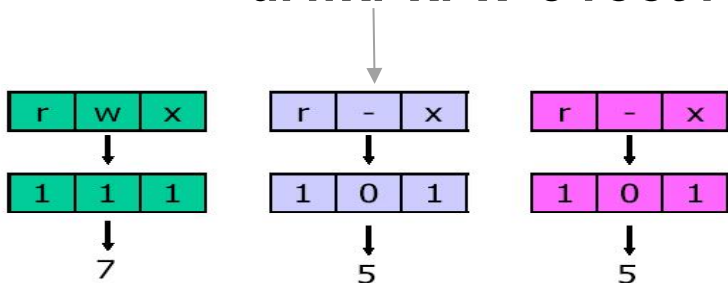
❖ Windows的访问控制

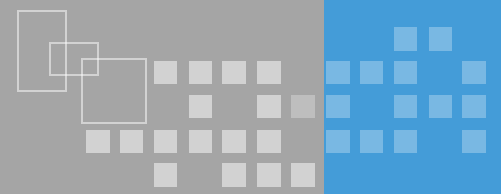
- 访问令牌（包含SID和特权列表），以用户身份运行的进程都拥有该令牌的一个拷贝
- 访问控制列表(ACL)，仅NTFS文件系统支持

❖ Linux下的访问控制

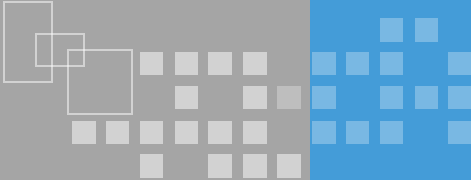
- 需要文件系统格式支持
- 权限类型：读、写、执行（UGO管理机制）
- 权限表示方式：模式位

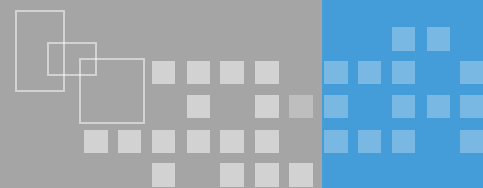
drwxr-xr-x 3 root root 1024 Sep 13 11:58 test





- ❖ Linux 系统中常用数字来表示文件的访问权限，假设某文件的访问限制使用了 755 来表示，则下面哪项是正确的（）
- ❖ A. 这个文件可以被任何用户读和写
- ❖ B. 这个可以被任何用户读和执行
- ❖ C. 这个文件可以被任何用户写和执行
- ❖ D. 这个文件不可以被所有用户写和执行

- 
- ❖ 以下关于 Windows 系统的账号存储管理机制 SAM（Security Accounts Manager）的说法哪个是正确的：（ ）。
 - ❖ A. 存储在注册表中的账号数据是管理员组用户都可以访问，具有较高的安全性
 - ❖ B. 存储在注册表中的账号数据只有 administrator 账户才有权访问，具有较高的安全性
 - ❖ C. 存储在注册表中的账号数据任何用户都可以直接访问，灵活方便
 - ❖ D. 存储在注册表中的账号数据只有 System 账户才能访问，具有较高的安全性



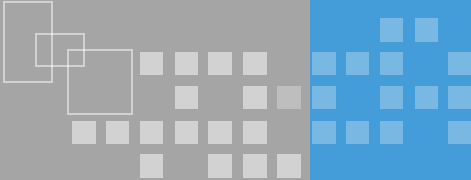
❖ Windows系统特权管理

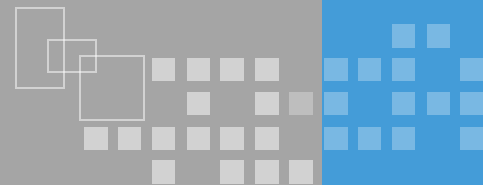
- 用户帐户控制（UAC）
 - 标准受限访问令牌&完全访问令牌

❖ Linux系统特权管理

- 限制对root使用，su及sudo命令
- Suid位：任何用户执行文件运行权限都为文件所有者的权限

```
-r-s--x--x  1 root  root    10704 Apr 15  2002 /usr/bin/passwd  
^SUID程序
```

- 
- ❖ Linux 系统对文件的权限是以模式位的形式来表示，对于文件名为test 的一个文件，属于admin 组中user 用户，以下哪个是该文件正确的模式表示？（系统安全）
 - ❖ A. `rwxr-xr- 3 user admin 1024 Sep 13 11: 58 test`
 - ❖ B. `drwxr-xr-x 3 user admin 1024 Sep 13 11: 58 test`
 - ❖ C. `rwxr-xr-x 3 admin user 1024 Sep 13 11: 58 test`
 - ❖ D. `drwxr-xr-x 3 admin user1024 Sep 13 11: 58 test`

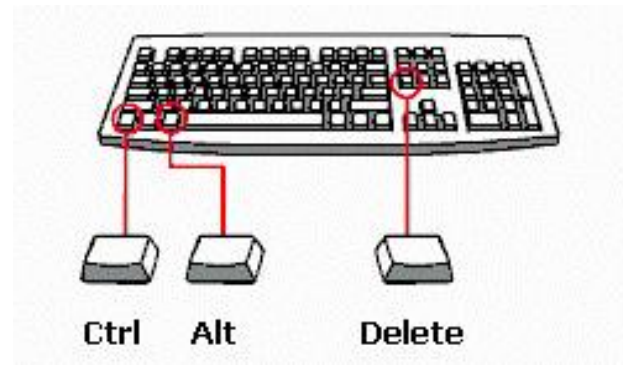


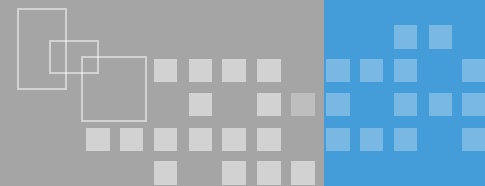
❖ 正常信道的保护

- 可信通路 (Trusted Path)
- 安全键 (SAK) 为基础

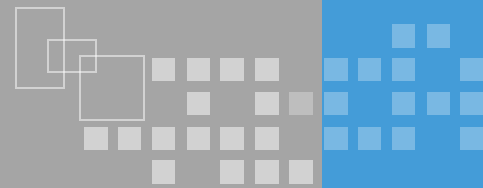
❖ 隐蔽信道保护

- 隐蔽信道指利用系统中那些本来不是用于通信的系统资源绕过强制存取控制进行非法通信的一种机制
- 发现隐蔽信道
 - 共同访问权限
 - 共同修改权限
 - 接收进程可检资源的改变，而发送进程有权限改变
 - 某种机制可启动通信并改变通信事件的顺序





- ❖ 对系统中有关安全的活动进行记录、检查以及审核，一般是一个独立的过程
- ❖ Windows系统的安全审计
 - Windows日志（系统、应用程序、安全）
 - 应用程序和服务日志（IIS日志等）
- ❖ Linux系统的安全审计
 - 连接时间日志
 - 进程统计
 - 错误日志
 - 应用程序日志

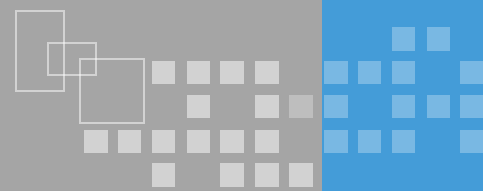


❖ 内存保护

- 进程间/系统进程内存保护
- 段式保护、页式保护和段页式保护

❖ 文件系统保护机制

- 访问控制列表
 - Windows (EFS、Bitlocker)
 - Linux (eCryptfs)
- 加密



❖ 安装

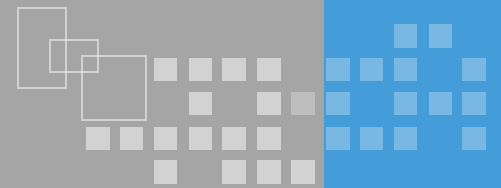
- 分区设置
- 安全补丁&最新版本
- 官方或可靠镜像（Md5校验）

❖ 最小化部署

- 明确需要的功能和组件，不需要的服务和功能都关闭

❖ 远程访问控制

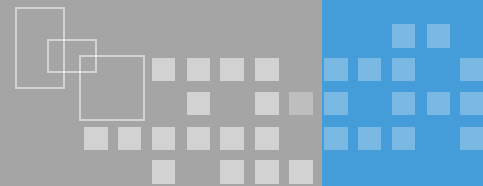
- 开放端口
- 远程连接的限制



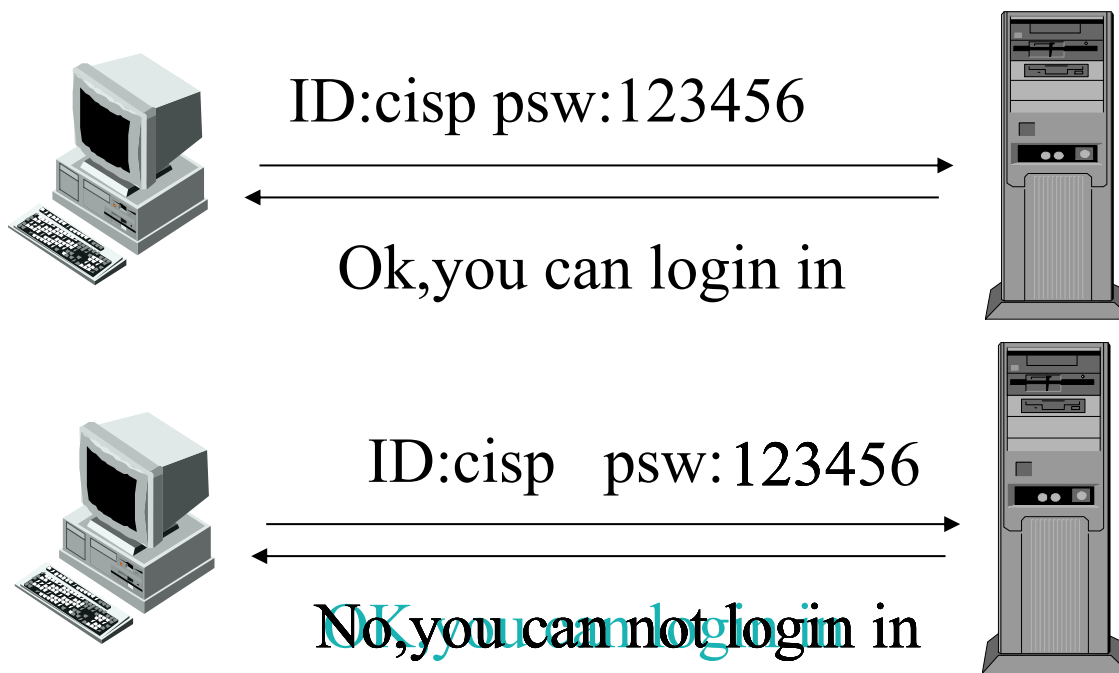
❖ 账户策略及密码策略

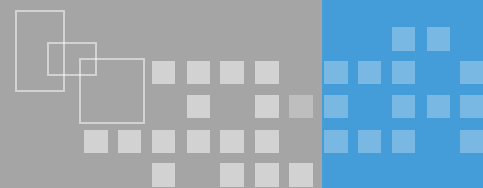
- 管理员更名并给予安全的口令
- 好的口令特点：自己容易记、别人不好猜
- 密码策略（避免弱口令）
 - 密码必须符合复杂性要求
 - 密码长度最小值
 - 强制密码历史
 -
- 帐号锁定策略（应对暴力破解）
 - 帐户锁定时间
 - 帐户锁定阈值
 - 重置帐户锁定计数器

密码远程暴力破解



- ❖ 简单但有效的攻击方式
- ❖ 利用人性懒惰的弱点



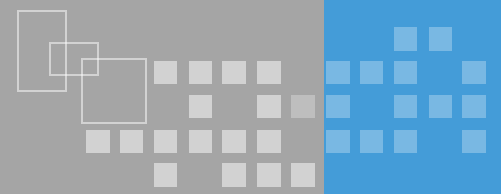


❖ 日志设置

- 日志项、存储空间、访问权限
- 日志服务器

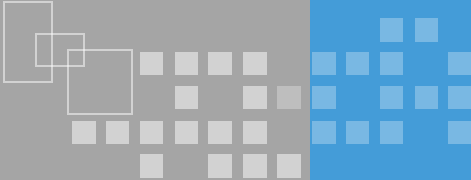
❖ 其他安全设置

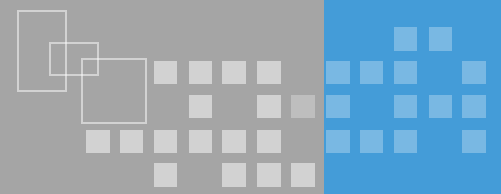
- 安全增强软件（防病毒、主机入侵检测、安全加固软件等）
- 针对操作系统特性的设置
 - Windows关闭共享、自动播放功能
 - Linux中默认创建文件权限等



某公司系统管理员最近正在部署一台Web 服务器，使用的操作系统是windows，在进行日志安全管理设置时，系统管理员拟定四条日志安全策略给领导进行参考，其中能有效应对攻击者获得系统权限后对日志进行修改的策略是：

- ❖ A. 在网络中单独部署syslog 服务器，将Web 服务器的日志自动发送并存储到该syslog 日志服务器中
- ❖ B. 严格设置Web 日志权限，只有系统权限才能进行读和写等操作
- ❖ C. 对日志属性进行调整，加大日志文件大小、延长日志覆盖时间、设置记录更多信息等
- ❖ D. 使用独立的分区用于存储日志，并且保留足够大的日志空间

- 
- ❖ 安全的运行环境是软件安全的基础，操作系统安全配置是确保运行环境安全必不可少的工作，某管理员对即将上线的Windows 操作系统进行了以下四项安全部署工作，其中哪项设置不利于提高运行环境安全？
 - ❖ A. 操作系统安装完成后安装最新的安全补丁，确保操作系统不存在可被利用的安全漏洞
 - ❖ B. 为了方便进行数据备份，安装Windows 操作系统时只使用一个分区C，所有数据和操作系统都存放在C 盘
 - ❖ C. 操作系统上部署防病毒软件，以对抗病毒的威胁
 - ❖ D. 将默认的管理员账号 Administrator 改名，降低口令暴力破解攻击的发生可能

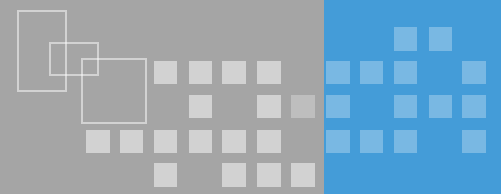


账号锁定策略中对超过一定次数的错误登录账号进行锁定是为了对抗以下哪种攻击？

- ❖ A. 分布式拒绝服务攻击 (DDoS) B. 病毒传染
- ❖ C. 口令暴力破解 D. 缓冲区溢出攻击

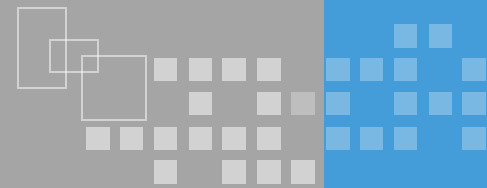
为了保证系统日志可靠有效，以下哪一项不是日志必需具备的特征。

- A. 统一而精确的时间
- B. 全面覆盖系统资产
- C. 包括访问源、访问目标和访问活动等重要信息
- D. 可以让系统的所有用户方便的读取



口令破解是针对系统进行攻击的常用方法，Windows 系统安全策略中应对口令破解的策略主要是账户策略中的账户锁定策略和密码策略，关于这两个策略说明错误的是：（ ）。

- ❖ A. 密码策略的主要作用是通过策略避免用户生成弱口令及对用户的口令使用进行管控
- ❖ B. 密码策略对系统中所有的用户都有效
- ❖ C. 账户锁定策略的主要作用是应对口令暴力破解攻击，能有效的保护所有系统用户应对口令暴力破解攻击
- ❖ D. 账户锁定策略只适用于普通用户，无法保护管理员 administrator 账户应对口令暴力破解攻击

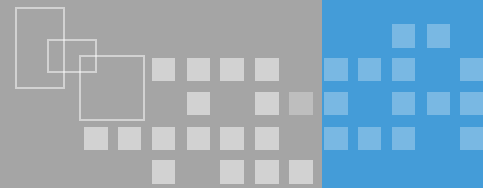


❖ 信息收集

- 理解信息收集的概念及公开渠道信息收集、网络服务信息收集的方式及防御措施。

❖ 缓冲区溢出攻击

- 理解缓冲区溢出的基本概念及危害；
- 理解缓冲区溢出攻击的技术原理及防御措施。



❖ 信息收集的概念

- 情报学中一个领域

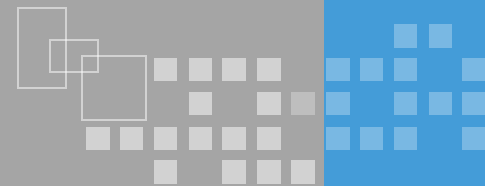
❖ 传统的信息收集

- 案例：著名的照片泄密案

❖ 互联网时代的信息收集

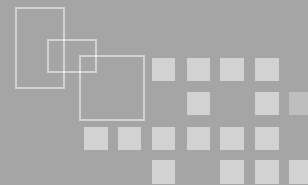
- 信息技术的发展使得数据大量被生产出来





❖ 收集哪些信息

- 目标系统的信息系统相关资料
 - 域名、网络拓扑、操作系统、应用软件、相关脆弱性
- 目标系统的组织相关资料
 - 组织架构及关联组织
 - 地理位置细节
 - 电话号码、邮件等联系方式
 - 近期重大事件
 - 员工简历
- 其他可能令攻击者感兴趣的任何信息



❖ 快速定位

- 某开源软件xxxx.jsp脚本存在漏洞，Google 搜索“xxxx.jsp”可以找到存在此脚本的Web网站

❖ 信息挖掘

- 定点采集
 - Google 搜索 “.doc+website” 挖掘信息
- 隐藏信息
 - .mdb、.ini、.txt、.old、.bak、.001……
- 后台入口

信息收集与分析

❖ 网络信息收集

- 正常服务（如whois）
- 系统功能
 - Ping
 - tracert

❖ 系统及应用信息收集

- 服务旗标
- 欢迎信息
- 端口扫描
- TCP/IP协议指纹识别

```
命令提示符

通过最多 30 个跃点跟踪
到 www.itsec.gov.cn [123.124.177.80] 的路由:

 1    1 ms    1 ms    <1 毫秒 bogon [10.64.191.1]
 2    6 ms   10 ms    4 ms   100.69.0.1
 3    *      *      4 ms   185.235.120.106.static.bjtelecom.net [106.120.235.185]
 4   12 ms   7 ms    9 ms   bj141-135-170.bjtelecom.net [219.141.135.170]
 5    *      6 ms    *      202.97.57.126
 6    7 ms   7 ms    7 ms   219.158.40.185
 7    *      *      *      请求超时。
 8    *      *      *      请求超时。
 9   10 ms   8 ms    9 ms   124.65.56.158
10   13 ms   8 ms    8 ms   bt-227-106.bta.net.cn [202.106.227.106]
11    9 ms   6 ms    6 ms   125.35.65.62
12    9 ms   7 ms   10 ms   123.124.177.80

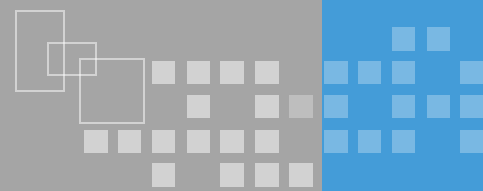
跟踪完成。

C:\Users\shencn>
```

```
C:\WINDOWS\system32\cmd.exe

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
  <title>501 Method Not Implemented</title>
</head><body>
  <h1>Method Not Implemented</h1>
  <p>get to /index.htm not supported.<br />
  </p>
  <hr>
  <address>Apache/2.0.59 (Win32) mod_jk/1.2.23</address>
</body></html>

失去了跟主机的连接。
```



❖ 公开信息收集防御

- 信息展示最小化原则，不必要的信息不要发布

❖ 网络信息收集防御

- 部署网络安全设备（IDS、防火墙等）
- 设置安全设备应对信息收集（阻止ICMP）

❖ 系统及应用信息收集防御

- 修改默认配置（旗标、端口等）
- 减少攻击面



严防死守！

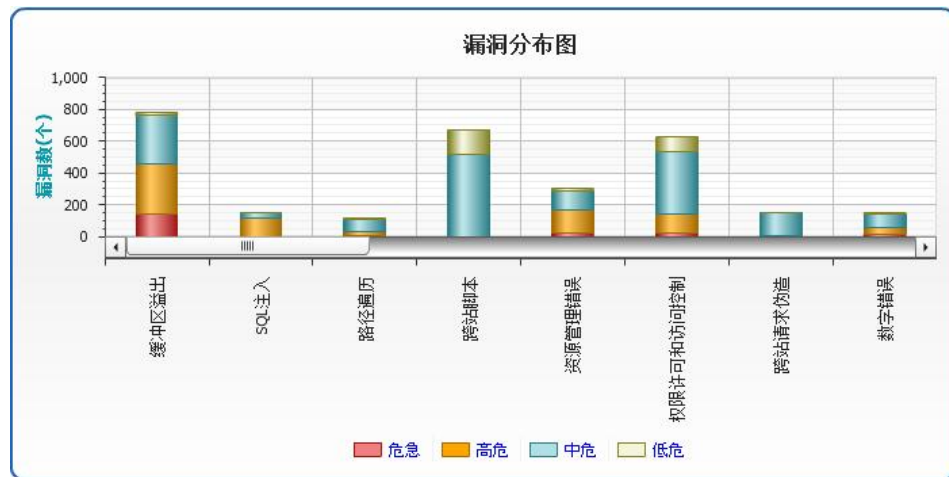
系统攻击-缓冲区溢出

❖ 缓冲区溢出攻击原理

- 缓冲区溢出攻击利用编写不够严谨的程序，通过向程序的缓冲区写入超过预定长度的数据，造成缓存的溢出，从而破坏程序的堆栈，导致程序执行流程的改变

❖ 缓冲区溢出的危害

- 最大数量的漏洞类型
- 漏洞危害等级高



国家漏洞库（CNNVD）2013年漏洞统计

缓冲区溢出基础-堆栈、指针、寄存器

❖ 堆栈概念

- 一段连续分配的内存空间

❖ 堆栈特点

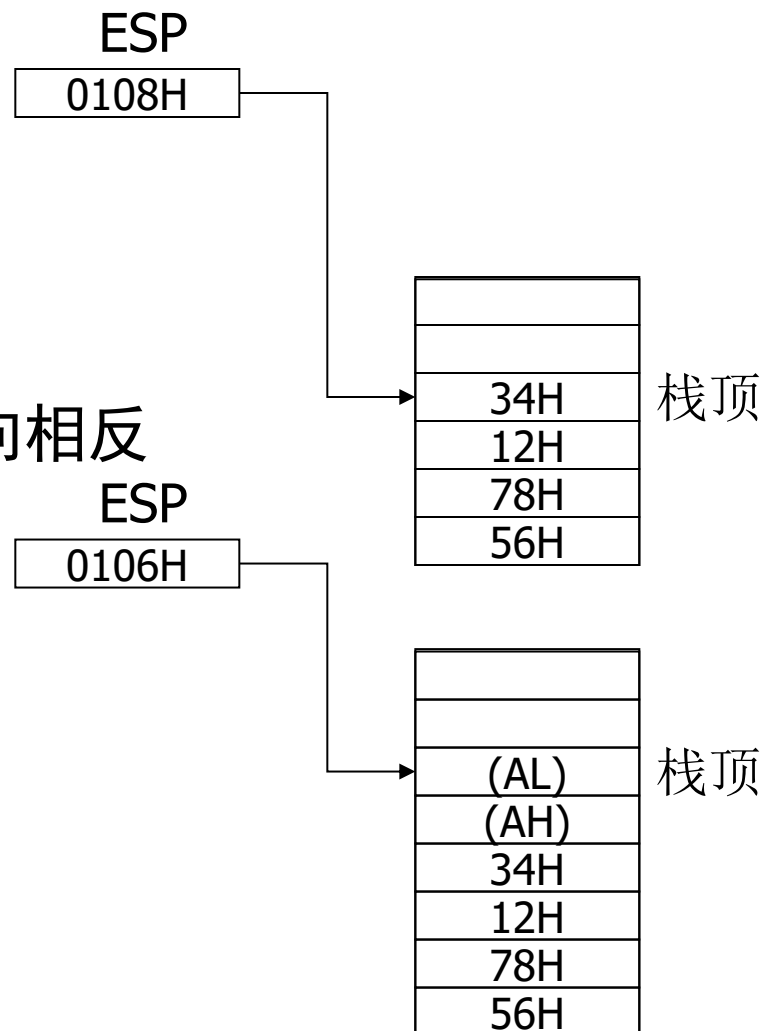
- 后进先出
- 堆栈生长方向与内存地址方向相反

❖ 指针

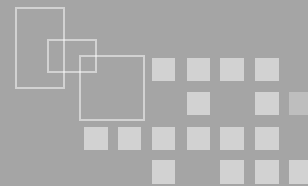
- 指针是指向内存单元的地址

■ 寄存器

- 暂存指令、数据和位址
- ESP（栈顶）
- EBP（栈底）
- EIP（返回地址）



缓冲区溢出简单示例

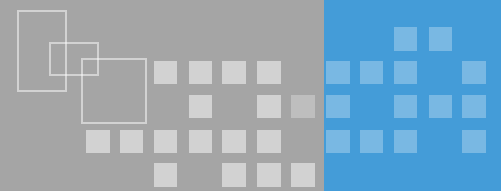


❖ 程序作用：将用户输入的内容打印在屏幕上

Buffer.c

```
#include <stdio.h>
int main ( )
{
    char name[8];
    printf("Please input your name: ");
    gets(name);
    printf("you name is: %s!", name);
    return 0;
}
```


缓冲区溢出示例

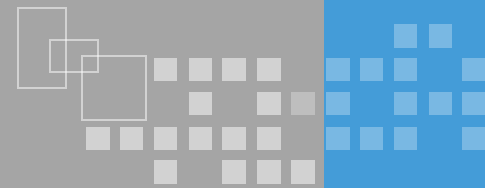


缓冲区溢出简单示例



当我们全部输入a时，错误指令地址为
0x616161，0x61是a 的ASCII编码

程序溢出堆栈情况



内存底部

内存顶部

正常状态
下的堆栈

name	XXX	EIP	XXX
[cispcisp]	[]	[]	[]

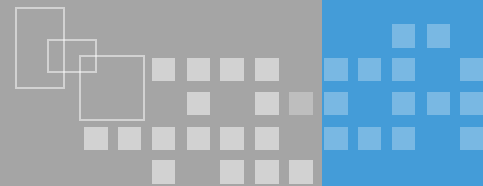
name	XXX	EIP	XXX
[aaaaaaaaa]	[aaaa]	[aaaa]	[aaaa]

溢出状态
下的堆栈

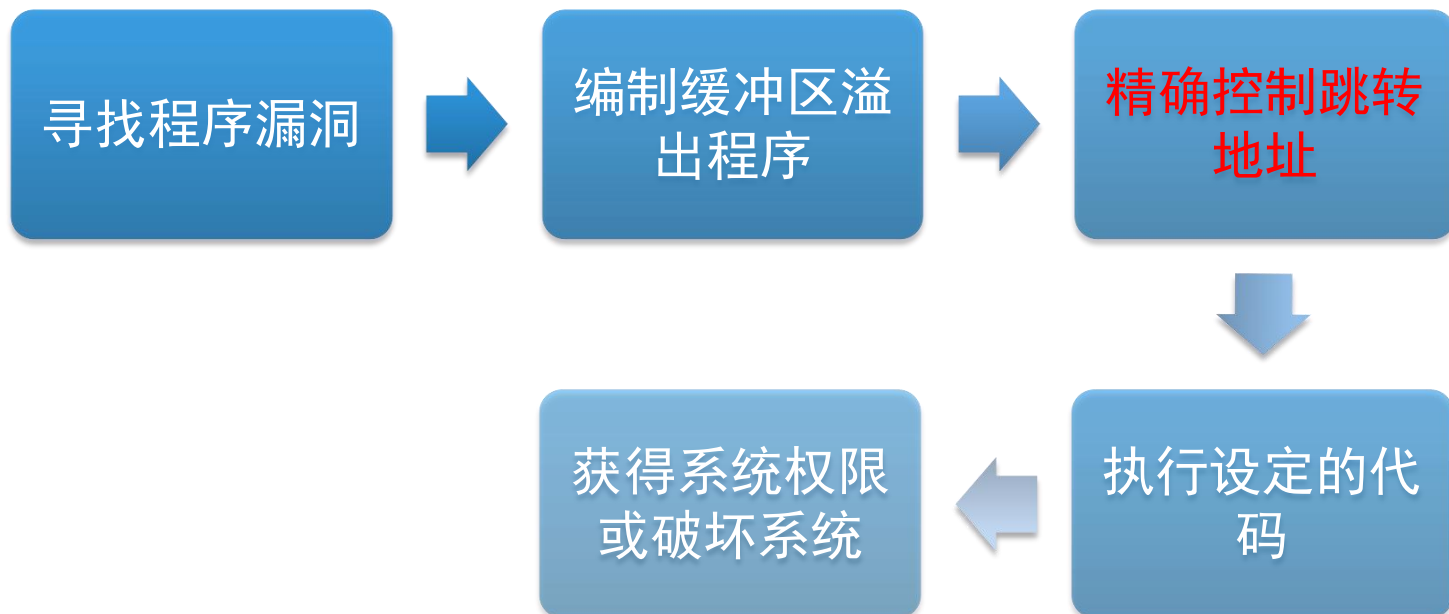
堆栈顶部

堆栈底部

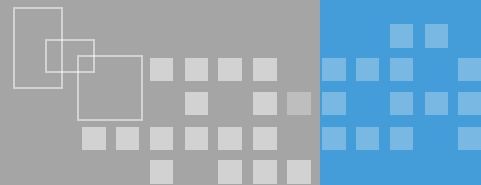
缓冲区溢出攻击过程



❖ 如果可精确控制内存跳转地址，就可以执行指定代码，获得权限或破坏系统



缓冲区溢出的防范



❖ 用户

- 补丁
- 防火墙

❖ 开发人员

- 编写安全代码，对输入数据进行验证
- 使用相对安全的函数

❖ 系统

- 缓冲区不可执行技术
- 虚拟化技术



❖ 恶意代码的预防

- 了解恶意代码的概念、传播方式及安全策略、减少漏洞和减轻威胁等针对恶意代码的预防措施；

❖ 恶意代码的检测分析

- 理解特征扫描、行为检测的区别及优缺点；
- 了解静态分析、动态分析的概念及区别。

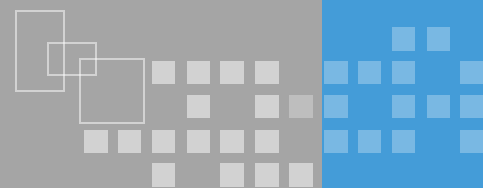
❖ 恶意代码的清除

- 了解感染引导区、感染文件、独立型和嵌入型恶意代码清除的方式。

❖ 基于互联网的恶意代码防护

- 了解基于互联网的恶意代码防护概念。

什么是恶意代码

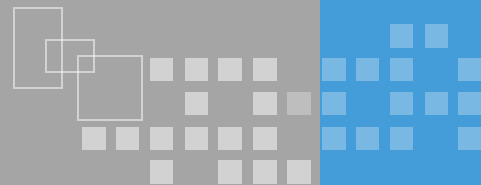


❖ 什么是恶意代码

- 《中华人民共和国计算机信息系统安全保护条例》第二十八条：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码（1994. 2. 18）
- 恶意代码，是指能够引起计算机故障，破坏计算机数据，影响计算机系统的正常使用的程序代码。指令

❖ 类型：二进制代码、脚本语言、宏语言等

❖ 表现形式：病毒、蠕虫、后门程序、木马、流氓软件、逻辑炸弹等



❖ 文件传播

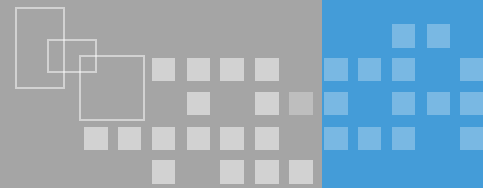
- 感染
- 移动介质

❖ 网络传播

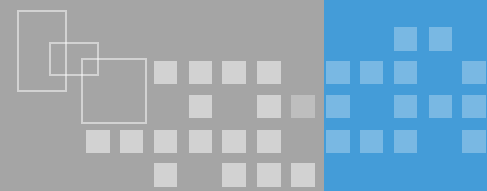
- 网页、电子邮件、即时通讯、共享、漏洞

❖ 软件部署

- 逻辑炸弹
- 预留后门
- 文件捆绑



- ❖ 增强安全策略与意识
- ❖ 减少漏洞
 - 补丁管理
 - 主机加固
- ❖ 减轻威胁
 - 防病毒软件
 - 间谍软件检测和删除工具
 - 入侵检测/入侵防御系统
 - 防火墙
 - 路由器、应用安全设置等



❖ 工作机制：特征匹配

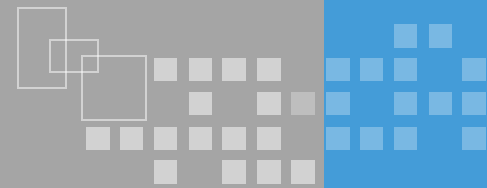
- 病毒库（恶意代码特征库）
- 扫描（特征匹配过程）

❖ 优势

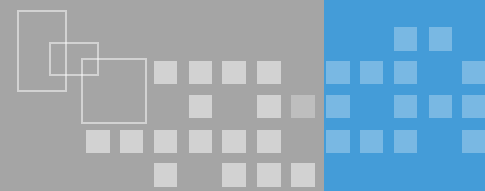
- 准确（误报率低）
- 易于管理

❖ 不足

- 效率问题（特征库不断庞大、依赖厂商）
- 滞后（先有病毒后有特征库，需要持续更新）
-



- ❖ 工作机制：基于统计数据
 - 恶意代码行为有哪些
 - 行为符合度
- ❖ 优势
 - 能检测到未知病毒
- ❖ 不足
 - 误报率高
 - 难点：病毒不可判定原则

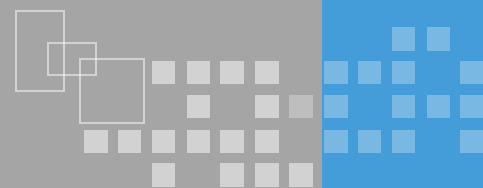


❖ 静态分析

- 不实际执行恶意代码，直接对二进制代码进行分析
 - 文件特性，如文件形态、版本、存储位置、长度等
 - 文件格式，如PE信息、API调用等

❖ 动态分析

- 运行恶意代码并使用监控及测试软件分析
- 本地行为：文件读写、注册表读写等
- 网络行为：远程访问、调用等



❖ 感染引导区

- 修复/重建引导区

❖ 感染文件

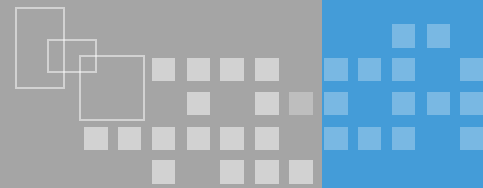
- 附着型：逆向还原（从正常文件中删除恶意代码）
- 替换型：备份还原（正常文件替换感染文件）

❖ 独立文件

- 内存退出，删除文件

❖ 嵌入型

- 更新软件或系统
- 重置系统

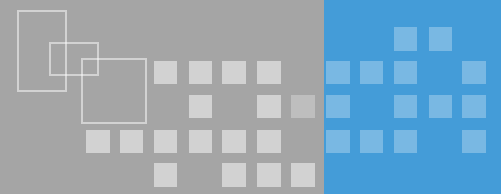


❖ 恶意代码监测与预警体系

- 蜜罐、蜜网

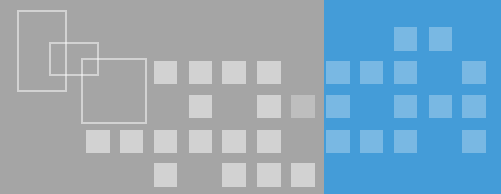
❖ 恶意代码云查杀

- 分布式计算

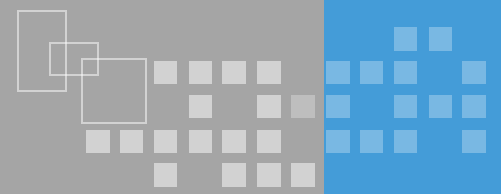


下列哪项内容描述的是缓冲区溢出漏洞？

- ❖ A. 通过把SQL 命令插入到web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL 命令
- ❖ B. 攻击者在远程WEB 页面的HTML 代码中插入具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行。
- ❖ C. 当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量溢出的数据覆盖在合法数据上
- ❖ D. 信息技术、信息产品、信息系统在设计、实现、配置、运行等过程中，有意或无意产生的缺陷

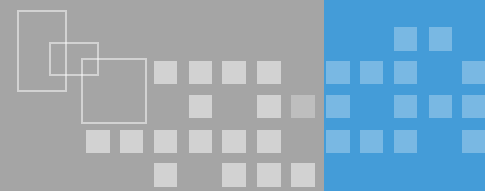


- ❖ 下面对“零日（zero-day）漏洞”的理解中，正确的是（
）
- ❖ A. 指一个特定的漏洞，该漏洞每年 1 月 1 日零点发作，可以被攻击者用来远程攻击，获取主机权限
- ❖ B. 指一个特定的漏洞，特指在 2010 年被发现出来的一种漏洞，该漏洞被“震网”病毒所利用，用来攻击伊朗布什尔核电站基础设施
- ❖ C. 指一类漏洞，即特别好被利用，一旦成功利用该漏洞，可以在 1 天内完成攻击，且成功达到攻击目标
- ❖ D. 指一类漏洞，即刚被发现后立即被恶意利用的安全漏洞。一般来说，那些已经被小部分人发现，但是还未公布、还不存在安全补丁的漏洞都是零日漏洞



为达到预期的攻击目的，恶意代码通常会被采用各种方法将自己隐藏起来。关于隐藏方法，下面理解错误的是（）

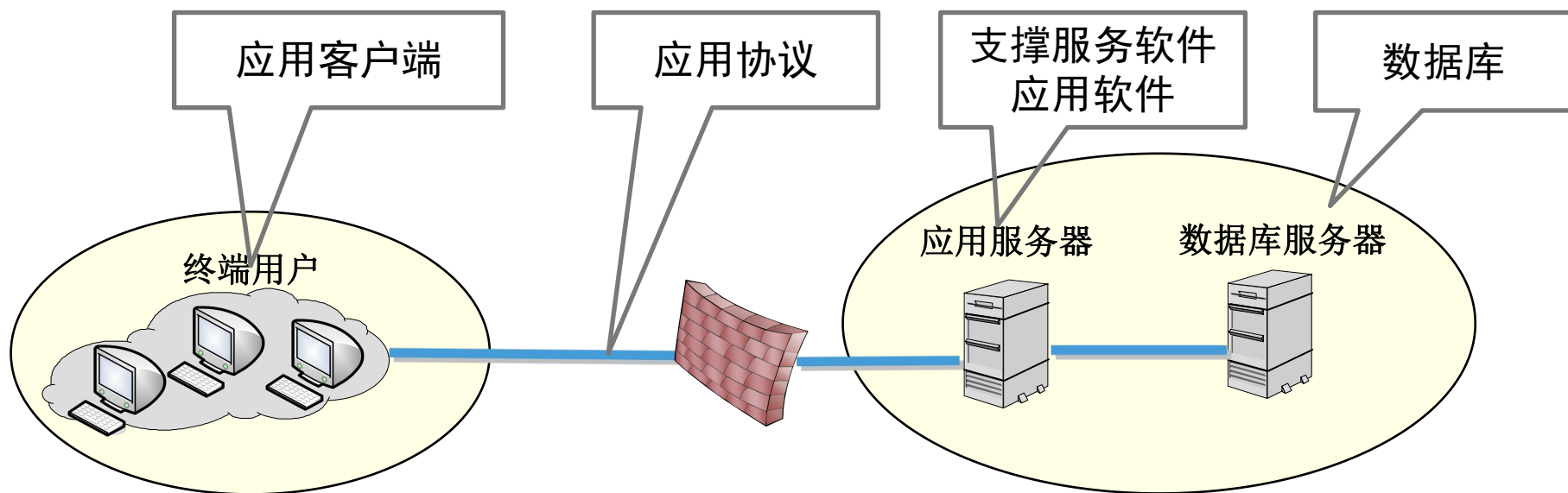
- ❖ A. 隐藏恶意代码进程，即将恶意代码进程隐藏来，或者改名和使用系统进程名，以更好的躲避检测，迷惑用户和安全检测人员
- ❖ B. 隐藏恶意代码的网络行为，复用通用的网络端口，以躲避网络行为检测和网络监控
- ❖ C. 隐藏恶意代码的源代码，删除或加密源代码，仅留下加密后的二进制代码，以躲避用户和安全检测人员
- ❖ D. 隐藏恶意代码的文件，通过隐藏文件、采用流文件技术或 HOOK 技术、以躲避系统文件检查和清除

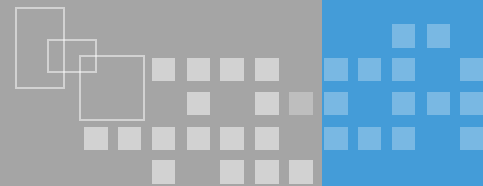


❖ Web应用安全

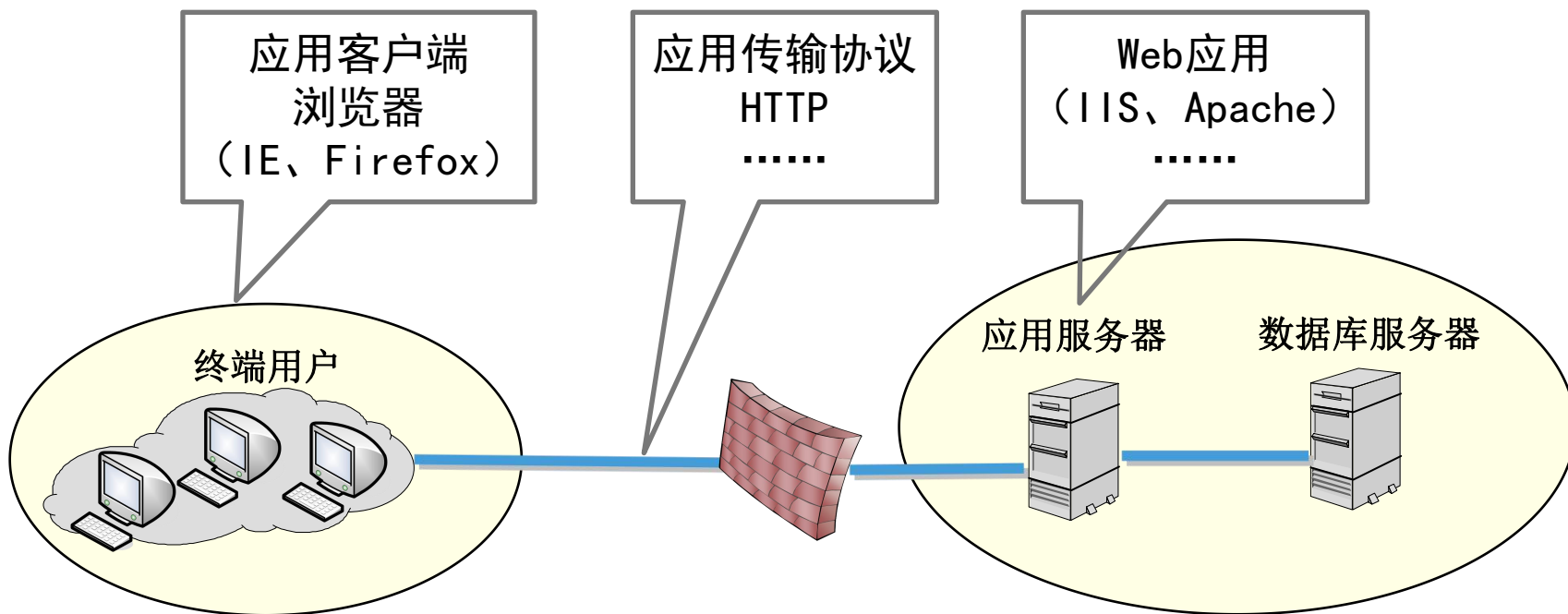
- 了解WEB体系架构；
- 理解HTTP协议工作机制及明文传输数据、弱验证、无状态等安全问题；
- 理解SQL注入攻击的原理及危害；
- 了解跨站脚本安全问题的原理及危害及其他针对WEB的攻击方式；
- 了解WEB 防火墙、网页防篡改等常见Web安全防护技术作用。

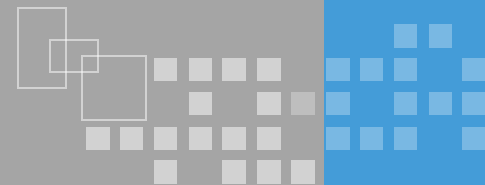
❖ 应用系统的复杂性和多样性使得安全问题也呈现出多样化的特点





- ❖ WEB服务器端安全问题（支撑软件、应用程序）
- ❖ Web客户端（浏览器）
- ❖ Web协议（Http）





❖ HTTP (超文本传输协议) 工作机制

■ 请求响应模式

- HTTP请求包含三个部分（方法 URL 协议/版本、请求头部、请求正文）
- HTTP响应包含三个部分（协议状态代码描述、响应包头、实体包）

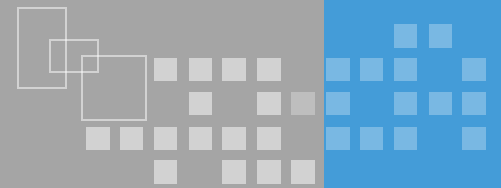
```
POST /servlet/default.JSP HTTP/1.1
Accept: text/plain; text/HTML
Accept-Language: en-gb
Connection: Keep-Alive
Host: localhost
Referer: http://localhost/ch0/SendDetails.htm
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Length: 33
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
LastName=Franks&FirstName=Michael
```

HTTP请求

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6.0
Date: Mon, 3 Jan 2010 13:13:33 GMT
Content-Type: text/HTML
Last-Modified: Mon, 11 Jan 2010 13:23:42 GMT
Content-Length: 112
```

实体内容

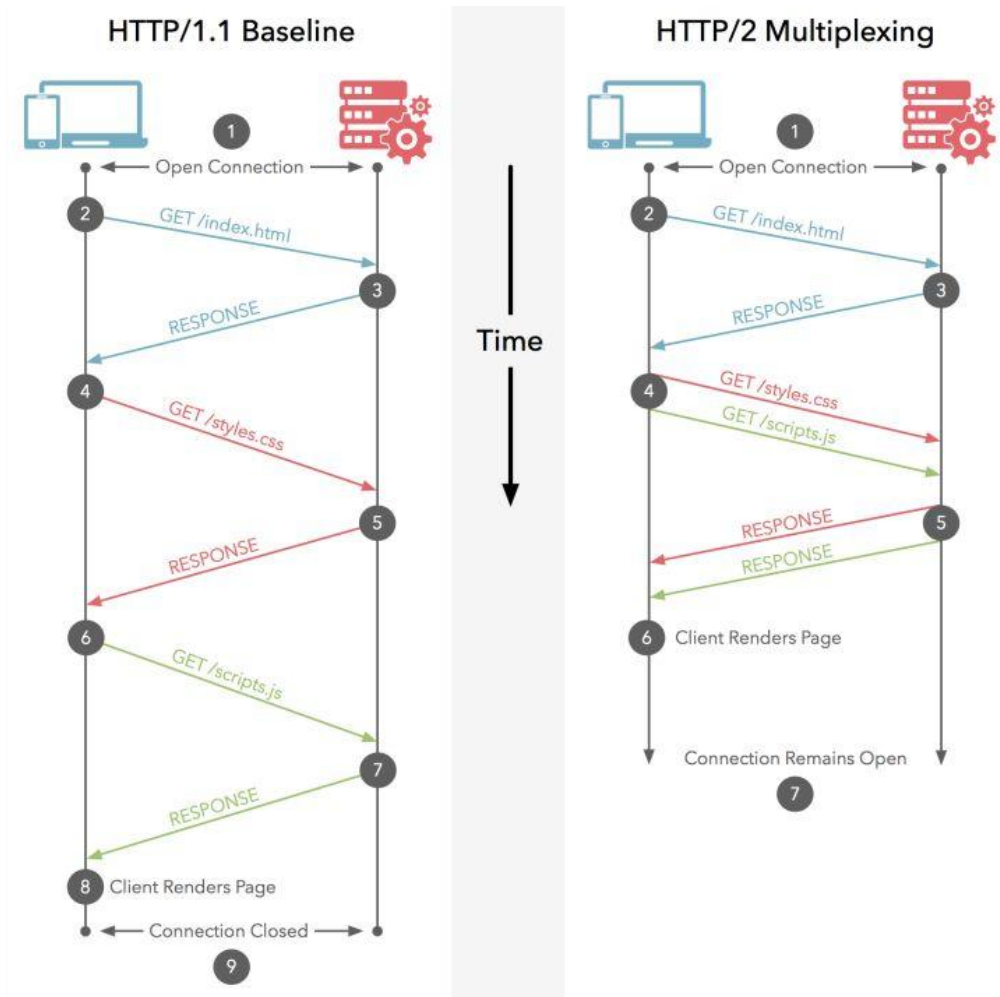
HTTP响应

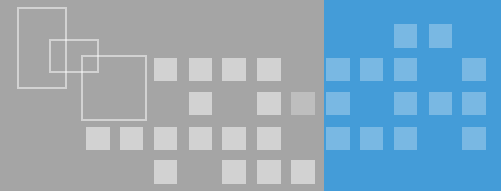


- ❖ 信息泄漏（传输数据明文）
- ❖ 弱验证（会话双方没有严格认证机制）
 - http1.1提供摘要访问认证机制，采用MD5将用户名、密码、请求包头等进行封装，但仍然不提供对实体信息的保护
- ❖ 缺乏状态跟踪（请求响应机制决定http是一个无状态协议）
 - Session解决方案带来的安全问题

HTTP1.0/1.1/2.0区别

- ❖ HTTP1.0是没有host域的，HTTP1.1才支持这个参数。
- ❖ HTTP1.1默认使用长连接，可有效减少TCP的三次握手开销。
- ❖ HTTP 1.1支持只发送header信息。
- ❖ HTTP2.0使用多路复用技术，新增首部压缩。





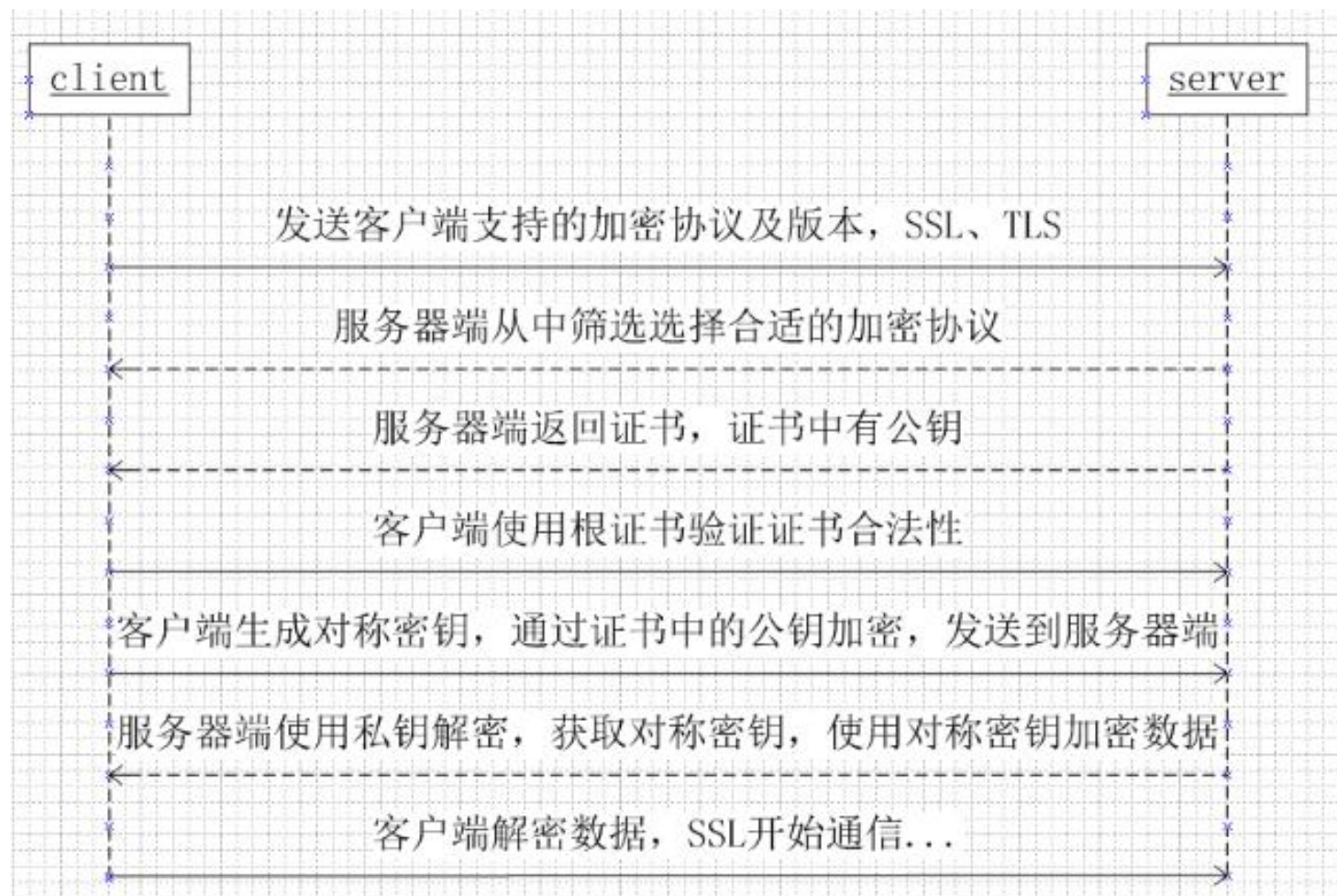
❖ 服务支撑软件安全问题

- 软件自身安全漏洞
 - 例：IIS 5.0超长URL拒绝服务漏洞
 - 例：Unicode解码漏洞
- 软件配置缺陷
 - 默认账号、口令
 - 不安全的配置
 - 例：IIS配置允许远程写入

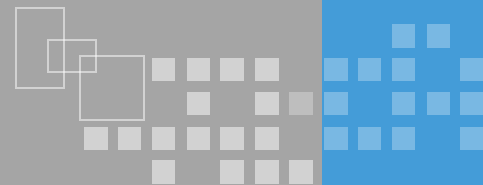
❖ 应用软件安全问题

- 明文传输
- 弱验证
- 缺乏状态跟踪

HTTPS连接建立过程



典型注入攻击-SQL注入



- ❖ 原理：程序没有对用户输入数据的合法性进行判断，使攻击者可以绕过应用程序限制，构造一段SQL语句并传递到数据库中，实现对数据库的操作

- ❖ 示例

用户登陆

用户

密码

用户登陆

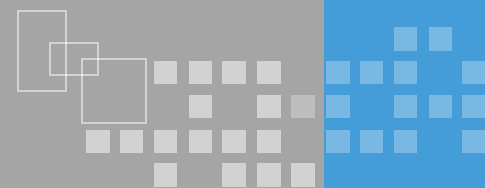
用户

密码

**Select * from table where
user='admin' and pwd='ABCDEFGH!';**

由于密码的输入方式，使得查询语句返回值永远为True，因此通过验证！

**Select * from table where
user='admin' and pwd='123' or '1=1',**

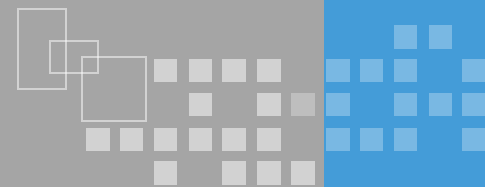


❖ 可以传递到数据库的数据都是攻击对象

❖ 示例

- `http://www.test.com/showdetail.asp?id=49'`
`And (update user set passwd= '123' where`
`username= 'admin');--`
- `Select * from 表名 where 字段=' 49' And`
`(update user set passwd= '123' where`
`username= 'admin');`

非法的SQL语句被传递到数据库中执行！



❖ 数据库信息收集

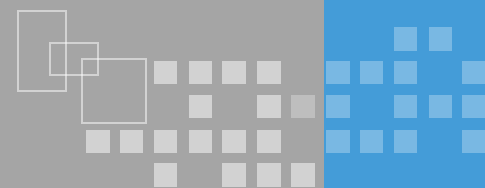
- 数据检索

❖ 操作数据库

- 增加数据
- 删除数据
- 更改数据

❖ 操作系统

- 借助数据库某些功能（例如：SQLServer的内置存储过程XP_CMDShell）



❖ 防御的对象：所有外部传入数据

- 用户的输入
 - 提交的URL请求中的参数部分
 - 从cookie中得到的数据
- 其他系统传入的数据

❖ 防御的方法

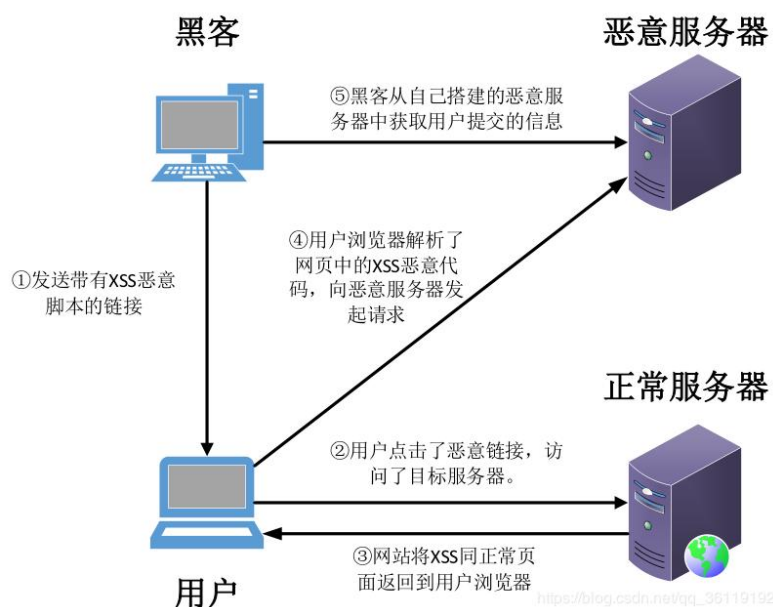
- 白名单：限制传递数据的格式
- 黑名单：过滤
 - 过滤特殊字串：update、insert、delete等
 - 开发时过滤特殊字符：单引号、双引号、斜杠、反斜杠、冒号、空字符等的字符
- 部署防SQL注入系统或脚本

针对Web应用的攻击-跨站脚本

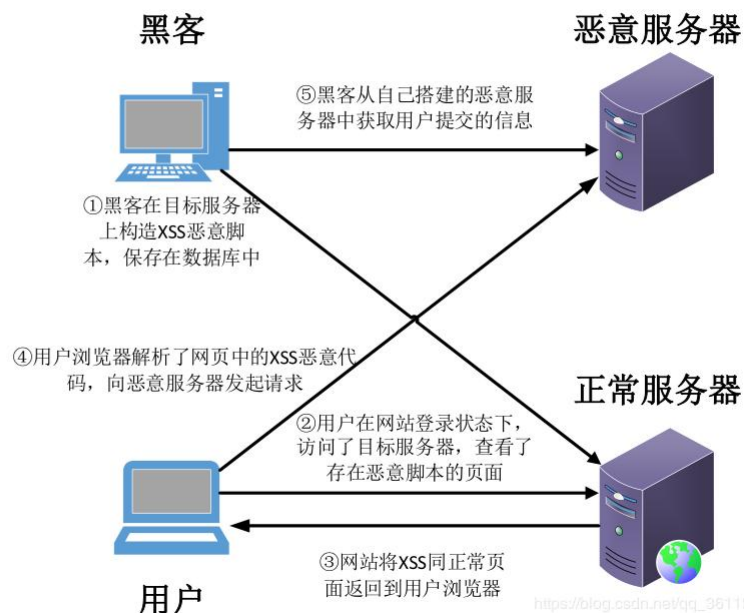
❖ 原理

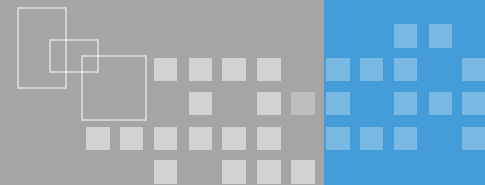
- 由于程序没有对用户提交的变量中的HTML代码进行过滤或转换，使得脚本可被执行，攻击者可以利用用户和服务端之间的信任关系实现恶意攻击

反射型XSS攻击流程



存储型XSS攻击流程





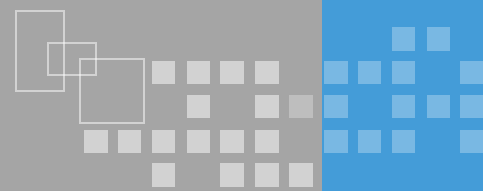
❖ 危害

- 敏感信息泄露、账号劫持、Cookie欺骗、拒绝服务、钓鱼等

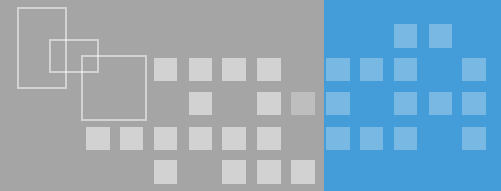
❖ 防范

- 不允许HTML中脚本运行
- 对所有脚本进行严格过滤

针对WEB应用的攻击



- ❖ 失效的验证和会话管理
- ❖ 不安全的对象直接引用
- ❖ 跨站请求伪造
- ❖ 不安全的配置管理
- ❖ 不安全的密码存储
- ❖ 错误的访问控制
- ❖ 传输保护不足
- ❖ 未经验证的网址重定向
- ❖ 不恰当的异常处理
- ❖ 拒绝服务攻击

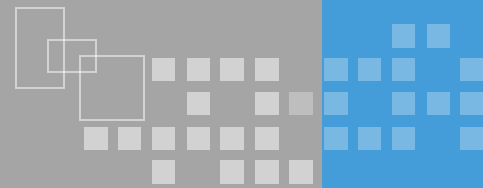


❖ Web防火墙

- 工作在应用层
- 基本功能
 - 审计并拦截HTTP数据流
 - Web应用访问控制
 - Web应用加固

❖ 网页防篡改

- 监控Web服务器上的页面文件，防止被篡改
- 机制
 - 备份文件对比、摘要文件对比、删改操作触发、系统底层过滤



❖ 电子邮件安全

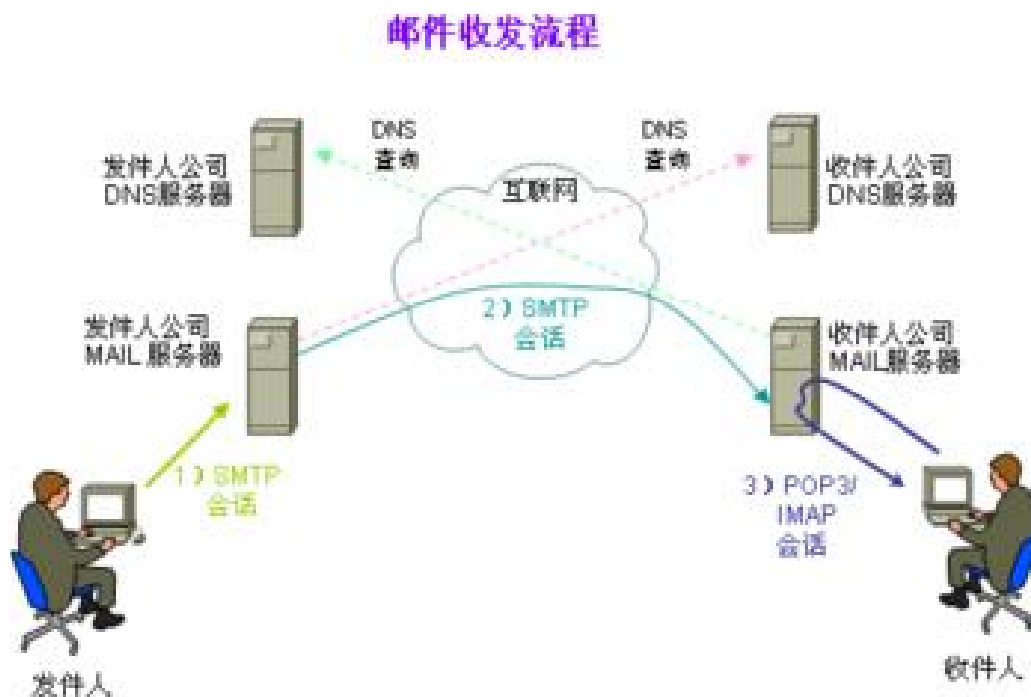
- 理解电子邮件工作机制及SMTP、POP3协议；
- 了解电子邮件安全问题及解决方案。

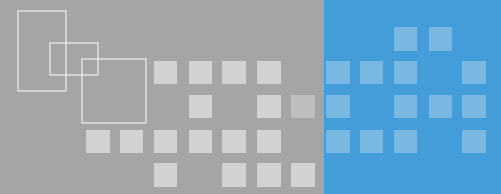
❖ 其他互联网应用

- 了解远程接入、域名系统、即时通讯等其他互联网应用安全问题及解决措施。

SMTP、POP3协议

- ❖ SMTP：简单邮件传输协议, 用于从源地址到目的地地址传输邮件的规范，通过它来控制邮件的中转
- ❖ POP：电子邮局传输协议
- ❖ IMAP：互联网邮件访问协议，交互式





❖ POP3/SMTP协议工作机制

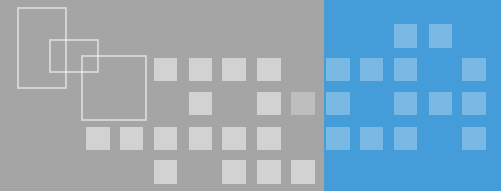
- 简单的请求响应模式

❖ 安全问题

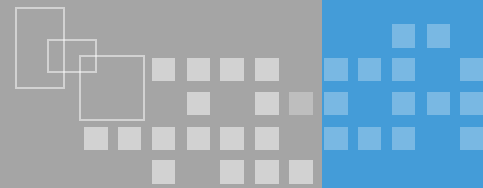
- 信息泄漏（用户帐号密码、邮件内容）
- 身份验证不足（社会工程学攻击、垃圾邮件）

❖ 安全解决

- 服务器端
 - 安全邮件协议, S/MIME、PGP
 - 使用SSL保护会话
 - 安全策略
- 客户端



- ❖ 远程接入
- ❖ 域名系统
- ❖ 即时通信

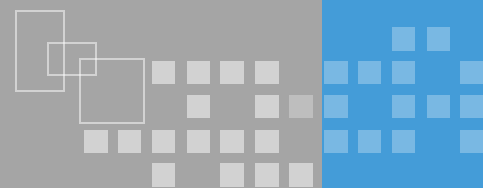


❖ 数据库安全

- 了解数据库安全要求；
- 掌握数据库安全防护的策略和要求。

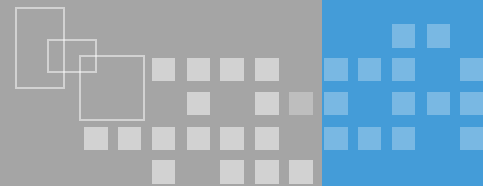
❖ 数据泄露防护

- 了解数据泄露防护的概念。

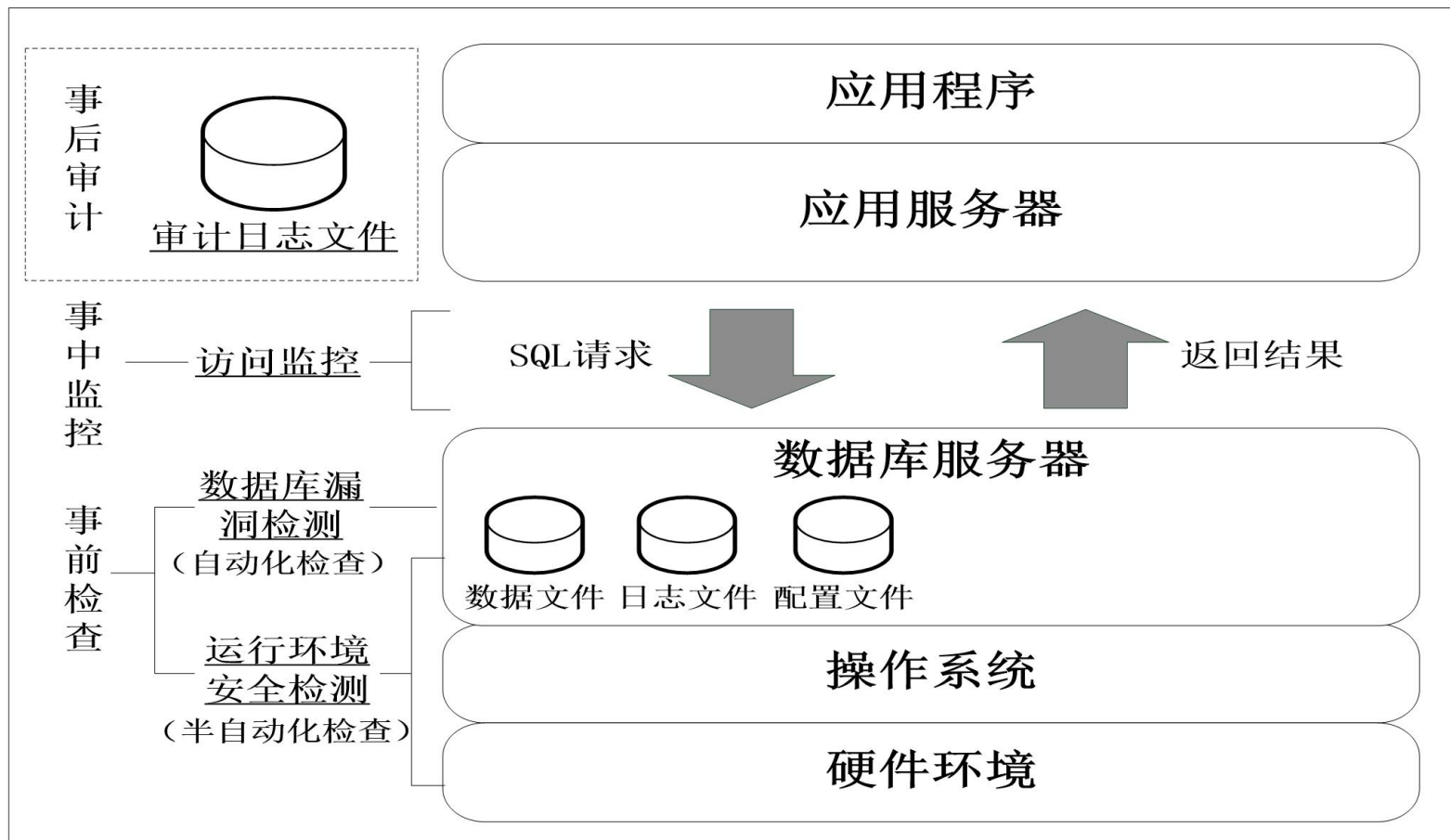


- ❖ 用户标识与鉴别
- ❖ 授权与访问控制
- ❖ 数据加密
- ❖ 安全审计
- ❖





❖ 检查、监控、审计



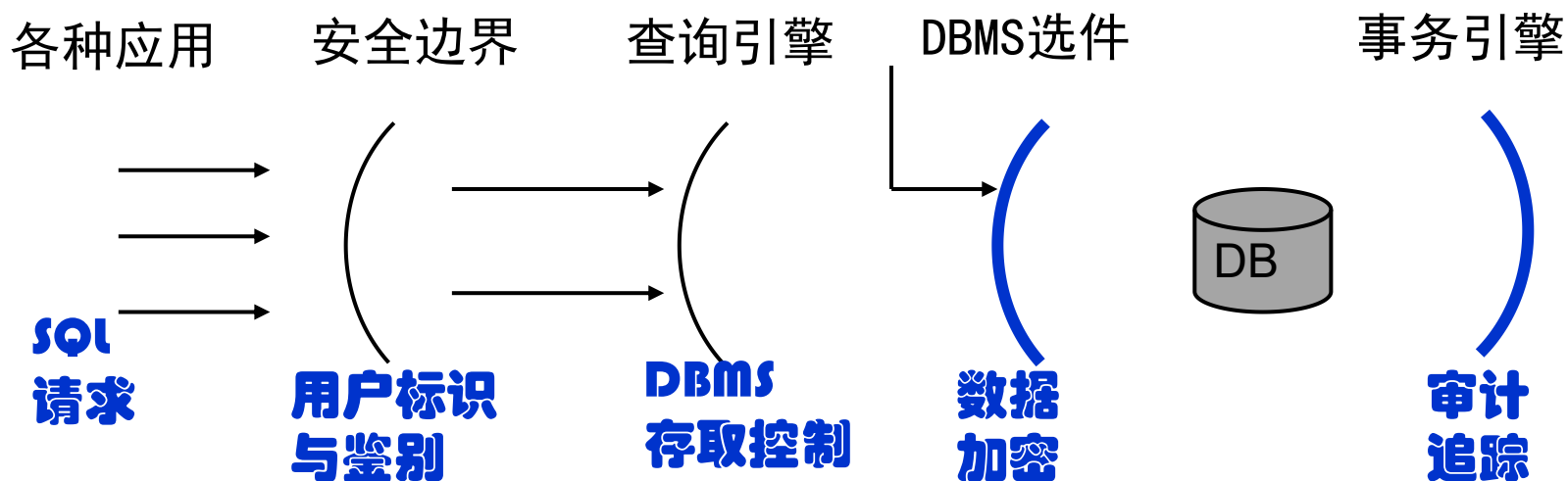
数据库安全防护-构建深度防御体系

❖ 安全机制

- 标识与鉴别、访问控制、传输加密、审计等

❖ 安全策略

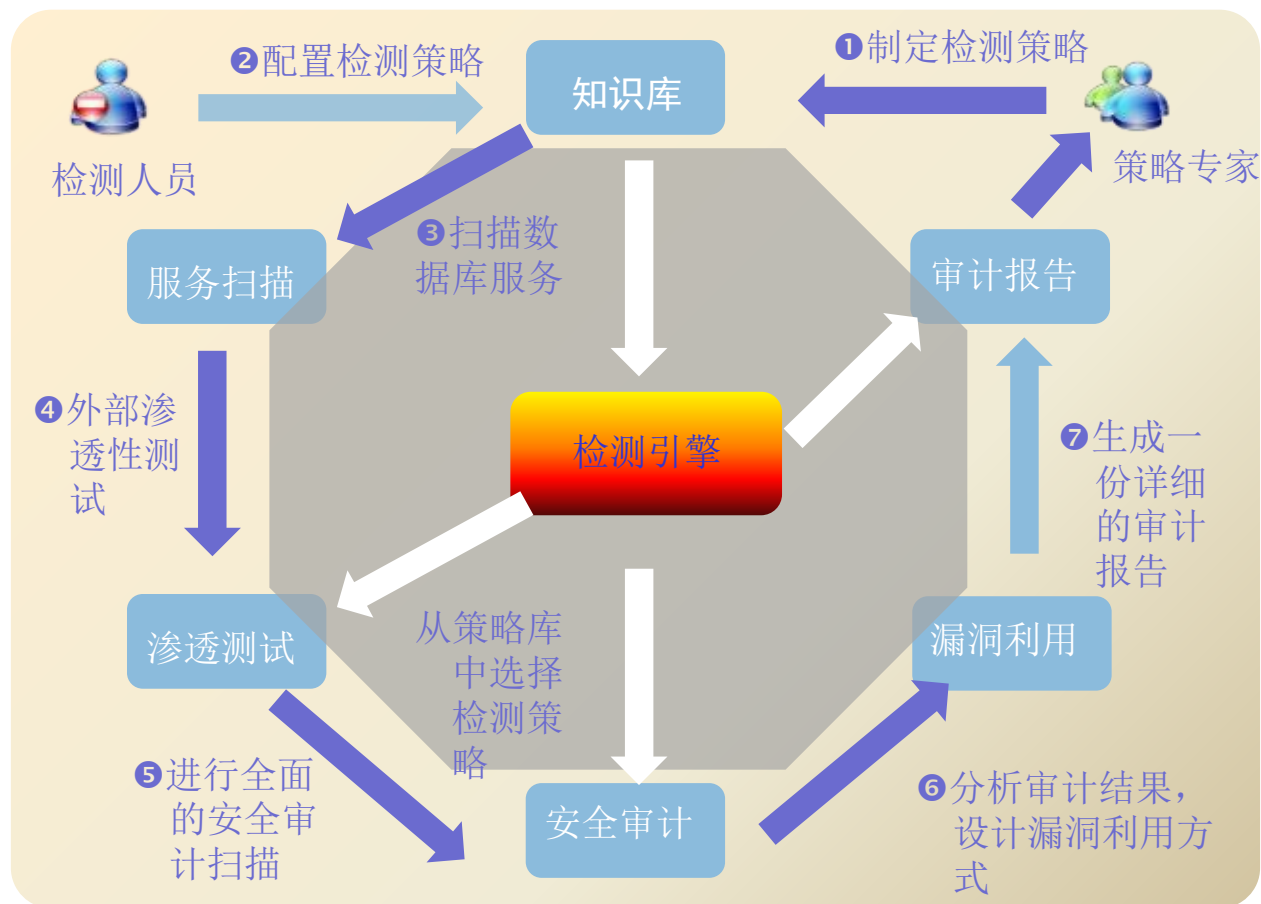
- 密码策略、备份策略等

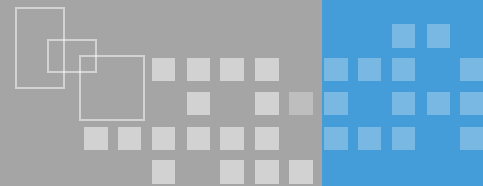


数据库安全防护-安全特性检查

❖ 数据库系统漏洞

❖ 数据库配置缺陷





❖ 安全配置

- 补丁
- 协议（端口、传输协议）

❖ 账号

- 用户名及密码
- 口令策略
- 权限

❖ 存储过程

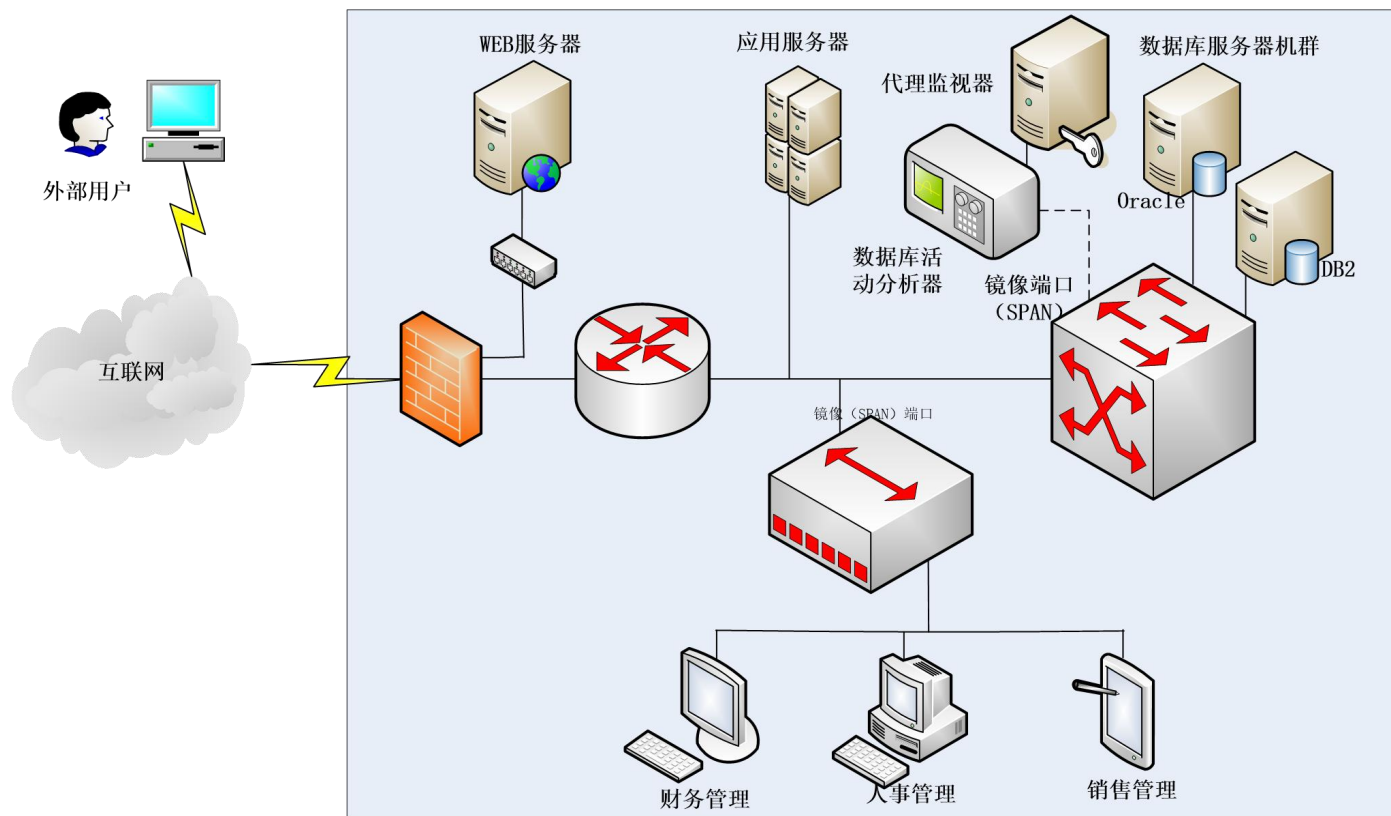
❖ 触发器

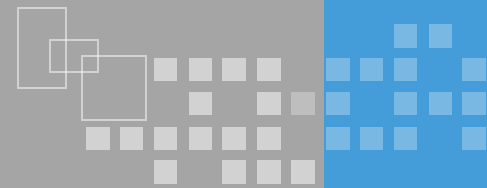
❖ 备份

数据库安全防护-运行监控

❖ 入侵检测

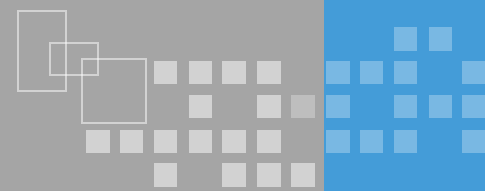
❖ 数据库审计





❖ 审计：数据库审计关注的问题

- 审计对象（对谁进行审计）
 - 标准审计（系统级、用户级）
 - 细粒度审计（对象级）
- 审计内容（对什么行为进行审计）
 - 访问数据库应用程序、位置及用户信息，包括用户操作、操作日期与时间、操作涉及的相关数据、操作是否成功等

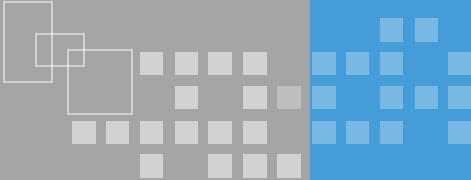


❖ 网络安全法中对数据保护的要求

- “未经被收集者同意，不得向他人提供个人信息”
- “采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。”

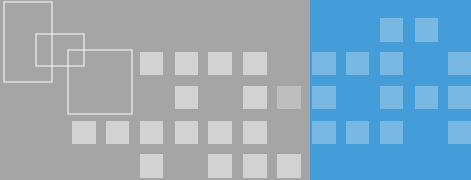
❖ 数据泄露防护应覆盖可能的数据外泄渠道，需要关注的问题

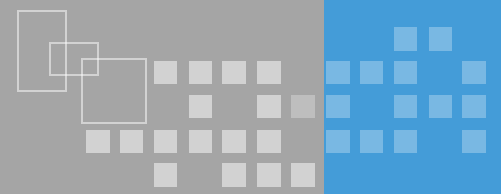
- 什么敏感数据需要发出；
- 谁会发出敏感数据；
- 这些数据要发往哪；
- 使用什么协议、端口等；
- 违反了哪些安全策略；
- 违规程度如何。



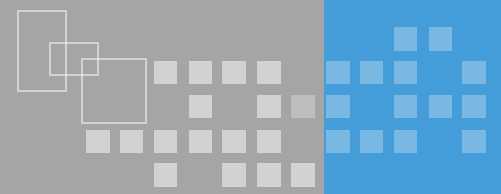
❖ 在对某面向互联网提供服务的某应用服务器的安全检测中发现，服务器上开放了以下几个应用，除了一个应用外其他应用都存在明文传输信息的安全问题，作为一名检测人员，你需要告诉用户对应用进行安全整改以外解决明文传输数据的问题，以下哪个应用已经解决了明文传输数据问题：

❖ A. SSH B. HTTP C. FTP D. SMTP

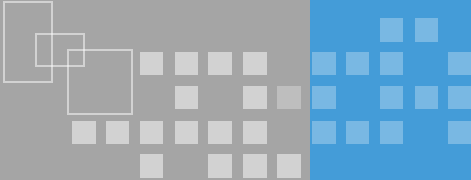
- 
- ❖ 近年来利用DNS 劫持攻击大型网站恶性攻击事件时有发生，防范这种攻击比较有效的方法是？
 - ❖ A. 加强网站源代码的安全性
 - ❖ B. 对网络客户端进行安全评估
 - ❖ C. 协调运营商对域名解析服务器进行加固
 - ❖ D. 在网站的网络出口部署应用级防火墙

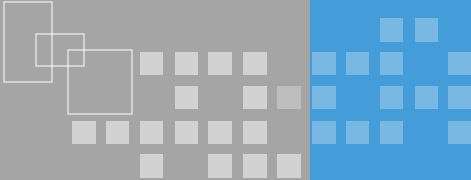


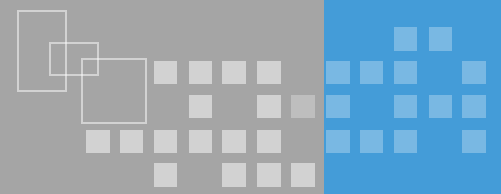
- ❖ 应用软件的数据存储在数据库中，为了保证数据安全，应设置良好的数据库防护策略，以下不属于数据库防护策略的是？
- ❖ A. 安装最新的数据库软件安全补丁
- ❖ B. 对存储的敏感数据进行安全加密
- ❖ C. 不使用管理员权限直接连接数据库系统
- ❖ D. 定期对数据库服务器进行重启以确保数据库运行良好



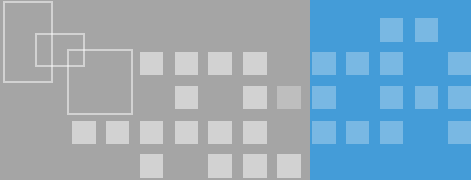
- ❖ 数据库的安全很复杂，往往需要考虑多种安全策略，才能更好地保护数据库的安全。以下数据库常用的安全策略使用不正确的是：（ ）
- ❖ A. 最小特权原则，是让用户可以合法的存取或修改数据的前提下，分配最小的特权，使得这些信息恰好能够完成用户的工作
- ❖ B. 最大共享策略，在保证数据库的完整性、保密性和可用性的前提下，最大程度地共享数据库中的信息
- ❖ C. 粒度最小策略，将数据库中的数据项进行划分，粒度越小，安全级别越高，在实际需求中需要选择最小粒度
- ❖ D. 按内容存取控制策略，不同权限的用户访问数据库的不同部分

- 
- ❖ Apache HTTP Server（简称 Apache）是一个开放源码的 Web 服务运行平台，在使用过程中，该软件默认会将自己的软件名称和版本号发送给客户端。从安全角度出发，为隐藏这些信息，应当采取以下哪种措施：（ ）。
 - ❖ A. 不选择 Windows 平台，应选择在 Linux 平台下安装
 - ❖ B. 安装后，修改配置文件 http.conf 中的有关参数
 - ❖ C. 安装后，删除 Apache HTTP Server 源码
 - ❖ D. 从正确的官方网站下载 Apache HTTP Server，并安装使用

- 
- ❖ Internet Explorer, 简称 IE, 是微软公司推出的一款 Web 浏览器, IE 中有很多安全设置选项, 用来设置安全上网环境和保护用户隐私数据, 以下哪项不是 IE 中的安全配置项目:
 - ❖ A. 设置 Cookie 安全, 允许用户根据自己的安全策略要求设置 Cookie 策略, 包括从阻止所有 Cookie 到接受所有 Cookie, 用户也可以选择删除已经保存过的 Cookie
 - ❖ B. 禁用自动完成和密码记忆功能, 通过设置禁止 IE 自动记忆用户输入过的 Web 地址和表单, 也禁止 IE 自动记忆表单中的用户名和口令信息
 - ❖ C. 设置每个链接的最大请求数, 修改MaxKeepAliveRequests, 如果同时请求数达到阈值就不再响应新的请求, 从而保证了系统资源不会被某个链接大量占用
 - ❖ D. 为网站设置适当的浏览器安全级别, 用户可以将各个不同的网站分到 Internet、本地Internet、受信任的站点、受限制的站点等不同安全区域中, 以采取不同的安全访问策略

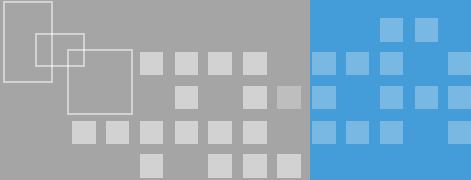


- ❖ 以下关于 HTTPS 协议与 HTTP 协议相比的优势说明，哪个是正确的？
- ❖ A. HTTPS 协议对传输的数据进行了加密，可以避免嗅探等攻击行为
- ❖ B. HTTPS 使用的端口与 HTTP 不同，让攻击者不容易找到端口，具有较高的安全性
- ❖ C. HTTPS 协议是 HTTP 协议的补充，不能独立运行，因此需要更高的系统性能
- ❖ D. HTTPS 协议使用了挑战机制，在会话过程中不传输用户名和密码，因此具有较高的安全性



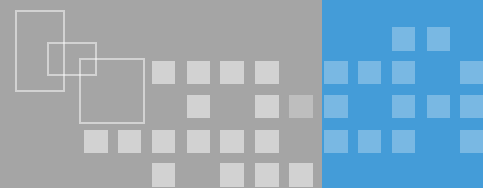
❖ 某公司在互联网区域建立了一个 WEB 网站, 为了保护该网站主页安全性, 尤其是不能让攻击者修改主页内容, 该公司应当购买并部署下面那个设备?

- ❖ A. 负载均衡设备
- ❖ B. 网页防篡改系统
- ❖ C. 网络防病毒系统
- ❖ D. 网络审计系统



❖ 小王在某 web 软件公司工作，她在工作中主要负责对互联网信息服务（IIS）软件进行安全配置，这是属于（ ）方面的安全工作。

- ❖ A. web 服务支撑软件
- ❖ B. web 应用程序
- ❖ C. web 浏览器
- ❖ D. 通信协议



- ❖ 操作系统安全
 - 安全机制
 - 安全部署原则
- ❖ 针对系统的攻击
 - 信息收集
 - 口令破解
 - 缓冲区溢出
- ❖ 应用安全
 - Web应用安全
 - 针对web的攻击
- ❖ 数据库安全防护



谢谢，请提问题！