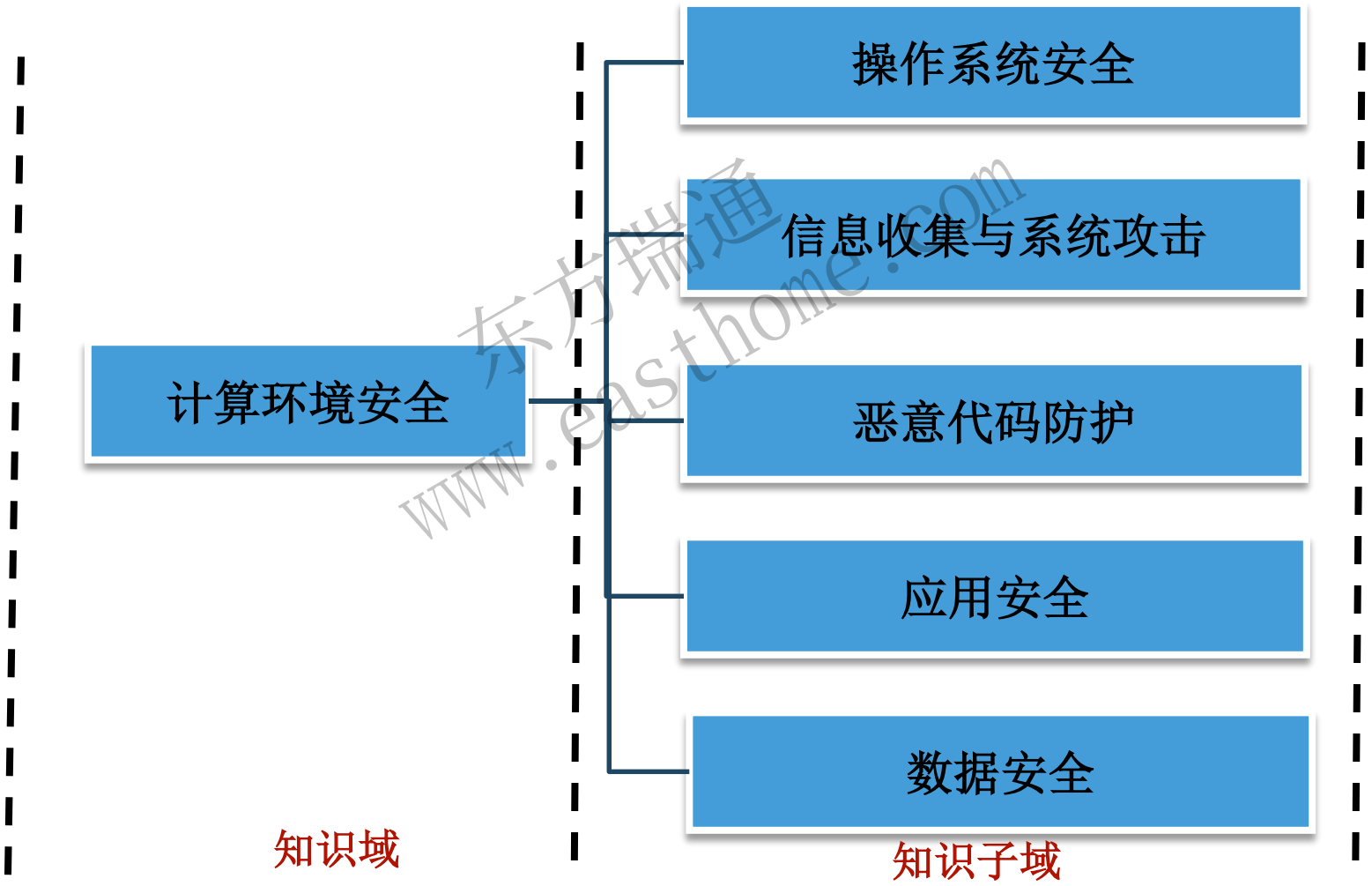
计算环境安全

版本：4.2

讲师姓名　　机构名称

课程内容



知识子域：操作系统安全

- 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

- 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

标识与鉴别

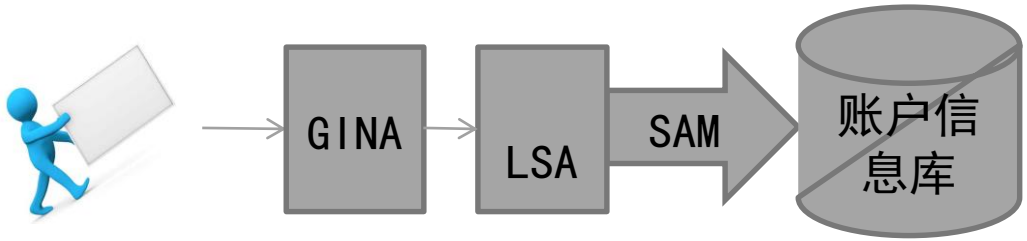
- Windows系统的标识
  - 安全主体（账户、计算机、服务等）
  - 安全标识符（Security Identifier，SID）
    - 安全主体的代表（标识用户、组和计算机账户的唯一编码）
    - 范例：S-1-5-21-1736401710-1141508419-1540318053-1000
- Linux/Unix系统的标识
  - 安全主体：用户标识号（User ID）

标识与鉴别

- Windows系统用户信息管理
  - 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）

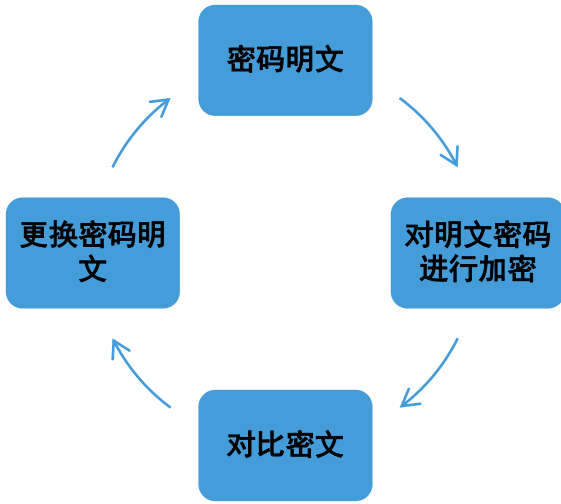
Administrator:500:C8825DB10F2590EAAAD3B435B51404EE
:683020925C5D8569C23AA724774CE6CC:::

- 身份鉴别
  - 远程鉴别
    - SMB、LM、NTLM
  - 本地鉴别



标识与鉴别

- 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

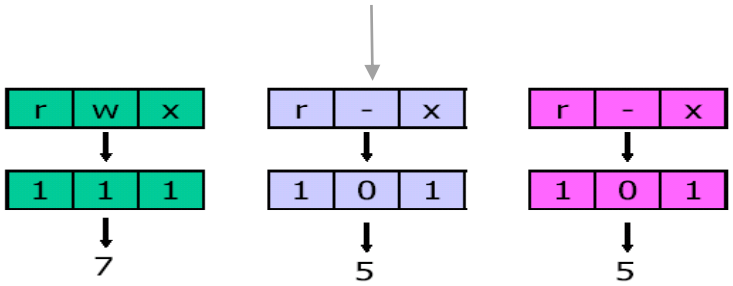


#root:**1acXMce89**:13402:0:99999:7:::

访问控制

- 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



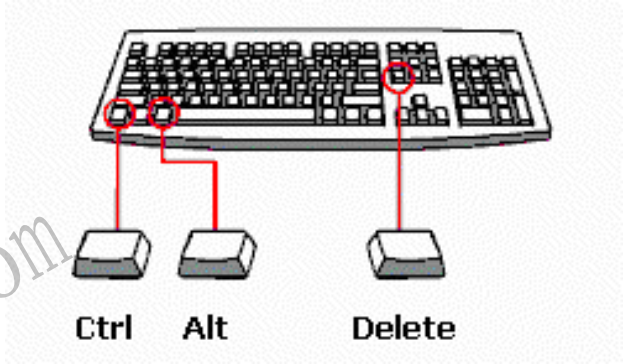
权限管理

- 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
```

信道保护

- 正常信道的保护
  - 可信通路（Trusted Path）
  - 安全键（SAK）



- 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

安全审计

- 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

内存保护与文件系统保护

- 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
  - 加密
    - Windows(EFS、Bitlocker)
    - Linux(eCryptfs)

操作系统安全配置

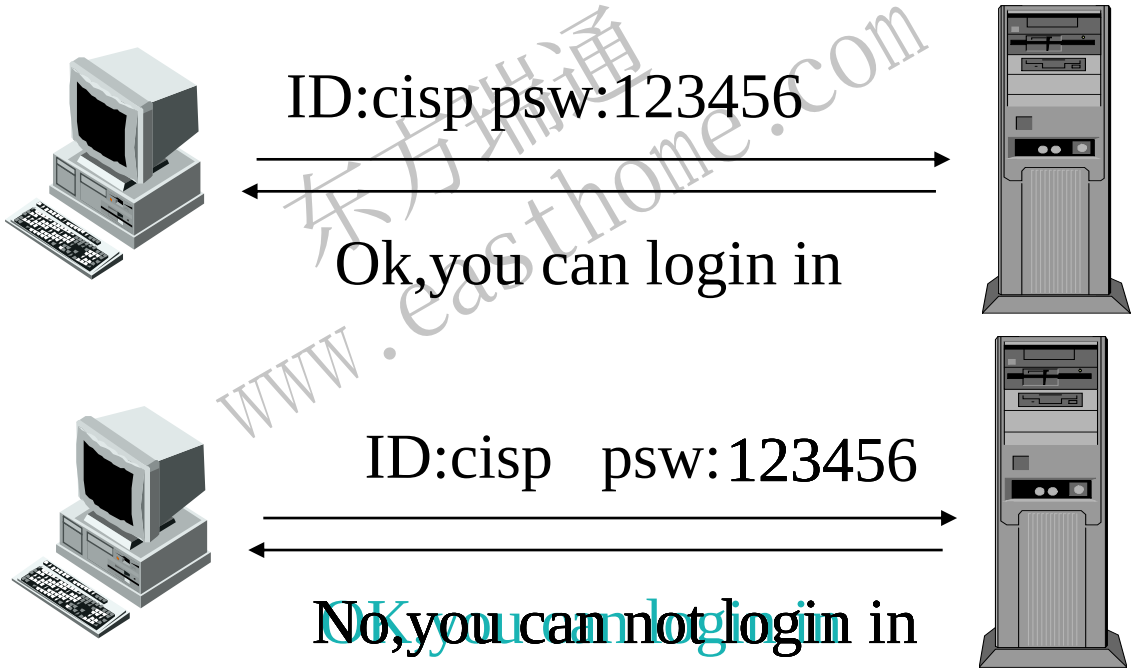
- 安装
  - 分区设置
  - 安全补丁&最新版本
  - 官方或可靠镜像（Md5校验）
- 最小化部署
  - 明确需要的功能和组件，不需要的服务和功能都关闭
- 远程访问控制
  - 开放端口
  - 远程连接的限制

操作系统安全配置

- 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
    - 帐户锁定阀值
    - 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



安全审计

- 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

知识子域：信息收集与系统攻击

- 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。

信息收集与情报析

- 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

信息搜集和分析

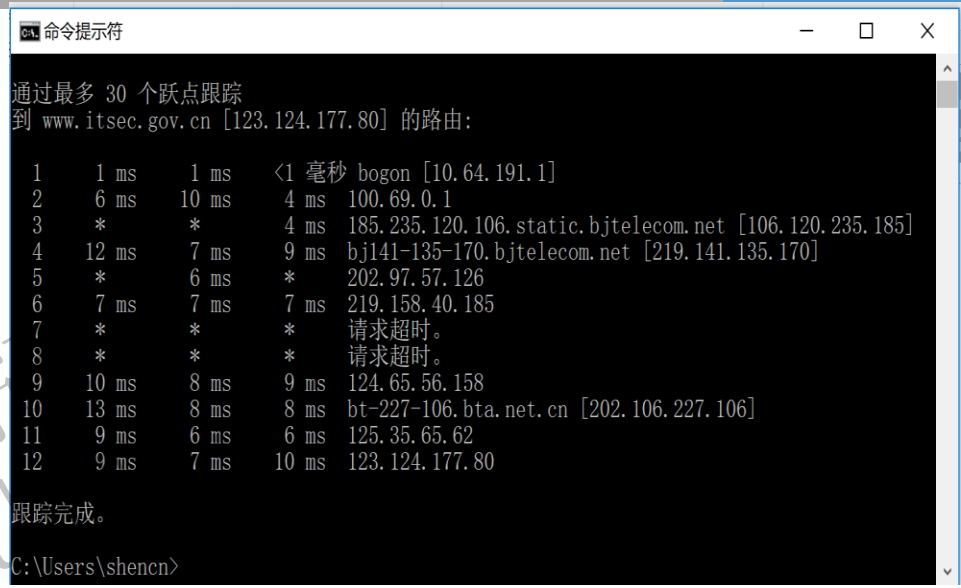
- 收集哪些信息
  - 目标系统的信息系统相关资料
    - 域名、网络拓扑、操作系统、应用软件、相关脆弱性
  - 目标系统的组织相关资料
    - 组织架构及关联组织
    - 地理位置细节
    - 电话号码、邮件等联系方式
    - 近期重大事件
    - 员工简历
  - 其他可能令攻击者感兴趣的任何信息

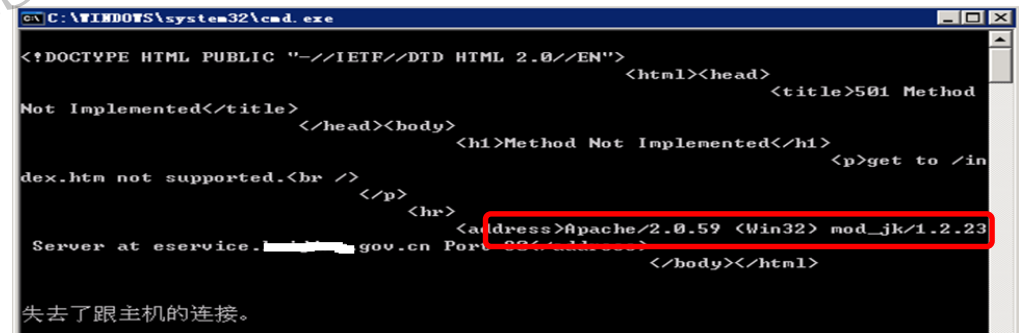
公开信息收集-搜索引擎

- 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



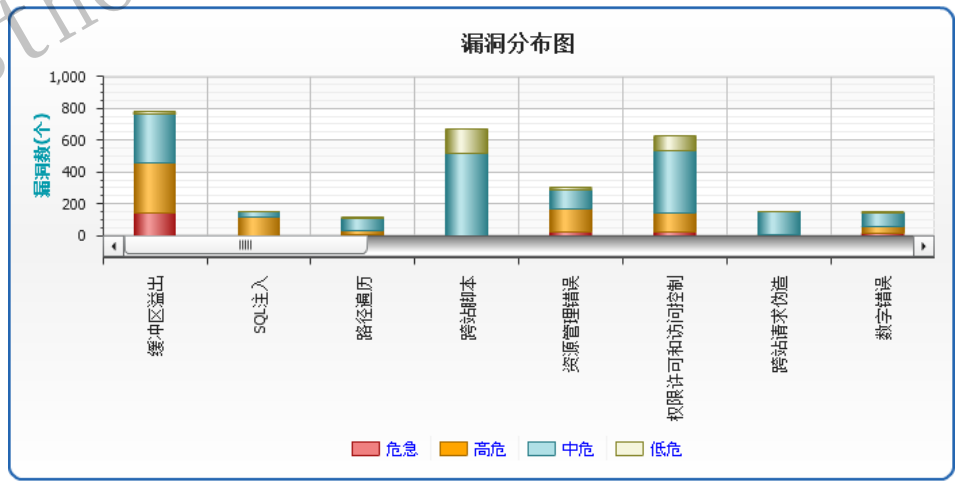


信息收集与分析的防范

- 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

系统攻击–缓冲区溢出

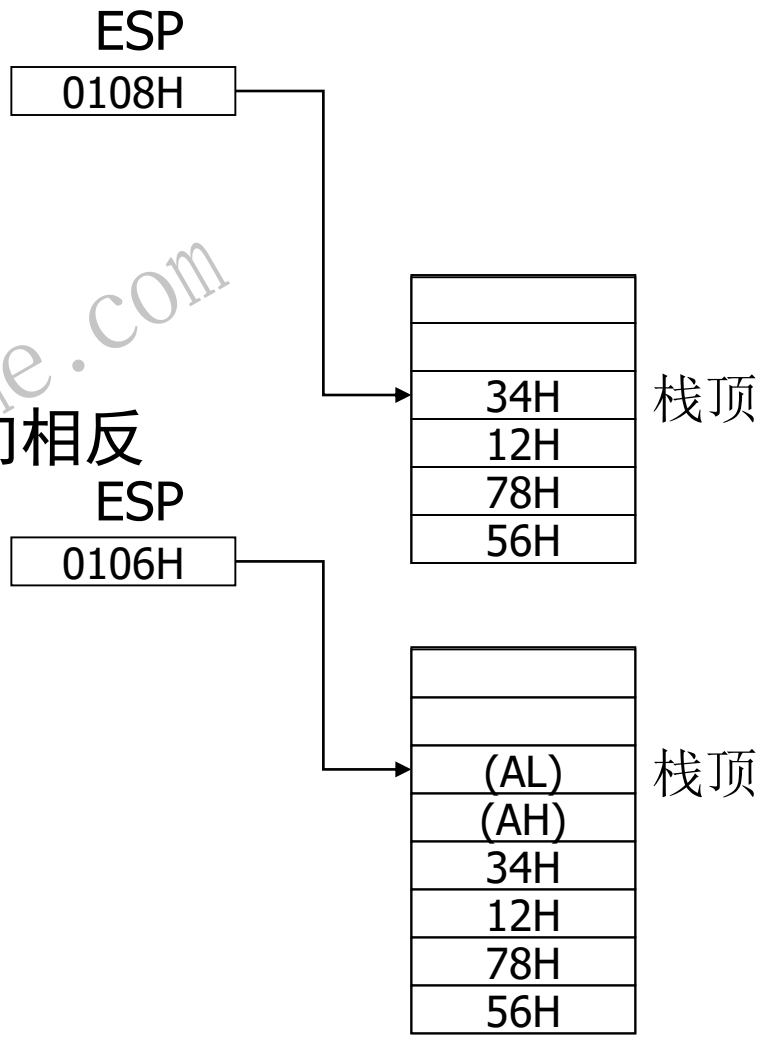
- 缓冲区溢出攻击原理
  - 缓冲区溢出攻击利用编写不够严谨的程序，通过向程序的缓冲区写入超过预定长度的数据，造成缓存的溢出，从而破坏程序的堆栈，导致程序执行流程的改变
- 缓冲区溢出的危害
  - 最大数量的漏洞类型
  - 漏洞危害等级高



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）



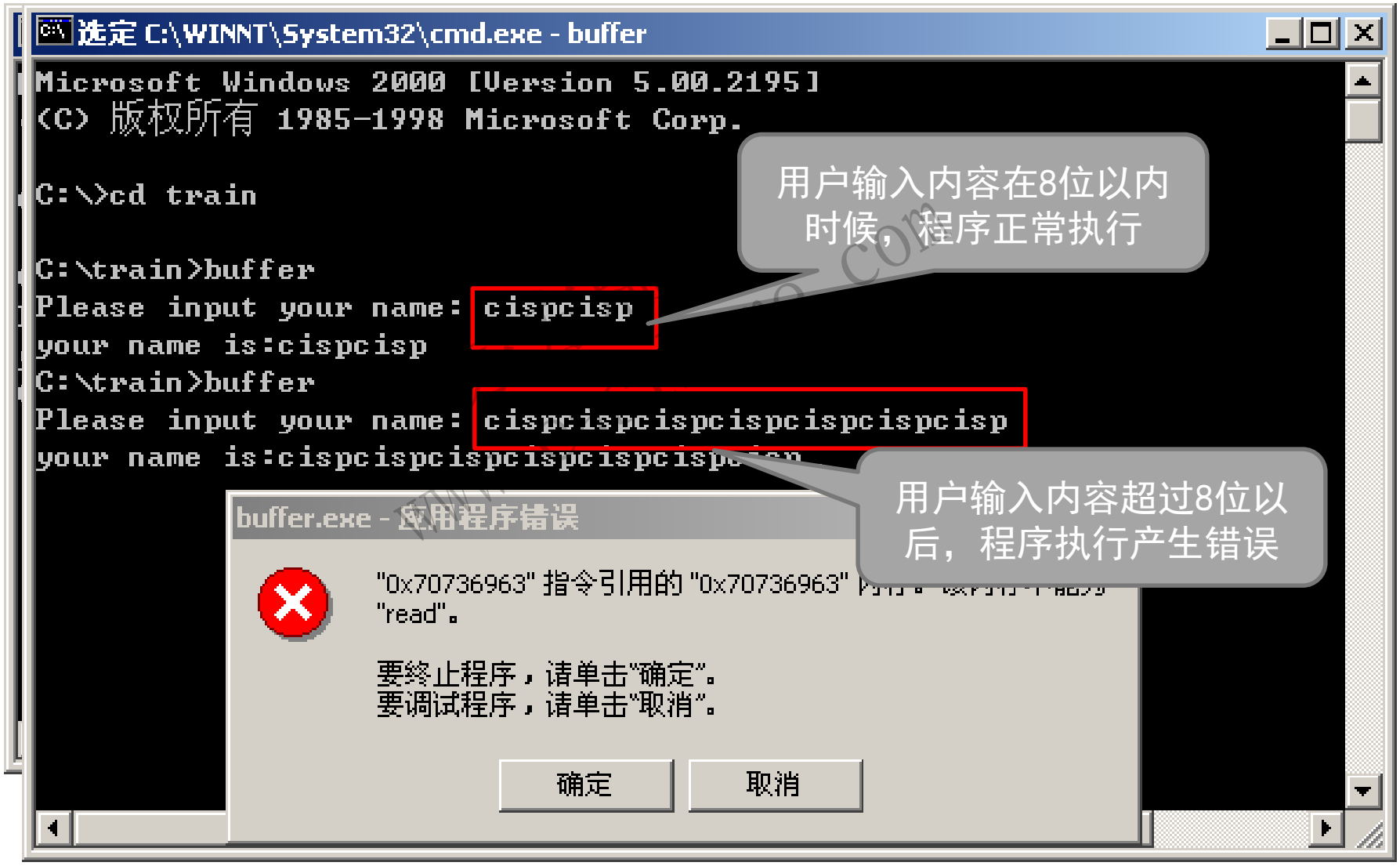
缓冲区溢出简单示例

- 程序作用：将用户输入的内容打印在屏幕上

Buffer.c

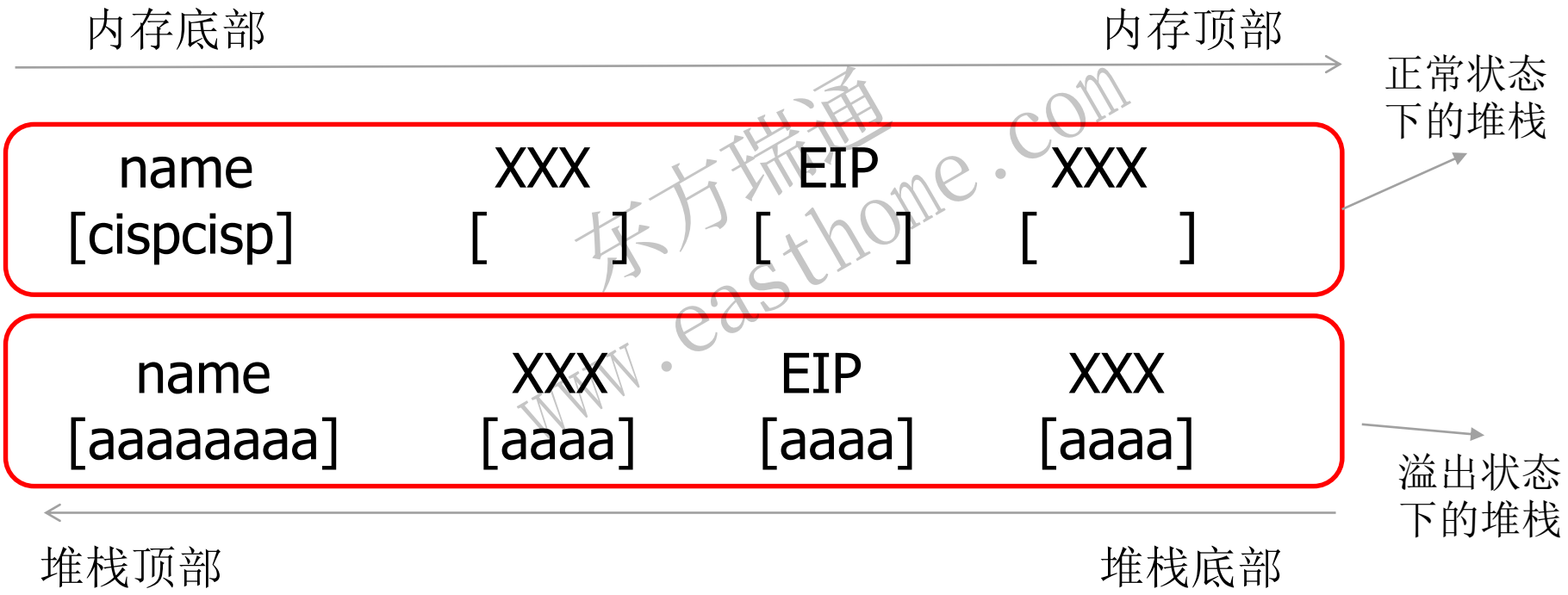
```
#include <stdio.h>
int main ( )
{
        char name[8];
        printf("Please input your name: ");
        gets(name);
        printf("you name is: %s!", name);
        return 0;
}
```

缓冲区溢出示例


选定 C:\WINNT\System32\cmd.exe - buffer
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.
C:\>cd train
C:\train>buffer
Please input your name: cispcisp
your name is:cispcisp
C:\train>buffer
Please input your name: cispcispcispcispcispcispcisp
用户输入内容在8位以内时候，程序正常执行
用户输入内容超过8位以后，程序执行产生错误
buffer.exe - 应用程序错误
"0x70736963" 指令引用的 "0x70736963" 内存。该内存不能为 "read"。
要终止程序，请单击"确定"。
要调试程序，请单击"取消"。
确定
取消

缓冲区溢出简单示例

程序溢出堆栈情况



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

知识子域：恶意代码防护

- 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

恶意代码传播方式

- 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

恶意代码的预防技术

- 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

恶意代码检测技术-特征码扫描

- 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）
  - ……

恶意代码检测技术-行为检测

- 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

恶意代码分析技术

- 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

恶意代码的清除

- 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

基于互联网技术的防御

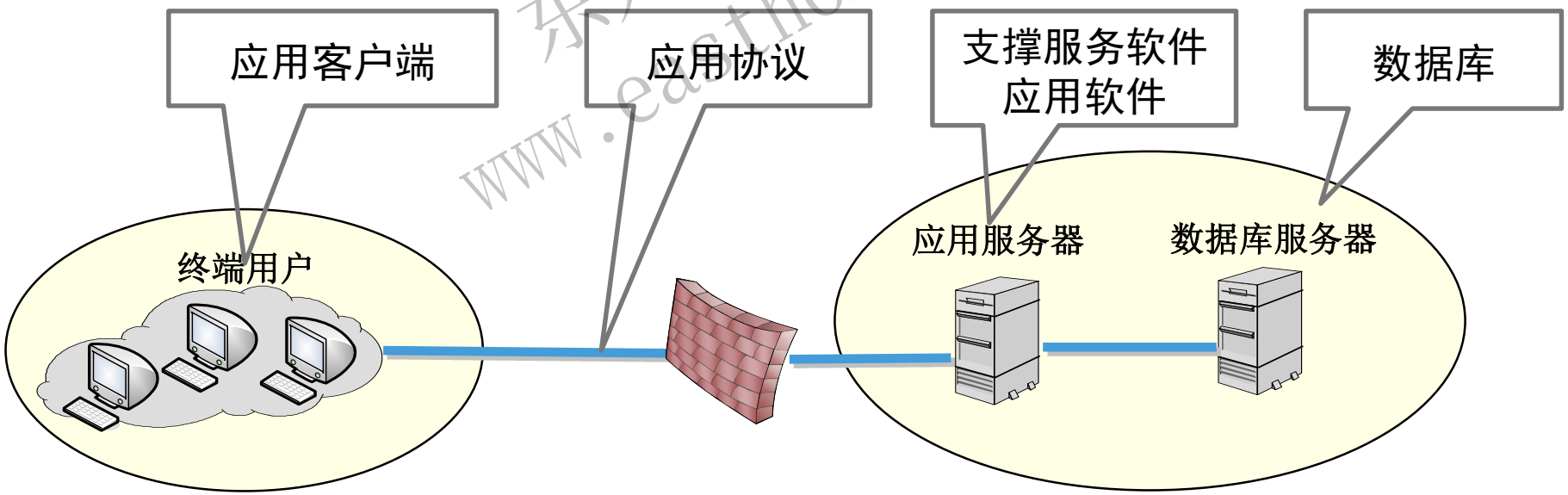
- 恶意代码监测与预警体系
  - 蜜罐、蜜网
- 恶意代码云查杀
  - 分布式计算

知识子域：应用安全

- 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。

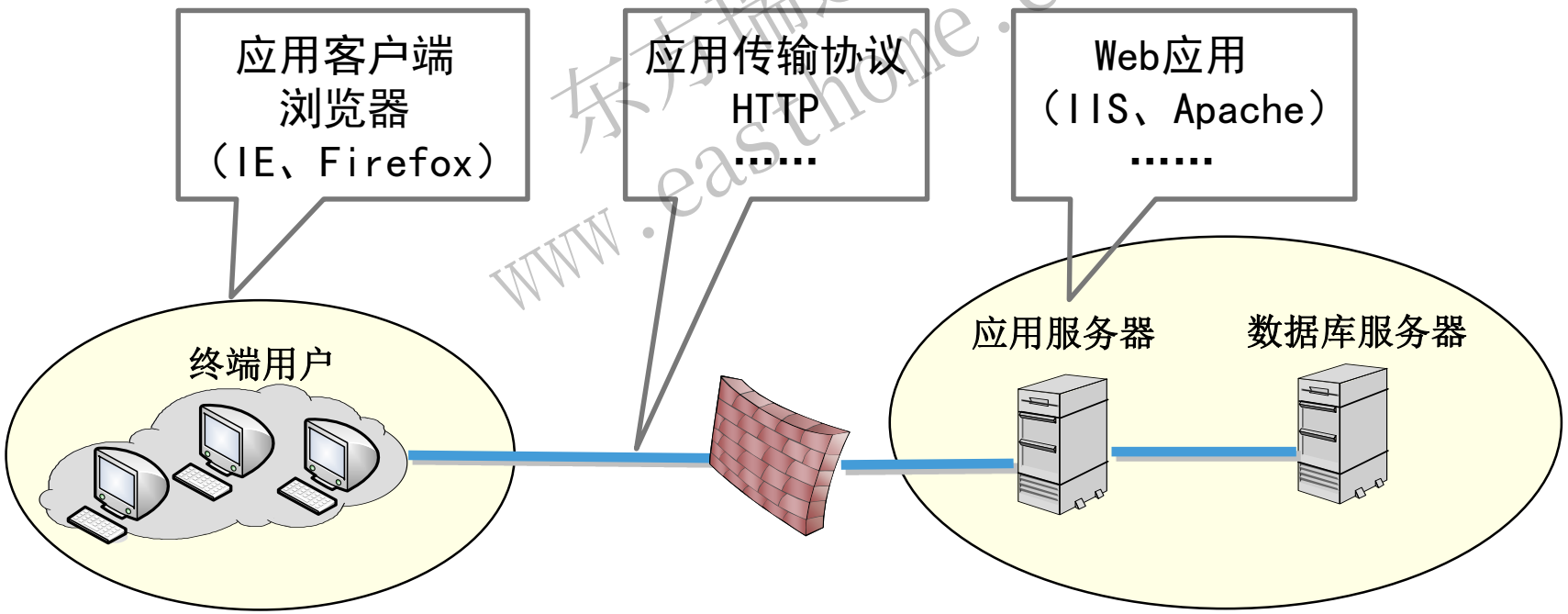
应用安全威胁

- 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应用安全

- 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协议

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（协议状态代码描叙、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

HTTP协议安全问题

- 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

Web服务端软件安全问题

- 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

Web安全防护技术

- 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

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

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

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'

SQL注入攻击

- 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！

SQL注入的危害

- 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）

SQL注入的防御

- 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器之间的信任关系实现恶意攻击
- 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

知识子域：应用安全

- 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。

电子邮件安全

- 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
    - 使用SSL保护会话
    - 安全策略
  - 客户端

其他互联网应用安全

- 远程接入
- 域名系统
- 即时通信

知识子域：数据安全

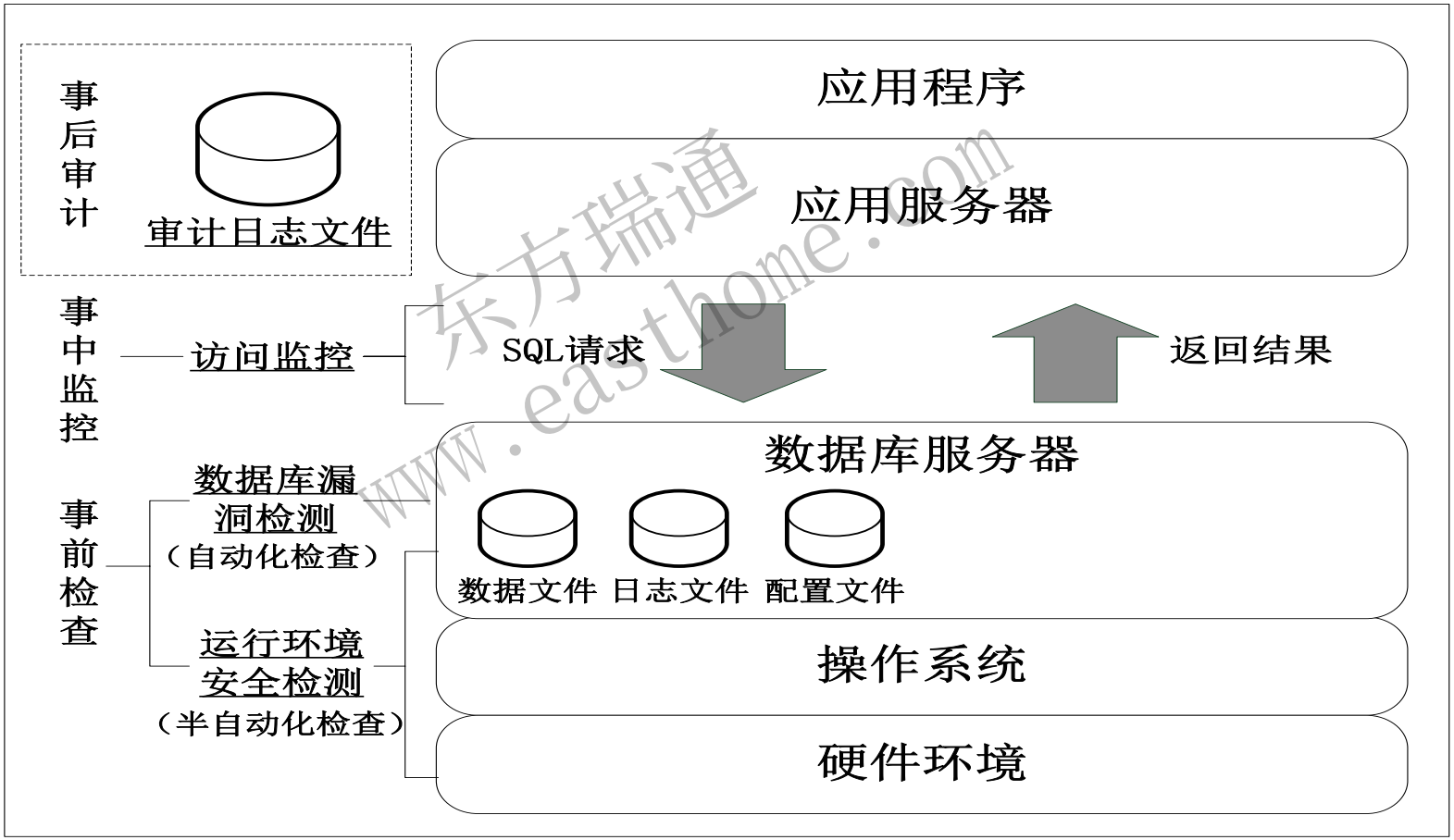
- 数据库安全
  - 了解数据库安全要求；
  - 掌握数据库安全防护的策略和要求。
- 数据泄露防护
  - 了解数据泄露防护的概念。

数据库安全措施

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

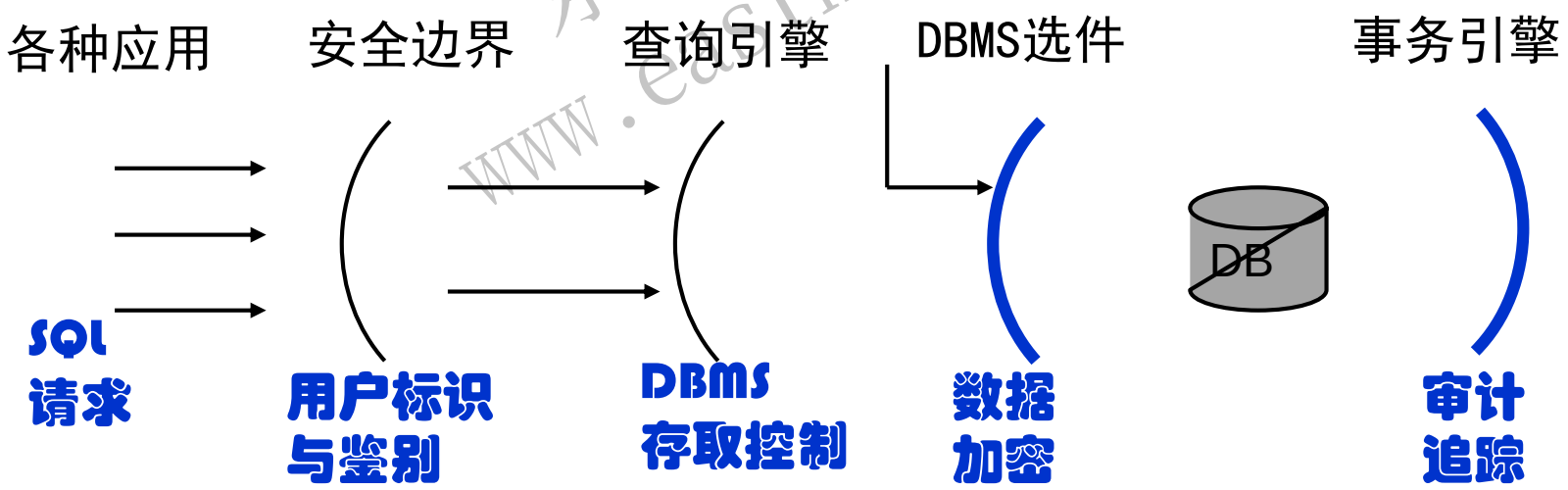
数据库安全防护

❖ 检查、监控、审计



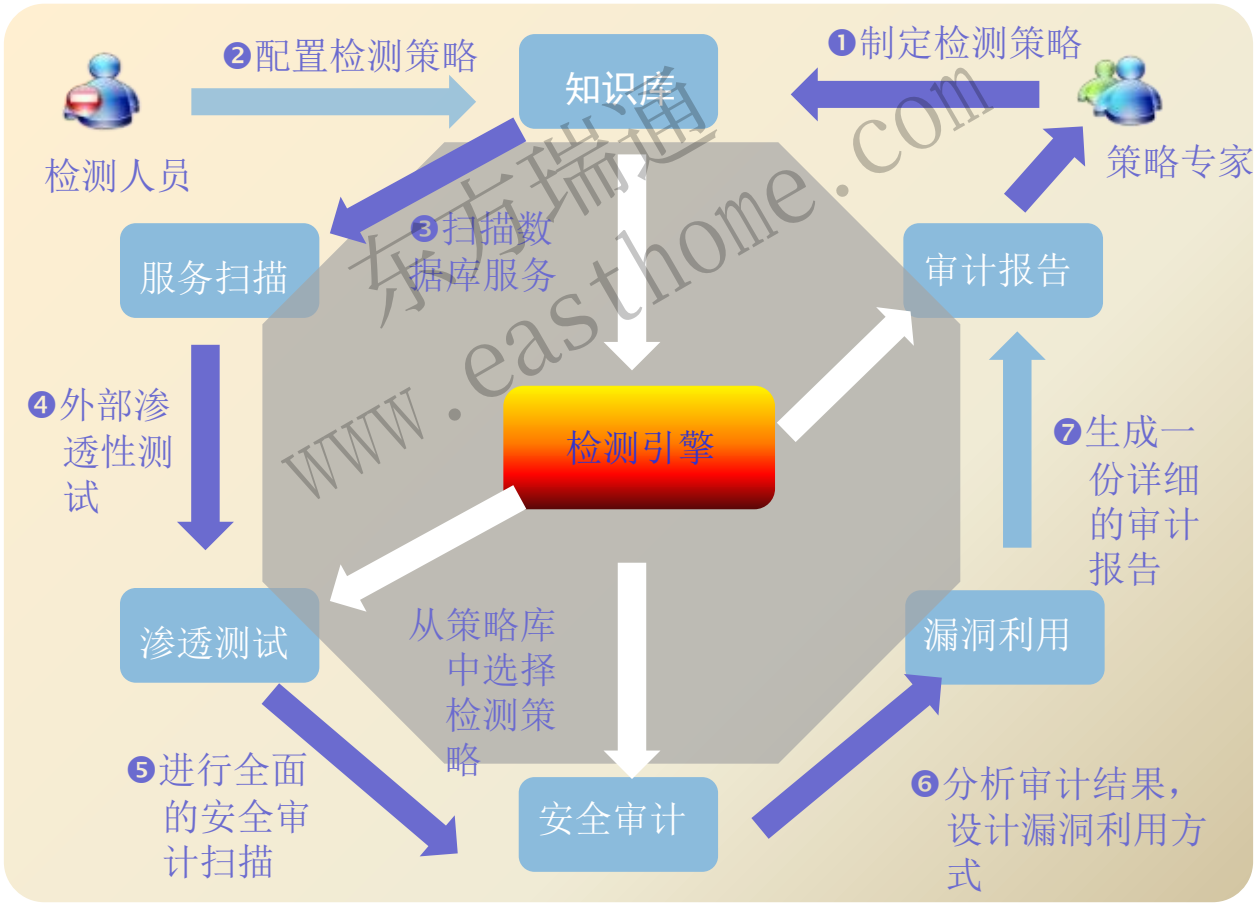
数据库安全防护-构建深度防御体系

- 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

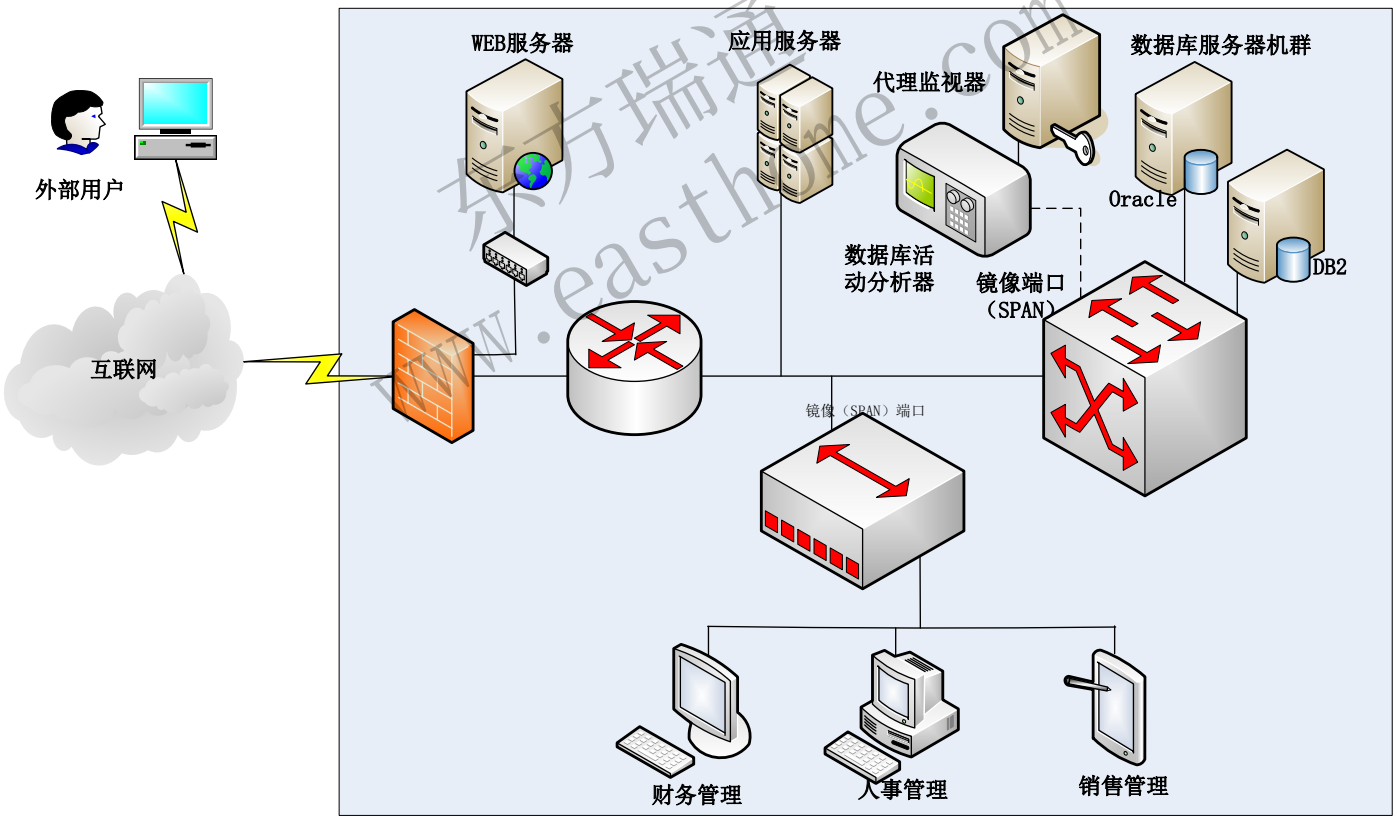


数据库安全特性检查

- 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



数据库安全防护-安全审计

- 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

数据防泄露

- 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。

总结

- 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

邀请您参与讲师考评

谢谢，请提问！