# 网络攻击与防御

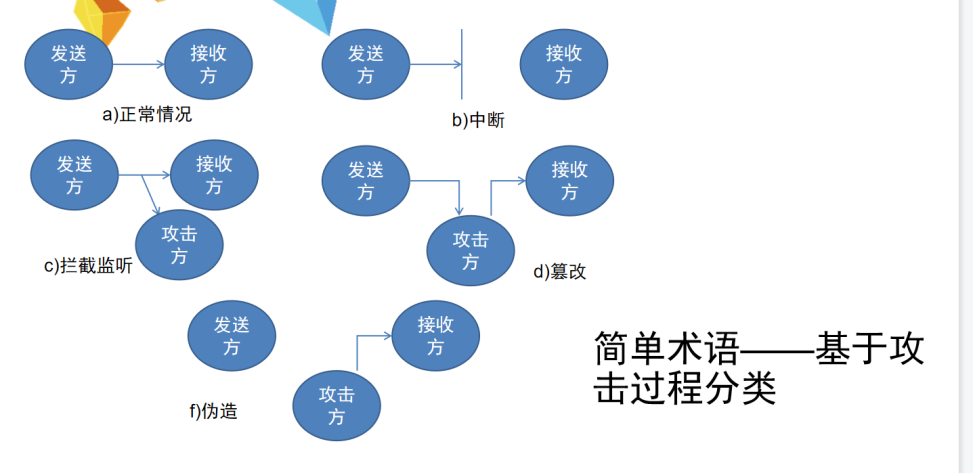
## 第一章

1. 信息安全三原则：

文本

描述已自动生成

1. 在安全漏洞生命周期中，从安全漏洞被发现到厂商发布补丁程序用于修补该漏洞之前的这段时间，被安全社区普遍地称为0day。
2. 国际标准化组织ISO对信息安全定义的建议是：为数据处理系统建立和采取的技术和管理的安全保护。保护计算机的硬件、软件和数据不因偶然的或恶意的原因而受到破坏、更改、泄漏。
3. 攻击手段：中断、拦截监听、篡改、伪造



1. APT是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。
2. EXP（或Exploit）是一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机理以及利用的方法。
3. POC: 是一段说明或者一个攻击的样例使得读者能够确认这个漏洞是真实存在的
4. 几个黑客组织：匿名者、海莲花、方程式组织、NSA

## 第二章

1. 信息收集：通过各种方式获取所需要的信息
2. 在使用Google搜索时，\*符号用于模糊匹配某些内容。当利用google进行搜索想要只搜某网站\某类型文件的内容时，可以使用site\filetype关键字。allinurl：限制搜索的词语是网页网址中包含的关键词
3. Sodan:一款搜索引擎
4. Web信息搜索与挖掘的防范：

（1）组织安全敏感信息和个人隐私信息不要在网上随意发布

（2）个人上网购物、支付时尽量保持匿名，或选择信誉良好的网站

（3）发现非预期的敏感信息泄漏时应采取行动进行清除

1. 国家代码域名支持组织CNNSO：负责国家顶级域名分配，包括.us、.cn、.jp等。
2. ICANN（互联网名称与数字地址分配机构）：负责互联网协议（IP）地址的空间分配、协议标识符的指派、通用顶级域名（gTLD）以及国家和地区顶级域名（ccTLD）系统的管理、以及根服务器系统的管理
3. ASO(地址支持组织)
4. CNNIC(域名注册管理机构和域名根服务器运行机构)
5. CDNC(中文域名国际协调组织):在国际上担负起中文域名的协调和规范工作
6. 基本名称支持组织GNSO :负责通用顶级域名（gTLD）分配包括.com、.net、.edu、.org和.info等
7. 可以使用Whois查询特定域名的详细注册信息。
8. 域名信息探测命令：

dig命令：

格式：dig @dnsserver name querytype（DNS服务器 要查询的域名 DNS记录类型A/AAAA/PTR/MX/ANY）（MX：邮件服务器记录，AAAA 地址记录（Ipv6）A：地址记录(Ipv4)，PTR：反向记录）

ANSWER SECTION:查询的结果

AUTHORITY SECTION:权威DNS查询结果

nslookup命令：

当nslookup的第一个参数是要查询的主机名或者主机地址时，将会使用该指令的非交互模式(如：nslookup www.baidu.com）

nslookup不带任何参数时，可以进入其交互模式

1. 路由信息探测

Ping：用于测试网络连接量的程序

Tracert(Win)\traceroute ：用于确定 IP数据包访问目标所采取的路径.

#### 第三章

1. 网络扫描类型及目的:

手机屏幕截图

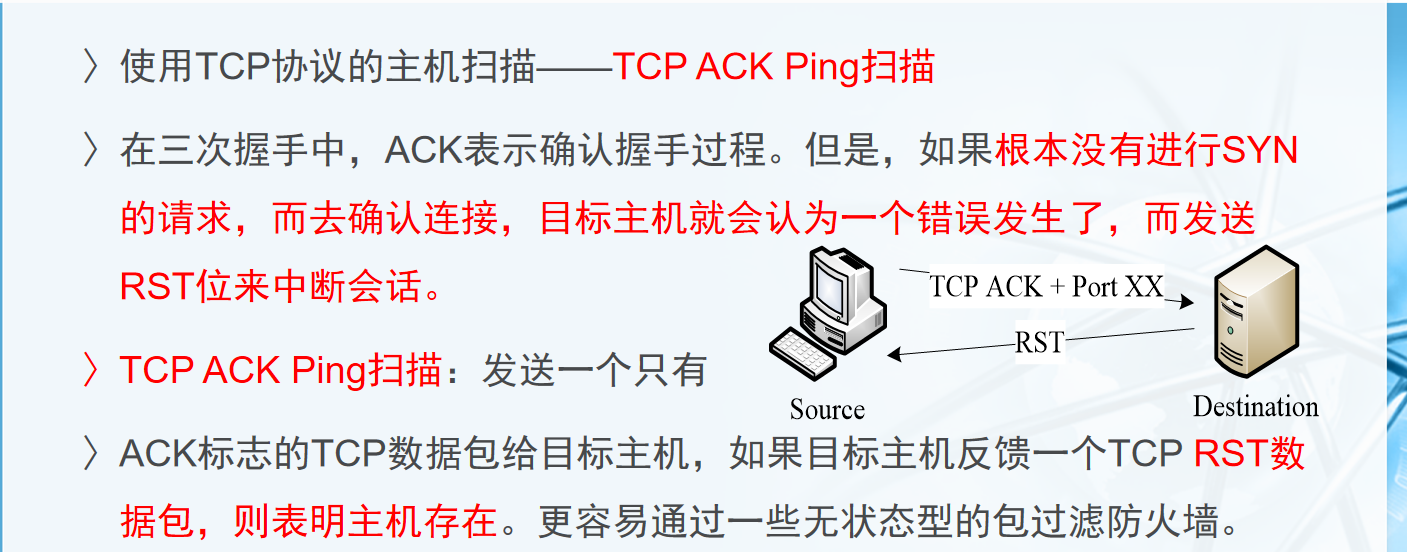
描述已自动生成

1. TCP/IP三次握手协议过程。

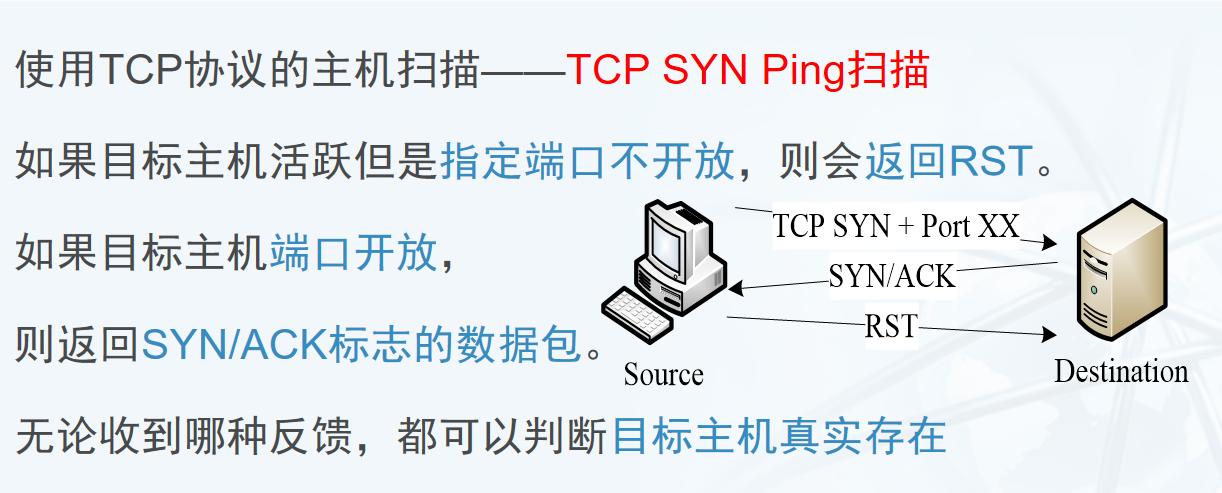
图示

描述已自动生成

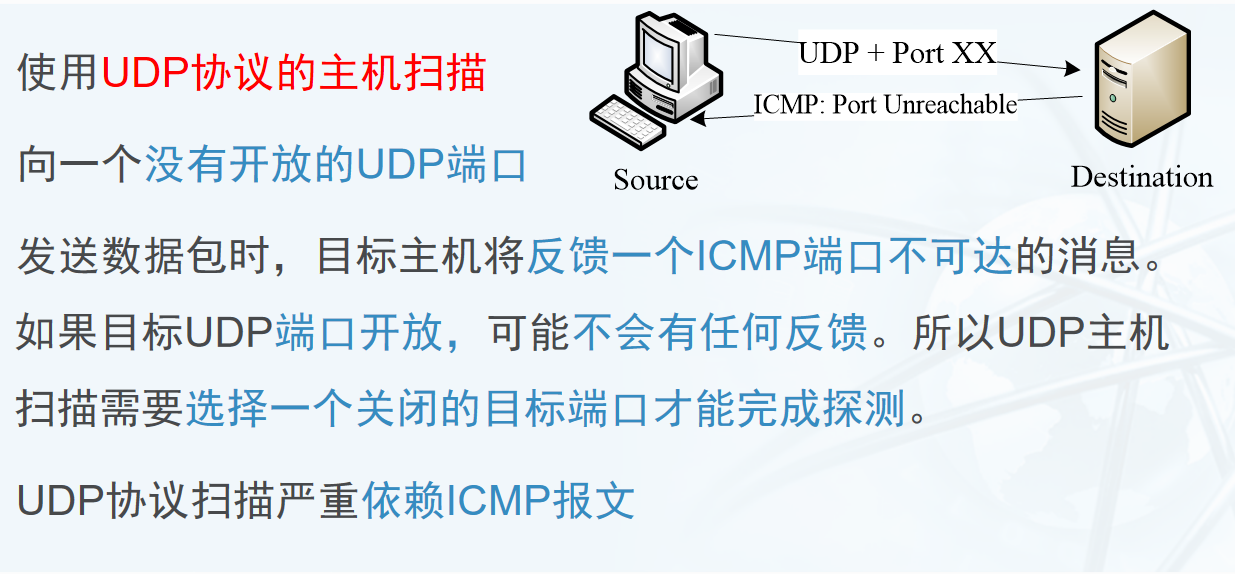
1. TCP ACK Ping主机扫描。



1. TCP SYN Ping主机扫描



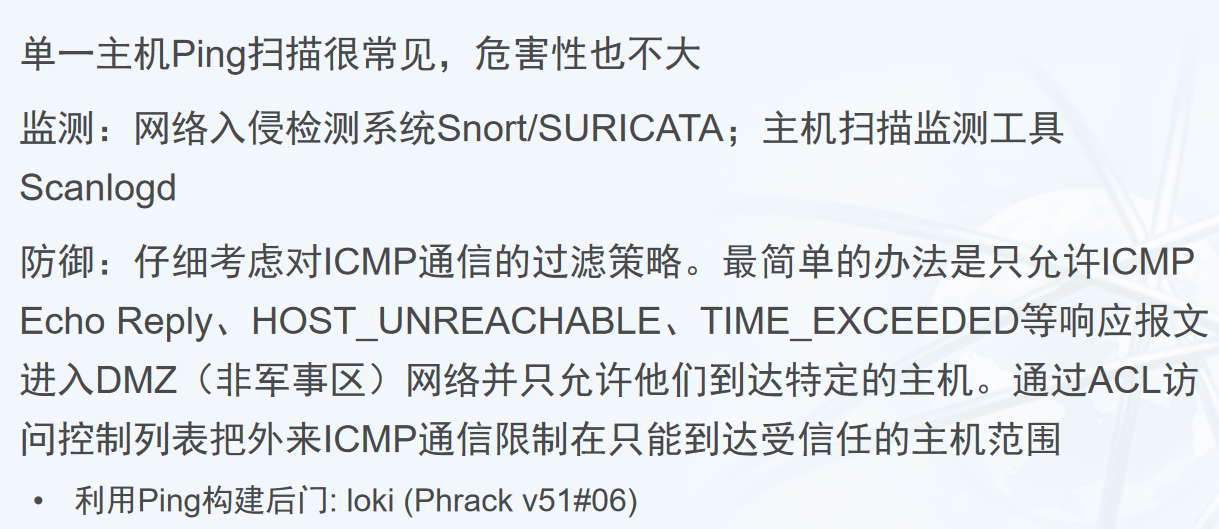
1. 使用UDP协议的主机扫描



1. 主机扫描工具-Nmap



1. 主机扫描防范措施



1. 端口扫描

是一种用来确定目标主机TCP端口和UDP端口状态的方法。开放某个端口，意味着提供某种网络服务

HTTP服务，默认的端口号为80/tcp；

HTTPS服务，默认的端口号为443/tcp 443/udp

SSH（安全登录），默认的端口号为22/tcp；

SMTP 默认的端口号为25/tcp

TOMCAT，默认的端口号为8080；

WINDOWS远程登陆，默认的端口号为3389；

FTP，默认的端口号为21/tcp

Oracle 数据库，默认的端口号为1521；

MS SQL\*SERVER数据库server，默认的端口号为1433/tcp

Mysql 数据库默认端口号3306

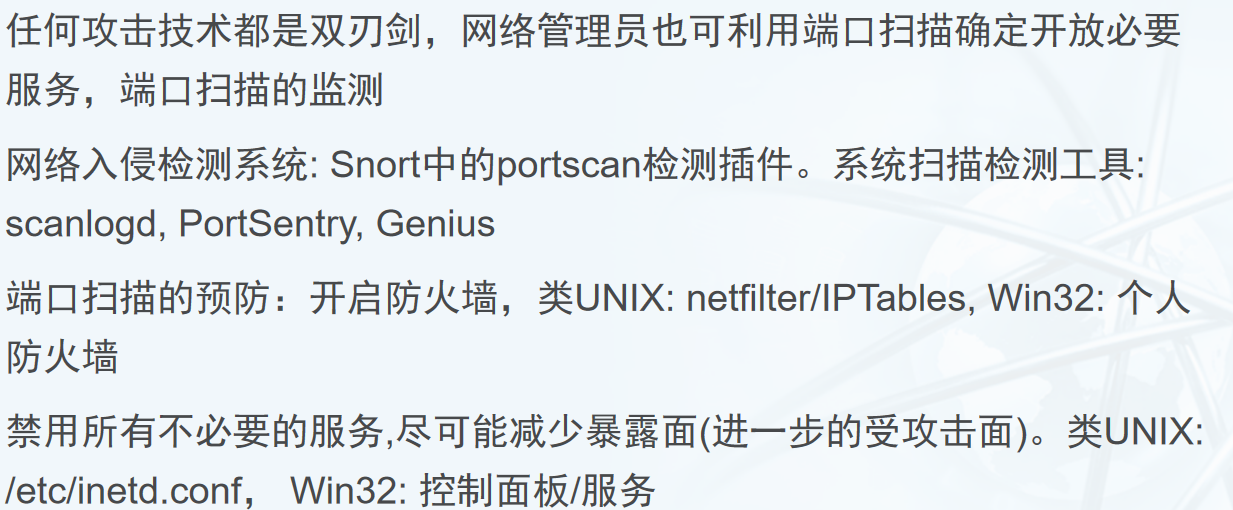
QQ，默认的端口号为1080/udp

Telnet，默认端口号为23/tcp

1. 端口扫描-Nmap



1. 端口扫描防范措施



1. 系统类型探查

探查活跃主机的系统及开放网络服务的类型

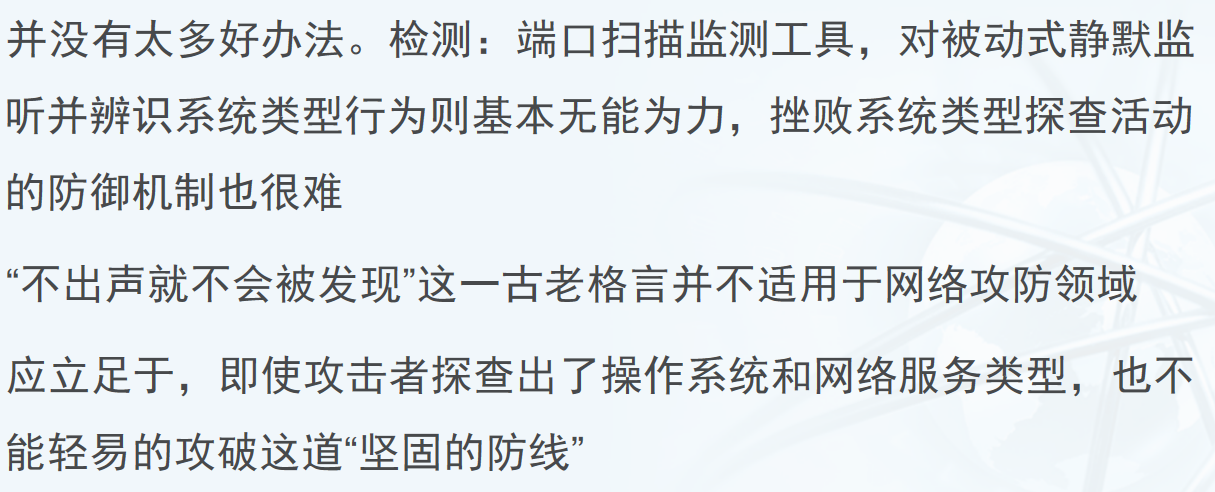
操作系统类型探查：通过各种不同操作系统类型和版本实现机制上的差异

协议栈实现差异－协议栈指纹鉴别（准确度更高）

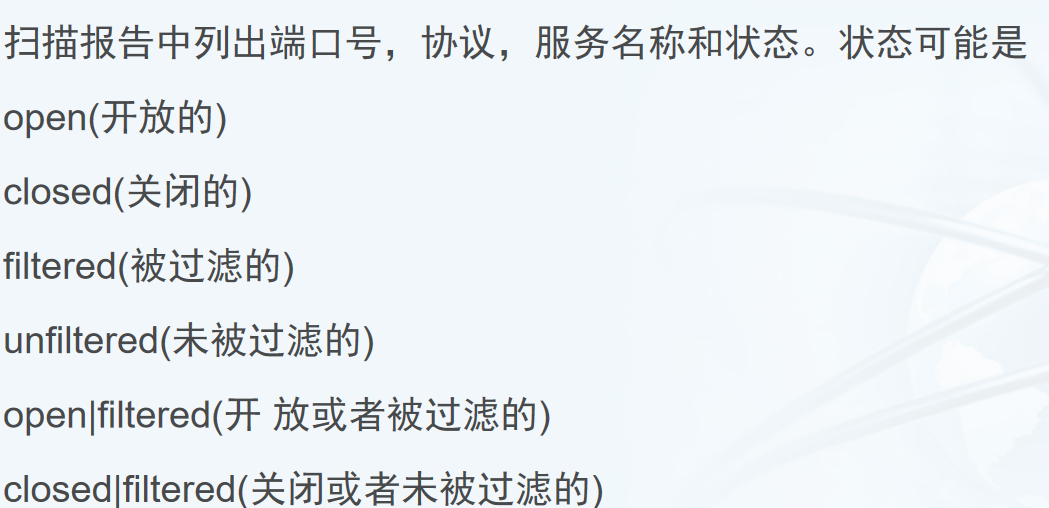
开放端口的差异－端口扫描

应用服务的差异－旗标攫取

1. 网络服务主动探测: nmap -sV
2. 系统类型探查防范措施



1. nmap扫描结果报告



1. 安全漏洞数据库

微软安全漏洞公告MSxx-xxx

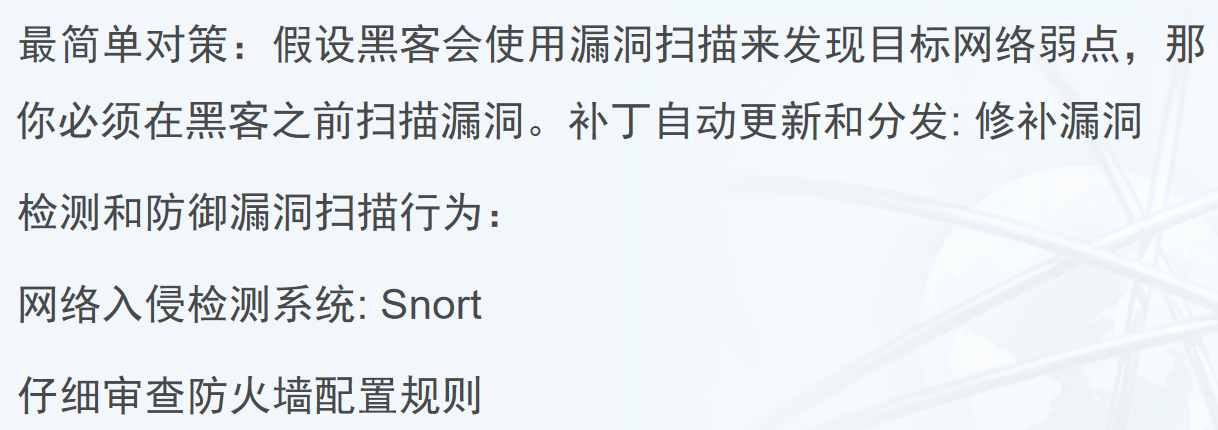
美国国家漏洞库NVD，NCSD国家网际安全部门US-CERT组负责维护

CNNVD：中国国家漏洞库，由中国信息安全测评中心维护

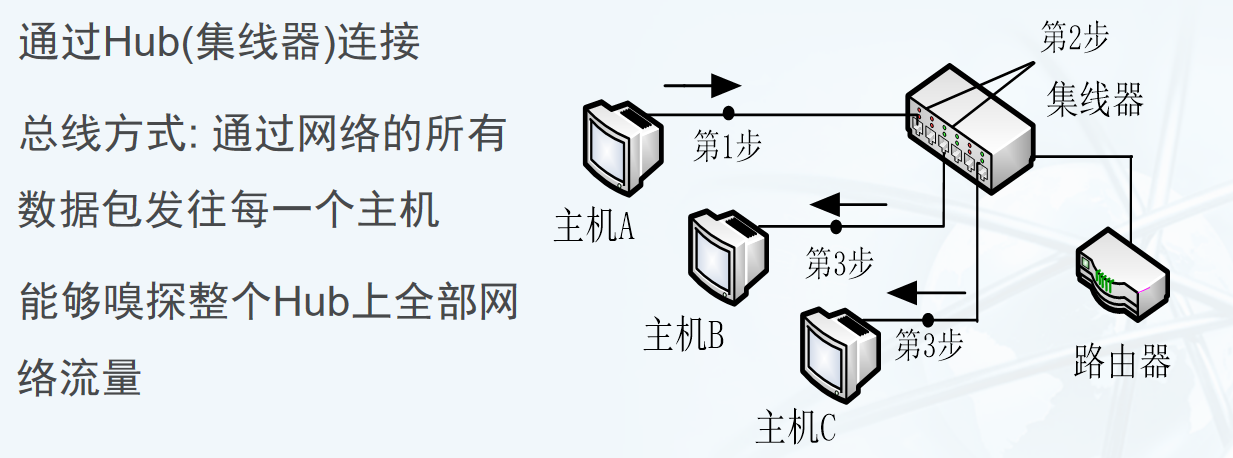
CNVD：中国国家信息安全漏洞共享平台，由国家计算机网络应急技术处理协调中心（CNCERT/CC）维护

CVE编号是业界标识该漏洞的标准索引号。

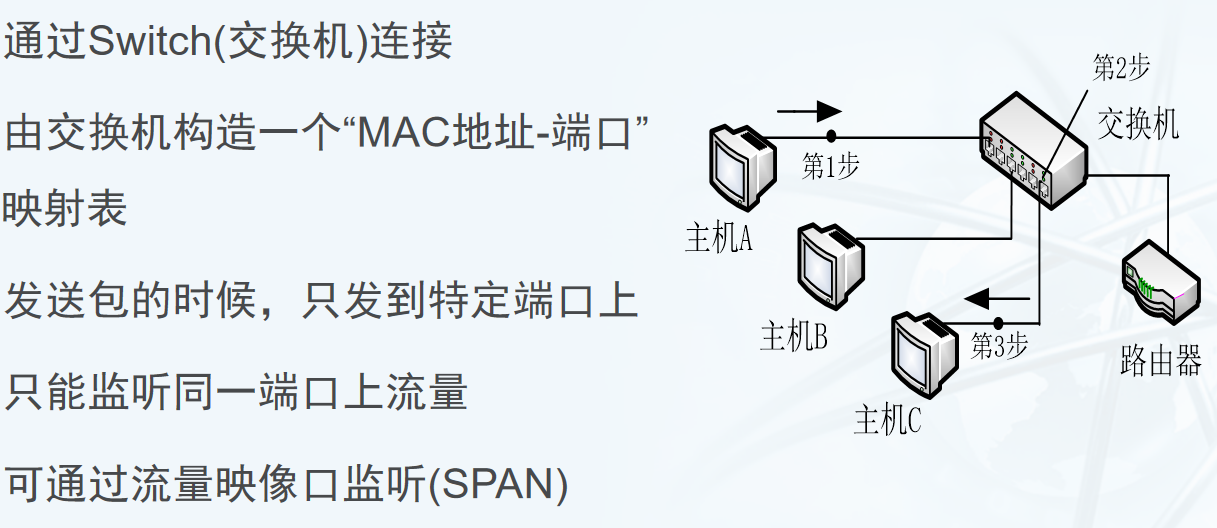
1. 漏洞扫描工具：Nessus、OpenVAS（基于C/S,B/S工作，通过浏览器下达扫描任务）、AWVS（网络爬虫）
2. 漏洞扫描防范措施



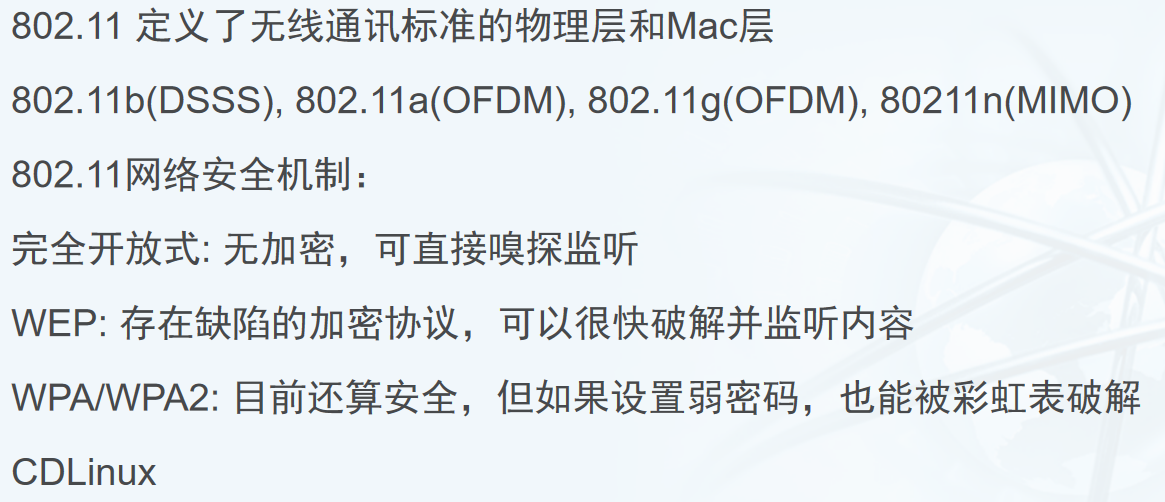
1. 共享式网络中的嗅探



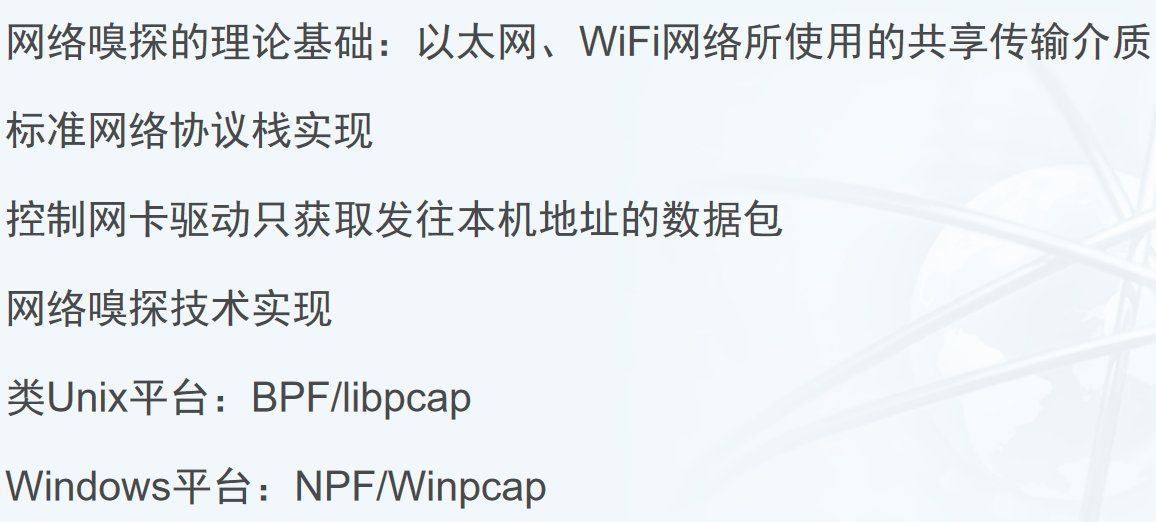
1. 交换式网络

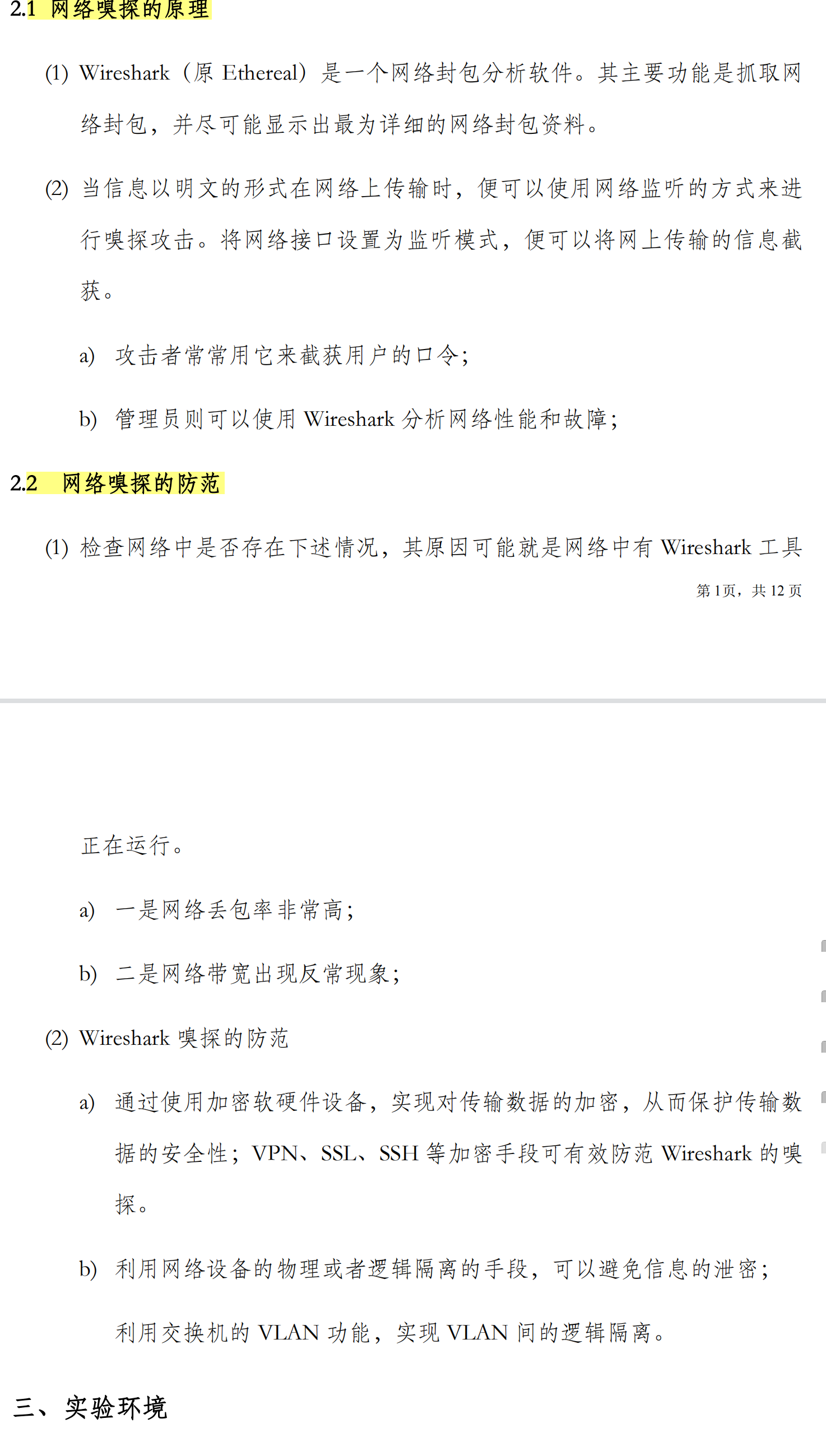


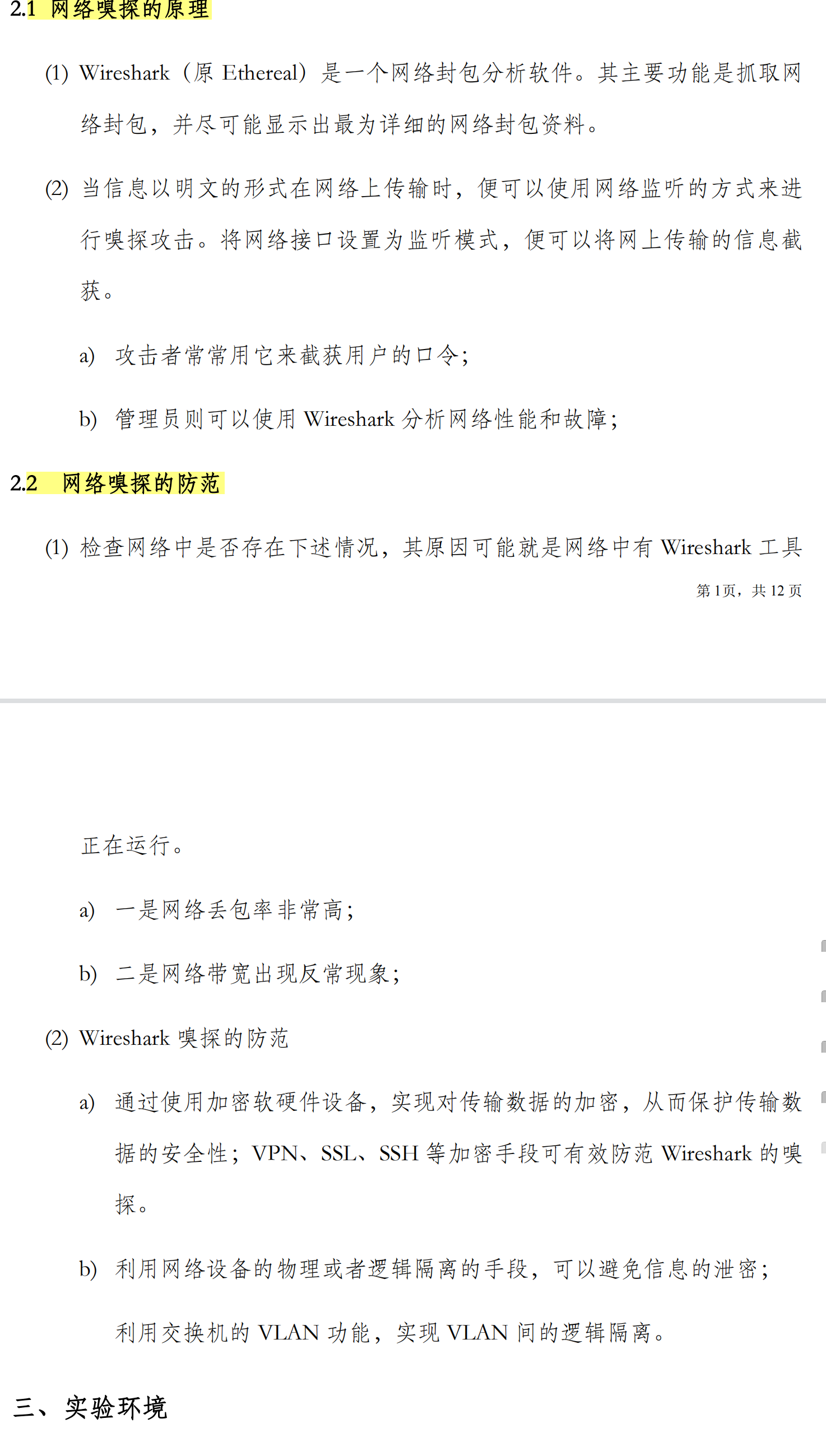
1. 802.11 (WiFi) 网络中的嗅探



1. BPF是一个核心态的组件，支持数据包“过滤”抓取，Network Tap接收所有的数据包。Kernel Buffer，保存过滤器送过来的数据包。User buffer用户态上的数据包缓冲区
2. 网络嗅探技术的具体实现机理







DHCP协议过程分析：

图形用户界面

低可信度描述已自动生成

No106：本机localhost（10.133.81.229）向DHCP server（10.133.0.1）发送了一个DHCP Release数据包，终止了ip租赁。将本机IP地址清空。

No267：本机localhost向局域网广播一个DHCP Discover包，此时本机localhost的IP地址为0.0.0.0。广播地址为255.255.255.255。本地端口为68，目的端口为67。

No277：Ipv4地址为10.133.0.1的DHCP服务器收到该包后，向本机发送一个DHCP Offer数据包。

No278：DHCP Request包由本机localhost广播，表示本机已经收到DHCP Offer包，对此事进行通告，通告的内容包括预分配给本机的IP地址，本机的MAC地址，本机的计算机名等信息。

No279：DHCP server（10.133.0.1）向本机localhost（10.133.81.229）发送了一个DHCP Ack数据包。确认IP地址，路由、DNS、IP租赁时间、子网掩码等信息。

1. Tracert命令使用IP 生存时间 (TTL)和ICMP 错误消息来确定从一个主机到网络上其他主机的路由。
2. 域名信息探测命令dig有交互式和非交互式两种模式。使用Dig命令查询邮件服务器时所使用的querytype选项是MX。域名信息探测命令：dig @dnsserver name querytype，其中参数querytype有A、AAAA、PTR、MX和ANY五种类型。
3. 用户代理(User-Agent)头字段确定用户使用的Web浏览器。
4. Nessus是一款综合型漏洞扫描工具。
5. TCP/UDP 均定义了1-65535端口范围，由ICANN负责分配。MySQL数据库默认的端口号是3306。MSSQL SERVER的默认端口号是1433。SSH的默认端口号是22。phpstudy默认的端口号为80。HTTP服务，默认的端口号为80。
6. Http状态码为404表明无法找到指定位置的资源。

## 第四章

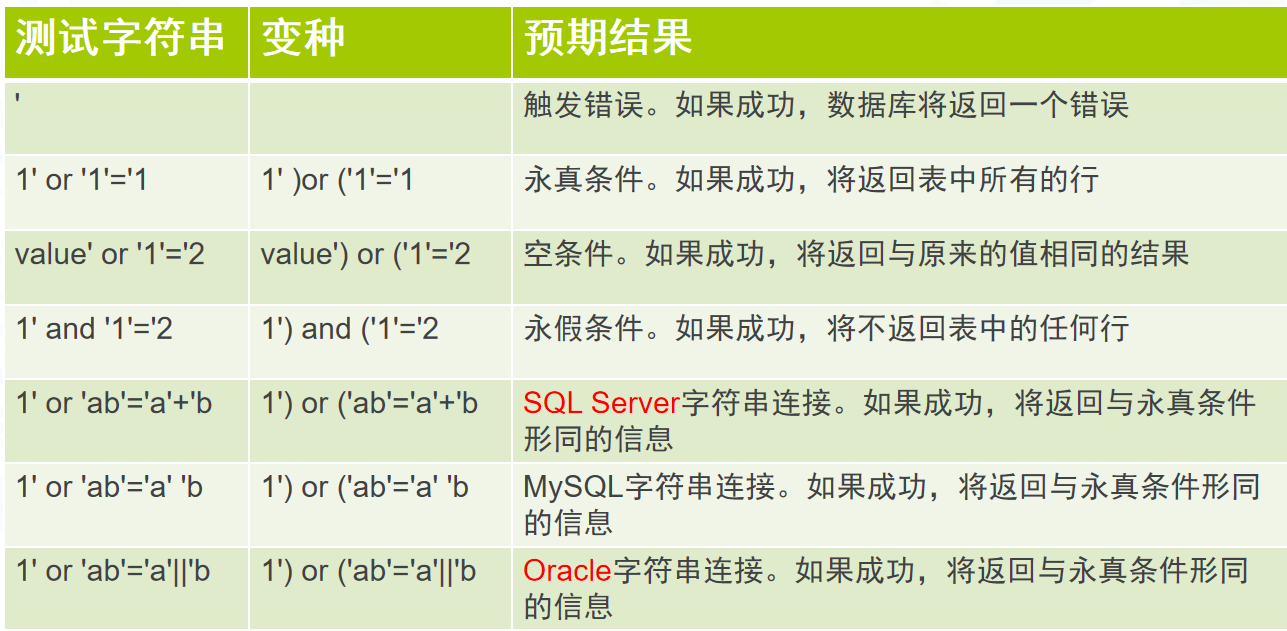
1. SQL注入的产生原因
2. 转义字符处理不当(Oracle中，空格、双竖线||、逗号、点号、\*/、双引号”都有特殊的含义)
3. 类型处理不当
4. 查询语句组装不当
5. 错误处理不当
6. 多个提交处理不当
7. 不安全的数据库配置

应该始终以普通用户身份运行服务，以便减少破坏。

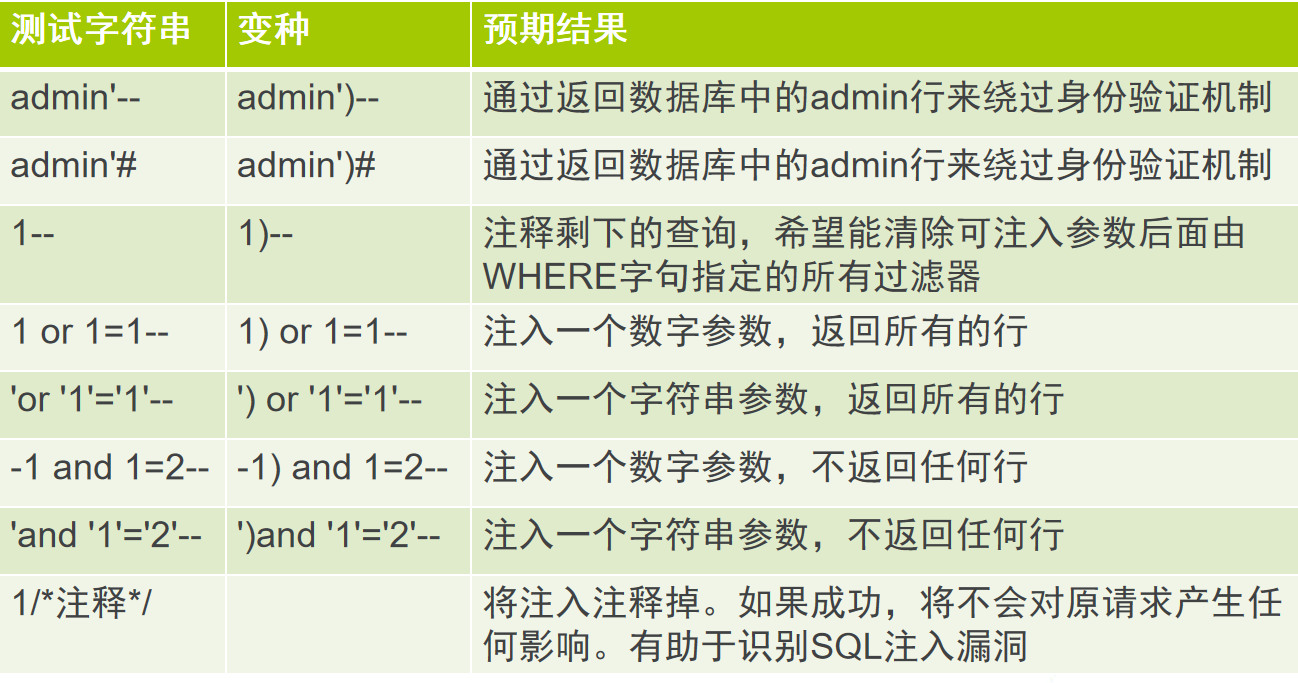
应保证程序的数据库访问在最低权限模型下运行

SQL Server可以通过INFORMATION\_SCHEMA或系统表及系统存储过程来访问元数据(数据库内部包含的数据,如数据库或表的名称、列的数据类型或访问权限)

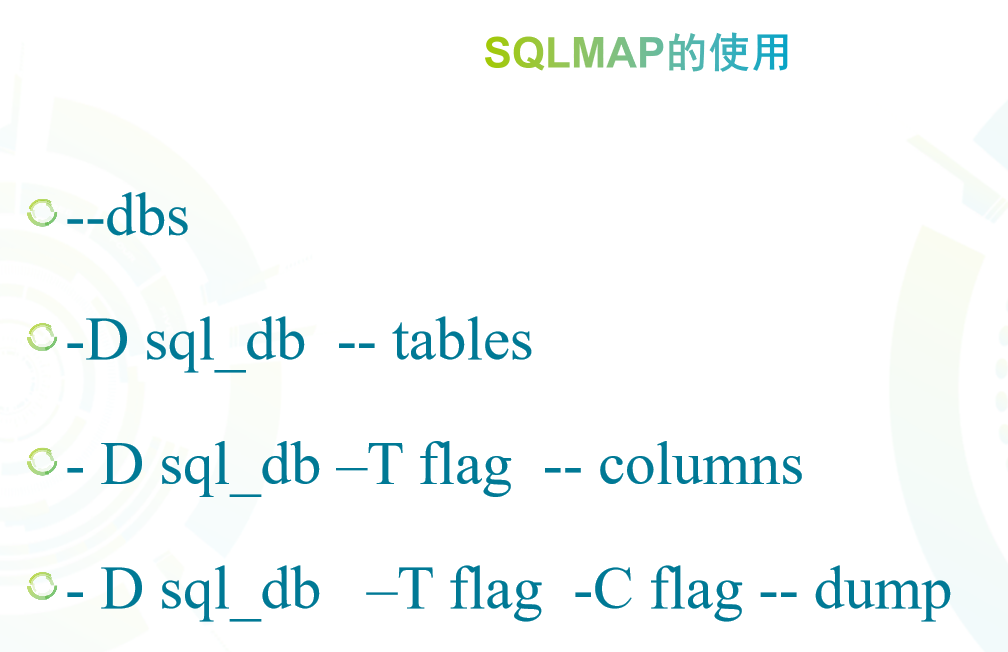
1. HTTP状态码：200,302,404,500
2. SQL语言规定，将单引号解析成代码与数据之间的分界线。
3. SQL盲注:攻击者可以操纵SQL语句，应用会针对真假条件返回不同的值。但是攻击者无法检索查询结果。
4. 万能密码:'OR 1=1 OR '1'='1
5. 数字值内联注入的特征值



1. 数据库注释时常用的特征值



1. MySQL数据库中的注释符有3种，分别是#、/\*\*/、-- 。
2. SQL Server数据库向查询引入延迟的内置命令：WAITFOR DELAY 'hours:minutes:seconds'。
3. MySQL数据库可以使用执行时间很长的函数来引入延迟。 if(left(version(),1)=5,sleep(1),1)%23
4. floor（rand（）\*2）函数返回值为0或者1。
5. UNION 操作符的作用：UNION 操作符用于合并两个或多个 SELECT 语句的结果集。
6. UNION使用要求：UNION 内部的 SELECT 语句必须拥有相同数量的列。列也必须拥有相似的数据类型。同时，每条 SELECT 语句中的列的顺序必须相同。



1. SQL注入漏洞的防范

（1）应该使用参数化语句（也称为预处理语句，PHP中使用PDO）而非动态SQL来组装SQL查询

（2）使用白名单对输入内容进行验证，确保验证应用收到的所有用户控制的输入类型、大小、范围和内容。总之，“一切用户输入都是有害的”

（3）确保对包含用户可控制输入的查询进行正确编码，以防止使用单引号或其他字符来修改查询

（4）使用防火墙、WAF、网站卫士等软硬件设备。

1. 常用数据库带有很多默认的用户预安装内容，如SQL Server使用sa作为默认的数据库系统管理员账户。
2. 为了安全起见，应保证程序的数据库访问在最低权限模型下运行。
3. SQL的时间延迟漏洞的识别。
4. 利用时间延迟进行数据库长度的猜测：攻击者可以构造and if(length(database())=100,sleep(1),1)# 语句来猜测数据库名的长度是否为100，如果检测到服务器响应时间延迟了1秒钟，则表明猜测正确，否则修改数字4为其他数字，依次猜测。

## 第五章

1. XSS是一种经常出现在Web应用程序中的计算机安全漏洞，是由于Web应用程序对用户的输入过滤不足而产生的。XSS跨站脚本攻击本身对Web服务器没有直接危害，它借助网站进行传播，使网站的大量用户受到攻击。XSS攻击可分为反射型、存储型和基于Dom的。
2. 同源是指：域名、协议、端口相同
3. 产生XSS的原因

（1）浏览器可以解析和执行JavaScript等脚本语言，但不会判断数据和代码是否恶意

（2）输入和输出是Web应用程序最基本的功能，如果没有做好安全防护，很容易出现XSS漏洞

（3）触发XSS漏洞的方式非常简单，只要向HTML代码中注入脚本即可。

1. javaScript用于设置Cookie的函数是setCookie。
2. Cookie，有时也用其复数形式Cookies，指某些网站为了辨别用户身份、进行**session跟踪而存储在用户本地终端**上的数据（通常经过加密）,它是用户和服务器之间的桥梁。
3. 同源策略，它是由Netscape提出的一个著名的安全策略。所谓同源是指：域名、协议、端口相同。
4. 文本

   描述已自动生成
5. 文本

   描述已自动生成
6. 文本

   描述已自动生成
7. CSRF攻击示例（只针对课件示例，请具体问题具体分析进行使用）：

图形用户界面, 文本

描述已自动生成

1. CSRF攻击代码示例（只针对课件示例，请具体问题具体分析进行使用）：

文本

描述已自动生成

1. 防范CSRF攻击的措施。

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

1. 上传漏洞的识别及绕过。

文本

描述已自动生成

1. MIME检测过滤的绕过：burpsuite抓包，修改content-type的值为白名单中的类型。
2. 暴力破解是一种针对密码或身份认证的破解方法，穷举各种可能，找到突破身份认证的一种攻击方法。Burpsuite 进行暴力破解时，需要把抓取到的包发送到Intruder功能页面。
3. 暴力破解的防御措施：

文本, 信件

描述已自动生成