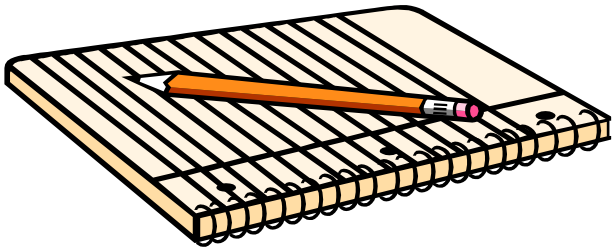
网络安全——

网络安全扫描

北京邮电大学
郑康锋
zkfbupt@163.com

本次课程内容（网络安全扫描）



- 网络安全扫描概述
- 网络安全扫描技术
- 网络协议安全
- 安全漏洞概述
- 安全漏洞发现与防御

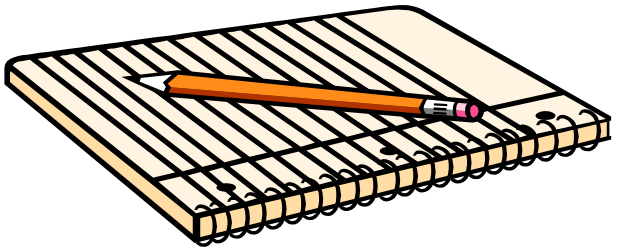
何为网络安全扫描

- 总体认识：是指对计算机网络系统进行相关的安全检测，进而找出安全隐患和漏洞，客观评估网络风险等级，有效地避免非法入侵行为，做到防患于未然。
- 主要功能：发现主机或网络、发现正在运行的服务进而发现潜在的漏洞、能够为漏洞提出解决方案。
- 主要分类：PING扫射（Ping Sweep）、操作系统探测（Operating System Identification）、如何探测访问控制规则（Firewalking）、端口扫描（Port Scan）、漏洞扫描（Vulnerability Scan）等。
- 不是攻击网络漏洞，而是发现网络漏洞

为何需要网络安全扫描

- 先下手为强，主动出击
  - 入侵检测技术、防火墙技术、病毒检测技术都是在攻击进行中或进行后的被动检测
  - 网络安全扫描技术则是在攻击进行前的主动检测，在黑客攻击之前做好安全防护
- 强强联合，坚不可摧
  - 网络安全扫描与防火墙、网络监控系统互相配合，能够有效提高网络的安全性
  - 根据扫描的结果更正网络安全漏洞和系统中的错误配置，使防火墙、网络监控系统更有效工作，系统更加坚固

本次课程内容（网络安全扫描）



- 网络安全扫描概述
- 网络安全扫描技术
- 网络协议安全
- 安全漏洞概述
- 安全漏洞发现与防御

网络安全扫描简介

- 网络安全扫描技术是一类重要的网络安全技术，基于Internet远程检测目标网络或本地主机安全性脆弱点

- 通过对网络的扫描，系统管理员能够发现所维护的Web服务器的各种TCP/IP端口的分配、开放的服务、Web服务软件版本和这些服务及软件呈现在Internet上的安全漏洞

- 网络安全扫描技术利用了一系列的脚本模拟对系统进行攻击的行为，并对结果进行分析

网络安全扫描步骤

- 发现目标主机或网络
- 发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。
  - ➔ 如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息
  - 根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞

发现目标

- 这一阶段就是通过发送不同类型的ICMP或者TCP、UDP请求，从多个方面检测目标主机是否存活。在这一阶段使用的技术通常称作ping扫射（Ping Sweep），包括：
  - ICMP扫射
  - 广播ICMP
  - 非回显ICMP
  - TCP扫射
  - UDP扫射

发现目标

名称	方法	优点	缺点
ICMP扫射	使用ICMP回显请求轮询目标主机	使用简单	速度较慢；如果目标关闭了对ICMP回显请求的响应，就不能被发现
广播ICMP	发送ICMP回显请求到目标网络的网络地址或广播地址	使用简单；速度比ICMP扫射快	不能发现Windows主机；如果目标关闭了对ICMP回显请求的响应，就不能被发现；可能造成扫描着的DoS
非回显ICMP	发送其它类型的ICMP报文到目标主机	不受目标阻止ICMP回显请求的影响	根据RFC的规定和不同操作系统的具体实现，某些类型的ICMP请求在探测目标是会受到限制
TCP扫射	发送TCP SYN或TCP ACK到目标主机	最有效的目标发现方法	对入侵者而言，防火墙可能影响这种方法的可靠性
UDP扫射	发送UDP数据报到目标网络广播地址或主机	不受目标阻止ICMP回显请求的影响；可以发送到目标网络广播地址	可靠性低；对于非Windows的目标主机，速度慢

攫取信息

- 在找出网络上存活的系统后，下一步就是要得到目标主机的操作系统和开放的服务信息。用到的技术主要有：
  - 端口扫描
  - 服务识别
  - 操作系统探测

端口扫描

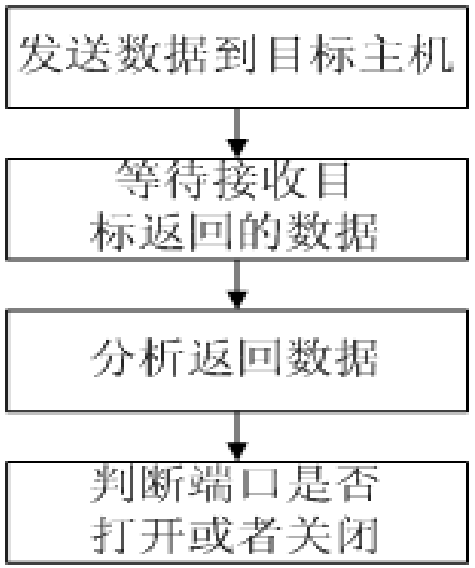
- 端口扫描就是要取得目标主机开放的端口和服务信息，从而为下一步的“漏洞检测”做准备。
- 根据RFC1700规定的已分配端口，网络服务和端口一一对应，常用的协议和端口对应值为：

21和20/tcp	FTP
53/udp	DNS
23/tcp	Telnet
25/tcp	SMTP
80/tcp	HTTP
110/tcp	POP3

进行端口扫描，就可以快速获得目标主机开设的服务。

端口扫描

- 端口扫描是最基本的网络安全扫描技术，它的基本流程为：



在这个流程中，发送数据是最重要的，而数据的产生主要是根据各种不同的网络协议而构造的。

服务识别

- 前面提到，端口扫描的主要目的是为了获取目标主机提供的服务，而通常获取服务类型的办法就是根据RFC1700直接推断的。
- 但是，仅凭端口号来判断服务类型还是不够的，对于非标准端口服务的识别需要更多的信息。如：
  - Web服务不一定开设在80/tcp端口
  - 非标准端口服务，端口号采用动态分配方法，如冰河开设的端口为7626

操作系统探测

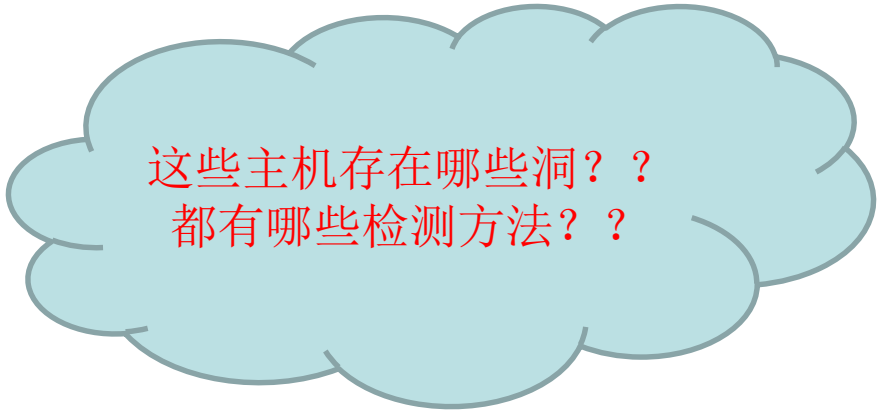
- 为何：许多安全漏洞都是和操作系统紧密相关的，只有精确地判别出目标主机的操作系统类型及版本，才能有针对地对其进行攻击或安全评估
- 可能：每个操作系统通常都有自己的IP栈实现；TCP/IP规范并不是被严格地执行，每个不同的实现将会拥有自己的特性；规范中一些选择性的特性可能在某些系统中使用，而在其他的一些系统中则没有使用；某些系统私自对IP协议做了改进
- 技术：主动探测技术；被动探测技术

操作系统探测

- 主动探测是指主动地、有目的地向目标发送探测数据包，通过提取和分析响应数据包的特征信息，对目标的操作系统类型进行识别
  - 标识攫取
  - 网络协议栈特征探测
- 被动探测是指通过网络监听等手段，从截获的数据中提取目标的操作系统类型信息
  - 基于TCP/IP协议栈的被动指纹探测技术
  - 基于应用层协议的被动探测技术

漏洞检测

- 经过发现目标和攫取信息两个步骤后，可以得到以下信息：
  - 目标网络上有哪些主机处于存活状态
  - 这些主机上都运行什么系统
  - 这些主机运行了哪些网络服务



漏洞检测方法-直接测试

- 使用针对漏洞特点设计的脚本或程序检测漏洞
- 特点：
  - 通常用于对Web服务器漏洞、拒绝服务（DoS）漏洞进行检测
  - 能够准确地判断系统是否存在特定漏洞
  - 攻击性强，可能对存在漏洞的系统造成破坏
  - 对于DoS漏洞，会造成系统崩溃
  - 不是所有漏洞的信息都能通过这种方法获得

漏洞检测方法-推断

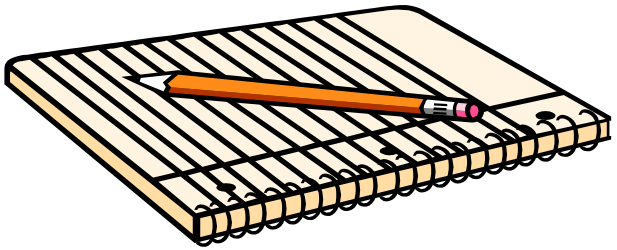
- 推断是指不利用系统漏洞而判断漏洞存在的方法，它并不直接渗透漏洞，只是间接寻找漏洞存在的证据。
- 检测手段：
  - 版本检查
  - 程序行为分析
  - 操作系统堆栈指纹分析
  - 时序分析

优点	攻击性小、对计算机和网络的要求低，快速检查大量目标时很有用
缺点	可靠性低

漏洞检测方法-带凭证的测试

- 凭证是指访问服务所需的用户名或者密码，包括UNIX的登录权限和从网络调用Windows NT的API的能力
- 很多攻击都是由拥有UNIX Shell访问权限或者NT资源访问权限的用户发起的
- 他们的目标在于将自己的权限提升成为超级用户，从而可以执行某个命令
- 对于这样的漏洞，前面两种方法很难检查出来
- 如果赋予测试进程目标系统的角色，将能够检查出更多的漏洞，这种方法就是带凭证的测试

本次课程内容（网络安全扫描）



- 网络安全扫描概述
- 网络安全扫描技术
- 网络协议安全
- 安全漏洞概述
- 安全漏洞发现与防御

网络安全扫描技术

- 网络安全扫描技术包括：
  - 端口扫描
  - 漏洞扫描
  - 操作系统探测
  - 如何探测访问控制规则
  - PING扫射

端口扫描技术和漏洞扫描技术是两种核心技术，广泛应用于当前较成熟的网络扫描器中，如著名的Nmap和Nessus

端口扫描技术

- 端口扫描技术是一项自动探测本地和远程系统端口开放情况的策略及方法，它使系统用户了解系统目前向外界提供了哪些服务，从而为系统用户管理网络提供了一种手段。
- 原理：向目标主机的TCP/IP服务端口发送探测数据包，并记录目标主机的响应，通过分析响应来判断服务端口是打开还是关闭，即可得知端口提供的服务或信息。也可以通过捕获本地主机或服务器流入流出IP数据包来监视本地主机的运行情况，通过对接收到的数据进行分析，帮助我们发现目标主机的某些内在的弱点。
- 分类：全连接扫描、半连接扫描、秘密扫描

端口扫描技术-全连接扫描

- 全连接扫描技术是TCP端口扫描的基础，包括：
  - TCP connect()扫描

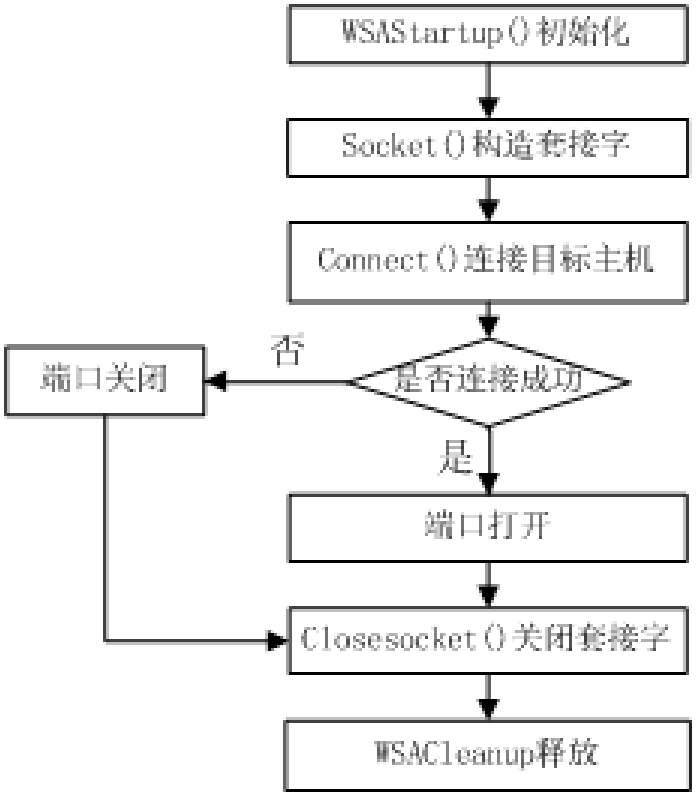
利用操作系统提供的connect()系统调用，与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态，那么connect()就能成功；否则，该端口是不能用的，即没有提供服务。

  - TCP反向ident扫描

ident协议允许（RFC1413）看到通过TCP连接的任何进程的拥有者的用户名，即使这个连接不是由这个进程开始的。

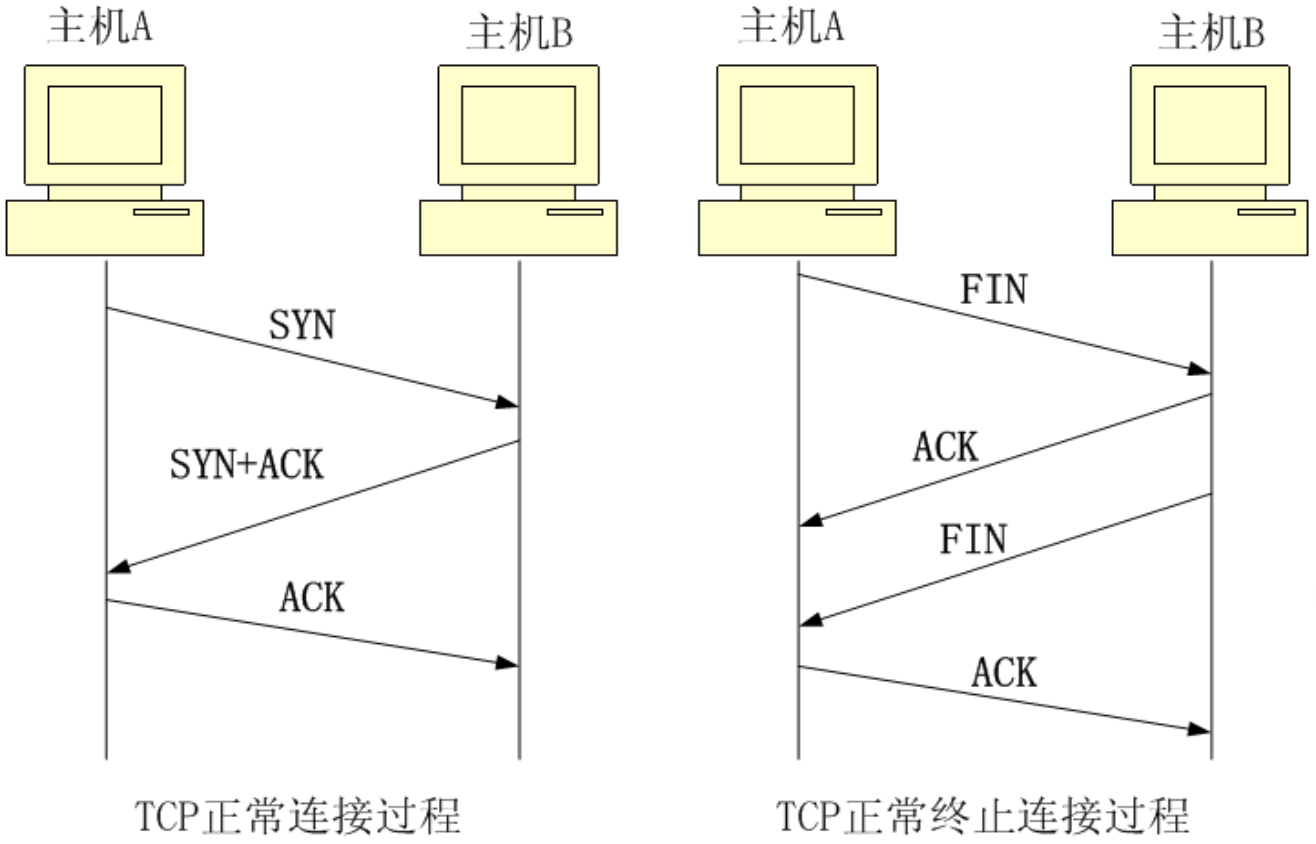
TCP connect()扫描

- TCP连接扫描利用了TCP协议的正常连接过程，其流程为：



TCP connect()扫描

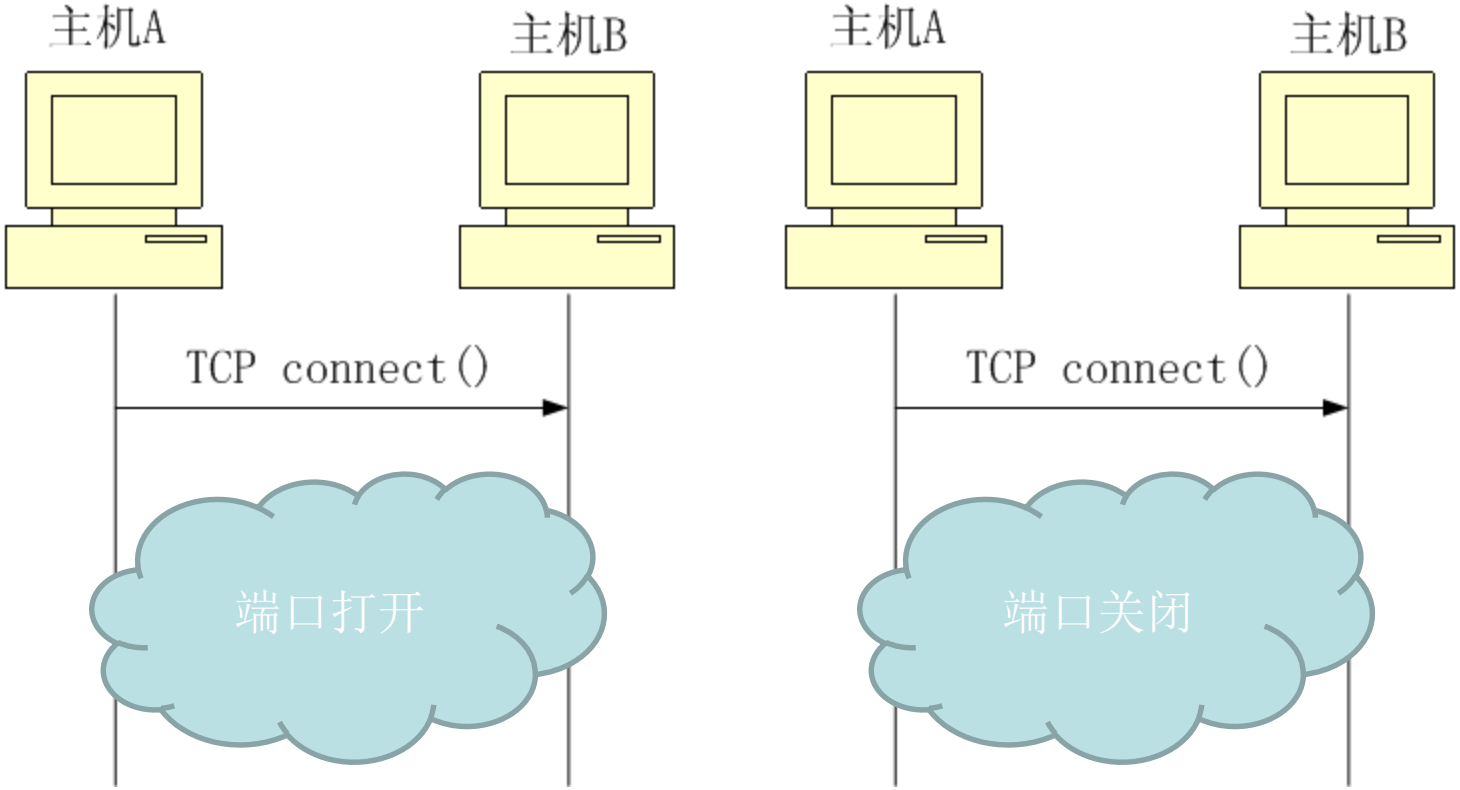
- 正常的TCP连接与终止连接过程为：



TCP正常连接过程　　TCP正常终止连接过程

TCP connect()扫描

- 基于TCP连接的扫描过程为：



TCP connect()扫描

- 优点
  - 扫描迅速
  - 准确而且不需要任何权限，系统中的任何用户可以使用这个调用
  - 可以同时打开多个套接字，加速扫描，使用非阻塞I/O还允许设置一个低的时间用尽周期，同时观察多个套接字
- 缺点
  - 扫描方式不隐蔽，服务器日志会记录下大量密集的连接和错误记录
  - 易被目标主机防火墙发觉而被过滤掉

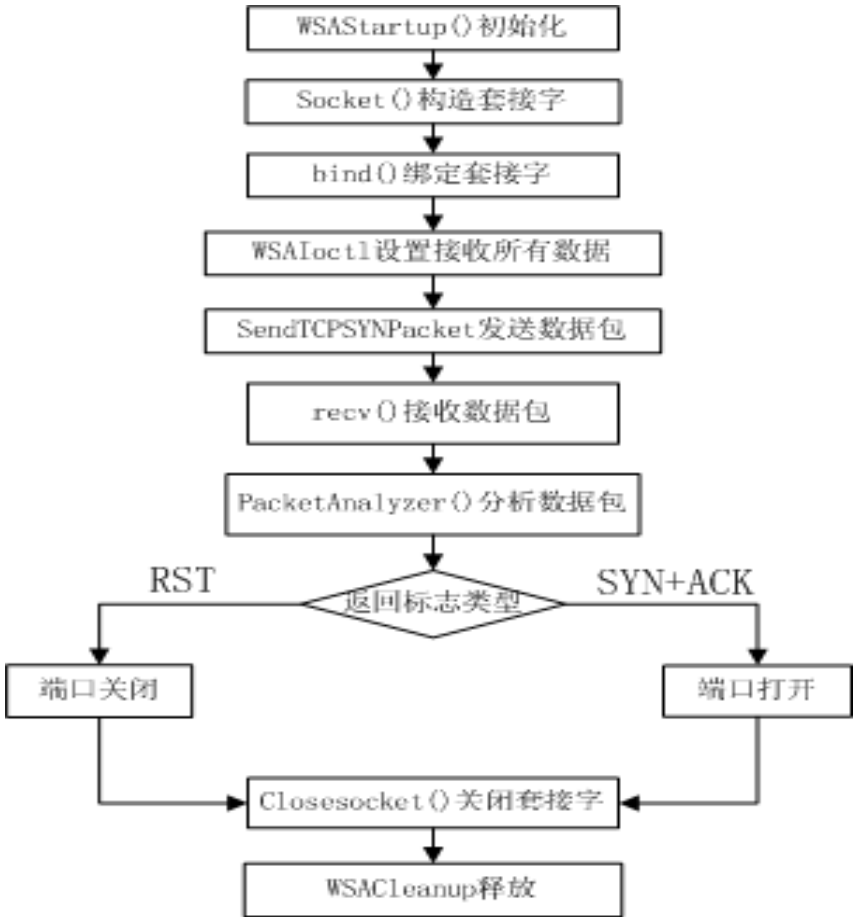
端口扫描技术-半连接扫描

- 也叫间接扫描，是指端口扫描没有完成一个完整的TCP连接，在扫描主机和目标主机的一指定端口建立连接时只完成了前两次握手，在第3步时扫描主机中断了本次连接，使连接没有完全建立起来。现有的半连接包括：
  - TCP SYN扫描

    向目标特定端口发送一个SYN报文，根据目标主机返回的数据包，只要辨别报文中是含有SYN+ACK标志还是RST标志，就能够知道目标的相应端口是处于监听还是关闭状态。
  - IP ID头dumb扫描

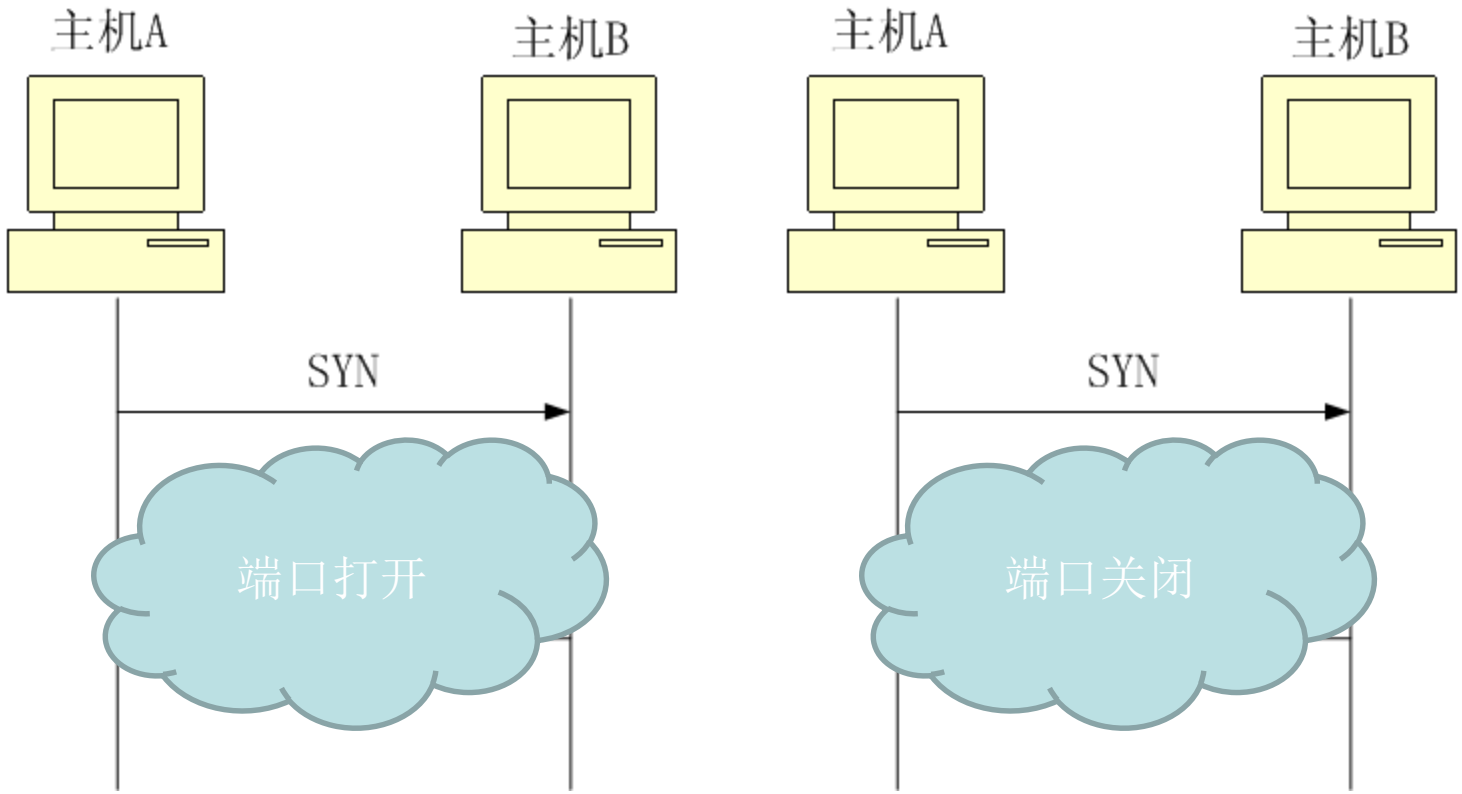
TCP SYN扫描

- TCP SYN扫描应用非常广泛，其流程为：



TCP SYN扫描

- 基于TCP SYN的扫描过程为：



TCP SYN扫描

- 优点
  - 扫描迅速快，效率高
  - 一般不会在目标计算机上留下记录，比较隐蔽
- 缺点
  - 在大部分操作系统下，扫描主机需要构造适合于这种扫描的包，而通常情况下，必须要有root权限才能建立自己的SYN数据包

端口扫描技术-秘密扫描

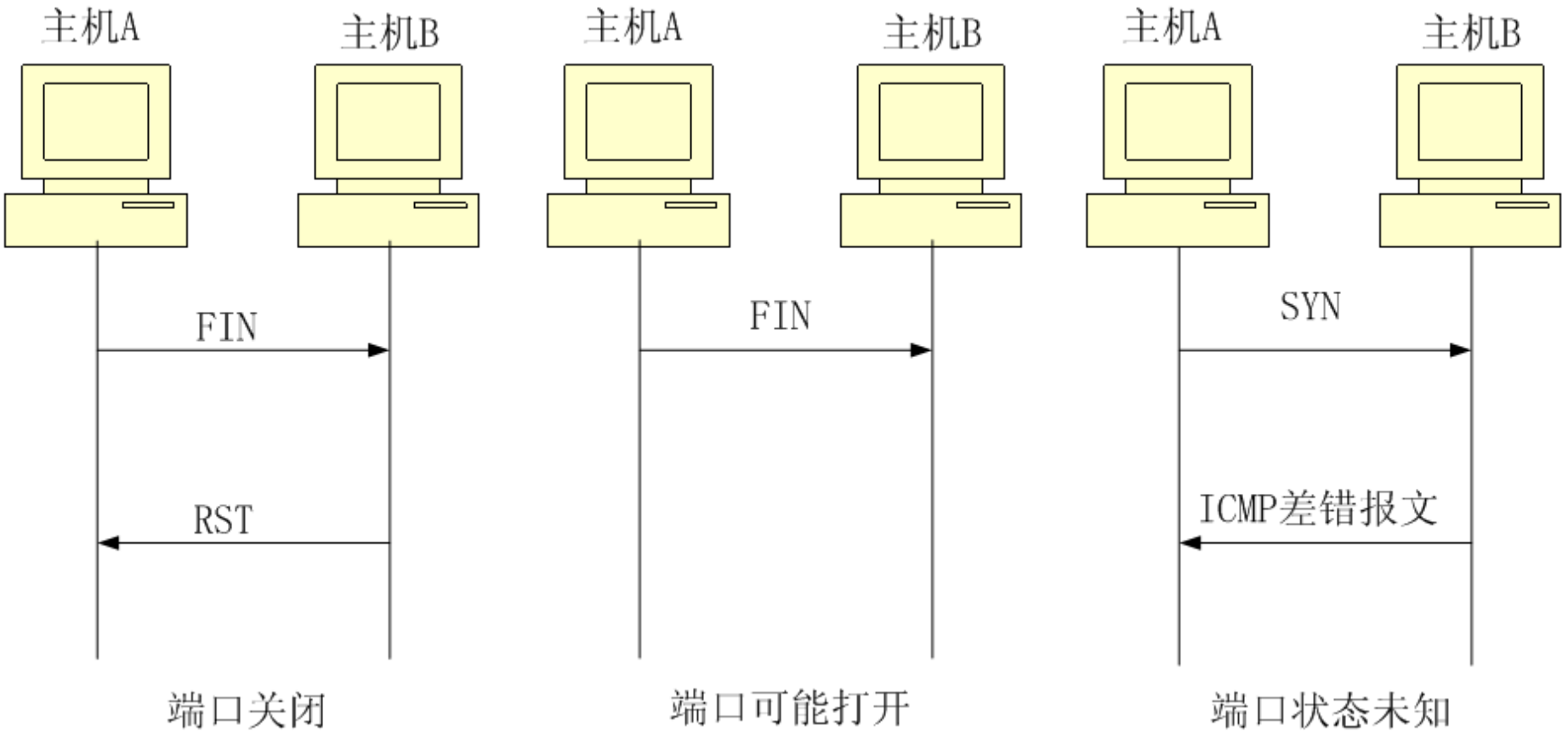
- 端口扫描容易被在端口处所监听的服务日志记录，这些服务看到一个没有任何数据的连接进入端口，就记录一个日志错误
- 秘密扫描是一种不被审计工具所检测的扫描技术，现有的秘密扫描主要有：
  - TCP FIN扫描
  - TCP ACK扫描
  - TCP NULL扫描
  - TCP XMAS扫描
  - TCP分段扫描

TCP FIN扫描

- SYN有可能都不够秘密，一些防火墙和包过滤器会对一些指定的端口进行监视，有的程序能检测到这些扫描
- FIN数据包可能会没有任何麻烦的通过，因为这种技术不包含标准的TCP三次握手协议的任何部分
- 原理
  - 关闭的端口会用适当的RST来回复FIN数据包，打开的端口会忽略对FIN数据包的回复

TCP FIN扫描

- TCP FIN扫描使用的是FIN标志，扫描过程为：



TCP FIN扫描

缺点

1.这种方法和系统的实现有一定的关系。有的系统（特别是Windows系统），无论端口是打开还是关闭都会响应一个RST报文，所以FIN扫描通常只工作在基于UNIX的TCP/IP协议栈上

2.需要自己构造数据包，要求由超级用户或者授权用户访问专门的系统调用

TCP ACK扫描

- TCP ACK扫描利用的是标志位ACK，但不是用于确定目标打开了哪些端口，而是用来
  - 扫描防火墙的配置
  - 发现防火墙规则
  - 确定它们是有状态还是无状态的
  - 确定哪些端口是被过滤的
  - 确定防火墙是简单的包过滤还是状态检测机制

TCP NULL和TCP XMAS扫描

- TCP NULL扫描和TCP XMAS扫描是FIN扫描的两个变种
- 原理
  - NULL扫描向目标发送一个所有标志位都置为0的报文，而 XMAS扫描则向目标发送一个URG/PSH/FIN报文，根据RFC793规定，如果目标的相应端口是关闭的话，应该会收到一个RST数据包，否则就不会收到来自目标的任何回应。
- 优点
  - 隐蔽性好
- 缺点
  - 需要自己构造数据包，要求有超级用户或者授权用户权限
  - 通常适用于UNIX目标主机，而Windows系统不支持

TCP 分段扫描

- 原理
  - 并不直接发送TCP探测数据包，而是将数据包分成两个较小的IP段，这样就将一个TCP头分成好几个数据包，从而包过滤器很难探测到
- 优点
  - 隐蔽性好，可穿越防火墙
- 缺点
  - 需要可能被丢弃
  - 某些程序在处理这些小数据包时会出现异常

端口扫描技术-其它扫描

- FTP反弹扫描
- UDP ICMP端口不可到达扫描

FTP反弹扫描

- 原理
  - 利用FTP协议支持代理FTP连接的特点，可以通过一个代理的FTP服务器来扫描TCP端口，即能在防火墙后连接一个FTP服务器，然后扫描端口
- 优点
  - 难以跟踪，可穿越防火墙
- 缺点
  - 速度很慢
  - 有的FTP服务器会关闭代理功能

UDP ICMP端口不可到达扫描

- 扫描主机发送UDP数据包给目标主机的UDP端口，等待目标端口的端口不可到达的ICMP信息
  - 若这个ICMP信息及时收到，则表明目标端口处于关闭状态
  - 若超时也未能接收到端口不可到达ICMP信息，则表明目标端口可能处于监听状态

漏洞扫描技术

- 漏洞扫描技术是建立在端口扫描技术的基础上的
- 漏洞扫描技术主要是基于以下两种方法：
  - 在端口扫描后得知目标主机开启的端口情况以及端口上的服务，将这些相关信息与网络漏洞扫描系统的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在
  - 通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等；若模拟攻击成功，则表明目标主机系统存在安全漏洞

漏洞扫描技术

- 漏洞扫描技术主要分为以下两种：
  - 基于网络系统漏洞库的漏洞扫描

这类漏洞扫描大致包括：CGI漏洞扫描、POP3漏洞扫描、FTP漏洞扫描、HTTP漏洞扫描等。

这些漏洞扫描基于漏洞库，将扫描结果与漏洞库相关数据比较得到漏洞信息。

  - 基于模拟攻击的漏洞扫描

主要包括：Unicode遍历目录漏洞探测、FTP弱势密码探测、OPENreply邮件转发漏洞探测等。

这些扫描通过使用插件（功能模块技术）进行模拟攻击，测试出目标主机的漏洞信息。

漏洞扫描技术

- 漏洞库的匹配方法

通过采用基于规则的匹配技术，即根据安全专家对网络系统安全漏洞、黑客攻击案例的分析和系统管理员对网络系统安全配置的实际经验，可以形成一套标准的网络系统漏洞库，然后在此基础上构成相应的匹配规则，由扫描程序自动进行漏洞扫描工作。

- 插件（功能模块）技术

插件是由脚本语言编写的子程序，扫描程序可以通过调用它来执行漏洞扫描，检测出系统中存在的一个或多个漏洞。添加新的插件就可以使漏洞扫描软件增加新的功能，扫描出更多的漏洞。

漏洞扫描举例

- 这里假设已知目标主机操作系统为Windows XP Professional SP2，先对目标主机进行端口扫描（利用漏洞对应的端口号为445）：

```
Target IP:172.16.0.147
Port   440 Close
Port   441 Close
Port   442 Close
Port   443 Open
Port   444 Close
Port   445 Open
Port   446 Close
Port   447 Close
Port   448 Close
Port   449 Close
Port   450 Close

time: 9125ms
```

- 可以看到445端口是开放的，所以初步断定目标存在此漏洞

漏洞扫描举例

- 然后，再模拟黑客攻击的手法对目标系统进行攻击（这里为直接让系统关机，倒计时为9秒），进一步验证漏洞的存在性，效果如下（实验环境为虚拟机）：

- 可以看到目标主机确实倒计时关机，所以几乎可以肯定目标主机确实存在该漏洞

操作系统探测技术

- 主动探测
  - 标识攫取
  - 网络协议栈特征探测
- 被动探测
  - 基于TCP/IP协议栈的被动指纹探测技术
  - 基于应用层协议的被动探测技术

主动探测-标识攫取

- 标识攫取探测法是指用户通过客户端程序访问服务器，在和服务器正常的交互过程中根据服务器返回的提示或一些正常的操作来判别操作系统类型

- 从目标主机上得到一个二进制可执行文件，再对它进行分析，也可以得到操作系统的某些信息

主动探测-标识攫取

- 优点
  - 大多数情况下，操作系统的多种服务都会暴露其“身份”，例如Telnet、WWW、FTP、SMTP等
  - 实现起来特别简单
  - 由于是通过正常的交互过程来获取信息的，因此不会受到防火墙的干扰及被IDS系统察觉
- 缺点
  - 通常以手工的方式进行，因此效率较低
  - 有可能被网络管理员通过修改或关闭提示信息所蒙蔽
  - 目标机器有可能并不提供有标识信息的服务

主动探测-网络协议栈特征探测

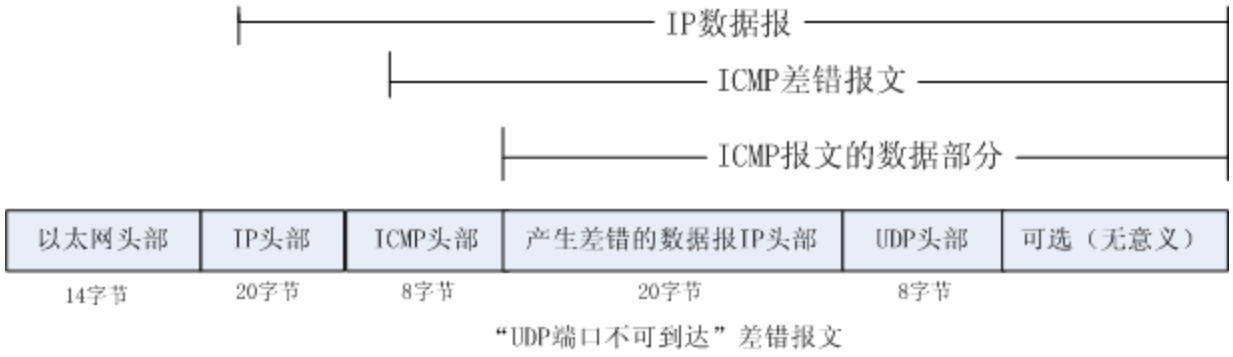
- ICMP 报文响应分析
  - 这种方法向目标发送UDP或ICMP报文，然后分析目标响应的ICMP报文的内容，根据不同的响应特征来判断操作系统
- TCP 报文响应分析
  - 这种技术就是通过区分不同操作系统对特定TCP报文（标准或非标准）的不同反应，实现对操作系统的区分，典型代表：Queso和Nmap
- TCP 报文延时分析
  - 这种方法的具体实现是在“3次握手”的过程中放弃对远程主机SYN/ACK报文的确认，迫使其重传，通过测量重传TCP报文之间的延时序列，获取远程操作系统指纹

ICMP报文响应分析

- ICMP数据报是封装在IP数据报之内的，这种方法就是利用了IP头部的字段内容，包括服务类型TOS、总长度、标识、DF位、生存期TTL、检验和等字段。具体技术有：
  - ICMP差错报文引用大小
  - ICMP差错报文回显完整性
  - ICMP差错报文的“优先权”字段
  - ICMP差错报文IP头部的不分片（DF）位
  - ICMP报文IP头部的TTL字段
  - 使用代码字段不为0的ICMP回显请求
  - TOS子字段回显

ICMP差错报文引用大小

- ICMP差错报文必须包括生成该差错报文的数据报IP头部（包括任何选项），还必须至少包括跟在该IP头部后面的前8个字节
- 大多数操作系统都只返回产生差错的数据报的IP头部后的前8个字节，然而有一些操作系统在这8个字节之后还返回更多的字节，包括Linux（内核2.0.x/2.2.x/2.4.x）、SUN Solaris、HPUX 11.x、MacOS 7.55/8.x/9.04、Nokia系统、Foundry交换机和其他一些操作系统或者网络设备



“UDP端口不可到达”差错报文

ICMP差错报文回显完整性

- 一般而言，在发送ICMP差错报文时，差错报文的数据部分，只有产生差错的数据报IP头部的TTL字段和IP头部检验和字段会与初始报文不同

- 然而，有些操作系统会改变产生差错的数据报IP头部的其它字段的内容和/或后面数据的内容

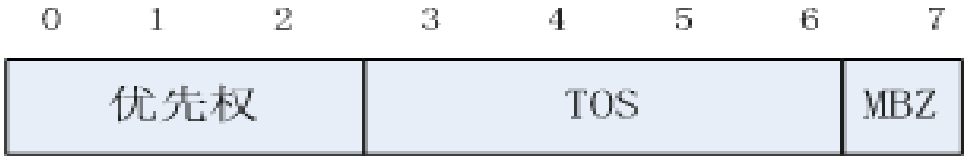
- 如果用UDP数据报产生的端口不可到达差错报文来进行分析，可以利用的特点包括：

ICMP差错报文回显完整性

IP数据报总长度	AIX4.x和BSDI4.1等操作系统的IP栈会将产生差错的数据报IP头部的总长度字段加上20，而另一些操作系统会减少20，更多的系统会保持不变
IP数据报标识（IPID）	FreeBSD4.0、OpenVMS和ULTRIX等系统的IP栈不能正确回显产生差错数据报的IPID，其它更多的系统则能够正确回显
分段标志（3位）和片偏移	一些系统会改变产生差错的数据报头部中3位分段标志和片偏移字段的位顺序，另一些系统只能正确回显
IP头部校验和	FreeBSD4.0、OpenVMS和ULTRIX等系统会将产生差错的数据报IP头部的校验和字段置为0，而大多数的系统只是将重新计算的校验和回显
UDP头部校验和	FreeBSD4.0/4.11、Compaq Tru64、DG-UX5.6、AIX4.3/4.2.1、ULTRIX和OpenVMS等系统会将差错报文中的UDP头部的校验和字段置为0，另外的系统则保持不变

ICMP差错报文的“优先权”字段

- IP头部中有一个8位的TOS字段，TOS字段包括一个3位的优先权字段、4位的TOS子字段和一位必须置0的未用位
- 除了Linux，其它的所有操作系统都将0作为ICMP差错报文的优先权值，而Linux使用6作为ICMP差错报文的优先权值（即使用0xC0作为IP头部TOS字节的值）



IP头部的TOS字段

ICMP差错报文IP头部的不分片（DF）位

- 有些操作系统在发送ICMP差错报文时，会根据引起差错的数据报的IP头部的DF位来设置差错报文本身IP头部的DF位

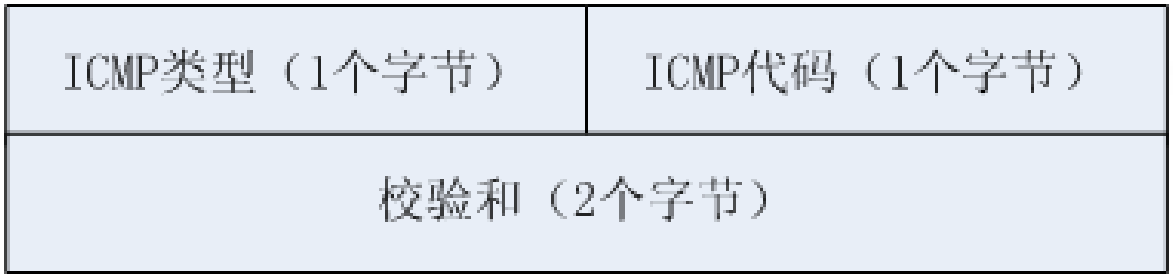
- Linux、ULTRIX、Novell Netware、HPUX、Windows98/98SE/ME、Windows NT4 Server SP6、Windows 2000 Family等系统则不会这么做

ICMP差错报文IP头部的TTL字段

- 不同的操作系统在设置ICMP报文IP头部的TTL字段时有不同的默认值；而且一般来讲，ICMP应答报文和ICMP查询报文的TTL还不一样。
  - Windows 95应答报文和查询报文的TTL都是32
  - Windows 98/98SE/ME/NT4应答报文的TTL是128、查询报文的TTL是32
  - Windows 2000应答报文和查询报文的TTL都是128

使用代码字段不为0的ICMP回显请求

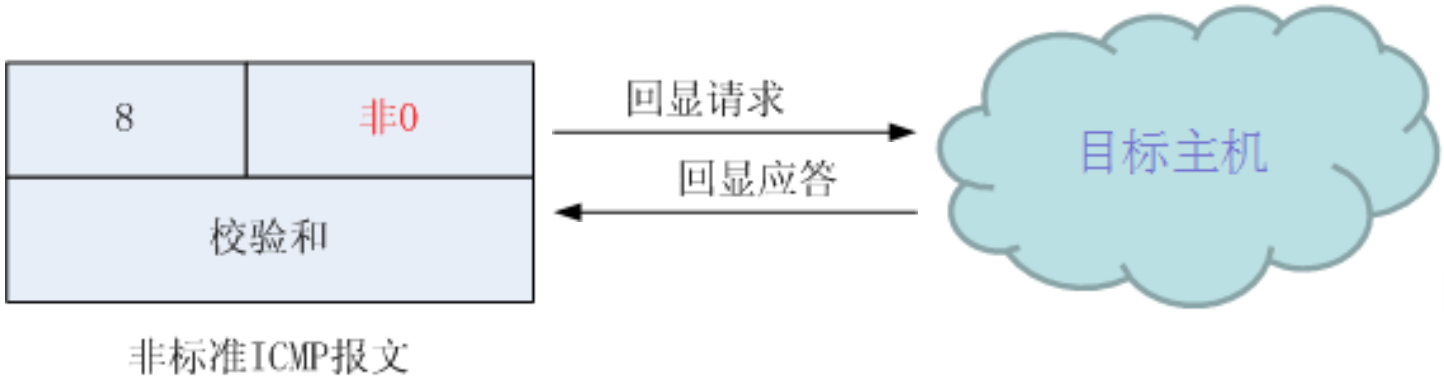
- ICMP报文的种类由第一个字节（类型字段）和第二个字节（代码字段）决定
- 回显请求的类型字段为8，默认的代码字段为0
- 如果把回显请求的代码字段设置为非0值，这样的回显请求就不是标准的ICMP报文
- 对于非标准的回显请求报文，不同类型的系统作出的回显应答的代码字段值不同



ICMP首部

使用代码字段不为0的ICMP回显请求

- Windows操作系统作出的回显应答（类型为0）的代码字段值为0
- 其它系统和网络设备作出的回显应答的代码字段值和它收到的回显请求中的代码字段值相同



非标准ICMP报文

TOS子字段回显

- RFC1349定义了ICMP报文使用TOS子字段的方法
  - 差错报文总是使用默认值0
  - 查询报文可以在TOS子字段中使用任何值
  - 应答报文应该在TOS子字段中使用造成应答报文的查询报文中使用的TOS值
- 有些操作系统（如Linux）在发送回显应答报文时忽略了这项规定
  - 无论查询报文使用何种TOS值，它的应答报文的TOS值都是一样

TCP报文响应分析

- 这种技术就是通过区分不同操作系统对特定TCP报文（标准或非标准）的不同反应，实现对操作系统的区分，典型代表：Queso和Nmap。探测技巧有：
  - FIN探测
  - 伪标记位探测
  - TCP ISN取样
  - DF位监视
  - TCP初始化窗口大小
  - ACK值
  - 片段处理
  - TCP选项

FIN探测和伪标记位探测

- 端口扫描时曾提到，“FIN扫描通常只工作在基于UNIX的TCP/IP协议栈上”，这就可以作为一个探测操作系统类型的判断依据

- TCP报文的头部有8个标志位，使用“伪标记位”（把SYN报文的CWR标记位的左边一位置为1），则低于2.0.35版本的Linux内核会在回应包中保持这个标记，而其他操作系统则没有这个问题

TCP ISN取样

- 原理：
  - 在操作系统对连接请求的回应中寻找TCP连接初始化序列号（ISN）的特征
- 目前可以区分的类别：
  - 传统的64000方式：旧UNIX
  - 随机增加方式：新版本的Solaris、IRIX、FreeBSD、Digital UNIX、Cray等
  - 真“随机”方式：Linux 2.0.x及更高版本、OpenVMS和新版本的AIX等
  - 基于时间方式：Windows平台和其他一些平台
  - 固定的ISN：某些3Com集线器、Apple LaserWriter打印机

DF位监视和TCP初始化窗口大小

- 许多操作系统在逐渐在它们发送的IP数据报中设置DF位，但并不是所有操作系统都进行这种设置。

- 有的操作系统总是使用比较特殊值的初始化TCP窗口大小
  - AIX是惟一使用0x3F25窗口值的操作系统
  - OpenBSD、FreeBSD、Windows 2000/XP使用的窗口值总是0x402E

ACK值

- 不同协议栈实现在TCP报文的ACK值的选择上存在差异
- 向一个关闭的TCP端口发送一个FIN/PSH/URG报文，许多操作系统会将ACK值设置为ISN值，但Windows和某些打印机会设置为接收到的报文的SEQ+1
- 向一个打开的端口发送SYN/FIN/URG/PSH报文，Windows的返回值就会非常不确定，有时是接收到的报文的SEQ，有时是SEQ++，而有时似乎是很随机的数值

片段处理

- 不同操作系统在处理IP片段重叠时采用了不同的方式
  - 有些用新的内容覆盖旧的内容
  - 有些是以旧的内容为优先

- 有很多探测方法能确定这些包是如何重组的，从而能确定操作系统类型

TCP选项

- 这是搜集信息的最有效方法之一，因为：
  - TCP提供了很多的选项，它们通常是“可选的”，并不是所有的操作系统都使用这些选项
  - 向目标主机发送带有可选项标记的数据包时，如果操作系统支持这些选项，会在返回包中也设置这些标记
  - 可以一次在数据包中设置多个可选项，从而增加探测的准确度
- 通过探测各种操作系统对各种选项的反应，可以搜集很多有效的信息

TCP报文延时分析

- 这是利用了TCP报文重传的特性
- 这种方法的具体实现是在“3次握手”的过程中放弃对远程主机SYN/ACK报文的确认，迫使其重传，通过测量重传TCP报文之间的延时序列，获取远程操作系统指纹
- 优点：只需一个打开的端口；使用了一个标准的TCP数据报，不会对目标主机造成任何的不利影响
- 缺点：需要时间较长

被动探测

- 这种方法不主动向目标系统发送数据包，而是通过网络监听等手段，嗅探目标网络的通信，从截获的数据中提取目标的操作系统类型信息，构成目标系统的指纹。
- 常用技术有：
  - 基于TCP/IP协议栈的被动指纹探测技术
  - 基于应用层协议的被动探测技术

基于TCP/IP协议栈的被动指纹探测技术

- 这种技术主要通过4个方面的因素来判断远程主机的操作系统：
  - TTL是IP首部中的生存时间字段（8位）。决定了报文在网络中被丢弃前可以传送多久，每经过一跳（Hop）TTL的值就会减1，到达0时数据报文就会被丢弃。这个值通常由源端主机设定。
  - 窗口大小是TCP首部窗口大小字段（16位），用于TCP的流量控制。这个字段的目的是告诉目标主机自己期望接收的每个TCP数据段的大小。
  - DF是IP首部中的分段标志字段（3位），用于标识报文是否允许被分段。这个字段的值也是由源端主机设定的。
  - TOS是IP首部中的服务类型字段（8位），用于设定报文的优先权、最小时延、最大吞吐量、最高可靠性和最小费用，详细的值可以参考RFC1349。

通过分析信息包的这些特征参数，就可以达到大致判断对方主机操作系统的目的，虽然探测结论不一定完全准确，但是通过综合研究多种特征信息，就可以增加探测的准确概率。

基于应用层协议的被动探测技术

- 针对Mail服务指纹特征进行检测
  - 在电子邮件的起始部位，通常都有一些系统特征信息，并可反映出操作系统信息。
- 针对Usenet服务指纹特征进行检测
  - 为了保证各种新闻阅读器的普遍使用性，大量的主机信息包含在新闻头部。通常操作系统版本、处理器和应用程序都被列在“User-Agent”域里。
- 针对Web服务指纹特征进行检测
  - 目前常用的Web服务器通常也可以反映出部分操作系统信息，通过构造适当的Web请求，就可以获得远程主机的操作系统信息。

操作系统探测举例

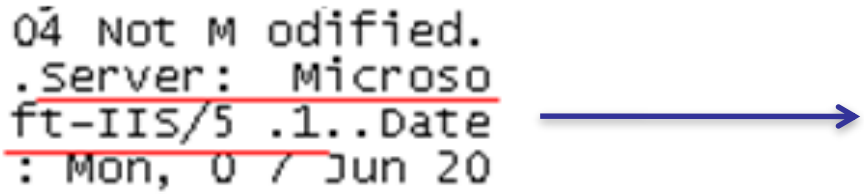
- 首先，IIS与操作系统的一般关系为：

IIS版本	IIS5.0	IIS5.1	IIS6.0
平台	Windows 2000	Windows XP Professional	Windows Server 2003 家族

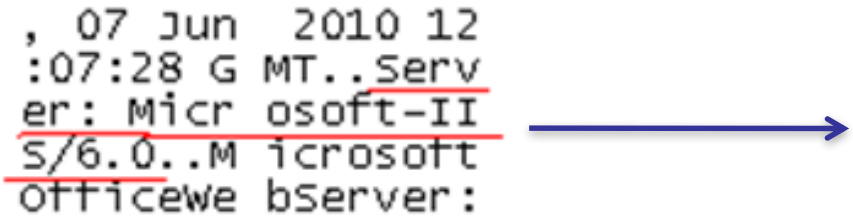
- 所以，通过向目标主机发送构造的请求，然后分析响应报文就可以知道目标主机的操作系统类型
- 当然，这是假设目标的Web服务器安装的是IIS
- 另外，Unix系统的探测也可以采取类似的探测方法

操作系统探测举例

- 通过向目标主机发送一般的HTTP GET请求，得到的分析结果为：



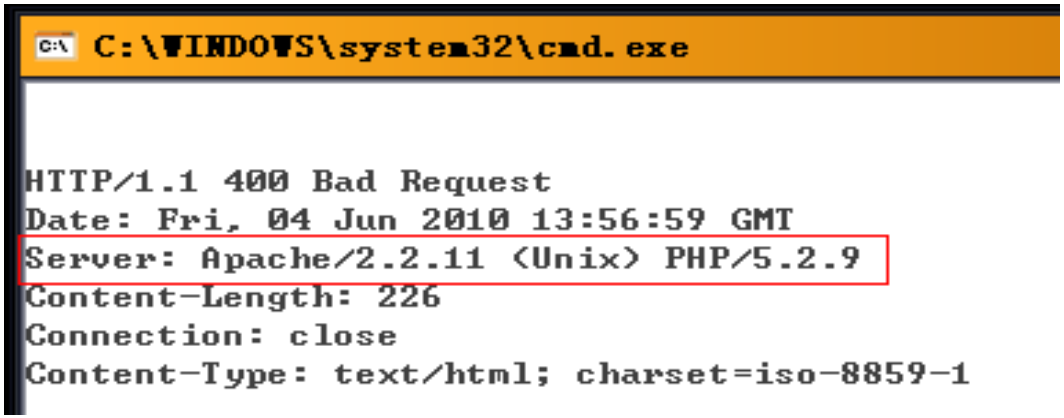
Windows XP Professional



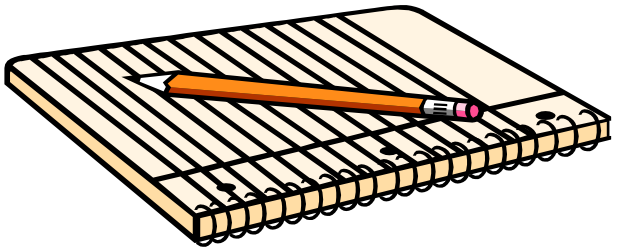
Windows Server 2003 家族

操作系统探测举例

- 而对Unix系统的探测构造相似的请求报文，得到的结果如下：



本次课程内容（网络安全扫描）



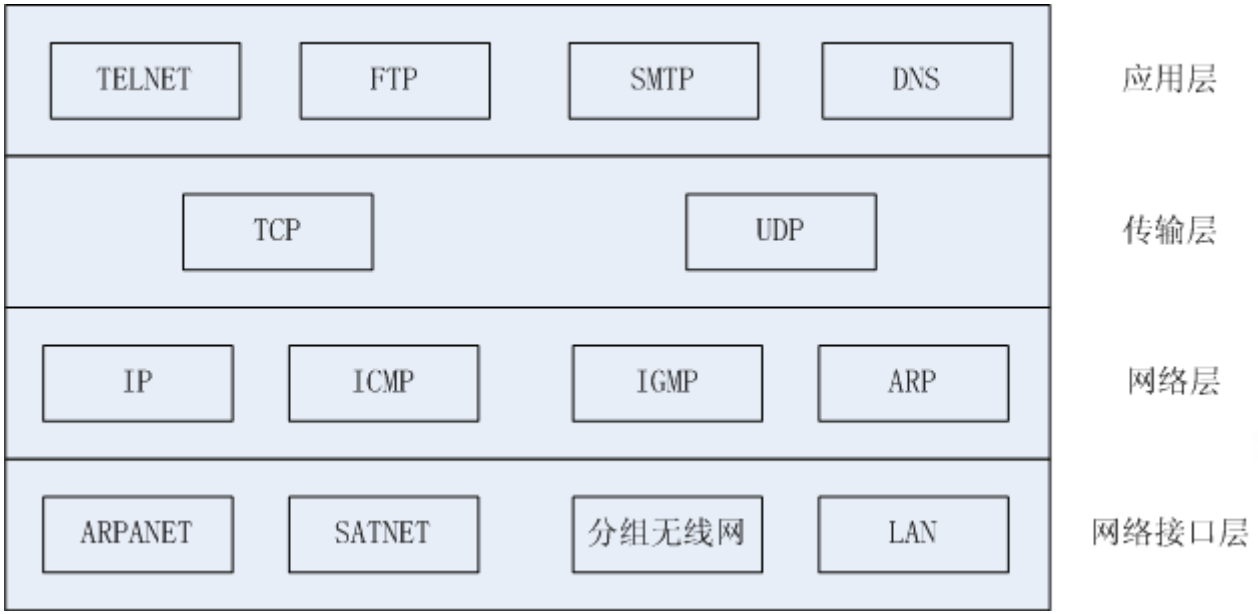
- 网络安全扫描技术概述
- 网络安全扫描技术
- 网络协议安全
- 安全漏洞概述
- 安全漏洞发现与防护

网络协议漏洞

- 对于底层的网络协议来说，对于安全的考虑有着先天的不足，部分网络协议具有严重的安全漏洞
- 由于先天的不足，一些协议上的漏洞是无法通过修改来弥补的

TCP/IP协议族

- TCP/IP协议实质是一种分层协议集合，分为网络接口层、网络层、传输层和应用层，协议的安全性主要集中在网络层、传输层和应用层



常用网络协议的缺陷

- TCP协议
- IP协议
- ARP协议
- UDP协议
- ICMP协议
- RIP协议
- 其它

TCP协议的缺陷

- TCP（Transmission Control Protocol，传输控制协议）协议在建立连接时所采用的三次握手机制提供了比其它协议更安全的措施，但攻击者依然可以通过发送伪造的数据包来迷惑目标主机，以达到攻击效果
  - TCP SYN Flood攻击
  - WinNuke攻击
  - TCP序列号预测攻击

IP协议的缺陷

- IP（Internet Protocol，网际协议）协议是一个非常重要的协议，是其他协议的基础，可以说是TCP/IP协议族中最核心的协议，主要的威胁有：
  - IP地址欺骗
  - Land攻击
  - IP碎片攻击

ARP协议的缺陷

- ARP（ Address Resolution Protocol，地址解析协议）是一种将IP地址解析成局域网硬件所使用的媒体访问控制地址(MAC)的协议
- 缺陷：
  - 有可能一个非法节点获取本网络的权限后，发布虚假的ARP报文使所有的通信都转向它，以达到窃取数据等目的
  - 当计算机接收到ARP应答数据包时，会对本地的ARP缓存进行更新，将包中的IP和MAC地址对存储在ARP缓存中，这一特点直接造成了ARP欺骗攻击实施的可能性
  - 直接向Windows系统主机发送大量无关的ARP数据包，会导致系统耗尽资源而停止响应，如果向广播地址发送ARP请求时，可能导致整个局域网停止响应

UDP协议的缺陷

- UDP（User Datagram Protocol，用户数据报协议）是一种无连接的协议，而且它不需要用任何程序建立连接来传输数据
- 缺陷：
  - 当受害系统接收到一个UDP数据包的时候，它会确定目的端口正在等待中的应用程序，当它发现该端口中并不存在正在等待的应用程序时，就会产生一个目的无法连接的ICMP数据包发送给源地址，当攻击者向目标系统发送足够多的UDP数据包时，就有可能发生UDP洪水攻击，受害系统就会瘫痪

ICMP协议的缺陷

- ICMP（Internet Control Message Protocol，因特网控制报文协议）协议用于差错控制和拥塞控制
- 缺陷：
  - ICMP重定向
  - 淹没攻击

RIP协议的缺陷

- RIP（Routing Information Protocol，路由信息协议）是动态发现合适的因特网路径的协议，它是运行TCP/IP的基础，因此也常容易受到攻击
- 缺陷：
  - IP 松散源路径选项（Loose Source Route）允许IP数据包自己指定通往目的主机的路径，攻击者可以由此越过防火墙而攻击其后的一个原本不可到达的主机
  - 伪造的RIP路由信息很容易欺骗主机或路由器，造成路由错乱或改向

其它协议的缺陷

- SMTP（简单邮件传输协议）由于过于信任的原则，缺少确认电子邮件发送者身份的全面手段，最容易受到电子邮件炸弹或廉价邮件(Spam) 的DoS 攻击
- FTP（文件传输协议）由于其代理服务特性，形成FTP反弹漏洞；可能形成控制连接是可信任的，而数据连接却不是；口令是以明文形式在网络中传送的
- DNS（Domain Name Server）主要负责将域名转化成网络可识别的IP地址，主要漏洞为：
  - 没有提供认证机制
  - 由于超高速缓存映射表的刷新问题，容易造成DNS欺骗或拒绝服务攻击

TCP/IP协议族的安全性改进

- 网络层的安全性改进
- 传输层的安全性改进
- 应用层的安全性改进

网络层的安全性改进

- 网络层安全协议的改进主要是IP封装技术
  - 对纯文本的数据包进行加密处理
  - 将其封装在外层的IP报头里，再在网络中路由选择
  - 到达目标主机后，拆开外层的IP报头后在对报文进行解密处理

- 安全协议工作组对IP安全协议（IPSP）进行标准化工作，使需要安全措施的用户能够使用相应的加密安全体制来保证其安全需要，该安全体制可以在IPv4和IPv6下工作
  - IPSP包含认证头（AH）和有效负载（ESP）两部分

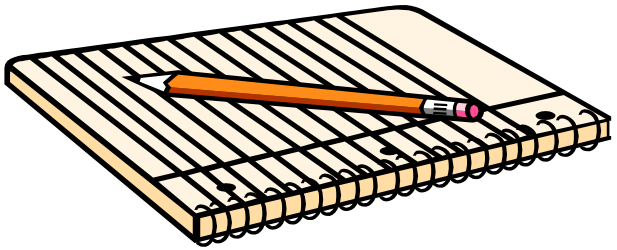
传输层的安全性改进

- Netscape通信公司制定了建立在可靠的传输服务基础上的安全套接层协议（SSL），该协议主要包含SSL记录协议和SSL握手协议
- 该层安全机制的主要缺点：基于UDP的通信很难在传输层上建立安全机制
- 主要优点：提供基于进程对进程的安全服务

应用层的安全性改进

- 网络层和传输层安全协议提高了主机或进程之间的数据通道安全性，却不能区分在同一通道上传输的一个具体文件的安全性要求
- 如果要区分一个具体文件的不同安全性需求，必须借助于应用层的安全协议，如：
  - 一个电子邮件系统可能需要对信件的个别段落实施数字签名，底层协议一般不知道信件的段落结构，从而不可能知道该对哪一部分进行签名，只有应用层是惟一能够提供这种安全服务的层次

本次课程内容（网络安全扫描）



- 网络安全扫描概述
- 网络安全扫描技术
- 网络协议安全
- 安全漏洞概述
- 安全漏洞发现与防御

安全漏洞概述

- 在计算机安全领域，安全漏洞通常又称作脆弱性（vulnerability），一般认为，漏洞是指硬件、软件或策略上存在的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统
- “计算机系统由一系列描述构成计算机系统的实体的当前配置状态组成，系统通过应用状态变换（即改变系统状态）实现计算。使用一组状态变换，从给定的初始状态可以到达的所有状态最终分为由安全策略定义的两类状态：已授权的和未授权的。”
- “脆弱状态是指能够使用已授权的状态变换到未授权状态的已授权状态。受损状态是指通过上述方法到达的状态。攻击是指以受损状态结束的已授权状态变换的顺序。”
- “脆弱性是指脆弱状态区别于非脆弱状态的特征。广义地讲，脆弱性可以是很多脆弱状态的特征；狭义地讲，脆弱性可以只是一个脆弱状态的特征。”

安全漏洞存在的原因

- Internet协议在最初设计时并没有考虑安全方面的需求
- 使用没有安全保证的信任策略
- Internet上传送的很多数据都是没有加密的明文
- Internet上高速膨胀的应用类型和服务
- 系统程序和应用程序是网络服务能过实现的必要基础，而其安全漏洞的产生几乎是不可避免的
- 网络技术管理人员由于本身技术能力的限制或疏忽等原因，对网络设定存在不当，增加了一些本来可以避免的漏洞

安全漏洞的来源

- 软件或协议设计时的瑕疵
- 软件或协议实现中的弱点
- 软件本身的瑕疵
- 系统和网络的错误配置

软件或协议设计时的瑕疵

- 协议定义了网络上计算机会话和通信的规则，如果在协议设计时存在瑕疵，那么无论实现该协议的方法多么完美，它都存在漏洞。例如NFS经常成为攻击者的目标
- 另外，在软件设计之初，通常不会存在不安全的因素，然而当各种组件不断添加进来的时候，软件可能就不会像当初期望那样工作，从而可能引入不可知的漏洞

软件或协议实现中的弱点

- 即使协议设计得很完美，实现协议的方式仍然可能引入漏洞
  - 和E-mail有关的某个协议的某种实现方式能够让攻击者通过与受害主机的邮件端口建立连接，达到欺骗受害主机执行意想不到的任务的目的
  - 如果入侵者在“To:”字段填写的不是正确的E-mail地址，而是一段特殊数据，受害主机就有可能把用户名和密码信息发送给入侵者，或者使入侵者具有访问受保护文件和执行服务器上程序的权限

软件本身的瑕疵

- 这类漏洞可以分为：
  - 没有进行数据内容和大小检查
  - 没有进行成功/失败检查
  - 不能正常处理资源耗尽的情况
  - 对运行环境没有做完整检查
  - 不正确地使用系统调用
  - 重用某个组件时没有考虑到它的应用条件
- 通过利用这些漏洞，即使不具有特权账号，也有可能获得额外的、未授权的访问

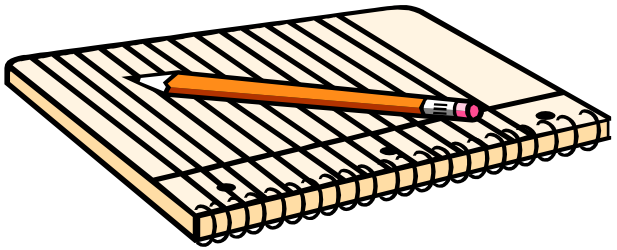
系统和网络的错误配置

- 这类漏洞并不是由协议或软件本身的问题造成的，而是由服务和软件的不正确部署和配置造成的
- 通常这些软件安装时都会有一个默认配置，如果管理员不更改这些配置，服务器仍然能够提供正常的服务，但是入侵者就能够利用这些配置对服务器造成威胁
  - SQL Server的默认安装就具有用户名为sa、密码为空的管理员账号
  - FTP服务器的匿名账号

公开的漏洞信息

- 漏洞本身不会对系统造成损坏，而只是为入侵者侵入系统提供了可能。但是，并不是知道漏洞的人越少，系统就越安全
- 建立在漏洞公开基础上的安全才是更可靠的安全
- 比较权威的漏洞信息资源：
  - 通用漏洞和曝光
  - BugTraq漏洞数据库
  - ICAT漏洞数据库
  - CERT/CC漏洞信息数据库
  - X-Force数据库

本次课程内容（网络安全扫描）



- 网络安全扫描概述
- 网络安全扫描技术
- 网络协议安全
- 安全漏洞概述
- 安全漏洞发现与防御

安全漏洞发现与防御

- 漏洞发现就是对计算机信息系统进行检查，发现其中可被黑客利用的漏洞

- 漏洞防御就是在漏洞发现的基础上，采取各种技术对漏洞进行防御，达到保护系统的目的

漏洞发现

- 漏洞发现技术可分为两种：
  - 基于主机的发现技术
    - 这种技术是对操作系统的各种配置、权限、补丁等方面进行检测，以发现主机潜在的安全漏洞
    - 主要从系统的文件、目录和设备文件的权限，重要系统文件的内容、格式、权限和重要的系统二进制文件的校验等方面进行检测
  - 基于网络的发现技术
    - 这种技术是利用了一系列的脚本对远端系统进行攻击，然后对远端系统的响应结果进行分析；可以发现远端不同平台的一系列漏洞
    - 检测范围包括所有的网络设备：服务器、防火墙、交换机、路由器以及主机等

漏洞防御

- 面对众多的漏洞，漏洞防御技术主要有：
  - 基于源码的防御技术
  - 基于操作系统的防御技术
  - 漏洞信息发布机制

基于源码的防御技术

- 漏洞产生的根源在于编写程序的机制，防御漏洞首先应该确保程序代码的正确性和安全性，避免程序中有不检查变量、缓冲区大小边界等情况存在
- 主要有：
  - 安全编写源码
    - 安全的共享库技术
    - 边界检查
  - 源码审计
    - 静态测试
    - 动态测试

基于操作系统的防御技术

- 底层系统自我保护
  - SEH校验机制
  - GS安全编译选项
  - DEP技术
  - ASLR技术
- 系统安全管理
  - 管理好Administrator账号
  - 关闭不用的端口和共享服务
  - 及时安装补丁
- 主动防御

漏洞信息发布机制

- 漏洞信息的发布应做好以下几个方面：
  - 实时性
  - 检索粒度
  - 发布方式

检索粒度

- 大部分的普通用户只希望得到与自己情况相关的漏洞信息，而不需要去了解其它众多的操作系统所存在的漏洞。为了方便用户进行查询，快速获得自己需要的信息，漏洞发布机制需要提供相应的查询功能。此外，检索粒度应当细一些，这样才能很好地满足用户的需要，在最短的时间内准确找出需要的信息。

发布方式

- 漏洞发布方式指这个机制采用什么办法为用户提供漏洞信息。需要漏洞信息的用户大致可以划分为3类：普通用户，特殊群体，需要使用漏洞库的厂商。针对这3种不同的用户需求，相应地提供3种发布方式：
  - 网页浏览
  - 邮件
  - 数据库