REVIEW

REVIEW
- Charter 1 网络防御与对抗
- Charter 2 网络攻击与防范的历史、现状与发展趋势
- Charter 3 拒绝服务攻击
- Charter 4 恶意代码
- Charter 5 应用层安全
- Charter 6 网络防火墙
- Charter 7 入侵检测与网络欺骗

Charter 1 网络防御与对抗

计算机网络：由通信信道连接的主机和网络设备的集合，以方便用户共享资源和相互通信。

因特网：多层次ISP结构的网络，包括核心部分（大量网络+路由器）和边缘部分（主机+接入网）。

网络的体系结构：计算机网络的各层及其协议的集合。协议为网络中相互通信的对等实体进行数据交换而建立的规则、标准或约定，三要素是语义、语法和同步。

计算机网络的脆弱性：分组交换、认证和可追踪性、尽力而为、匿名与隐私、对全球网络基础设施的依赖、无尺度网络、互联网的级联特性、中间盒子。

协议缺陷：

协议	缺陷
IEEE802.3	没有提供报文完整性和源地址认证
ARP	缺乏相应的认证机制，导致用户无法辨别ARP报文消息的真实性
RARP	缺乏必要的验证机制
IPv4	无状态、无认证
ICMP	利用目的站不可达发送Dos攻击，利用改变路由报文破坏路由表，利用ICMP进行隐蔽通信，利用回送请求或回答报文进行网络扫描
TCP	缺乏认证机制和报文的完整性检查
UDP	无连接，且没有任何认证机制和拥塞控制机制，容易伪造数据包
POP3	明文传输，容易被窃听
DNS	缺乏密码认证，加密DNS
FTP	使用简单用户名和密码认证机制
Telnet	用户名和口令明文传输

计算机网络安全：是指计算机网络中硬件资源和信息资源的安全性，它通过网络信息的产生、存储、传输和使用过程来体现：包括网络设备的安全性，使其能够正常地提供网络服务；信息的安全性，即网络系统地信息安全。目的是保护网络设备、软件、数据，使其能够被合法用户正常使用或访问，同时要免受非授权地使用或访问。

网络安全属性：

机密性：不被泄露给未经授权者

完整性：未经授权不能改变，系统完整性和数据完整性

可用性：可被授权者访问并按需使用，保证合法用户对资源的使用不会被不合理拒绝，它应包括可靠性、可生存性、可维护性、稳定性等子属性

不可否认性：不可抵赖性，所有地参与者都不可能否认或抵赖曾经完成地操作和承诺。发送方不能否认已发送的消息，接收方也不能否认已经收到的消息。

可靠性：能够在规定时间内和规定条件下完成规定功能

可控性：对信息的传播和内容具有控制能力

网络空间：”网络“——设施+数据（技术层面），”空间“——用户+操作（社会层面）

网络攻击技术：截获、中断、篡改、伪造

主动攻击：伪装、重放、修改报文、拒绝服务

被动攻击：监听传输的报文内容、通信流量分析

网络攻击过程：目标踩点→远端扫描→资源列举→权限获取→权限提升→设置后门→毁踪灭迹

PDRR模型：防护、检测、恢复、响应

P2DR模型：安全策略、防护、检测、响应

P2DR2模型：安全策略、防护、检测、恢复、响应

IATF框架（信息保障技术框架）：强调人、技术、操作三个核心要素，关注四个信息安全保障领域：保护网络和基础设施、保护边界、保护计算环境、支撑基础设施，为建设信息保障系统及其软硬件组件定义了一个过程，依据纵深防御策略，提供一个多层次的、纵深的安全措施来保障用户信息及信息系统的安全。在IATF中，人是信息体系的主体，是信息系统的拥有者、管理者和使用者，是信息保障体系的核心，同时也是最脆弱的

CGS框架：治理、保护、检测、响应与恢复

安全机制：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程。8类安全机制包括加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制、公证。5种普遍性的安全机制包括可信度功能、安全标记、事件检测、安全审计跟踪以及安全恢复。

安全服务：指加强数据处理系统和信息传输的安全性的处理过程或通信服务，主要利用一种或多种安全机制对攻击进行反制来实现。5类安全服务包括鉴别、访问控制、数据机密性、数据完整性和抗抵赖

表 1-1 安全服务与安全机制的关系

服务 \ 机制	加密机制	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证机制
对等实体认证	√	√			√			
数据原认证	√	√						
访问控制服务			√					
连接机密性	√						√	
无连接机密性	√						√	
选择字段机密性	√							
通信业务流机密性	√					√	√	
带恢复的连接完整性	√			√				
不带恢复的连接完整性	√			√				
选择字段连接完整性	√			√				
无连接完整性	√	√		√				
选择字段无连接完整性	√	√		√				
不可抵赖，带交付证据		√		√				√

安全技术：防火墙、入侵检测系统、虚拟专用网

Charter 2 网络攻击与防范的历史、现状与发展趋势

网络侦察：收集目标主机系统和计算机网络安全相关信息的过程，也称踩点。它是黑客实施网络入侵的第一步，也是网络管理员实施安全防御的第一步。

静态信息：主机或网络的IP地址（段）、名字或域名；各种联系信息，包括姓名、邮件地址、电话号码；DNS、邮件、Web等服务器；网络拓扑结构；目标机构的业务信息

动态信息：目标主机是否开机；目标主机是否安装了某种软件；目标主机的操作系统；目标主机的安全漏洞

网络侦察方法：搜索引擎、whois查询、DNS信息查询、网络拓扑结构发现、利用社交网络获取信息、其他侦察方法（社会工程学）

社会工程学：利用人的弱点进行诸如欺骗、伤害等危害手段，获取自身利益。

网络扫描：使用网络扫描软件对特定目标进行各种试探性的通信，以获取目标信息的行为。

网络扫描步骤：主机扫描→端口扫描→操作系统检测→漏洞扫描

主机扫描：向目标主机发送探测数据包，根据是否收到响应来推断主机的工作状态。可以发送ICMP报文或者异常的IP分组进行扫描（可以是错误的头部信息、分片错误、超长包）。

端口扫描类型：开放扫描——会产生大量的审计数据，容易被对方发现，但其可靠性高；隐蔽扫描——能有效避免对方入侵检测系统和防火墙的检测，但这种扫描使用的数据包在通过网络时容易被丢弃从而产生错误的探测信息；半开放扫描——隐蔽性和可靠性介于前两者之间。

扫描类型	方法
开放扫描	TCP Connect
半开放扫描	SYN
隐蔽扫描	FIN，Xmas，Null

UDP扫描：无连接，不可靠，没有复杂的交互，但判断主机端口的工作状态比较难。端口开放时无响应，关闭时回发ICMP消息，区分度比较好，但无论是UDP还是ICMP报文在传输过程中都容易丢失，引起误判。

扫描策略：随机端口扫描，慢扫描，数据包随机化扫描，分片扫描，诱骗，分布式协调扫描

操作系统检测方法：获取旗标信息，利用端口信息，分析TCP/IP协议栈指纹

漏洞扫描：向目标发送特定报文，根据相应判断是否存在漏洞，可以分为基于主机的漏洞扫描和基于网络的漏洞扫描

网络监听：是指在计算机网络接口处截获网上计算机之间通信的数据，也称网络嗅探，可分为共享式网络监听和交换式网络监听，共享式网络可以直接监听，交换式的网络需要借助诸如镜像端口（把其他端口的数据镜像到一个端口上）、MAC泛洪（用欺骗性的MAC地址源填充交换机的MAC地址表，表满时交换机的工作像集线器）、ARP欺骗、端口盗用

Charter 3 拒绝服务攻击

拒绝服务攻击：攻击者通过某种手段，有意地造成计算机或网络不能正常运转从而不能向合法用户提供所需要的服务或者使服务质量降低

分布式拒绝服务攻击：如果处于不同位置的多个攻击者同时向一个或多个目标发起拒绝服务攻击，或者一个或多个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施拒绝服务攻击。它的特点是攻击来源的分散性、协同性，攻击力度的汇聚性

DDoS成功的原因：TCP/IP协议存在漏洞，可以被攻击者利用；网络提供尽力而为得服务，并不区分数据流量是否是攻击流量；网络带宽和系统资源是有限的（根本原因）

DDoS攻击的对象：网站、路由器、DNS服务器、CDN和其他网络基础结构

剧毒包（杀手包）：利用协议本身或其软件实现中的漏洞，通过一些畸形的数据包使受害者系统崩溃，也称为“漏洞攻击”或“协议攻击”，典型例子有泪滴攻击、Land攻击、Ping of death攻击、循环攻击、WinNuke等，剧毒包型DoS是最早出现的一类Dos

风暴型DoS攻击：通过大量的“无用”数据包占用过多的资源以达到拒绝服务的目的，也称为“带宽攻击”。“风暴型”DoS攻击的过程：攻击者利用扫描工具探测一台或多台主机作为入侵目标，安装handler，攻击者在handler上扫描大量主机寻找入侵目标，攻击者设法通过handler入侵有安全漏洞的主机并获取控制权，接着从入侵计算机清单中选出满足建立网络所需要的主机作为代理端，再利用控制端，在攻击代理主机上安装已经编译好的守护程序，最后对目标发起DDoS攻击

直接风暴型拒绝服务攻击：

Ping风暴攻击——攻击者利用控制的大量主机向受害者发送大量的ICMP回应请求消息，使受害者系统忙于处理这些消息而降低性能，严重者可能导致系统无法对其他消息做出响应

SYN Flood攻击——发送大量的SYN报文，但对服务器的SYN+ACK应答报文不作应答，三次握手的第三次握手无法完成，服务器需要维护大量的半连接列表，消耗服务器半连接资源的攻击方式

TCP连接耗尽攻击——通过众多的TCP连接耗尽受害者资源，也称为“空连接攻击”，它不需要不断地向受害者发起连接

UDP风暴攻击——向目标主机连续发送大量较长的UDP数据包，占用网络带宽，达到阻塞网络的目的

HTTP风暴攻击——用HTTP协议对网页进行语义上合法的请求，不停地从受害者处获取数据，占用连接的同时占用带宽

对邮件的DoS攻击——邮件炸弹或者垃圾邮件

反射性拒绝服务攻击DRDoS：攻击者利用应用层协议，向互联网上大量开放特定服务的服务器发送请求数据包，其中源IP地址被伪造成攻击目标的IP地址，这些开放特定服务的服务器在此攻击过程中也被称为反射节点，当反射节点收到请求数据包后，则将应答数据包发送给攻击目标，当大量应答数据包到达时，即形成对攻击目标的DDoS攻击

NTP：网络时间协议，用于计算机间的时间同步

SSDP：简单服务发现协议，主要用于局部网里发现通用即插即用网络设备

SYN Flood、Ping、UDP风暴的反射变形：基本都是把源ip改成受害主机

Smurf攻击：发送ICMP ECHO请求，源地址是目标IP，目的地址是广播地址

Fraggle攻击：与smurf攻击类似，但使用的是UDP ECHO

重定向DoS攻击：通过求改网络中的一些参数或ARP表、DNS缓存，使得受害者发出的或者发向受害者的数据包被重定向到了其他地方，常被用于窃听或中间人攻击

僵尸网络：BotMaster通过命令与控制信道（C&C）控制具有协调性的恶意计算机群，分为IRC僵尸网络和P2P僵尸网络

拒绝服务攻击的检测是困难的，不容易定位到攻击者的位置（伪造IP地址，通过代理攻击，反射式攻击）

DoS检测方法：根据DoS攻击工具的特征检测、统计检测、异常流量检测

DoS响应：丢弃恶意分组、在源端控制DDoS、追溯端源，阻止它发起新的攻击、路由器动态检测流量并进行控制，但上述措施只能减轻DoS攻击所造成的危害

对抗风暴型DDoS的有效方法是流量清洗，净化掉DDoS攻击流量

DDoS攻击阻断过程一般包括攻击监测与判断、流量牵引、清洗过滤、流量回送

Charter 4 恶意代码

恶意代码：指在不为人知的情况下侵入用户的计算机系统，破坏系统、网络、信息的保密性、完整性和可用性的程序或代码，它具有非授权性、破坏性等特点

恶意代码的形式：计算机病毒、蠕虫、木马程序、逻辑炸弹、Rootkit、后门

类型	定义	特性
计算机病毒	在计算机程序中插入的破坏计算机功能并能自我复制的一组程序代码	潜伏、传染、破坏
计算机蠕虫	通过计算机网络自我复制，消耗系统资源和网络资源的程序	扫描、攻击、扩散
特洛伊木马	指一种与远程计算机建立连接，使远程计算机能够通过网络控制本地计算机的程序	欺骗、隐蔽、信息窃取
逻辑炸弹	通过特殊的数据或时间作为条件出发，试图完成一定破坏功能的程序	潜伏、破坏
RootKit	指通过替代或修改系统功能模块，从而实现隐藏和创建后门的程序	隐蔽，潜伏

计算机病毒的特征：潜伏性、传染性、触发性、寄生性、非授权执行性和破坏性

计算机病毒的结构：引导模块、搜素模块、感染模块、表现模块、标识模块

计算机蠕虫的结构：搜索模块、攻击模块、传输模块、负载模块、控制模块

计算机蠕虫存在漏洞的依赖性：针对漏洞进行攻击

计算机蠕虫与病毒的本质区别：自动入侵

影响蠕虫传播速度的因素：潜在的脆弱目标的数量、漏洞主机被发现的速度、蠕虫自身复制的速度

比较：

项目	病毒	蠕虫
存在形式	代码片段	独立个体
复制机制	插入到宿主程序	自身的复制
传染机制	宿主的运行	系统存在漏洞
攻击目标	本地文件系统	网络上的计算机
使用者角色	病毒传播的关键	无关
防治措施	从宿主文件中删除	打系统补丁

木马的危害：自动搜索已中木马的计算机、管理对方资源、跟踪监视对方屏幕、直接控制对方的键盘、鼠标、随意修改注册表和系统文件、共享被控计算机的硬盘资源、监视对方任务并可终止对方任务、远程重启和关闭机器

木马的分类：密码窃取型木马、投放器型木马、下载型木马、监视型木马、代理型木马、点击型木马、远程控制型木马

木马结构：服务器端程序（植入受害主机）、客户端程序（运行在攻击者的主机上）

木马的特性：隐蔽性、非授权性

木马入侵的过程：配置木马、传播木马、运行木马、信息反馈、建立连接、远程控制

木马隐藏的技术：通信隐藏（端口复用，反向连接，ICMP通信）、进程隐藏（图标，名字，Hook，DLL运行，远程线程插入）

木马欺骗的手段：捆绑欺骗、网站挂马、漏洞攻击

端口复用：多个应用进程在同一个合法端口监听，利用合法端口掩护，木马程序优先接收，决定自己处理或转发

端口反弹：反向连接，改进反向连接

Charter 5 应用层安全

DNS：域名解析系统（DNS）负责将域名解析成IP地址

本地域名服务器：权威域名服务器——存有某域名空间的所有信息、递归域名服务器

根域名服务器：管理顶级域

权威域名服务器：每一个主机必须在权威域名服务器注册登记，可将管辖域名转换为IP地址

DNS原理：本地DNS查询记录，递归查询本地DNS服务器，迭代查询上级DNS

DNS面临的威胁：协议脆弱性、实现脆弱性、操作脆弱性

域名欺骗：域名系统接受或使用来自未授权主机的不正确信息、事务ID欺骗和缓存投毒

缓存投毒：控制DNS缓存服务器，把原本准备访问某网站的用户不知不觉中带到黑客指向的其他网站，可以攻击ISP端的DNS网络服务器，改变一整个访问域的响应结果，或者利用权威域名服务器上的漏洞进行缓存投毒，将错误的域名存入缓存，使所有使用该缓存服务器的用户得到错误的DNS解析结果

网络通信攻击：针对DNS的网络通信攻击主要是DDoS攻击，恶意网址重定向和中间人攻击。DDoS攻击可以攻击DNS服务器本身或者将其作为反射型DDoS的反射节点攻击目标服务器，DNS劫持...

DNSSEC基本思想：依赖于数字签名和公钥系统去保护DNS数据的可信性和完整性

DNSSEC工作原理：权威域名服务器用它的私钥来签名资源记录，解析服务器用权威服务器的公钥来验证来自权威域名服务器的数据

web应用的安全威胁：web客户端的脆弱性，浏览器漏洞可能被利用渗透主机，活动内容执行，客户端软件漏洞的利用，交互站点脚本的错误；web服务器的脆弱性，web服务器软件存在漏洞，利用漏洞可发动DDoS攻击，获得服务器权限，数据库访问权限；传输，窃听、SSL重定向；数据库的安全脆弱性，SQL注入；web应用程序的脆弱性，攻击授权，认证，站点结构，输入验证，应用程序逻辑

HTTP的脆弱性：无状态使得攻击变得容易，基于ASCII码攻击者可以了解其中的明文信息，互联网中存在大量的中间盒子

Cookie的脆弱性：Cookie中包含了一些敏感信息，攻击者可以利用它来进行窃密和欺骗攻击

SQL注入攻击：SQL注入攻击以网站数据库为目标，一般利用Web应用程序对特殊字符串过滤不完全的缺陷，通过精心构造的SQL语句达到非法访问网站数据库内容或在数据库中执行命令的目的

SQL注入的防范：

1.使用特定语言的库函数来代替shell命令和系统调用，

2.对用户输入的信息进行严格检查和过滤，

3.禁止将敏感数据以明文存放在数据库中，

4.遵循最小特权原则，尽量不要使用动态拼接的SQL语句，可以使用参数化的SQL或者存储过程进行数据查询，

5.应用的异常信息尽可能给出少的提示，以免给攻击者提供参考

XSS跨站脚本攻击：输入嵌有JS或者其他恶意脚本的HTML标签代码，其问题的根源在于不当的服务器输入检查，从而允许用户输入可被客户端浏览器揭示的脚本命令，XSS是最普遍的web应用程序安全问题

XSS攻击类型：反射型XSS（非持久性），本地脚本漏洞攻击/DOM式跨站脚本攻击，存储式跨站脚本攻击（持久性）

反射型XSS：web客户端使用server端脚本生成页面为用户提供数据时，如果未经验证的用户数据被包含在页面中而未经HTML实体编码，客户端代码便能注入到动态页面中，web程序本身不存储恶意脚本，它会将未经验证的数据通过请求发给客户端，攻击者就可以构造恶意的URL链接或者表单诱骗用户访问，达到利用受害者身份运行恶意代码的目的

存储型XSS：如果web程序允许存储用户数据，并且存储的输入数据没有经过正确的过滤，就有可能发生存储型XSS

XSS防范：服务器端——黑名单过滤，白名单过滤，字符转换；客户端——禁用动态脚本，阻止访问已知的恶意网站，对用户进行培训

会话管理安全性：Session ID可能泄露或被猜解，攻击者能拥有和受害者相同的特权

认证和会话管理攻击防范：1.区分公共区域和受限区域2.对最终用户账户使用账户锁定策略3.支持密码有效期4.能够禁用账户5.不要在本地存储中存储密码6.要求使用强密码7.不要再网络上以纯文本形式发送密码8.保护身份验证Cookie9.使用SSL保护会话身份验证Cookie10.对身份验证cookie内容进行加密11.限制会话寿命

Cookie欺骗：Cookie中保存了用户名、口令和权限信息，可以伪造Cookie信息绕过网站验证过程

Cookie欺骗防范：一般情况下，网站会话管理机制仅将会话ID保存至Cookie，而数据本身保存在web服务器的内存或文件、数据库中

CSRF跨站请求伪造：是一种诱骗受害者提交恶意请求的攻击。它继承了受害者的身份和特权，可以代表受害者执行不希望的功能

CSRF防范：采用POST提交进行数据更新、设定短暂的用户会话时间，超时自动删除所有cookie，每次提出一个可信性为，对发出请求的用户进行验证、谨慎让网站保存用户名和密、在URL和表单中增加的每个请求，必须提供基本会话令牌意外的每个请求用户验证、从web应用程序删除所有的XSS漏洞

目录遍历：服务器在处理用户请求时不对文件名进行充分校验，就可能导致文件被非法获取、文件被篡改或者文件被删除，产生目录遍历漏洞的原因有：外界能够指定文件名、能够使用绝对路径或者相对路径等形式来指定其他目录的文件名，没有对拼接的文件名进行校验就允许访问该文件

目录遍历的防范：避免由外界指定文件名，禁止包含目录名，限定文件中仅包含字母或数字，锁定web目录，对每一次对象的引用都要重新授权，禁止通过参数暴露内部对象，使用间接映射的方式代替简单的直接对象引用

操作系统命令注入：shell支持连续执行多条命令，如果传入shell的参数中出现元字符，就会引起多条指令被执行，产生os注入

os注入的防范：选择不调用操作系统命令的实现方法，避免使用可能调用shell的函数，不将外部输入的参数作为命令行参数，使用安全的函数对传递给操作系统的参数进行转义，消除shell元字符带来的威胁

HTTP消息头注入：HTTP响应头信息一般以文本格式逐行定义消息头，即消息头之间互相以换行符隔开。攻击者可以利用这一特点，在指定重定向目标URL或Cookie值的参数中插入换行符且该换行符又被直接作为响应输出，从而在受害者的浏览器上任意添加响应消息头或伪造响应消息体

HTTP消息头注入防范：不将外部传入参数作为HTTP响应消息头输出，如不直接使用URL指定重定向目标，而是将其固定或通过编号等方式来指定，或使用Web应用开发工具中提供的会话变量来转交URL，由专门的API来进行重定向或生成Cookie，并严格检验生成消息头的参数中的换行符

不安全的通信：web流量往往是不加密的，攻击者可以从网络上任何一个被攻陷的系统或设备上嗅探网络流量，使用SSL也可能遭受“中间人”攻击

不安全通信的防范：保证所有用来认证和传输敏感信息的连接都使用基于SSL/TLS的HTTPS

web应用防火墙分析方法：基于规则的分析方法，异常检测方法

web应用防火墙的部署模式：反向代理、透明代理、旁路

Charter 6 网络防火墙

防火墙：是在两个网络之间执行访问控制策略的一个或一组安全系统。它是一种计算机硬件和软件系统集合，是实现网络安全策略的有效工具之一，被广泛应用到内部网络和外部网络的边界位置

防火墙的主要功能：保护脆弱和有缺陷的网络服务，实施安全策略，加强对网络系统的访问控制，防止内网信息暴露，加强隐私，对内外网之间的通信进行审计监控

防火墙分类：软件防火墙、硬件防火墙、芯片级防火墙（按照硬件软件形式分）、包过滤防火墙、应用网关（按照监控的网络协议层次分）、单一主机防火墙、路由器集成防火墙、分布式防火墙（按照组成结构划分）、个人/单机防火墙、网络防火墙（按照受保护的对象划分）

包过滤防火墙：根据包头信息，依据事先制定好的规则，决定是否允许数据包通过，它的工作对象是数据包，对TCP/IP协议组来说，包过滤技术主要是对数据包包头的各个字段进行操作

包过滤技术的优点：

1.将包过滤防火墙部署在网络边界上就可以实现对整个网络的保护，实现简单、快速，很多路由器可以做包过滤，不需要添加设备

2.包过滤技术的检查规则相对简单，检查操作耗时极短，执行效率非常高，不会给用户网络性能带来不利的影响

3.包过滤防火墙对用户和应用都是透明的，内网用户无需对主机进行特殊设置

包过滤技术的缺点：

1.安全判决的信息不足，仅依赖网络层和传输层信息

2.支持规则的数量有限，规则过多会降低网络效率

3.正确规则的设定并不容易

4.不可能引入认证机制

状态检测包过滤防火墙：对连接的初始数据报文进行规则过滤，如果允许通过，就将该连接的信息记录下来并添加规则，然后向目的地转发该报文，凡是属于该连接的数据包防火墙将一律放行，在连接结束之后，防火墙将删除关于该连接的过滤规则

状态检测包过滤防火墙的优点：

1.安全性比静态包过滤防火墙高

2.与静态包过滤技术相比，提升防火墙的性能

状态检测包过滤防火墙的缺点：

1.主要工作在网络层和传输层，对报文的数据部分检查很少，安全性还不够高

2.检查内容多，对防火墙性能提出了更高的要求

应用网关防火墙：代理内部网络用户与外部网络服务器进行信息交换的程序，应用代理可以分析数据包的数据区，并以此为依据判断是否允许数据通过

应用级代理的优点：

1.代理技术能够提供更高的安全等级

2.实现网络隔离

3.包过滤技术通常由路由器实现

应用级代理的缺点：

1.对于每一类应用都需要使用专门的代理

2.性能比包过滤防火墙差

3.更昂贵

4.不能使用户免于协议本身的缺陷

5.有些服务要求直接建立连接，不能使用代理

防火墙体系结构：屏蔽路由器结构、双宿主机结构、屏蔽主机结构、屏蔽子网结构

防火墙的评价标准：并发连接数、吞吐量、时延、丢包率、背靠背缓冲、最大TCP连接建立速率

防火墙的不足：

1、不能防范不经过防火墙的攻击

2、由于防火墙性能上的限制，它通常不具备实时监控入侵的能力

3、防火墙不能防止策略配置不当或错误配置引起的安全威胁

4、防火墙不能防止受病毒感染的文件的传输

5、防火墙不能防止利用服务器系统和网络协议漏洞所进行的攻击

6、防火墙不能防止数据驱动式的攻击

7、防火墙不能防止内部的泄密行为

8、防火墙不能防止本身安全漏洞的威胁

Charter 7 入侵检测与网络欺骗

入侵检测：通过计算机系统或者网络关键点收集信息并进行分析，从中发现系统或网络中是否有违反安全策略的行为和被攻击的迹象

入侵检测系统：是指实施入侵检测的软件和硬件的组合

入侵防御系统：入侵检测+主动防御，主动防御是预先对入侵活动和攻击流量进行拦截，避免其造成任何损失，而不是简单地在恶意流量传送时或传送后才发出警报，需要发现攻击并做出响应，但存在误报导致合法数据被阻塞的问题

IDS，IPS，IMS

入侵检测系统的作用：

1、发现内部攻击事件和合法用户的越权访问行为

2、及时发现针对防火墙开放服务的网络攻击并进行报警

3、发现利用防火墙漏洞穿越防火墙的攻击行为

4、发现入侵企图

5、提供审计信息，记录攻击过程，发现脆弱点

IDS数据源：来自主机、来自应用，来自网络

来自主机的数据：操作系统审计记录，系统日志文件

来自应用的数据：应用程序日志、应用程序行为记录

网络数据源的优点：

1、网络数据的收集和分析不会影响业务主机的性能

2、以被动监听的方式获取数据包，不会降低网络性能

3、不容易遭受攻击

4、相比主机数据源，可更快速有效地检测网络攻击

5、网络数据包格式标准化程度高，更容易兼容不同系统

网络数据源的不足：

1、对加密数据包无法分析

2、数据流量大，处理开销高

3、对主机的保护精确度不如来自主机数据

4、不同系统对TCP/IP协议实现存在差异，使得IDS系统对数据包的处理和数据内容的理解上产生差异

入侵检测系统分类：

分类方式	分类
按系统各模块的运行方式来分	集中式、分布式
根据时效性来分	脱机分析、联机分析
根据数据源来分	基于主机的，基于应用的，基于网络的，混合的
根据检测方法来分	基于特征、基于异常、混合

检测方法：特征检测、异常检测

特征检测：收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中记录相匹配时，系统就认为这种行为是入侵，针对的是已知攻击，检测率取决于攻击特征库的正确性与完备性

特征检测的实现方式：

1、模式匹配

2、专家系统法

3、状态迁移法

异常检测方法：首先总结正常操作应该具有的特征，当用户活动与正常行为有重大偏离时即被认为是入侵

异常检测的实现方法：

1、统计分析法

2、神经网络法

3、聚类分析法

4、人工免疫

异常检测的优点：无需维护更新特征库，管理开销较小，不依赖具体的、已知的攻击特征来检测，可以判断更广泛的未知攻击

异常检测的缺点：在发现攻击时不能准确告知攻击类型、异常检测的准确度通常没有特征检测高

IDS目前存在的问题：漏报率和误报率两项指标偏高、用户隐私与系统安全的矛盾

不具备主动发现安全漏洞的能力、不断丰富的网络应用对入侵检测提出了挑战

网络欺骗：采用引诱或欺骗战略，诱使入侵者相信网络与信息系统中存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源，而将入侵者引向错误的资源，同时安全可靠地记录入侵者的所有行为，以便全面地了解攻击者的攻击过程和使用的攻击技术

网络欺骗用途：吸引攻击流量、检测入侵者的攻击并获知其攻击技术和意图、拖延攻击者攻击真实目标、了解入侵者

蜜罐：蜜罐是一类安全资源，其价值就在于被探测、被攻击和被攻陷

蜜罐分类：

分类方式	分类
按照部署目的	生产型蜜罐、研究型蜜罐
按照交互度	低交互、中交互、高交互
按实现方式	物理蜜罐、虚拟蜜罐

低交互蜜罐的功能：攻击数据捕获与处理、攻击行为分析

高交互蜜罐的功能：网络欺骗、攻击捕获、数据控制、数据分析