第二章 网络攻击行径分析

1. 利用向目标主机发送非正常消息而导致目标主机崩溃的攻击方法有哪些

PingOfDeath、IGMP Flood、Teardrop、UDP flood、SYN flood、Land、Smurf、Fraggle、畸形消息攻击、分布式拒绝服务攻击、目的地不可达攻击、电子邮件炸弹、对安全工具的拒绝服务攻击、拒绝服务攻击、网络远程拒绝服务攻击、本地拒绝服务攻击。

2. 简述破坏型攻击的原理及其常用手段 P9

3. 简述 IP 欺骗 P14

4. 叙述扫描的作用于并阐述常用的扫描方法 P12

5. 简要叙述攻击的一般过程及注意事项

攻击的准备阶段、攻击的实施阶段、攻击的善后阶段。*注意*: ①确定攻击目的、准备攻击工具、收集目标信息; ②隐藏自己的位置、利用收集到的信息获取账号和密码，登陆主机、利用漏洞或者其他方法获得控制权并窃取网络资源和特权; ③清理痕迹如 Web 服务器的日志，事件日志等，可用以下方法:禁止日志审计、清除事件日记、清除 IIS 服务日记。

6. 为什么要进行攻击善后 P20 如果完成攻击后……留下的痕迹

资料：

1. IGMP flood：

> Internet Group Management Protocol（因特网组管理协议）是用于管理因特网协议多播组成员的一种通信协议。IP主机和相邻的路由器利用IGMP来建立多播组的组成员。

攻击者使用受控主机向被攻击目标发送大量的ICMP/IGMP报文，进行洪水攻击以消耗目标的宽带资源，这种类型的攻击出现的很早，使用hping等工具就能简单的发起攻击。但现在使用这种方法发动的攻击已见不多，被攻击目标可以在其网络边界直接过滤并丢弃ICMP/IGMP数据包使攻击无效化。

但是这种直接方式通常依靠受控主机本身的网络性能，所以效果不是很好，还容易被查到攻击源头。于是反射攻击就出现。

第三章 网络侦察技术

1. 扫描有几种类型？简述它们的功能

三种：地址扫描、端口扫描、漏洞扫描。功能：P30~35
（端口扫描：判断运行服务的方法就是通过端口扫描，因为常用的服务时使用标准的端口，只要找到相应的端口，就能知道目标主机上运行着什么服务）

2. 什么是网络监听

是一种见识网络状态、数据流程以及网络上信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上锁传输的信息。(或 P39)

3. 简述以太网的网络监听

① 共享以太网；②Sniffer；③交换式网络上的嗅探器　P40~45

4. 如何防范网络监听　P45~46

资料：

1. ARP 欺骗的破绽特征？/防护

ARP 欺骗的特征就是不断的发 arp 包，让被攻击主机相信并修改 arp 表。

使用 wireshark 开启混杂模式后，只需抓取 arp 类型的包，看密集程度。一旦出现攻击态势，就可以快速对攻击和被攻击双方进行定位。

防护时：

1 最理想的防制方法是网络内的每台电脑 ARP 一律改用静态的方式，不过大型的网络是不可行，因为需要经常更新每台电脑的 ARP 表。

2 使用例如 DHCP snooping，网络设备可借 DHCP 保留网络上各电脑的 MAC 地址，在伪造的 ARP 数据包发出时即可侦测到。

2. 僵尸主机多怎么办？

僵尸主机(沦为肉鸡)是指感染僵尸程序病毒，从而被黑客程序控制的计算机设备。其可以随时按照黑客的命令与控制指令展开 DoS 攻击或发送垃圾信息。一般被侵占的电脑只是僵尸网络里面众多中的一个，会被用来去运行一连串的或远端控制的恶意程序

解决/检测：(特征 发动攻击时突然产生大量网络流量)

事前检测及预防：

- 关闭不必要端口：计算机要与外界进行通信，必须通过一些端口 。 黑客想要成功入侵控制某台电脑，肯定是通过某些端口进行攻击的 。
- 卸载不必要程序：为了方便远程管理，服务器会安装远程管理的软件，如 ： Pcanywhere、 Radmin、VNC 等，但远程管理软件在方便远程管理的同时，也给人们带来了巨大的安全隐患 。
- 定期安全检查及加固：黑客成功入侵，一般是利用了某些安全漏洞，所以必须定期对服务器做安全检查，如 ： 端口扫描 、 弱口令检查 、 合规配置检查 、 系统漏洞扫描 、 Web 漏洞扫描 、渗透测试等 。

事中防御：

- 入侵检测防护设备：入侵检测 / 防护系统是指对计算机系统或网络进行实时监控，一旦发现异常情况后进行告警或阻断 。
- 下一代防火墙：下一代防火墙，是可以全面应对应用层威胁的高性能防火墙 。 通过深入洞察网络流量中的用户 、 应用和内容，并借助全新的高性能单路径异构并行处理引擎 ,NGFW 能够提供有效的应用层一体化安全防护 。
- Web 应用防火墙 WAF：Web 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一种安全防护技术手段 。
- 防恶意代码软件或安全 Agent：服务器安全是系统的最后一道防线，要建立纵深防御体系，服务器安全是必不可少的一环，服务器安通过安装在服务器上的插件和云端防护中心的联动，精准捕获服务器上各种安全事件，对入侵和异常行为进行实时监控告警与拦截，是防止黑客入侵，提升系统安全的一个重要保障 。

事后溯源：

- 网络流量恶意代码检测系统：网络流量恶意代码检测系统部署在 IP 网络中，用于对网络恶意流量进行发现和检测，能够根据预先配置的策略，如恶意流量特征和基于云安全计算平台支撑的特征对恶意流量进行检测，从而发现蠕虫 、 木马 、 僵尸网络和部分攻击的系统 。
- 抗 DDOS 防护设备：DDOS （Distributed Denial of Service） 分布式拒绝服务攻击指通过很多 " 僵尸主机 " 向受害主机发

第四章 拒绝服务攻击

1. 外部用户针对网络连接发动拒绝服务攻击有哪几种模式？举例说明 P57

2. 如何对抗 TearDrop 攻击？

TearDrop 攻击原理 P70。*防御方法*：网络安全设备将接收到的分片报文先放入缓存中，并根据源 IP 地址和目的 IP 地址对报文进行分组，源 IP 地址和目的 IP 地址均相同的报文归入同一组，然后对每组 IP 报文的相关分片信息进行检查，丢弃分片信息存在错误的报文。为了防止缓存益处，当缓存快要存满是，直接丢弃后续分片报文。*反攻击方法*：添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。

3. 如何发现自己正在受到消耗网络资源的 DoS 攻击？

① 服务器主机上有大量等待的 TCP 连接；② 检查网站后台服务器发现大量无用的数据包；③ 一段时期中 IP 请求异常且源地址虚假；④ 网络流量出现异常变化突然暴涨；⑤ 当发现 Ping 超时或丢包严重时，注意连接错误。假如遇到无法访问网站这种情况，并看到类似于“无法访问站点”之类的错误，且无法访问其他 Internet 服务，则可能是 DoS 攻击带来的影响。⑥ 查看自己的邮箱里是否突然收到大量的垃圾邮件。

4. 对付分布式拒绝服务攻击的方法有哪些？举例说明 P76~77

资料：

1. 怎么应对 DDos 攻击(属于黑客中的暴力犯罪)，利用数据包的哪些特征？

攻击发生时的 cap 文件(wireshark 抓包)进行仔细的分析，找出攻击者忽略的地方，找出攻击数据包与正常业务流量中有区别的地方。

1、 使用wireshark 过滤器tcp.flags==0x02 过滤检查数据包分布情况。如图所示，SYN Flood攻击发生时数据包分布发生明显改变，Syn包比例明显增加。

2、 使用wireshark static->ipv4->endpoint分析数据包源地址分布。当使用伪造IP地址的DDoS攻击发生时，抓包文件中的数据包数目和源地址对应关系会发生明显变化。从图中实例可以发现，除了被攻击的目的IP意外，wireshark统计每个源地址对应的数据包数目较小，数据包大小字节数（Bytes）几乎一致。

3、TTL分析发现攻击者的蛛丝马迹。当使用随机源进行DDoS攻击时，虽然使用了伪造源地址进行攻击，但攻击者无法伪造攻击主机与目标主机之间的位置关系。有时候通过观察数据包的TTL值变化，也能够获得攻击者的蛛丝马迹，为攻击防御提供辅助支持。下图所示的这个攻击程序并没有修改攻击数据包的TTL值，所有的攻击数据包使用相同的TTL值。聪明的你可能已经发现了，没错，这个攻击数据包是由局域网内的一个windows计算机发

UDP FLOOD攻击的主要目的是通过发送大量的UDP数据包来堵塞服务器的带宽。同时针对DNS，语音和流媒体等互联网业务，也会有通过UDP承载的应用层攻击出现。图示是著名的蜗牛攻击器产生的攻击数据包，可以明显的看出，这种数据包的payload固定，使用UDP大包进行攻击，同时使用真实源地址进行攻击。

与UDP FLOOD相同，ICMP FLOOD主要以阻塞服务器带宽为主。但与UDP FLOOD不同的是，ICMP通常不会承载数据业务，比较容易通过交换机ACL或者服务器的iptables等进行防御。同时，攻击实施者为了更加有效的利用手上的僵尸主机，会使用包大小较大的数据包和IP层分片的数据包进行攻击，这种攻击会绕过没有设置IP层分配的ACL，也会加重服务器分配重组的负担。值得一提的是，window客户端发出的ping数据包有特定的格式和

除了传统的网络层攻击之外，一些针对特定应用系统比如apache的应用层攻击也能够取得很好的效果。例如CVE-2011-3192 Range header DoS vulnerability Apache HTTPD，是典型的使用应用层漏洞进行DDoS攻击的攻击方法。在这种攻击中，攻击者刻意构造畸形的http头，其中包含了大量重复的range字段。Apach在处理这种http请求时，会不断的进行range重组，最终导致目标系统CPU繁忙而无法响应正常请求。

第五章 缓冲区溢出攻击

1. 什么程序会发生缓冲区溢出

➢ 代码在操作缓冲区时，没有对缓冲区边界进行检查

➢ 使得写入缓冲区的数据量超过缓冲区能够容纳的范围，从而导致溢出的数据改写了与该缓冲区相邻存储单元的内容。

➢ C 语言中许多字符串处理函数如：Strcpy、Strcat、Gets、Sprintf 等都没有对数组越界加以检测和限制

2. 缓冲区溢出攻击的一般目标是什么

（修改程序的返回地址，让它去执行一段精心准备的程序。）

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权。如果该程序具有足够的权限，那么整个主机就被控制了。攻击者必须达到如下的两个目标：

①在程序的地址空间里安排适当的代码；②通过适当的初始化寄存器和内存，让程序跳转到入侵者安排的地址空间执行。

3. 要让程序跳转到安排好的地址空间执行，一般有哪些方法 P83

第六章 程序攻击

1. 逻辑炸弹与病毒有哪些相同点与不同点？

共同点：1）都具有隐蔽性，用户一般不会察觉；2）具有攻击性，发作后会干扰屏幕显示，或降低电脑运行速度，或删除程序，或破坏数据。

不同点：1）病毒具有“传染性”，而逻辑炸弹是没有“传染性”的；2）逻辑炸弹的逻辑条件具有不可控制的意外性，逻辑炸弹本身虽然不具备传播性，但是诱因的传播是不可控的，由于逻辑炸弹还原和清除更加困难。

2. 为什么后来的木马制造者制造出反弹式木马，反弹式木马的工作原理是什么？画出反弹式木马的工作流程图 P134

为什么：随着……反弹式木马；原理：它利用……目的；流程图：图 6-6

3. 嵌入式木马不同于主动型木马和反弹式木马的主要特点是什么？为什么这种木马更厉害，更不易被清除？ 主要特点 P135、137

因为嵌入式木马隐藏于常用的网络程序中，不像另两者会建立新的 Socket 连接，所以杀毒软件难以发现、清除和隔离，多数情况只能手工清除。

4. 木马技术包括哪些，这些技术有什么特点？

①自动启动技术，木马程序第一次运行需要用户来执行，以后会启动系统时候自动装在服务端程序。②隐藏技术，木马程序不同于普通程序的最大特定就是

想尽一切办法隐藏自己。③远程监控技术，木马的最主要功能，也是木马的最终目的。 P140~144

资料：

1. 如何存放/投放逻辑炸弹？

逻辑炸弹可以以软件和硬件形态存在，如操作系统、应用软件、主板、CPU、FPGA 等。例子：

逻辑：硬盘启动/装载时触发 死循环 装载不了

硬盘逻辑炸弹其实是由于硬盘的主引导记录被修改所引起的。因此，要想了解其原理就必须先了解主引导记录。硬盘的主引导记录位于0柱面0磁头1扇区，它是由3部分组成的，其中从0h到1Beh这446个字节称为引导程序；从1Beh到1Feh这64个字节被称为硬盘分区表，一共可容纳4个分区的数据；从1Feh到200h这2个字节被称为自举标志，在启动时BIOS检查用的。后来我们检查被炸硬盘的主引导记录，结果发现：1?引导程序部分被修改了；2?硬盘分区表也被修改了，而且被改成一个循环链，即C盘的下一个分区指向D区，D区的下一个分区又指向C区，这样一直循环下去造成一个死循环；3?自举标志55AA没被修改。

第七章 欺骗攻击

1. 请简述 DNS 的工作原理，并指出在整个 DNS 解析过程中，可能存在的被欺骗攻击的地方

工作原理 P156（DNS 实现……域名服务器）。

可能存在的被欺骗：在当提交给某个域名服务器的域名解析请求的数据包被捕获，然后按截获者的意图将一个虚假的 IP 地址作为应答信息返回给请求者。

2. 假如你的主机正在面临 DNS 欺骗攻击，你打算采取什么解决策略和方案

（①直接用 IP 访问重要的服务，从而避开 DNS 欺骗攻击。②使用自定义的 DNS 服务器并刷新 DNS 解析缓存）

注意 MAC 地址和 IP 地址是否遭到了替换和修改。如果确认 MAC 地址为真，可打开路由器，通过相互对应的 MAC 查找 IP 地址，或将 MAC 地址添加到路由器的安全地址过滤功能当中进行处理并启用，这样有问题的电脑会自动断线。若安装了 ARP 防火墙，一般情况下能够防御大部分攻击，但如果在拥有防火墙的情况下遭到攻击，首先要做的是查出攻击来源，然后将主机系统重新设置并重启。

3. Web 欺骗攻击有哪些具体形式？请简述其原理。 P165~168

4. TCP/IP 是否存在考虑其安全的地方？哪些建议？

TCP/IP 的层次不同提供的安全性也不同，例如，在网络层提供虚拟私用网络，在传输层提供安全套接服务。

物理层安全问题是指由网络环境及物理特性产生的网络设施和线路安全性，致使网络系统出现安全风险，如设备问题、意外故障、信息探测与窃听等。

网络层的主要功能主要用于数据包的网络传输，其中 IP 协议是整个 TCP/IP 协议体系结构的重要基础。IPv4 在设计之初根本没有考虑到网络安全问题，IP 包本身不具有任何安全特性，从而导致在网络上传输的数据包很容易泄漏或受到攻击（如伪造 IP 包地址、拦截、窃取、篡改、重播等）。IPv6 简化了 IPv4 中的 IP 头结构，并增加了对安全性的设计。

传输层主要包括传输控制协议 TCP 和用户数据报协议 UDP,其安全措施主要取决于具体的协议.传输层的安全主要包括:传输与控制安全、数据交换与认证安

全、数据保密性与完整性等。为了保证传输层的安全设计了安全套接层协议 SSL，此协议提供了身份验证、完整性检验和保密性服务。

网络安全性问题主要重点解决的常用应用系统（协议），包括 HTTP、FTP、SMTP、DNS、Telnet 等。

建议：对物理层，由于以太网上存在交换设备并采用广播方式,可能在某个广播域中侦听、窃取并分析信息。为此，保护链路上的设施安全极为重要,物理层的安全措施相对较少，最好采用“隔离技术”将每两个网络保证在逻辑上能够连通，同时从物理上隔断，并加强实体安全管理与维护；对应用层，应注意不下载未经过检验的程序，SMTP 服务器应增加过滤、扫描及设置拒绝指定邮件等功能，可采用防火墙保护 DNS 服务器并阻止各种区域传输。

5. 假如你负责开发、维护和管理某商业网站，面对潜在的 Web 欺骗攻击，你将采取哪些手段避免你的网站受到攻击？ P168

资料：

1. **针对 Email 应用，除了 Email 欺骗，还有哪种攻击方式？**

Email 电子邮件轰炸攻击，见书 P161 P72 存储资源消耗 Dos 攻击

2. **TCP 会话劫持 监听者如何猜测序列号**

书 P170

第八章 漏洞攻击/利用处理程序错误

1. 跳板的作用是什么？

跳板的作用是进行攻击源的隐藏。为了更好地隐蔽自己，一些网络攻击者通常并不直接从自己的系统向目标发动攻击，而是先攻破若干中间系统,让它们成为“跳板”，再通过这些“跳板系统”完成攻击行动。

2. 如何避免多个服务系统之间的连带关系？

3. 简述用 ASP 编写的网站的常见攻击方式有哪些？ P200~206

第九章 访问控制技术

1. 什么是自主访问控制？方法有哪些？ P218/P219

2. 为什么自主访问控制无法抵御特洛伊木马攻击？ P221

3. 口令认证技术的认证方法。哪些方法可提高口令认证技术安全性？ P209

口令认证也成通行字认证，是一种根据已知事物验证身份的方法。需要考虑和规定选择方法，使用期限，字符长度，分配和管理及在计算机系统内的保护等。

提高安全性：每个用户需分配有专用的同行字，系统可知道哪些用户在联机、采用随时间变化的通行字、采用通行短语代替通行字、在通行字后填充随机数。

4. 网络的物理隔离技术包含哪几方面？各自采用了什么样的技术？ P212

5. 什么是基于角色的访问控制技术？它与传统的访问控制技术有何不同？

什么是：（P226）。*不同*：和 DAC、MAC 相比，优点在于：它是一种策略无关的访问控制技术，具有自管理的能力，使得安全管理更贴近应用领域的机构或组织的实际情况。缺点在于：技术不够成熟、较复杂、RBAC 的策略无关性需要用户自己定义适合本领域的安全策略。（P228）

资料：

1. DAC 和 MAC 结合

通常 MAC 与 DAC 结合使用，并实施一些附加的、更强的访问限制。一个主体只有通过自主与强制性访问限制检查后，才能访问其客体。用户可利用 DAC 来防范其他用户对自己客体的攻击，由于用户不能直接改变强制访问控制属性，所以强制访问控制提供了一个不可逾越的、更强的安全保护层，以防范偶然或故意地滥用 DAC。

2. 设置客户端物理隔离过渡区？

双硬盘：一个对应一个网络

单硬盘：单个硬盘上磁道的读写控制技术，在一个硬盘上分隔出两个工作区间 网络安全隔离卡(物理方式 PC 物理层) 在任何时候，数据只能通往一个分区。

数据交换/过渡区：在两个分区以外，在硬盘上另外设置一个功能区，用于不同的状态转换，表现为硬盘的 D 盘，各个分区可以通过功能区作为一个过渡区来交换数据。

3. 网卡、隔离卡区别？

网卡 链路层 类似一个系统 通过不同的网卡 连接不同网段 上内外网

隔离卡 物理层 每次换内外网 需要重启系统 类似双系统

第十章 防火墙技术

1. 防火墙体系结构

（经典）双重宿主主机体系结构、被屏蔽主机体系结构、被屏蔽子网体系结构、（扩展）合并内部和外部路由器、合并堡垒主机和外部路由器、多台内/外部路由器、多个周边网络（见 PPT）

2. 使用应用层代理访问外部 Web 站点时，会出现访问某些经典网站的响应速度较快，而其他站点响应速度较慢，原因何在？

因为代理有缓存功能。会把常用的网站页面缓存下来,所以速度快。不常用的网页要远程读取,所以慢些。

3. 若防火墙允许周边网络上的主机访问内部网络上的任何基于 TCP 协议的服务，而禁止外部网络访问周边网络上的任何基于 TCP 的服务，给出实现思路？

P284~285，图 10-27，编辑规则然后防火墙按要求对数据包进行过滤。

资料：

1. 防火墙指标 内网控制 稳定性 工作原理

防火墙性能衡量：

（一）吞吐量。作为衡量防火墙性能的重要指标之一，吞吐量小会造成网络的瓶颈，从而影响整个网络的性能。性能测试仪测定的是被测设备在不丢包的情况下，正常转发的最大吞吐量。一般选端口的理论最大值（如100%），通过二分算法得出最终不丢包的情况下的最大吞吐

（二）延迟。延迟能力将体现防火墙的数据处理速度。一般延迟是通过按一个固定的持续时间发送帧，每一秒会有一个打了时间戳T1的帧被传输出去，当测试仪收到这个帧时，将完成传输时的时间与帧携带的时间戳T2的比较，从而计算出延时值为T2-T1。考虑时钟同步问题，

（三）丢包率。丢包率对防火墙的稳定性、可靠性有很大影响。一般测试时按初始速率开始发送帧，记录收到的帧数量，如果被测设备不能完全转发，会降低一点速率再次发送，测试会一直持续到防火墙可完全转发为止，最后的结果会显示出各种帧长度的帧丢失情况。丢包率测试是通过发送端向防火墙发送一定数量的测试帧，帧数计为A；接收端在收到数据包后对其进行统计，得出成功转发的数据帧个数为B；则可得丢包率为B/A×100%。

（四）背靠背。该指标能体现出被测防火墙的缓冲能力。通过向被测设备连续发送具有最小帧间隔的N个帧，并统计被测设备转发帧的个数。如果发送帧的个数和转发帧的个数相等，则增加N值，再重复上述测试过程。

（五）最大并发连接数。主要用来测试被测防火墙建立和维持TCP连接的性能。利用性能测试仪测试最大并发连接数时，在服务器上设定一定大小的时延，使服务器和客户端一直保持联接状态，然后使客户端和服务器快速建立大量联接，直到设备达到最大承受的连接数。

（六）最大新建连接速率。主要用来衡量单位时间内防火墙建立和维持TCP连接的能力。利用性能测试仪测试每秒新建联接时，客户端向服务器发起建立联接并请求一个设定好的网页，收到请求的网页立即关闭联接，不断提高建立联接的速率，直到设备中有联接没有成功建立为止。

第十一章 入侵检测技术

1. 某用户平均每天登录 3 次，但是某日突然登录 30 次 异常检测

2. 运行程序后不测试超级用户密码，绑定端口.... 模式匹配

资料：

1. 和防火墙不同？

1) 防火墙：防火墙是设置在被保护网络（本地网络）和外部网络（主要是Internet）之间的一道防御系统，以防止发生不可预测的、潜在的破坏性的侵入。它可以通过检测、限制、更改跨越防火墙的数据流，尽可能的对外部屏蔽内部的信息、结构和运行状态，以此来保护内部网络中的信息、资源等不受外部网络中非法用户的侵犯。
2) 入侵检测系统：IDS是对入侵行为的发觉，通过从计算机网络或计算机的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

防火墙只是被动防御为主，通过防火墙的数据便不再进行任何操作，IDS 则进行主动实时的检测，发现入侵行为即可做出反应，是对防火墙弱点的修补，但可能误报等；防火墙可以允许内部的一些主机被外部访问，IDS 则没有这些功能，只是监视和分析用户和系统活动。

二、 入侵检测系统和防火墙的联系

1. IDS是继防火墙之后的又一道防线，防火墙是防御，IDS是主动检测，两者相结合有力的保证了内部系统的安全；

2. IDS实时检测可以及时发现一些防火墙没有发现的入侵行为，发行入侵行为的规律，这样防火墙就可以将这些规律加入规则之中，提高防火墙的防护力度。

2. IDS 评估标准

TP: True Positive(正确报告) = "正确检测到入侵"

FP: False Positive(误报) = "发出错误的警报"

FN: False Negative(漏报) = "没有检测到实际发生的入侵"

TN: True Negative(正确漏报) = "正确检测到网络完整性"

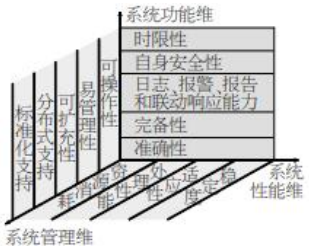
IDS 响应	+ 入侵	−
+	TP	FP
−	FN	TN

图 1 敏感性和特异性

(1) 敏感性(Sensitivity):它反映了正确报告(TP)的比率,也就是IDS正确检测到的入侵次数在实际发生的总入侵次数中所占的比率。敏感性用数学公式表示成 Sensitivity = TP/(TP + FN)。显然,漏报(FN)率 = 1 - 敏感性。IDS的敏感性

(2) 特异性(Specificity)[5]:它反映了系统准确报告的程度。用数学公式表示成 Specificity = TN/(TN + FP)。正确漏报(TN)表示IDS正确报告了没有入侵;误报(FP)则表示IDS错误地发出一次入侵警报(实际上并没有发生入侵),误报(FP)率 = 1 - 特异性。当网络管理员要从海量的报警信息中

准确性：所有检测结果的正确率



系统功能维：反映 IDS 的攻击检测、报告、审计、报警 等能力。

系统性能维：主要是检验 IDS 在不同环境下的承受强度，包括检测引擎的吞吐量、过滤的效率等指标

系统可管理维：主要评估系统用户界面的可用性、完整性、扩充性以及平台的兼容性。

第十二章 VPN

1. 简述 IPSec 中 AH 协议的功能

AH 协议包头可以保证信息源的可靠性和数据的完整性.

2. 简述 IPSec 中 ESP 协议的功能

ESP 可以提供数据的完整性和可靠性.

3. 比较 PPTP 与 L2TP

网络基础

- **PPTP：IP网络**
- **L2TP：面向数据包的点对点的连接**
  - **例如：IP（UDP），虚拟电路、ATM交换电路**

隧道

- **PPTP：单一隧道，不支持隧道验证**
- **L2TP：支持多隧道和隧道验证，不同服务质量创建不同隧道**

压缩头的开销

- **PPTP/L2TP：6/4 byte**