1. 入侵检测系统

1) 基于网络的入侵检测系统

基于网络的入侵检测系统用原始的网络包作为数据源，它将网络数据中检测主机的网卡设为混杂模式，该主机实时接收和分析网络中流动的数据包，从而检测是否存在入侵行为。

基于网络的 IDS 通常利用一个运行在随机模式下的网络适配器来实时检测并分析通过网络的所有通信业务他的攻击辨识模块通常使用四种常用技术来标识攻击标志：模式、表达式或自己匹配；频率或穿越阀值；低级时间的相关性；统计学意义上的非常规现象检测，一旦检测到了攻击行为，IDS 响应模块就提供多种选项以通知，报警并对攻击采取响应的反应，尤其适应于大规模网络的 NIDS 可扩展体系结构，知识处理过程和海量数据处理技术等。

2) 基于主机的入侵检测系统

通常，HIDS 监视分析系统、事件和安全记录。例如，当有文件发生变化时，HIDS 将新的记录条目与攻击标记相比较，看其是否匹配，如果匹配系统就会向管理员报警。在 HIDS 中，对关键的系统文件和可执行文件的入侵检测是主要内容之一，通常进行定期检查校验和，以便发现异常变化。此外，大多数 HIDS 产品都监听端口的活动，在特定端口被访问时向管理员报警。

HIDS 的主要特点如下：

a. 监视特定的系统活动

HIDS 监视用户和访问文件的活动，包括文件访问、改变文件权限，试图建立新的可执行文件或者试图访问特殊的设备。

b. 能够检查到基于网络的入侵检查系统检查不出的攻击

HIDS 可以检测到那些基于网络的入侵检测系统察觉不到的攻击。例如，来自主要服务器键盘的攻击不经过网络，所以可以躲开基于网络的入侵检测系统。

c. 适用于采用了数据加密和交换式连接的子网环境

由于 HIDS 安装在遍布子网的各种丰机上，它们比基于网络的入侵检测系统更加适于交换式连接和进行了数据加密的环境。

d. 有较高的实时性

尽管 HIDS 不能提供真正实时的反应，但如果应用正确，反应速度可以非常接近实时。尽管在从操作系统作出记录到 HIDS 得到检测结果之间的这段时间有一段延迟，但大多数情况下，在破坏发生之前，系统就能发现入侵者，并中止他的攻击。

e. 不需增加额外的硬件设备

HIDS 存在于现行网络结构之中，包括文件服务器，Web 服务器及其他共享资源。这使得基于主机的系统效率很高。

2. TearDrop 攻击

Teardrop 是基于 UDP 的病态分片数据包的攻击方法,其工作原理是向被攻击者发送多个分片的 IP 包(IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息)，某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。(利用 UDP 包重组时重叠偏移（假设数据包中第二片 IP 包的偏移量小于第一片结束的位移，而且算上第二片 IP 包的 Data，也未超过第一片的尾部，这就是重叠现象。）的漏洞对系统主机发动拒绝服务攻击，最终导致主机宕机；对于 Windows 系统会导致蓝屏死机，并显示 STOP 0x0000000A 错误。）

对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。

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。尽可能采用最新的操作系统，或者在防火墙上设置分段重组功能，由防火墙先接收到同一原包中的所有拆分数据包，然后完成重组工作，而不是直接转发。因为防火墙上可以设置当出现重叠字段时所采用的规则。

3. 缓冲区溢出攻击的防范

缓冲区溢出攻击占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的 Internet 用户有机会获

得一台主机的部分或全部的控制权。如果能有效地消除缓冲区溢出的漏洞，则很大一部分的安全威胁可以得到缓解。

有四种基本的方法保护缓冲区免受缓冲区溢出的攻击和影响。

1) 通过操作系统使得缓冲区不可执行，从而阻止攻击者植入攻击代码。
2) 强制写正确的代码的方法。
3) 利用编译器的边界检查来实现缓冲区的保护。这个方法使得缓冲区溢出不可能出现，从而完全消除了缓冲区溢出的威胁，但是相对而言代价比较大。
4) 一种间接的方法，这个方法在程序指针失效前进行完整性检查。虽然这种方法不能使得所有的缓冲区溢出失效，但它能阻止绝大多数的缓冲区溢出攻击。分析这种保护方法的兼容性和性能优势。

4. ARP 欺骗的基本原理及防范措施

ARP 欺骗又称 ARP 毒化（ARP poisoning，网上上多译为 ARP 病毒）或 ARP 攻击，是针对以太网地址解析协议（ARP）的一种攻击技术，通过欺骗局域网内访问者 PC 的网关 MAC 地址，使访问者 PC 错以为攻击者更改后的 MAC 地址是网关的 MAC，导致网络不通。此种攻击可让攻击者获取局域网上的数据包甚至可篡改数据包，且可让网上上特定计算机或所有计算机无法正常连线。

最理想的防制方法是网上内的每台计算机的 ARP 一律改用静态的方式，不过这在大型的网上是不可行的，因为需要经常更新每台计算机的 ARP 表。

另外一种方法，例如 DHCP snooping，网上设备可借由 DHCP 保留网上上各计算机的 MAC 地址，在伪造的 ARP 数据包发出时即可侦测到。此方式已在一些厂牌的网上设备产品所支持。

有一些软件可监听网上上的 ARP 回应，若侦测出有不正常变动时可发送邮箱通知管理者。例如 UNIX 平台的 Arpwatch 以及 Windows 上的 XArp v2 或一些网上设备的 Dynamic ARP inspection 功能。

ARP 欺骗的防范方法：一，主机级被动检测：当系统接收到来自局域网上的 ARP 请求时，系统检查请求发送端的 IP 地址是否与自己的 IP 地址相同，如果相同则说明该网络上另有一台机器与自己具有相同的 IP 地址，可以拒绝该 ARP 请求；二，主机级主动检测：主机定期向所在局域网发送查询自己 IP 地址的 ARP 请求报文。如果能够收到另一 ARP 响应报文，则说明该网络上另有一台机器与自己具有相同的 IP 地址。三，服务器级检测：当服务器收到 ARP 响应时，为了证实它的真实性，根据反向地址解析协议(RARP)可以用从响应报文中给出的源 MAC 地址再生成一个 RARP 请求，它询问这样一个问题：“如果你是这个 MAC 地址的拥有者，请回答你的 IP 地址”。这样就会查询到这个 MAC 地址对应的 IP 地址，比较这两个 IP 地址，如果不同，则说明对方伪造了 ARP 响应报文。四，网络级检测：配置主机定期向中心管理主机报告其 ARP 缓存的内容，这样中心管理主机上的程序就会查找出两台主机报告信息的不一致，以及同一台主机前后报告内容的变化，或者利用网络嗅探工具连续监测网络内主机硬件地址与 IP 地址对应关系的变化以发现隐患。

5. DNS 欺骗

定义： DNS 欺骗就是攻击者冒充域名服务器的一种欺骗行为。 原理：如果可以冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了

使用最新版本的 DNS 服务器软件，并及时安装补丁

关闭 DNS 服务器的递归功能。DNS 服务器利用缓存中的记录信息回答查询请求或是 DNS 服务器通过查询其他服务获得查询信息并将它发送给客户机，这两种查询成为递归查询，这种查询方式容易导致 DNS 欺骗。

保护内部设备：像这样的攻击大多数都是从网络内部执行攻击的，如果你的网络设备很安全，那么那些感染的主机就很难向你的设备发动欺骗攻击。

不要依赖 DNS：在高度敏感和安全的系统，你通常不会在这些系统上浏览网页，最后不要使用 DNS。如果你有软件依赖于主机名来运行，那么可以在设备主机文件里手动指定。

使用入侵检测系统：只要正确部署和配置，使用入侵检测系统就可以检测出大部分形式的 ARP 缓存中毒攻击和 DNS 欺骗攻击。

使用 DNSSEC： DNSSEC 是替代 DNS 的更好选择，它使用的是数字前面 DNS 记录来确保查询响应的有效

性，DNSSEC 还没有广泛运用，但是已被公认为是 DNS 的未来方向。

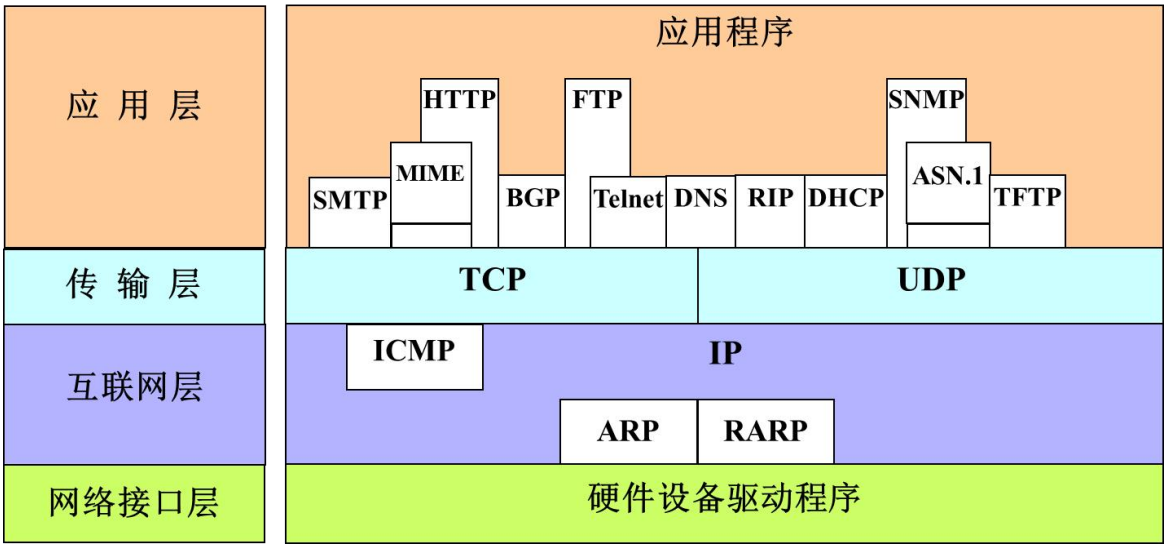
6. IP 欺骗

指行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。按照 Internet Protocol(IP)网络互联协议，数据包头包含来源地和目的地信息。 而 IP 地址欺骗，就是通过伪造数据包包头，使显示的信息源不是实际的来源，就像这个数据包是从另一台计算机上发送的。

IP 欺骗的防范，一方面需要目标设备采取更强有力的认证措施，不仅仅根据源 IP 就信任来访者，更多的需要强口令等认证手段；另一方面采用健壮的交互协议以提高伪装源 IP 的门槛。

有些高层协议拥有独特的防御方法，比如 TCP（传输控制协议）通过回复序列号来保证数据包来自于已建立的连接。由于攻击者通常收不到回复信息，因此无从得知序列号。不过有些老机器和旧系统的 TCP 序列号可以被探得。

7. 协议层次关系



2.1 SSL 连接攻击

Thc-ssl-dos 仅需要少量数据包就会导致相当大的服务器遭受拒绝服务，其工作原理是启动常规 SSL 握手，然后立即请求协商加密密钥，不断重复此服务器资源密集型重新协商请求，知道服务器资源被耗尽。对于 thc-ssl-dos，虽然没有办法完全消除这种攻击漏洞，但是可以利用以下几种方法来缓解：

限制或禁用 SSL 密钥重新协商

为服务器配备 SSL 加速器

3.2 入侵检测系统

OSSIM 即开源安全信息管理系统(OPEN SOURCE SECURITY INFORMATION MANAGEMENT)，是一个非常流行和完整的开源安全架构体系。OSSIM 通过将开源产品进行集成，从而提供一种能够实现安全监控功能的基础平台。 它的目的是提供一种集中式、有组织的、能够更好地进行监测和显示的框架式系统。

OSSEC 是一个运行在 OSSIM 系统中的开源的入侵检测系统，从架构上看它属于 C/S 架构，从功能上看它可以执行日志收集与分析、完整性检测、rootkit 检测、蠕虫检测、Windows 注册表和实时报警等任务。它不仅支持 OSSIM 本身，还可以在 UNIX、Linux、Mac、Windows 系统中运行。由于 OSSEC Server 端就安装在 OSSIM 系统中，并和 iptables 实现了联动功能，因此只需在客户端安装代理即可，也就是通过 OSSEC Server+Agent 方式，以实现 HIDS 系统功能。

4.1 跨站脚本攻击的防范

（一）网站开发者角度

输入验证：某个数据被接受为可被显示或存储之前，使用标准输入验证机制，验证所有输入数据的长度、类型、语法以及业务规则

输出编码：数据输出前，确保用户提交的数据已被正确进行 entity 编码，建议对所有字符进行编码而不仅局限于某个子集

注意黑名单验证方式的局限性：仅仅查找或替换一些字符很容易被 XSS 变种攻击绕过验证机制

警惕规范化错误：验证输入前，必须进行解码及规范化以符合应用程序当前的内部表示方法

（二）网站用户角度

将浏览器的安全级别设置为“高”

增强安全意识，只浏览值得信任的网站或内容

通过检测工具进行 XSS 漏洞检测，若发现漏洞需及时更新、修复

4.2 跨站脚本攻击

1. 反射型 XSS

反射型 XSS 是非持久性、参数型的跨站脚本攻击，这种攻击需要用户点击才能实现。

2. 存储型 XSS

存储型 XSS 又称为持久型跨站脚本攻击，这种 XSS 攻击代码一般存储在网站数据库，当一个页面被用户打开时会执行这些恶意代码。

3. 基于 DOM 的 XSS

通过修改页面的 DOM 节点形成的 XSS，称为基于 DOM 的 XSS，有时候也称为 typeOXSS，当用户能够通过交互修改浏览器页面中的 DOM(Document Object Model)并显示在浏览器上时，就有可能产生这种漏洞，从效果上来说它也属于反射型 XSS。

综合来说，XSS 漏洞存在的原因是没有对用户提交的数据进行严格的过滤处理，相应的处理手段有：

将 html 实体转换为相应的实体编号

将用户提交上来的数据进行 html 编码，将相应的符号转换为实体名称再进行下一步的处理

对数据进行 html encode 处理

过滤或移除特殊的 html 标签，如：<script>,<iframe>,&quot for

过滤 JavaScript 事件的标签

5.1 SQL 注入

SQL 注入是比较常见的网络攻击方法，实现 SQL 注入攻击的基本思路为：寻找到 SQL 注入点->判断服务器类型和后台数据库类型->针对不同的服务器和数据库特点进行 SQL 注入攻击。防御 SQL 注入攻击的主要方法有：

PreparedStatement：采用预编译语句集

使用正则表达式过滤传入的参数

字符串过滤

✧ 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在客户端直接使用 IP Address 访问重要的站点，从而避免 DNS 欺骗;

②对 DNS Server 和 Client 的数据流进行加密，Server 端可以使用 SSH 加密协议，Client 端使用 PGP 软件实施数据加密。