整理（of pcr）

一、概述：

1、硬件软件漏洞例子

硬件：(芯片漏洞植入为主)

一些网络安全人员给电脑的芯片（CPU）刷入恶意的 Firmware 固件，使未经许可的攻击者轻易地进入系统，而电脑管理员本身在系统里却无法发觉，用这种攻击方式的人被称为“硬件黑客”。

软件：(xss 跨站脚本、注入、跨站指令 cookie 等)

一、跨站脚本（XSS）

（一）问题

XSS漏洞是最普遍和最致命的网络应用软件安全漏洞，当一款应用软件将用户数据发送到不带认证或者不对内容进行编码的网络浏览器时容易发生。黑客可以利用浏览器中的恶意脚本获得用户的数据，破坏网站，插入有害内容，以及展开钓鱼式攻击和恶意攻击。

（二）真实案例

恶意攻击者去年针对Paypal发起了攻击，他们将Paypal用户重新引导到另一个恶意网站并警告用户，他们的账户已经失窃。用户们被引导到另一个钓鱼式网站上，然后输入自己的Paypal登录信息、社会保险号和信用卡资料。Paypal公司称，它在2006年6月修复了那个漏洞。

二、注入漏洞

（一）问题

当用户提供的数据被作为指令的一部分发送到转换器（将文本指令转换成可执行的机器指令）的时候，黑客会欺骗转换器。攻击者可以利用注入漏洞创建、读取、更新或者删除应用软件上的任意数据。在最坏的情况下，攻击者可以利用这些漏洞完全控制应用软件和底层系统，甚至绕过系统底层的防火墙。

（二）真实案例

俄罗斯黑客在2006年1月份攻破了美国罗得岛政府网站，窃取了大量信用卡资料。黑客们声称SQL注入攻击窃取了5.3万个信用卡账号，而主机服务供应商则声称只被窃取了4113个信用卡账号。

三、恶意文件执行

（一）问题

黑客们可以远程执行代码、远程安装rootkits工具或者完全攻破一个系统。任何一款接受来自用户的文件名或者文件的网络应用软件都是存在漏洞的。漏洞可能是用PHP语言写的，PHP是网络开发过程中应用最普遍的一种脚本语言。

（二）真实案例

一位青少年程序员在2002年发现了Guess.com网站是存在漏洞的，攻击者可以从Guess数据库中窃取20万个客户的资料，包括用户名、信用卡号和有效期等。Guess公司在次年受到联邦贸易委员会调查之后，同意升级其安全系统。

2、TCP/IP 协议栈面临的五大网络安全问题

1）IP 欺骗

IP Spoof 即 IP 电子欺骗，可以理解为一台主机设备冒充另外一台主机的 IP 地址与其他设备通信。

2）SYN Flooding

SYN Flooding 为 DoS 攻击形式。它利用 TCP 三次握手协议的缺陷，向目标主机发送大量的伪造源地址的 SYN 连接请求，消耗目标主机的资源，从而不能够为正常用户提供服务。

3）ACK Flooding

ACK Flooding 攻击是在 TCP 连接建立之后，所有的数据传输 TCP 报文都是带有 ACK 标志位的，主机在接收到一个带有 ACK 标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在，存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果不合法，例如该数据包所指向的目的端口在本机并未开放，则主机操作系统协议栈会回应 RST 包告诉对方此端口不存在。

4）UDP flooding

UDP Flooding 是日渐猖厥的流量型 DoS 攻击，利用大量 UDP 小包冲击 DNS 服务器，或 Radius 认证服务器、流媒体视频服务器

5）Connection Flooding

Connection Flooding 是利用小流量冲击大带宽网络服务的攻击方式。利用真实的 IP 地址向服务器发起大量的连接，建立连接之后很长时间不释放，占用服务器的资源，造成服务器上残余连接(WAIT 状态)过多，效率降低，甚至资源耗尽，无法响应其他客户所发起的连接。

3、U 盘双击容易中毒原理

就是“autorun.inf 文件”。病毒首先把自身复制到 u 盘,然后创建一个 autorun.inf，当你在插入 U 盘或者双击 u 盘时，autorun.inf 中的设置会运行 u 盘中的病毒。

二、攻击行径

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。

三、网络扫描/侦察技术

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

四、DOS 攻击

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。

例子：

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。

六、处理程序错误攻击

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。

七、欺骗攻击

1、如何识别服务器应答包与虚假包

2、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

3、TCP 会话劫持 监听者如何猜测序列号

书 P170

九、访问控制

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

4、思考题

十、防火墙

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。

十一、入侵检测

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"

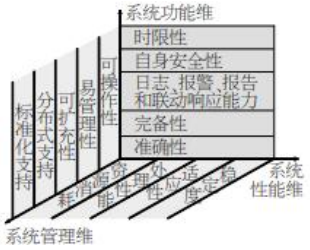
IDS 响应	+ 入侵	−
+	TP	FP
−	FN	TN

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。