**信息安全第1次作业**

小组编号：

本次作业负责人：

1~6题答案：

1. 端口探测技术

1.1 基本概念和原理

端口实际上是一种信息传递的潜在通道，端口扫描就是对每一段端口或者某个指定的端口进行扫描。通过端口扫描不仅可以了解到每台计算机提供的服务项目，还可以及时发现计算机中存在的漏洞。

端口扫描技术的工作原理是当主机向远方的服务器的某一个端口发出建立连接的请求时，如果对方有这项服务，对方就会允许连接，但如果没有此项服务，则无法进行连接。利用这个工作原理，我们不仅可以很快了解到所有熟悉的终端服务器都安装了哪些服务，还可以得到许多与目标主机相关的有使用价值的信息资源。

1.2 端口扫描的几种方式

（1）TCP connect（）扫描方式。这是常用的端口扫描类型，通过对操作系统提供的connect（）函数调用可以连接任意一个目标计算机端口，不需要任何权限，也能够节省单位访问时间。该方式的隐蔽性不够好，很容易被过滤掉。

（2）TCP SYN 扫描方式。这种扫描方式是通过SYN数据包实现的，从技术角度来说属于“半开放”形式。这种扫描方式要有相应的root权限，它克服了隐蔽性差的缺点，而且不易引起计算机监控系统的注意，也不会留下记录。

（3）TCP FIN 扫描： SYN扫描虽然是“半开放”方式扫描，但在某些时候也不能完全隐藏扫描者的动作，防火墙和包过滤器会对管理员指定的端口进行监视，有的程序能检测到这些扫描。相反，FIN数据包在扫描过程中却不会遇到过多问题， 这种扫描方法的思想是关闭的端口会用适当的RST来回复FIN数据包。另一方面，打开的端口会忽略对FIN数据包的回复。这种方法和系统的实现有一定的关 系，有的系统不管端口是否打开都会回复RST，在这种情况下此种扫描就不适用了。另外这种扫描方法可以非常容易的区分服务器是运行Unix系统还是NT系统。

（4）IP 段扫描。IP 段扫描通过一些网络工具就可以轻松地实现，通过扫描工具只需要确定要扫描的IP段，就可以找出这个IP范围内主机通过路由器的状态。由于这种方式并不直接通过 TCP 探测数据包发送，所以隐蔽性很强。

（5）FTP 返回攻击： FTP 协议的一个有趣的特点是它支持代理（proxy）FTP连接，即入侵者可以从自己的计算机 [self.com](http://self.com/) 和目标主机 [target.com](http://target.com/) 的 FTP server-PI(协议解释器)连接，建立一个控制通信连接。然后请求这个server-PI激活一个有效的server-DTP(数据传输进 程)来给Internet上任何地方发送文件。对于一个User-DTP，尽管RFC明确地定义请求一个服务器发送文件到另一个服务器是可以的，但现在这个方法并不是非常有效。这个协议的缺点是“能用来发送不能跟踪的邮件和新闻，给许多服务器造成打击，用尽磁盘，企图越过防火墙”。

1.3 防范措施

（1）关闭闲置和有潜在危险的端口，计算机的一些网络服务会有系统分配默认的端口，将一些闲置的服务关闭掉, 其对应的端口也会被关闭了。也可以设置 “只允许”系统的一些基本网络通讯需要的端口。

（2）检查各端口，有端口扫描的症状时,立即屏蔽该端口，这种预防端口扫描的方式需要借助网络防火墙来实现。

参考文献：

1. 陈瑾. 试论端口扫描与检测技术[J]. 网络安全技术与应用, 2013(12):69-69.
2. 付欣. 计算机网络中端口扫描技术研究[J]. 硅谷, 2013(19):41-42.

二、操作系统探测技术

2.1 基本概念和原理

操作系统识别是进行入侵或安全检测需要收集的重要信息。目前操作系统探测主要有两种方式主动探测和被动探测。主动探测是指主动有目的地向目标系统发送探测数据包通过提取和分析响应数据包的特征信息判断出目标主机的操作系统信息被动探测是指通过网络监听手段从截获的数据包中来分析目标主机的操作系统信息。

2.2 攻击方式

（1）传统的操作系统探测大多是借助一些应用服务直接登录主机的途径来实现的。利用查询DNS服务器的主机信息也可获取登记域名时申请的机器类型和操作系统类型。还可以借助某些主机开放的snmp公共组查询来获取机器类型和操作系统类型。

防御方法：以通过删除某些标志性的信息或者使操作系统故意提供错误的信息来达到自我保护的目的。

（2）基于 ISN的分析。当客户端发起连接的时候，服务器收到客户端的SYN包之后，将回应一个包含初始序列号（ISN）的SYN/ACK响应包。不同的系统，其初始序列号的产生 方式具有不同的规律，根据这些规律可以判断出操作系统的类型。

防御方法：改变初始序列号（ISN）的特征。由于ISN是由tcp\_ init函数确定的，且随着时间的变化而有相对固定或者随机的增加，需要设法改变随机数的生成机制。

（3）基于ICMP数据包的响应。ICMP数据报文可分为两大类：查询报文和差错报文。首先，可以通过发送多种查询报文来捕获目标主机的应答报文进行分析。其次，还可以通过构造某些TCP/UDP报文来使目标主机触发ICMP差错报文，然后根据差错报文的差异来进行辨识。

防御方法：由于这种探测技术是基于ICMP协议，因此可以设置防火墙阻塞所有到达的ICMP数据包来达到防范的效果。此外，大多数情况下，探测时需要利用一个关闭的端口来触发“端口不可达”的ICMP错误消息，那么利用防火墙来屏蔽所有的对外UDP端口也不失为一种较好的防范对策。

（4）基于对RTO的分析借助数据报超时重传RTO ( Retransmission Timeout)机制，可通过分析目标主机在各次重传数据报之间的延迟来判断远程主机操作系统的类型。

防御方法：将主机隐藏于 代理服务器之后或使用防火墙技术来实现SYN代理或SYN网关。

（5）基于TCP数据包的响应。TCP初始化窗口在TCP连接建立的时候，服务器通告的窗口大小有固定的规律。防御方法: 对抗此种扫描方式 ,可以通过修改TCP初始化窗口值来达到隐蔽操作系统类型的目的

参考文献

1. 罗红, 迟强. 操作系统远程探测技术综述[J]. 计算机与信息技术, 2009(5):69-70.
2. 陈家东, 朱建军. 操作系统探测防御方法研究[J]. 电脑开发与应用, 2007, 20(2):4-6.

三、漏洞分析技术

3.1 基本概念和原理

（1）网络协议漏洞：TCP/IP 协议组是目前使用最为广泛的网络互连协议之一。（2）应用软件系统漏洞：任何一种软件系统都或多或少存在一定的脆弱性，安全漏洞可以看作是已知的系统脆弱性。（3）配置不当引起的漏洞：在一些网络系统中忽略了安全策略的制定，即使采取了一定的网络安全措施，但由于系统的安全配置不合理或不完整，安全机制没有发挥作用；或者在网络系统发生变化后，由于没有及时更改系统的安全配置而造成安全漏洞。

3.2 分析方法

漏洞扫描技术主要是从环境错误注入入手，模拟攻击者的攻击行为，根据系统对合法和不合法数据包的回应来探测存在的漏洞。从获取远程主机信息的角度来看，扫描方法 可以分为信息获取和模拟攻击。（1）信息获取：信息获取是通过与目标主机TCP端口建立连接并请求某些服务(如TELNET、FTP、WEB 等)，记录目标主机的应答，从而收集目标系统的信息，根据这些信息来判断目标主机是否存在漏洞。（2）模拟攻击：模拟攻击就是通过模拟攻击者对目标主机实施攻击，比如采用缓冲区溢出、DOS 攻击等攻击方法对目标系统可能存在的已知漏洞进行逐项检查，从而发现系统的漏洞。

参考文献

1. 龚建锋, GongJianfeng. 网络漏洞分析技术研究[J]. 电脑与电信, 2009(9):51-52.
2. 吴世忠, 郭涛, 董国伟, et al. 软件漏洞分析技术进展[J]. 清华大学学报(自然科学版), 2012(10):1309-1319.

四、基于字典的口令破解技术

4.1 基本概念和原理

字典破解是一种简单有效的口令破解方法，字典是根据人们设置备己账号令的习惯总结出来的常用口令列表文件。通过假定字典中的密码是用户选择的密码，对该密码进行特定的哈希操作并和密文进行比较。一个高效的字典在字典破解中具有至关重要的作用。

4.2 防御方法

设置一个好的口令使自己的口令不在字典中，一个好的口令应当至少有8个字符长，不要用个人信息。口令中要有一些非字母字符。

参考文献

1. 刘建. 基于专用字典的密码破解方法研究与应用[D].
2. 冷红生,林闯,王元卓.基于随机Petri网模型的远程口令破解和防御分析[C].//中国计算机学会.第十二届全国petri网理论与应用学术年会论文集.2009:136-139.

五、缓冲区溢出攻击

5.1 基本概念和原理

[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)溢出攻击是利用缓冲区溢出漏洞所进行的攻击行动。缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统关机、重新启动等后果。其特点是，[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)溢出是指当[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA/140338)向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上。理想的情况是：程序会检查数据长度，而且并不允许输入超过缓冲区长度的字符。但是绝大多数程序都会假设数据长度总是与所分配的储存空间相匹配，这就为缓冲区溢出埋下隐患。操作系统所使用的缓冲区，又被称为“[堆栈](https://baike.baidu.com/item/%E5%A0%86%E6%A0%88)”，在各个操作进程之间，指令会被临时储存在“堆栈”当中，“堆栈”也会出现[缓冲区溢出](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA%E6%BA%A2%E5%87%BA/678453" \t "_blank)。

通过向程序的[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的[堆栈](https://baike.baidu.com/item/%E5%A0%86%E6%A0%88)，使程序转而执行其它指令，以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。

5.2 攻击手段

（1）植入法。攻击者向被攻击的程序输入一个字符串，程序会把这个字符串放到[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)里。这个字符串包含的资料是可以在这个被攻击的硬件平台上运行的指令序列。在这里，攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方：[堆栈](https://baike.baidu.com/item/%E5%A0%86%E6%A0%88)（stack，[自动变量](https://baike.baidu.com/item/%E8%87%AA%E5%8A%A8%E5%8F%98%E9%87%8F" \t "_blank)）、堆（[heap](https://baike.baidu.com/item/heap/5156468" \t "_blank)，动态分配的内存区）和静态资料区。

（2）利用已经存在的代码。有时攻击者想要的代码已经在被攻击的程序中了，攻击者所要做的只是对代码传递一些参数。

5.3 防御手段

（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）利用[编译器](https://baike.baidu.com/item/%E7%BC%96%E8%AF%91%E5%99%A8" \t "_blank)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。

（3）在程序[指针](https://baike.baidu.com/item/%E6%8C%87%E9%92%88" \t "_blank)失效前进行完整性检查。它能阻止绝大多数的缓冲区溢出攻击。

（4）强制写正确的代码的方法。

参考文献

1. 钟达夫. 缓冲区溢出攻击语言研究与实现[D]. 广西师范大学.

六、注入类型的攻击

6.1 基本概念和原理

注入攻击是众多攻击之一，在注入攻击中，攻击者给程序提供恶意的输入，解析引擎把恶意输入作为命令或者查询的一部分，并且改变了程序执行的流程。

6.2 攻击方式与防御手段

（1）CSRF注入。全称是跨站请求伪造(cross site request forgery)，指通过伪装成受信任用户的进行访问，通俗的讲就是说我访问了A网站，然后cookie存在了浏览器，攻击者利用用户的cookie进行认证，然后伪造用户发出请求。

防御手段：可以采用token（不存储于浏览器）认证。通过referer识别，HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理。

（2）XSS。全称是跨站脚本攻击（Cross Site Scripting），指攻击者在网页中嵌入恶意脚本程序，将输入的数据变成了代码。XSS是Web程序中常见的漏洞，XSS属于被动式且用于客户端的攻击方式，所以容易被忽略其危害性。其原理是攻击者向有XSS漏洞的网站中输入(传入)恶意的HTML代码，当其它用户浏览该网站时，这段HTML代码会自动执行，从而达到攻击的目的。如，盗取用户Cookie、破坏页面结构、重定向到其它网站等。

（3）SQL注入。所谓SQL注入，就是通过把SQL命令插入到Web[表单](http://baike.baidu.com/view/296684.htm)递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。攻击者注入SQL语句来读取和修改数据库数据，攻击者能执行SQL语句写服务器上的任意文件和甚至执行系统命令。

防御手段：可以使用预编译语句(PreparedStatement)，这样的话即使我们使用sql语句伪造成参数，到了服务端的时候，这个伪造sql语句的参数也只是简单的字符，并不能起到攻击的作用。也可以对密码使用md5进行加密，为了加大破解成本。

参考文献

1. 章明.Web应用程序客户端脚本安全技术研究[D].上海:上海交通大学,2012.
2. 孙国栋. XSS漏洞攻击与防御研究[D]
3. 陈小兵[1], 张汉煜[2], 骆力明[2], et al. SQL注入攻击及其防范检测技术研究[J]. 计算机工程与应用, 2007(11):150-152.

本题分工：

7~13题答案：

七、木马

7.1基本概念和原理

计算机网络中的木马(Trojan),是指隐藏在正常程序中的一-段具有特殊功能的代码，它实质上也是-一种远程控制软件，但它和常规远程控制软件的本质区别:木马是未经用户授权，通过网络攻击或欺骗手段安装到目标计算机中，而常规远程控制软件是用户有意安装的。典型的木马工作原理是:当服务器端在目标计算机上被执行后，木马打开一个默认的端口进行监听，当客户机向服务器端提出连接请求，服务器上的相应程序就会自动运行来应答客户机的请求，服务器端程序与客户端建立连接后，由客户端发出指令，服务器在计算机中执行这些指令，并将数据传送到客户端，以达到控制主机的目的。木马服务器端与客户端之间也可以不建立连接。由于建立连接容易被察觉,因此就要使用ICMP来避免建立连接或使用端口,使用ICMP来传送封包可让数据直接从木马客户端程序送至服务器端。木马客户端与服务器端可以通过中间件通信，从而达到隐蔽通信的效果。

7.2实现方法

传统EXE程序文件木马指的是存在最普遍、以.exe文件运行的木马。这种木马通常是以电子邮件作为载体,将木马伪装成图片、视频等吸引眼球的内容,骗取警惕性差的用户点开附在邮件上的木马,也可以利用捆绑的方式达到植入木马的目的,例如冰河这种以.exe结尾的木马程序文件,这种木马在运行时会产生进程,很容易被杀毒软件发现进而被消除。DLL/.sys木马利用内核驱动或者系统启动作为运行的载体,挂在调用它的程序进程中,不易被杀毒软件查到。在Windows中多数的DLL木马在远程线程技术的支持下将自己挂在系统进程中,只有进程结束运行时木马才会随之停止。还有溢出型木马，这种类型的木马有着多种实现方式和优势,是近阶段涌现的较新的木马类型。程序开发的过程中很容易出现系统漏洞,这时候溢出型木马就会将实现自身功能的shellcode写入缓冲区空间,实现对计算机系统的远程控制。溢出型木马代码量少、寄生性强、隐蔽性好,是一种很难发现和清除的新型木马。

参考文献

1. 商海波. 木马的行为分析及新型反木马策略的研究[D]. 浙江工业大学, 2006.
2. 王超.木马攻击原理及防御技术[J].信息与电脑(理论版),2016

八、蠕虫病毒

8.1基本原理

蠕虫是一种可以自我复制的代码，并且通过网络传播，通常无需人为干预就能传播。蠕虫病毒入侵并完全控制一台计算机之后，就会把这台机器作为宿主，进而扫描并感染其他计算机。当这些新的被蠕虫入侵的计算机被控制之后，蠕虫会以这些计算机为宿主继续扫描并感染其他计算机，这种行为会—直延续下去。蠕虫使用这种递归的方法进行传播，按照指数增长的规律分布自己，进而及时控制越来越多的计算机。

8.2实现方法

网络蠕虫由四个模块组成: 攻击模块、感染模块、传播模块和功能模块, 其中攻击模块和感染模块最为关键, 决定了蠕虫的影响范围和传播速度, 关系到能否对目标主机造成巨大破坏。蠕虫的一般传播过程为:①扫描。由蠕虫的扫描功能负责探测存在漏洞的主机 。当程序向某个主机发送探测漏洞信息并收到成功的反馈信息后, 就得到一个可传播的对象。②攻击。攻击模块自动攻击在第①步中找到的对象,取得该主机的权限(一般为管理员权限)。③现场处理。使计算机在被感染后保留一个后门以便发动分布式拒绝服务攻击。④复制。复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并激活。

扫描主机漏洞是蠕虫传播的前提, 蠕虫传播经常用 ICM P Ping包、TCP SYN、FIN、RST和 ACK包来进行探测[。影响蠕 虫传播的主要因素是如何能快速找到新的目标主机,所以扫描 方法的性能直接决定着蠕虫传播的速度。下面比较几种常用 的扫描方法, 我们主要研究了在一定的地址空间内均匀地扫描 情况, 所以可以使用简单流行病传播模型, 其中没有考虑感染 时的延时。

参考文献

[1] 尹传勇, 刘寿强, 黄伟, et al. 蠕虫病毒深度解析[J]. 计算机安全, 2003(9):73-75.

[2] 翟光群, 张玉凤. 网络蠕虫病毒分析与防范研究[J]. 河南科学, 2005, 23(6):935-937.

[3] 刘晨. 蠕虫病毒的研究与防治[D]. 沈阳工业大学, 2005.

[4] 周然,庹宁.蠕虫病毒的传播原理与防治[J].金融科技时代,2011,(2):93-94.

九、拒绝服务攻击

9.1基本原理

拒绝服务攻击，英文名称是Denial of Service，简称DOS，即拒绝服务,造成其攻击行为被称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽, 最后导致合法的用户请求无法通过。

连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。常用攻击手段有：同步洪流、WinNuke、死亡之PING、Echl攻击、ICMP/SMURF、Finger炸弹、Land攻击、Ping洪流、Rwhod、tearDrop、TARGA3、UDP攻击、OOB等。

DOS攻击方法有 TCP SYN Flood、 ICM P Ping 包攻击、病毒和邮件轰炸、 U DP Flood等。 在目前的 TCP /IP协议体系中 , IP包头中分别 有 4个字节的源 IP地址和目的 IP地址 ,用于标识 网络中的 IP包发出主机和接收主机。现在的互联网 是由路由器将一个个的 IP子网连接起来 ,通过分析 iP包头的目的地址 ,按照路由协议选定的路径上的 端口转发 IP包 ,一般并不分析和检查 IP源地址 ,当目的主机要给发送主机回传信息时 ,就把收到的 IP 包的源地址设为回送 IP包的目的地址。这种网络通 信过程虽然简单、高效 ,但由于不对源地址进行检查 核对 ,使得 IP包源地址欺骗很容易出现 ,即发送者 发出的 IP包的源地址不是该主机的真实地址 ,而是一个虚假地址。攻击者可能利用这种协议上的漏洞 进行拒绝服务攻击。 常见的 TCP SYN Flood攻击正是利用了 TCP /IP协议的缺陷。 TCP协议 ( Transport Control Protocol)是一种面向连接的、可靠的传输层协议 , 一次正常的 TCP传输需要通过在TCP客户端和 TCP服务端建立特定的虚连接来完成 ,该过程是 “三次握手”的过程。

9.2实现方法

客户端主机向服务端提出连接的请求后,服务端作出回应 ,确认收到客户端的请求,然后按照 IP源地址返回 ISN数据包给客户端。客户端收到该包后,向服务端返回 ACK确认信息 ,建立完整的 TCP 连接。通常情况下 ,服务端的操作系统会使用一块 TCP BACKLOG内存来缓存 TCP连接请求队列。 如果这个缓存队列被填满 ,客户新的 TCP连接请求会被丢弃。攻击者利用该特点 ,向服务器发起大量的TCP连接请求,这些请求包的源 IP地址是虚假的、 不可达。当服务器收到这些 IP包并按照包头中的源 地址进行回送时 ,这些回送包的路径不可能到达 ,于 是服务器将不会收到确认信息 ,导致TCP连接不能 完成。在很短的时间内出现大量的这种 TCP半连接 时,会填满整个缓存队列并根本无法清空以响应新 的连接请求,严重时甚至会引起系统崩溃。

参考文献

[1] 李禾,王述洋. 拒绝服务攻击/分布式拒绝服务攻击防范技术的研究[J]. 中国安全科学学报,2009,(01):132-136.

[2] 林梅琴[1], 李志蜀[1], 袁小铃[1], et al. 分布式拒绝服务攻击及防范研究[J]. 计算机应用研究, 2006(8).

[3] 李光灿.浅谈计算机网络系统面临的安全威胁[J].电子世界,2020.

十、钓鱼类型的攻击

10.1基本原理

钓鱼式攻击是一种企图从电子通讯中，通过伪装成信誉卓著的法人媒体以获得如用户名、密码和信用卡明细等个人敏感信息的犯罪诈骗过程。这些通信都声称（自己）来自社交网站拍卖网站\网络银行、电子支付网站\或网络管理者，以此来诱骗受害人的轻信。网钓通常是通过e-mail或者即时通讯进行。它常常导引用户到URL与界面外观与真正网站几无二致的假冒网站输入个人数据。就算使用强式加密的SSL服务器认证，要侦测网站是否仿冒实际上仍很困难。

网钓者目标是针对银行和在线支付服务的客户。理应来自于美国国内税收服务(Internal Revenue service)电子邮件，已被用来收集来自美国纳税人的敏感数据。虽然第一次这样的例子被不分青皂白的寄送，其目的是期望某些收到的客户会泄漏其银行或者服务数据，而最近的研究表明网钓攻击可能会基本上确定潜在受害者会使用哪些银行，并根据结果递送假冒电子邮件。有针对性的网钓版本已被称为鱼叉网钓(spear phishing)。最近几个网钓攻击已经具体指向高层管理人员，以及其他企业大户，而术语“鲸钓”(whaling)一辞被创造出来描述这类型的攻击。

10.2实现方案

10.2.1链接操控

大多数的网钓方法使用某种形式的技术欺骗，旨在使一个位于一封电子邮件中的链接（和其连到的欺骗性网站）似乎属于真正合法的组织。拼写错误的网址或 使用子网域是网钓所使用的常见伎俩。在下面的网址例子里，http://www.您的银行.范例.com/，网址似乎将带您到“您的银行”网站的“示例” 子网域;实际上这个网址指向了“示例”网站的“您的银行”（即网钓）子网域。另一种常见的伎俩是使锚文本链接似乎是合法的，实际上链接导引到网钓攻击站点。另一种老方法是使用含有 '@' 符号的欺骗链接。原本这是用来作为一种包括用户名和密码（与标准对比）的自动登入方式。例如，可能欺骗偶然造访的网民，让他认为这将打开上的一个网页，而它实际上导引浏览器指向上的某页，以用户名该页面会正常开启，不管给定的用户名为何。这种网址在 Internet Explorer 中被禁用，而 Mozilla Firefox 与 Opera 会显示警告消息，并让用户选择继续到该站浏览或取消。还有一个已发现的问题在网页浏览器如何处理国际化域名 （International Domain Names，下称IDN），这可能使外观相同的网址，连到不同的、可能是恶意的网站上。尽管人尽皆知该称之为的IDN欺骗 或者同形异义字攻击的漏洞，网钓者冒着类似的风险利用信誉良好网站上的网域名称转址服务来掩饰其恶意网址。

10.2.2过滤器规避

网钓者使用图像代替文本，使反网钓过滤器更难侦测网钓电子邮件中常用的文本。

10.2.3网站伪造

一旦受害者访问网钓网站，欺骗并没有到此退出。一些网钓诈骗使用 JavaScript 命令以改变地址栏。这由放一个合法网址的地址栏图片以盖住地址栏，或者关闭原来的地址栏并重开一个新的合法的URL达成。攻击者甚至可以利用在信誉卓著网站自己的脚本漏洞对付受害者。这一类型攻击（也称为跨网站脚本）的问题尤其特别严重，因为它们导引用户直接在他们自己的银行或服务的网页登入，在这里从网络地址到安全证书的一切似乎是正确的。而实际上，链接到该网站是经过摆弄来进行攻击，但它没有专业知识要发现是非常困难的。这样的漏洞于2006年曾被用来对付PayPal。还有一种由RSA信息安全公司发现的万用中间人网钓包，它提供了一个简单易用的界面让网钓者以令人信服地重制网站，并捕捉用户进入假网站的注册表细节。为了避免被反网钓技术扫描到网钓有关的文本，网钓者已经开始利用 Flash 构建网站。 这些看起来很像真正的网站，但把文本隐藏在多媒体对象中。

10.2.4电话网钓

并非所有的网钓攻击都需要个假网站。声称是从银行打来的消息告诉用户拨打某支电话号码以解决其银行帐户的问题。一旦电话号码（网钓者拥有这支电话，并由IP电话服务提供）被拨通，该系统便提示用户键入他们的账号和密码。话钓 (Vishing，得名自英文 Voice Phishing，亦即语音网钓）有时使用假冒来电ID显示，使外观类似于来自一个值得信赖的组织 。

10.2.5热点网钓

网络黑客在公共场所设置一个假Wi-Fi热点，引人来连接上网，一旦用户用个人电脑或手机，登录了黑客设置的假Wi-Fi热点，那么个人数据和所有隐私，都会因此落入黑客手中。你在网络上的一举一动，完全逃不出黑客的眼睛，更恶劣的黑客，还会在别人的电脑里安装间谍软件，如影随形。

10.2.6隐蔽漏洞

2014年5月，新加坡南洋理工大学壹位名叫王晶(Wang Jing)的物理和数学科学学院博士生，发现了OAuth和OpenID开源登录工具的"隐蔽重定向漏洞"(英语：Covert Redirect）。攻击者创建一个使用真实站点地址的弹出式登录窗口——而不是使用一个假的域名——以引诱上网者输入他们的个人信息。黑客可利用该漏洞给钓鱼网站“变装”，用知名大型网站链接引诱用户登录钓鱼网站，壹旦用户访问钓鱼网站并成功登陆授权，黑客即可读取其在网站上存储的私密信息。

参考文献

[1] 彭文波. 2005年热门：钓鱼式攻击剖析[J]. 计算机安全, 2005(9):60-62.

[2] 张建国. 全面解析“网络钓鱼”式攻击[J]. 计算机与网络, 2014(17).

1. 张国战. 网络钓鱼的攻击方式与识别技术[J]. 价值工程, 2013(34):164-165.
2. 池亚平, 凌志婷, 许萍, et al. 鱼叉式网络钓鱼攻击检测方法[J]. 计算机工程与设计, 2018, 39(11):58-63.

十一、网络嗅探技术

11.1基本原理

嗅探器（Sniffer）最初是作为网络管理员检测网络通信的一种工具，它既可以是软件，又可以是一个硬件设备。软件Sniffer应用方便，针对不同的操作系统平台都有多种不同的软件Snif-fer，而且很多都是免费的；硬件Sniffer通常被称作协议分析器，其价格一般都很高昂。

在局域网中，由于以太网的共享式特性决定了嗅探能够成功。因为以太网是基于广播方式传送数据的，所有的物理信号都会被传送到每一个主机节点，此外网卡可以被设置成混杂接收（Promiscuous），这种模式下，无论监听到的数据帧目的地址如何，网卡都能予以接收。而TCP/IP协议栈中的应用协议大多数明文在网络上传输，这些明文数据中，往往包含一些敏感信息（如密码、账号等），因此使用Sniffer可以悄无声息地监听到所有局域网内的数据通信，得到这些敏感信息。同时Sniffer的隐蔽性好，它只是“被动”接收数据，而不向外发送数据，所以在传输数据的过程中，根本无法觉察到有人监听。当然，Sniffer的局限性是只能在局域网的冲突域中进行，或者是在点到点连接的中间节点上进行监听。

在交换网络中，虽然避免了利用网卡混杂模式进行的嗅探。但交换机并不会解决所有的问题，在一个完全由交换机连接的局域网内，同样可以进行网络嗅探。主要有以下三种可行的办法：MAC洪水（MACFlooding）、MAC复制（MAC Duplicating）、ARP欺骗，其中最常用的是ARP欺骗。

11.2基本方法

11.2.1MAC洪水

交换机要负责建立两个节点间的“虚电路”，就必须维护一个交换机端口与MAC地址的映射表，这个映射表是放在交换机内存中的，但由于内存数量的有限，地址映射表可以存储的映射表项也有限。如果恶意攻击者向交换机发送大量的虚假MAC地址数据，有些交换机在应接不暇的情况下，就会像一台普通的Hub那样只是简单地向所有端口广播数据，嗅探者就可以借机达到窃听的目的。当然，并不是所有交换机都采用这样的处理方式，况且，如果交换机使用静态地址映射表，这种方法就失灵了。

11.2.2MAC复制

MAC复制实际上就是修改本地的MAC地址，使其与欲嗅探主机的MAC地址相同，这样，交换机将会发现，有两个端口对应相同的MAC地址，于是到该MAC地址的数据包将同时从这两个交换机端口发送出去。这种方法与后面将要提到的ARP欺骗有本质的不同，前者是欺骗交换机，后者是毒害主机的ARP缓存而与交换机没有关系。

但是，只要简单设置交换机使用静态地址映射表，这种欺骗方式也就失效了。

11.2.3ARP欺骗

按照ARP协议的设计，为了减少网络上过多的ARP数据通信，一台主机，即使受到的ARP应答并非自己请求得到的，它也会将其插入到自己的ARP缓存表中，这样，就造成了“ARP欺骗”的可能。如果黑客想探听同一网络中两台主机之间的通信，他会分别给这两台主机发送一个ARP应答包，让两台主机都

“误”认为对方的MAC地址是第三方的黑客所在的主机，这样，双方看似“直接”的通信连接，实际上都是通过黑客所在的主机间接进行。黑客一方面得到了想要的通信内容，另一方面，只需要更改数据包中的一些信息，成功地做好转发工作即可。在这种嗅探方式中，黑客所在主机是不需要设置网卡的混杂模式的，因为通信双方的数据包在物理上都是发给黑客所在的中转主机的。

参考文献

[1] 王晓薇. 网络嗅探技术[J]. 微计算机信息, 2003(11):80-81.

[2] 蔡林. 网络嗅探技术在信息安全中的应用[J]. 计算机时代, 2008(6):16-18.

[3] 高强[1]. 探析网络嗅探技术[J]. 农业网络信息, 2012(5):84-86.

[4] 杨明涛. 基于嗅探技术的网络监控系统设计与实现[D]. 中南大学, 2007.

1. 李莹, 张俊杰. 谈网络嗅探技术的实现[J]. 中国科技信息, 2006(1):50-51.

十二、跨站攻击技术

12.1基本原理

Internet 上的所有动态网站都会允许用户向网络提交各种各样输入的信息. 但是由于用户输 入信息的不可预见性,就造成了入侵者可以通过正常的动态输入而向网站注入不正常的恶意代码,这就是跨 站脚本攻击,也称为 CSS 攻击或 XSS 攻击[ 1 ](为区别网页设计中的 CSS 分层样式表而特别设立). 这种入侵 方式的基本原理就是入侵者在远程的 WEB 页面的 HTML 代码中写入特殊的字符串. 当用户浏览此页面 时,嵌入页面中的这些字符就会被作为一段脚本代码而执行. 从而起到入侵客户主机进行破坏的目的。

造成跨站攻击的主要原因, 是由于网站服务器端的程序, 对客户的输入没有进行有效的验证而产生 的.入侵实现的方法很多, 例如在网站登记个人信息处或者在网站的留言处、 再或者在论坛中发帖时, 总 之只要是能够输入信息, 并能够被保存至网站服务器当中就可实现入侵. 入侵的主要方式是在网站的信息录入框构造一段 Script 程序代码, 只要网页程序设计时没有对用户输 入的数据, 如 “<”、“>”、“/”、 空格等字符进行有效的过滤, 代码就可以成功的写入到网站服务器中而 等待执行的机会. 例如某网站的留言界面如下, 在其相关输入框内输入相关信息, 在内容一栏中输入< iframe src=http : //www . taobao.com/width =300 height=500 >< /iframe>, 其它输入框内容任意, 提交信息后提 示为信息已保存.但是在后台打开相关留言信息后可发现, 留言内容处已被淘宝网的网页的所代替 (图 2 所示) , 这说明语句已嵌入服务器, 入侵已成功.现在如果将一段网页木马的真实地址接在 “src=” 后 面, 而不是接淘宝的网页, 并且将页面的框架隐蔽起来, 则木马就被神不知鬼不觉的注入了。

12.2实现方法

12.2.1 Reflection 跨站脚本攻击

在这种攻击模式下，攻击者是对攻击，用户实施诱骗来让攻击用户点击链接，进而对用户进行攻击。 当被攻击的用户在正常情况下登录网站之后，在登录过程中所 产生的小型文本文件会含有一些会话的标识内容。在被攻击用 户登录完成之后，攻击者会向用户发送链接，进而诱导被攻击 用户进行点击。如果被攻击用户点击这一链接之后，攻击者所 编写的跨站脚本会变成一种请求参数，进而被上传到带有跨站 脚本漏洞的网页服务器之中。由于服务器无法正常识别这种信 息，会将其当做简单的文本进行返回，当被攻击用户的浏览器 将攻击者所编写的跨站脚本进行执行操作后，被攻击者的信息 就会传到攻击者手中，使攻击者完成信息盗取。

12.2.2 Stored 跨站脚本攻击

这是一种与上述第一种跨站脚本攻击类型有很 大不同的攻击形式。在实施这种攻击类型之后，攻击者需要向 网页提交两次请求，第一主要是构造跨站脚本，将其发送至网 页的服务器之上进行保存，第二次是攻击者将自己伪装成为被 攻击者发送请求，使被攻击者所使用的浏览器能够执行这些脚 本。这一种攻击模式也是在被攻击用户登录网站之后，让用户 自主浏览带有脚本攻击内容的页面，网站将这一页面内容返回 给被攻击的用户之后，被攻击代表用户就会进行自动加载跨站 脚本攻击中的代码，将被攻击的用户的信息传送给攻击者。

参考文献

[1] 王凤利, 高希云. CSS跨站攻击技术的分析与检测防范措施研究[J]. 河北北方学院学报：自然科学版, 2011(1):57-58.

[2] 刘建亮,乔兴华.跨站脚本攻击及防范方法研究[J].科学技术创新,2020.

十三、APT攻击

13.1基本原理

APT 攻击是指精通复杂技术的攻击者利用多种攻击手段，借 助丰富资源，在目标组织的信息技术基础设施内部建立和扩 大立足点，为的是窃取数据(如将数据从内网输送到外网)， 执行或阻止一项任务、程序，或者潜入对方架构中伺机进行偷 取数据;会在长时间内反复攻击，和防御者维持交互从而能够执行它的命令，并且会应对防御者的反抗而采取相应对策。 APT 攻击的主要目的是获取高价值机密信息或者破坏目 标系统，是一种网络间谍行为。杜跃进等［2］认为 APT 攻击的 本质是非常有目标的攻击，它并没有固定的方法， APT 攻击不 一定要用社会工程学、零日漏洞、未知恶意代码和加密通信， 其本质在于目的非常明确。如果目标系统的安全水平在不断 提高，攻击者便会不断尝试，这时候就体现出了持续性，而为 了达到持续进攻，必须隐蔽地行动。APT 攻击的特征可归纳 为以下三点: 针对性——通常针对特定目标的重要价值资产，一般军 工、能源、金融、政府最容易遭到 APT 攻击。并且针对收集到 的常用软件、常用防御策略与产品、内部网络部署等信息，攻 击者能编写可以绕过目标系统现有防护体系检查的攻击代 码。 持续性——为了长期控制重要目标获取更多利益，攻击 者通过隐藏实现长期潜伏，同时攻击处于动态发展以应对新 的系统漏洞及防御体系的更新，并通过外部被控制的命令与 控制(Command and Control， C＆C)服务器与目标系统保持通 信以及传输数据。 隐蔽性——为了避免被安全防护系统检测到， APT 攻击代码的编写者使用了各种伪装、隐藏手段，通过修改系统程 序，隐藏病毒进程、隐藏文件、隐藏目录的方式实现长期潜伏; 通过对恶意程序压缩、加密、变体及加壳等技术手段降低其被 检测到的概率;运用动态域名解析实现 C＆C 服务器的隐藏与 长期生存;通过合法的加密数据通道、加密技术或信息隐藏技 术隐蔽地传输数据。

13.2实现方法

典型的 APT 攻击，通常会通过如下途径入侵到网络当中： 1）通过 SQL 注入等攻击手段突破面向外网的 Web Server； 2）通过被入侵的 Web Server 做跳板，对内网的其他服 务器或桌面终端进行扫描，并为进一步入侵做准备； 3）通过密 码爆破或者发送欺诈邮件，获取管理员帐号，并最终突破 AD 服务器或核心开发环境； 4）被攻击者的私人邮箱自动发送邮 件副本给攻击者； 5）通过植入恶意软件，如木马、后门、 Downloader 等恶意软件，回传大量的敏感文件（WORD、PPT、 PDF、CAD 文件等）； 6）通过高层主管邮件，发送带有恶意程序 的附件，诱骗员工点击并入侵内网终端。

[1] 贺诗洁, 黄文培. APT攻击详解与检测技术[J]. 计算机应用, 2018, 38(S2):175-178+187.

[2] 张帅. 对APT攻击的检测与防御[J]. 信息安全与技术, 2011(9):125-127.

[3] 陈剑锋, 王强, 伍淼. 网络APT攻击及防范策略[J]. 信息安全与通信保密, 2012(7).

本题分工：