网络安全 – 网络攻击行径分析

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾

网络安全 - 概述

- 网络安全
- 信息系统安全
- 安全策略及其原则

- 安全策略的特点?
- PDRR, PPDR区别?
- 信息安全的目标?
- 网络安全，信息安全的区别?
- 网马，远程攻击的区别?

攻击类型

攻击步骤及技巧

攻击类型

攻击步骤及技巧

攻击类型 - 章节分解

1. 攻击事件
2. 攻击分类
3. 攻击动机

攻击事件 - 1

攻击动机

- 恶作剧
- 恶意破坏
- 商业目的
- 政治军事

安全威胁

- 外部攻击、内部攻击和?

攻击分类

- 破坏型攻击
- 利用型攻击
- 信息收集型攻击
- 网络欺骗攻击
- 垃圾信息攻击

攻击事件 - 2

外部攻击

- **登录情况**

内部攻击

- **试图连接特定文件内容**

较高特权的内部攻击

- **调查操作审计功能的操作**

攻击分类

破坏型攻击

- 以破坏对方系统为主要目标
- 其中，病毒攻击、DoS是最常见手段

利用型攻击

- 直接对目标计算机进行控制的攻击
- 一旦被控制，涉及信息窃取、篡改等

信息收集型攻击

- 不对目标本身造成危害，被用来为进一步入侵提供有用信息

破坏型攻击

产生大量无用突发流量，降低网络性能

利用协议特征，发送超出目标主机处理能力的“正常”服务请求

利用系统漏洞，发送特殊否早的数据报文，导致瘫痪

针对系统漏洞，在目标系统编制破坏程序或特殊系统操作

破坏型攻击 - Ping of Death - 1

ICMP全称是Internet Control Message Protocol (网际控制信息协议)。

控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。

它属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。

当遇到IP数据无法访问目标、IP路由器无法按当前的传输速率转发数据包等情况时，会自动发送ICMP消息。

破坏型攻击 - Ping of Death - 2

根据有关IP协议规定的RFC791，占有16位的总长度控制字确定了IP包的总长度为65535字节，其中包括IP数据包的包头长度。

Ping of death攻击发送超大尺寸的ICMP数据包，使得封装该ICMP数据包的IP数据包大于65535字节，目标主机无法重新组装这种数据包分片，可能造成缓冲区溢出、系统崩溃。

IGMP?

破坏型攻击 - ICMP Flood

攻击者向一个子网的广播地址发送多个ICMP Echo请求数据包。并将源地址伪装成想要攻击的目标主机的地址。

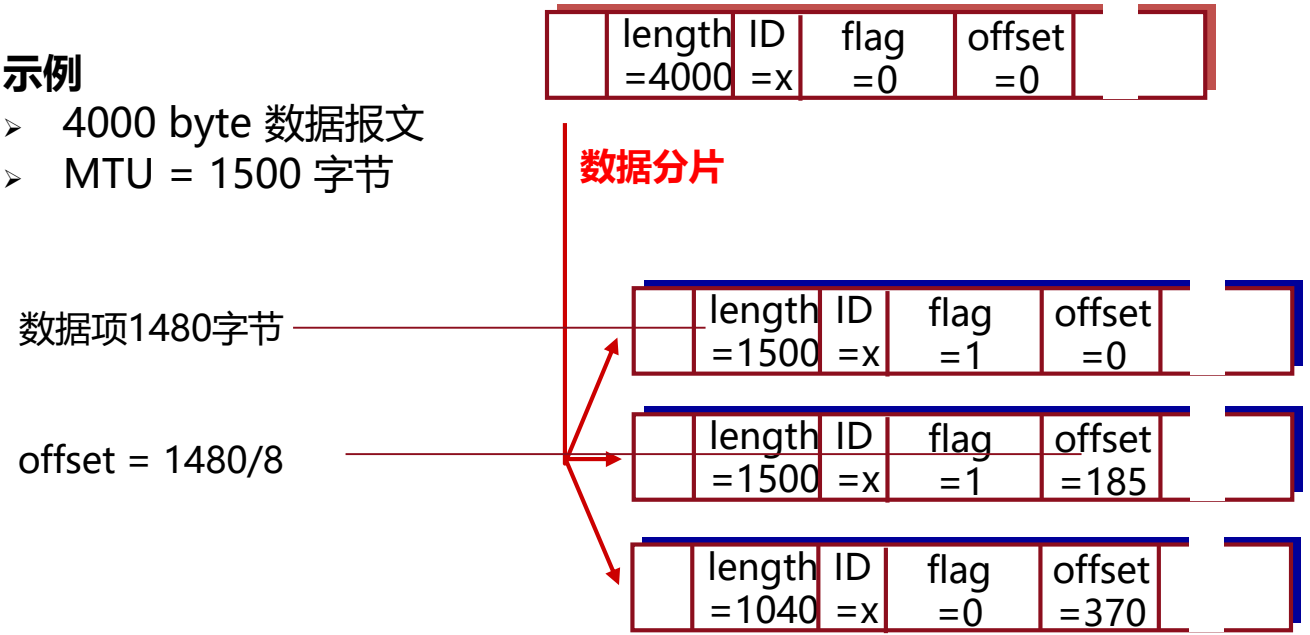
然后该子网上的所有主机均会对此ICMP Echo请求包作出答复，向被攻击的目标主机发送数据包，使此主机受到攻击，导致网络阻塞。

ICMP实质是控制信息协议，攻击者利用ICMP获取主机信息，时间、路由信息等。

破坏型攻击 – Teardrop - 2

示例

- 4000 byte 数据报文
- MTU = 1500 字节



破坏型攻击 – Teardrop - 2

Teardrop攻击是一种畸形报文攻击。

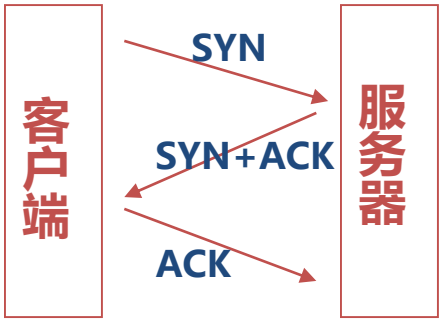
是基于UDP的病态分片数据包的攻击方法

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。

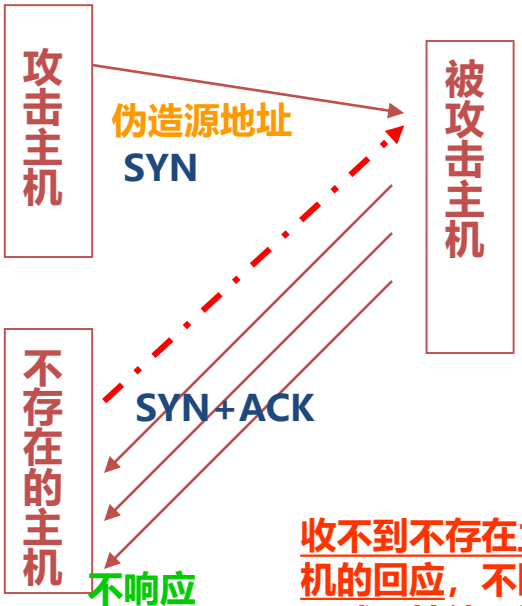
破坏型攻击 - SYN Flood

正常的TCP/IP三次握手



握手完成，开始传送数据，系统消耗很少

SYN Flood攻击



收不到不存在主机的回应，不断重试及等待，消耗系统资源

其他攻击

Land攻击

- 构造SYN包，源地址、目的地址均为攻击目标。

Fraggle攻击

- 基于UDP发送伪造来源的包，类似SYN Flood攻击

畸形攻击

- 没有针对收到消息的错误效验，导致处理时发生崩溃

破坏型攻击 – 总结

通过网络远程操作

- **突发流量、网络协议、软件漏洞**

通过本地操作

- **系统漏洞**

利用型攻击

口令猜测

- 通过网络通信监听或收集账号，获取口令

特洛伊木马

- 秘密安装程序，远程控制目标系统

缓冲区溢出

- 破坏程序运行堆栈，转而执行其他预设指令

信息收集型攻击

扫描技术

- **地址扫描**
- **端口扫描**
- **反响映射**
- **慢速扫描**
- **漏洞扫描**

体系结构探测

- **通过将响应与数据库中的已知响应对比，攻击者可确定目标主机的操作系统等**

利用信息服务

- **DNS域转换**
- **Finger服务**
- **LDAP服务**

利用信息服务

DNS协议不对转换信息进行身份认证。针对DNS服务器，攻击者只需实施一次与转换操作，就能得到所有的主机名称和对应IP地址

Finger服务是互联网最古老协议之一，主要提供站点及用户的基本信息。利用Finger可查询到站点上的在线用户清单

Lightweight Directory Access Protocol (LDAP) 服务，以树形结构存储网络内部及其用户信息。一般利用LDAP客户端进行信息窃取

网络欺骗攻击

DNS欺骗攻击

- **把用户引向攻击者自己主机**

电子邮件欺骗

- **伪装成内部发件者，附带木马链接或者附件**

Web欺骗

- **钓鱼网站**

IP欺骗

- **基于源IP地址、认证访问等攻击**

攻击的动机

- 偷取国家机密
- 商业竞争行为
- 内部员工对单位的不满
- 对企业核心机密的企望
- 网络接入帐号、信用卡号等金钱利益的诱惑
- 利用攻击网络站点而出名
- 对网络安全技术的挑战
- 对网络的好奇心

攻击类型

攻击步骤及技巧

攻击步骤及技巧 - 章节分解

1. 攻击目的
2. 攻击步骤
3. 攻击基本机巧

攻击目的

攻击性质

- **破坏**
- **入侵（需要获取一定权限，建立跳板远程操作）**

攻击目的

- **破坏目标工作**
- **窃取目标信息**
- **控制目标机器**
- **利用假消息欺骗对方**

攻击的步骤

一般的攻击都分为三个阶段：

- 攻击的准备阶段
- 攻击的实施阶段
- 攻击的善后阶段

攻击准备阶段

确定攻击目的

准备攻击工具

- **熟悉的工具, 多种工具组合**

收集目标信息

- **操作系统， 版本号，端口**

攻击实施阶段

隐藏自己的位置

- 盗用他人IP

利用收集到的信息获取账号和密码，登录主机

利用漏洞或者其它方法获得控制权，并窃取网络资源和特权

攻击善后阶段

日志相关的处理 为什么?

Windows

- 禁止日志审计，清除事件日志，清除Internet Information Services (IIS)服务日志

Unix

- messages、lastlog、loginlog、sulog、utmp、utmpx、wtmp、wtmpx、pact

为了下次攻击的方便，攻击者都会留下一个后门，充当后门的工具种类非常多，最典型的是木马程序

攻击基本技巧 - 1

口令入侵

- **获取账号：Finger，X.500，电子邮件地址，默认账号习惯**
- **获取密码：网络监听，Bruce，漏洞与失误**

特洛伊木马程序

WWW欺骗

电子邮件攻击

- **电子邮件轰炸 ， 电子邮件欺骗**

攻击基本技巧 - 2

黑客软件

- **Back Orifice2000、冰河**

安全漏洞攻击

- **Outlook，IIS，Serv-U**

对防火墙的攻击

- **Firewalking、Hping**

渗透

路由器攻击

中间人攻击

常用攻击工具

网络侦查工具

- superscan，Nmap

拒绝服务攻击工具

- DDoS攻击者 1.4, sqldos, Trinoo

木马

- BO2000，冰河，NetSpy

课后习题

1. 简述破坏型攻击的原理及其常用手段

2. 简要叙述攻击的一般过程及注意事项

3. 简述IP欺骗

4. 为什么要进行攻击善后?

谢谢!