



源耗尽,无法响应其他客户所发起的连接。

### 3.5 HTTP Get 攻击

这种攻击主要是针对存在 ASP、JSP、PHP、CGI 等脚本程序,特征是和服务端建立正常的 TCP 连接,并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用。这种攻击的特点是可以绕过普通的防火墙防护,可通过 Proxy 代理实施攻击,缺点是攻击静态页面的网站效果不佳,会暴露攻击者的 IP 地址。

### 3.6 UDP DNS Query Flood 攻击

UDP DNS Query Flood 攻击采用的方法是向被攻击的服务器发送大量的域名解析请求，通常请求解析的域名是随机生成或者是网络世界上根本不存在的域名，域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成 DNS 服务器解析域名超时。

## 4 DDoS 攻击检测及防范

DDoS 通过发送海量数据包淹没目标主机,耗尽目标主机的带宽与资源。DDoS 攻击在手段上更为隐蔽,成功率也更高,使得对其的检测十分困难,也更难以防范。

#### 4.1 DDoS 攻击的检测

当网络的通讯量突然急剧增长,及时检测网络的通讯状况;当发现大量 TCP 和 UDP 数据包通过或内容可疑时都要留神。及时分析情况,防患于未然,做好系统漏洞安装,通过扫描工具发现并删除可疑程序。

## 4.2 DDoS 攻击的防范

针对于 DDoS 攻击具有隐蔽性,我们要加强安全防范意识,提高网络系统的安全性。可采取的安全防御措施有以下几种:

- 1) 确保服务器的系统文件是最新的版本,并及时更新系统补丁,关闭不必要的服务。
- 2) 限制同时打开的 SYN 半连接数目,缩短 SYN 半连接的 time out 时间。
- 3) 正确设置防火墙,认真检查网络设备和主机/服务器系统的日志。

预防和控制 DDoS 不是某一方面的力量单独可以完成的,需要 ISP、用户及中间各环节的通力合作。虽然目前没有办法从根本上解决 DDoS 攻击问题,但是我们可以尽量减少 DDoS 攻击的发生,或者将 DDoS 所产生的危害尽量减至最小。

## 参考文献:

- [1] 杨学良, 张占军. 分布式多媒体计算机系统教程[M]. 电子工业出版社, 2006.
- [2] 刘利, 苏德富. 基于路由器的 DDOS 攻击防御系统的设计[J]. 计算机应用, 2008(8).
- [3] 曹爱娟, 刘宝旭, 许榕生. 抵御攻击的陷阱系统 DDOS[J]. 计算机工程, 2007(1).

(上接第 2372 页)

并行工程与协同设计思想已经渗透到制造业的各个层面,制造业全球化的进程也正在加速。如何使地理上分布于世界各地的设计、工艺以及制造人员参与到产品装配设计及验证过程中来,是虚拟装配需要解决的问题。因此,建立基于 Internet 的协同虚拟环境是虚拟装配的发展方向之一。

#### 4 虚拟装备配网路环境

在 VRML 与 ASP 技术的支持下,虚拟装配系统在网络方面的应用有着广阔的适用面。VRML 文件本身就是一种在网络上创建逼真的三维虚拟场景的工具,更由于 VRML 文件格式的体积小,使得它在网络上传输的数据量大大减少,而且把立体的动画生成放在本地,当用户在虚拟世界中浏览漫步时,依靠的只是本地主机的性能,在目前低带宽的 Internet 上就可以实现虚拟三维场景的传输、显示以及交互。同时,ASP 这种动态网页生成技术使虚拟装配系统与 Web 服务器实现信息的通信,完成数据库的查询工作。VRML 与 ASP 的良好结合方式,为虚拟装配系统基于网络的应用提供了保证。在便捷的网络支持下,虚拟装配系统不仅可以在单机上进行装配的操作,还能通过网络,随时随地进行查看、演练,为遍布各地的客户提供了可网上查看产品信息的便利,也为装配操作的技术工人提供便捷的训练方式。

## 5 总结

基于网络的虚拟装配为虚拟制造领域提供了崭新的思路和方法。作为虚拟制造的核心内容,虚拟装配可以在计算机设置的虚拟环境下,完成对产品的总体设计进程,以缩短产品的开发周期,提高产品质量。

## 参考文献:

- [1] 贺雪晨, 赵彦. 基于 VRML 的虚拟现实技术在世博会场馆模型中的应用[J]. 现代电子技术, 2005(7): 114-116.
- [2] 沈建华, 丁玉兴, 邵立康, 等. 运用 VRML 语言网上虚拟机械结构实验室[J]. 机械设计与制造, 2004, 4(8): 16-17.
- [3] 王洪, 朱清新. 用 VRML 实现虚拟校园的实时漫游[J]. 计登和应用, 2004, 24(12): 141-143.