TippingPoint IPS蠕虫攻击防护配置

潘猛 2007-03-20 发表

TippingPoint IPS蠕虫攻击防护配置

1. 蠕虫攻击的过程

蠕虫攻击一般为以下三个步骤：

1) 扫描：由蠕虫的扫描功能模块负责探测存在漏洞的主机；

2) 攻击：攻击模块按漏洞攻击步骤自动攻击步骤1中找到的对象,取得该主机的权限(一般为管理员权限),获得一个shell；

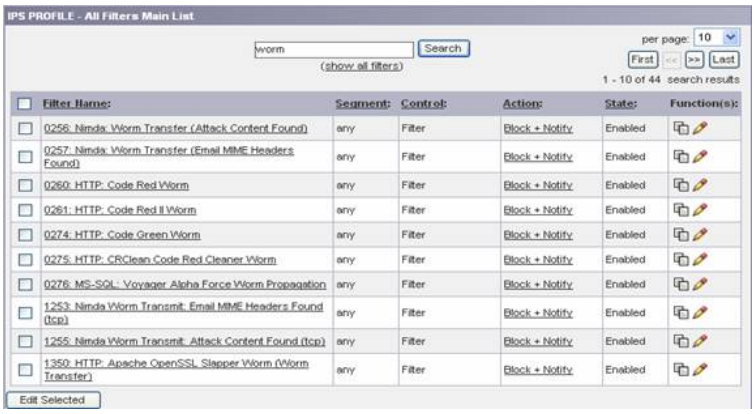
3) 复制：复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动类.

2. 防御蠕虫攻击配置

1) 选择“IPS >> Filter”在“Search”栏目中输入“Worm”,搜索结果如图：

图表 1 Worm Edit

2) 编辑蠕虫过滤器,设置响应动作为“Block + Notify”,对蠕虫进行阻断防护：



图表 2 Worm Edit