TippingPoint对网络隔离和重定向的典型配置

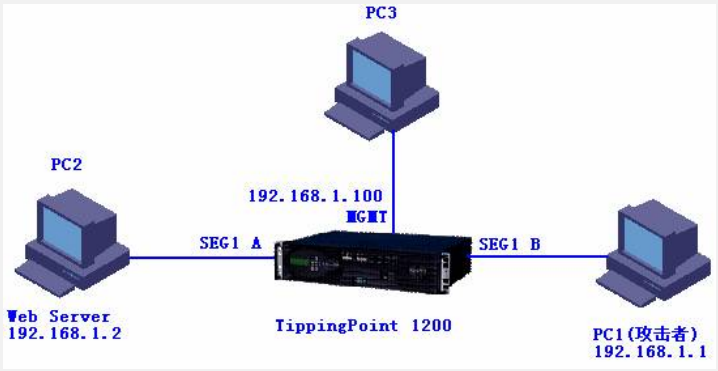
赵彪 2006-11-09 发表

TippingPoint对网络隔离和重定向的典型配置

一、 组网需求：

验证PC1向PC2发起攻击经过TP后被隔离，PC1访问PC2的网页被重定向。

二、 组网图



TippingPoint 1200：TOS Version：2.2.4.6519，Digital Vaccine：2.2.0.5720；

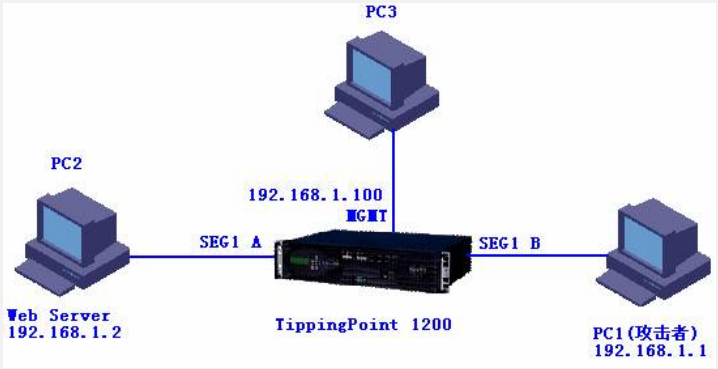
PC1：Windows XP、可执行程序MS05_039.exe、IE；

PC2：没有打补丁的Windows 2000 Server、IIS；

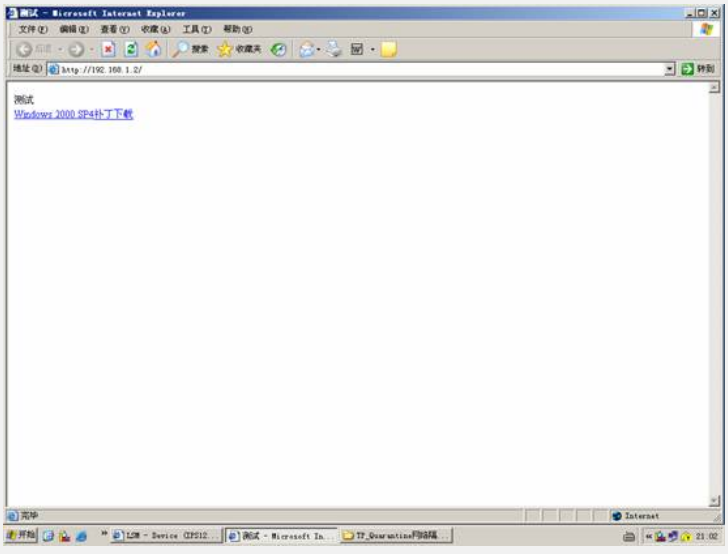
PC3：Windows XP，管理TippingPoint 1200。

三、 配置步骤

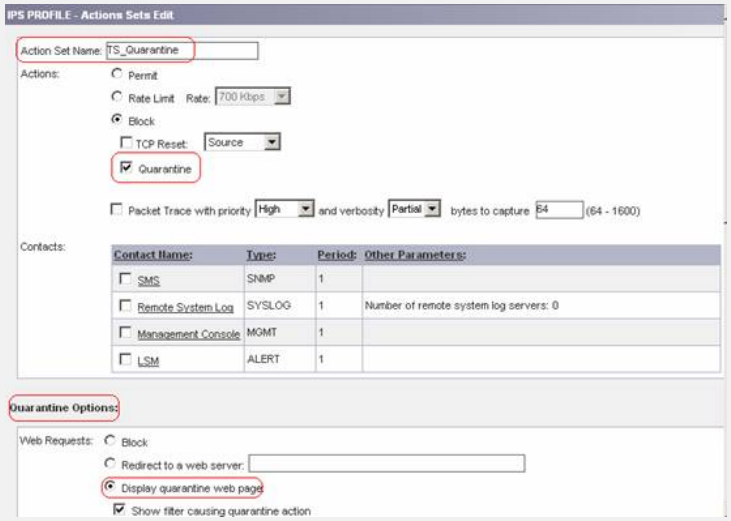
步骤1：在PC1向PC2发起攻击前，验证Web访问：



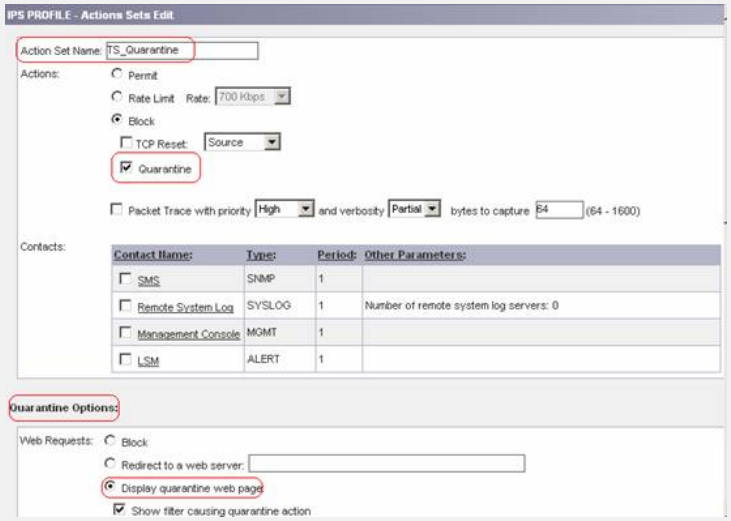
步骤2：“IPS”->“Fliters”->“Action Sets”->“Create”：



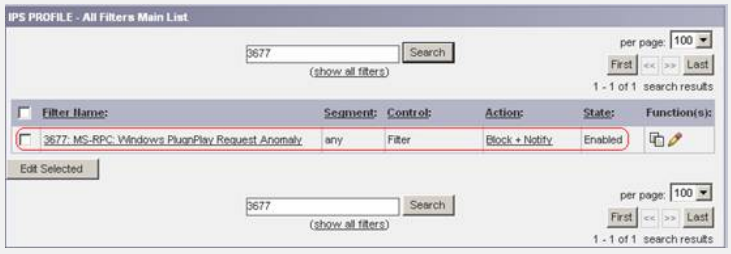
步骤3：查找“3677”过滤器：



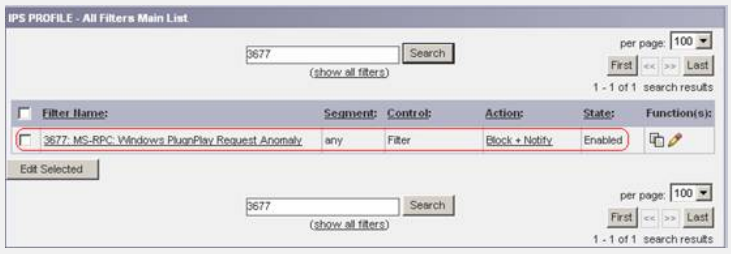
步骤4：修改“3677”过滤器：



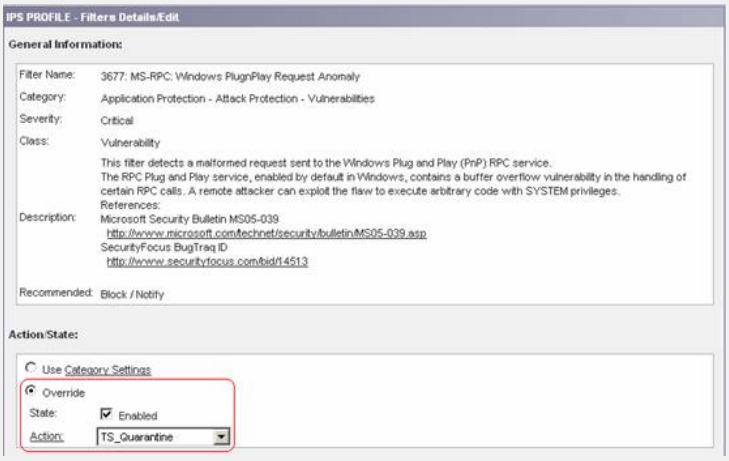
步骤5：查看修改过的“3677”过滤器规则：



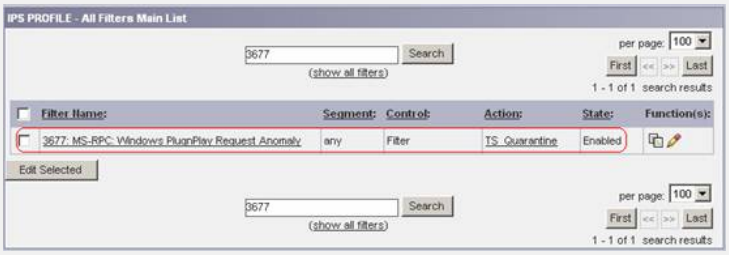
步骤6：在PC1上向PC2发起“MS039.EXE”攻击，攻击将被TP阻止，TP报警，并执行Quarantine特性：



步骤7：“Quarantine”->“Quarantined Addresses”：



步骤8：在PC1上通过IE访问PC2上的任意网页，这时，攻击机上的IE上将显示TP返回的网页，提示该攻击机有阻击波蠕虫的信息（相当于攻击机被隔离，无法成功访问其他网页）：



四、 配置关键点

略。