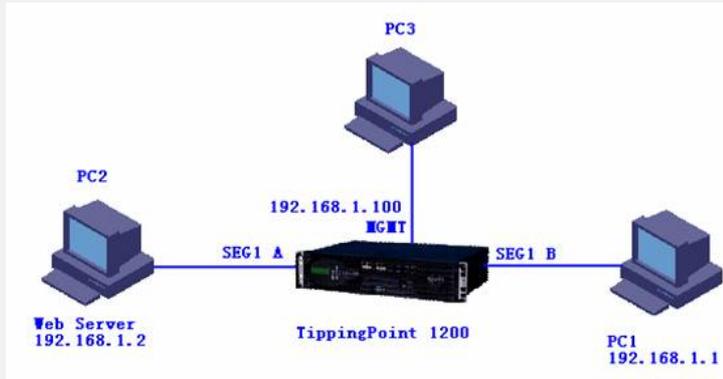


TippingPoint对恶意代码防御的功能演示 操作指导

一、组网需求:

演示TippingPoint对恶意代码防御的功能。

二、组网图



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

PC1: 目标机: Windows XP, IE, Norton;

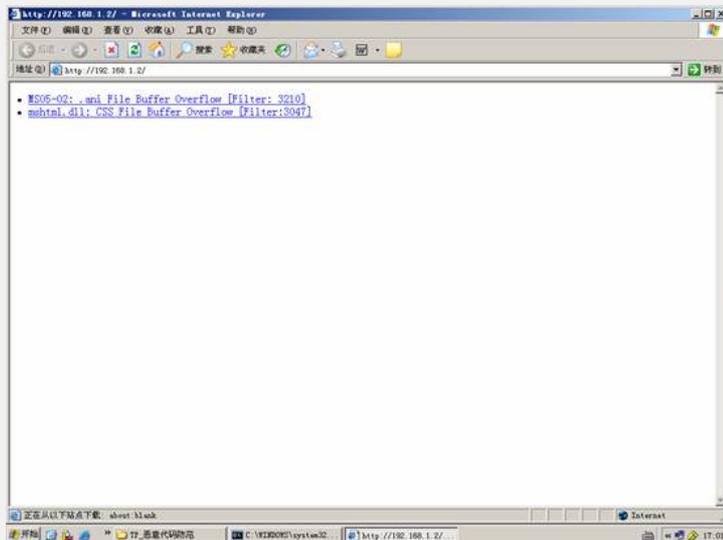
PC2: 攻击机: Windows, IIS, 带有恶意代码的网页;

PC3: Windows XP, 管理TippingPoint 1200.

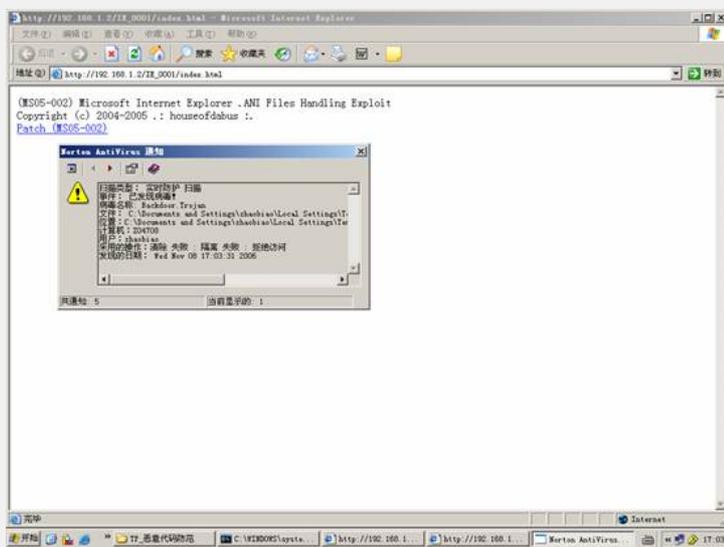
三、测试步骤

1、在不加入TippingPoint 1200时, 诺顿检查出网页有病毒:

步骤1: 在PC1上访问PC2的Web页面:

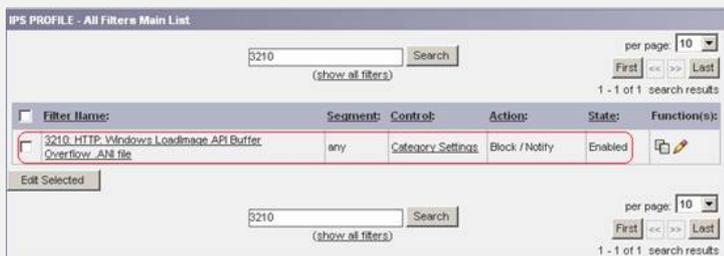


步骤2: 点击“MS05-02”, 检测到病毒:

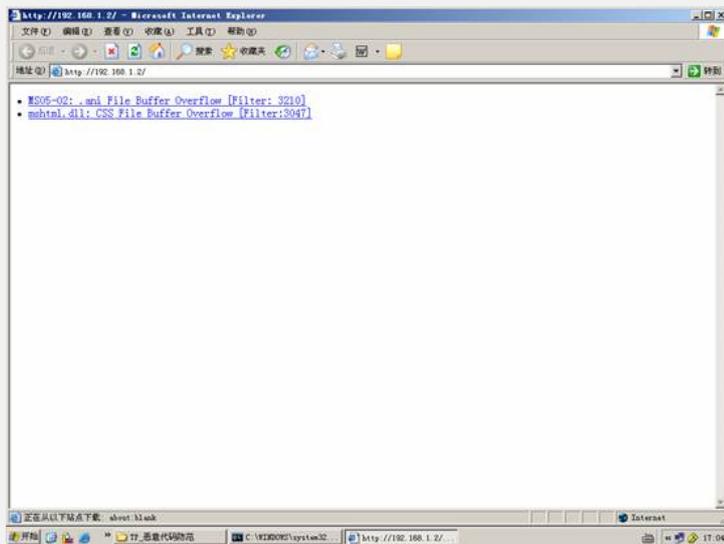


2、加入TippingPoint 1200后，验证“”TippingPoint对恶意代码防御的功能：

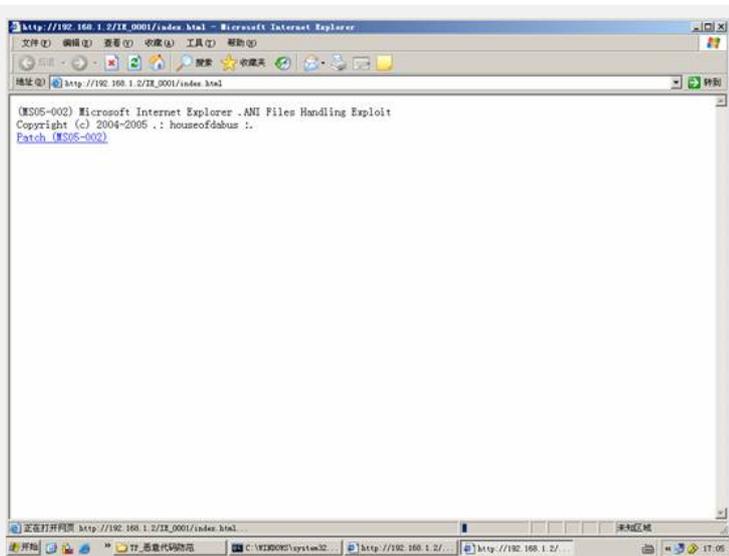
步骤1：缺省情况下，过滤器“3210”启用



步骤2：PC1攻击PC2，由于经过了TP防御，攻击失败



点击“MS05-02”，页面很久不能弹出，说明被TP拦截：



步骤3: 查看“Block”日志

EVENTS - Block Log

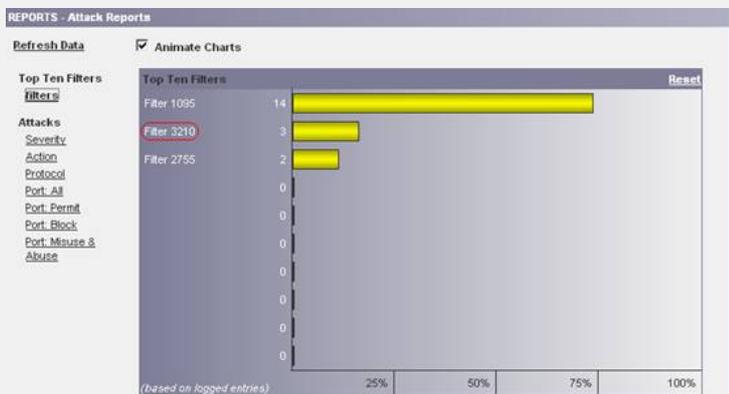
per page: 50

Freeze | Refresh in 28

Log ID:	Date/Time:	Severity:	Filter Name:	Protocol:	Segment:	Source Address:	Dest Address:	Packet Trace:	Hit Count:
111911	2005-11-08 16:07:56	Critical	3210: HTTP: Windows LoadImage API Buffer Overflow .ANI file	tcp	Segment 1	192.168.1.2:80	192.168.1.1:2067		1
111910	2005-11-08 16:06:34	Critical	3210: HTTP: Windows LoadImage API Buffer Overflow .ANI file	tcp	Segment 1	192.168.1.2:80	192.168.1.1:2066		1

per page: 50

步骤4: 查看攻击报告



四、演示关键点略。