赵彪 2006-11-08 发表





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

| 3210 | 3210 Search (show all filters) | | | | First << >> Last 1 - 1 of 1 search results | |
|--|--------------------------------|-------------------|----------------|--------------|---|--|
| Filter Ilame: | Segment | Control: | Action: | State: | Function(s): | |
| 2210: HTTP: Windows Loadimage API Buffer Overflow: ANI file | any | Category Settings | Block / Notify | Enabled | 60 | |
| Edit Selected 3210 | (show all filter | Search | | per First | r page: 10 | |

步骤2: PC1攻击PC2, 由于经过了TP防御, 攻击失败

| http://192_168_1_2/ - Bicrosoft Internot Explorer | |
|---|---------------|
| 文件化 機構化 養養化 秋康化 工具化 帮助化 | A7 |
| 🕜 💷 · 🕑 · 🗷 🙆 🏠 🔎 🗱 ஜ 🟘 🛠 🎯 🍰 · 🌽 🖬 · 🗾 | |
| 地位 ② 1 119-//192 100 1 2/ | - 🖸 特別 |
| - MODE-02: and Hile Buffer Onerflort [Hilton: 3210] | 2 |
| mshtnl, dll: CSS File Buffer Overflow [Filter:3047] | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | *1 |
| D ZERUFRAF& about black | S Internet |
| ●开始 🕞 🏡 🍠 * 😋 17 長泉代明知亮 🛛 🗰 C. \#100095\xystex32 📦 http://192.188.1.2/ | 🚔 = 🖷 🤌 17.04 |

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
```

| Log ID: | Date Time: | Severity: | Filter Hame: | Protocol: | Segment: | Source Address: | Dest Address: | Packet Trace: | Hit Count |
|---------|------------------------|-----------|--|-----------|-----------|-----------------|------------------|---------------|-----------|
| 111911 | 2006-11-08 16:07:56 | Critical | 3210: HTTP: Windows Loadinage API Buffer Overflow ANI file | tcp | Segment 1 | 192.168.1.2.80 | 192.168.1.1.2067 | | 1 |
| 111910 | 2006-11-08 16:06:34 | Critical | 3210: HTTP: Windows Loadinage API Buffer Overflow ANI file | tcp | Segment 1 | 192.168.1.2:80 | 192.168.1.1:2066 | | 1 |

步骤4: 查看攻击报告

| Top Ten Filters | Top Ten Filtern | | | | | Reset |
|-------------------------------------|------------------------|----|-----|-----|-----|-------|
| filters | Filter 1095 | 14 | | | | |
| ttacks <u>Severity</u> Action | Filter 3210 | 3 | | | | |
| Protocol Port: All | Fater 2100 | 0 | _ | | | |
| Port: Permit Port: Block | | 0 | | | | |
| Port: Misuse & Abuse | | 0 | | | | |
| | | 0 | | | | |
| | | • | | | | |
| | | 0 | | | | |
| | | 0 | | | | |
| | (based on looped entri | | 25% | 50% | 75% | 100% |