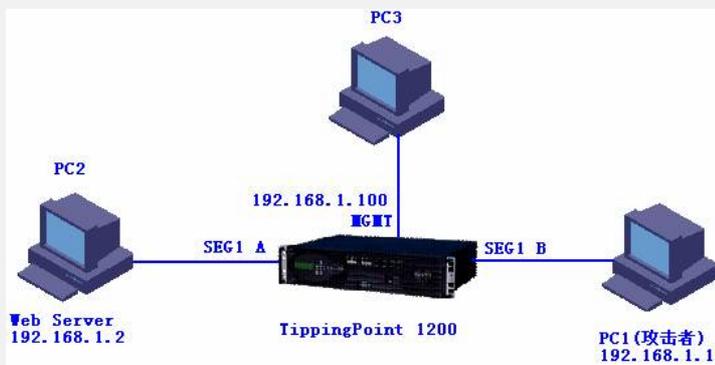


TippingPoint对网络隔离和重定向的典型配置

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。

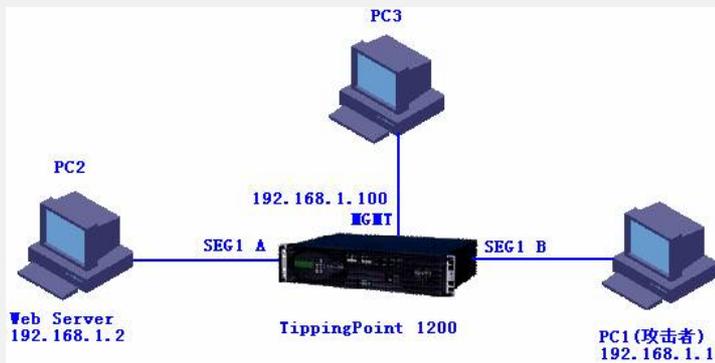
二、组网图



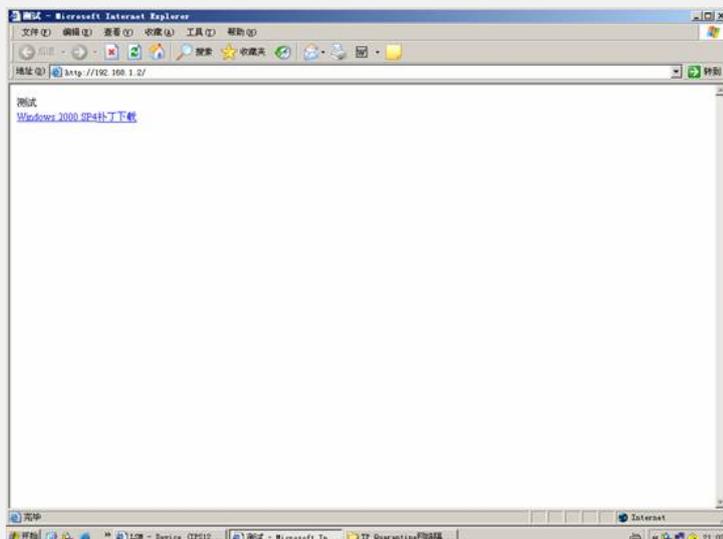
TippingPoint 1200: TOS Version: 2.2.4.6519, Digital Vaccine: 2.2.0.5720;
PC1: Windows XP、可执行程序MS05_039.exe、IE;
PC2: 没有打补丁的Windows 2000 Server、IIS;
PC3: Windows XP, 管理TippingPoint 1200。

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"->"Filters"->"Action Sets"->"Create":



步骤3: 查找"3677"过滤器:

IPS PROFILE - Actions Sets Edit

Action Set Name:

Actions:

- Permit
- Rate Limit Rate:
- Block
 - TCP Reset:
 - Quarantine
 - Packet Trace with priority and verbosity bytes to capture (64 - 1600)

Contacts:

Contact Name:	Type:	Period:	Other Parameters:
<input type="checkbox"/> SMS	SNMP	1	
<input type="checkbox"/> Remote System Log	SYSLOG	1	Number of remote system log servers: 0
<input type="checkbox"/> Management Console	MGMT	1	
<input type="checkbox"/> LSM	ALERT	1	

Quarantine Options:

Web Requests: Block

- Redirect to a web server:
- Display quarantine web page
- Show filter causing quarantine action

步骤4: 修改“3677”过滤器:

IPS PROFILE - Actions Sets Edit

Action Set Name:

Actions:

- Permit
- Rate Limit Rate:
- Block
 - TCP Reset:
 - Quarantine
 - Packet Trace with priority and verbosity bytes to capture (64 - 1600)

Contacts:

Contact Name:	Type:	Period:	Other Parameters:
<input type="checkbox"/> SMS	SNMP	1	
<input type="checkbox"/> Remote System Log	SYSLOG	1	Number of remote system log servers: 0
<input type="checkbox"/> Management Console	MGMT	1	
<input type="checkbox"/> LSM	ALERT	1	

Quarantine Options:

Web Requests: Block

- Redirect to a web server:
- Display quarantine web page
- Show filter causing quarantine action

步骤5: 查看修改过的“3677”过滤器规则:

IPS PROFILE - All Filters Main List

Search (show all filters) per page: 100 First << >> Last 1 - 1 of 1 search results

Filter Name:	Serment:	Control:	Action:	State:	Function(s):
<input type="checkbox"/> 3677: MS-RPC: Windows PlugPlay Request Anomaly	any	Filter	Block + Notify	Enabled	

Edit Selected

Search (show all filters) per page: 100 First << >> Last 1 - 1 of 1 search results

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:

IPS PROFILE - All Filters Main List

Search (show all filters) per page: 100 First << >> Last 1 - 1 of 1 search results

Filter Name:	Serment:	Control:	Action:	State:	Function(s):
<input type="checkbox"/> 3677: MS-RPC: Windows PlugPlay Request Anomaly	any	Filter	Block + Notify	Enabled	

Edit Selected

Search (show all filters) per page: 100 First << >> Last 1 - 1 of 1 search results

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

IPS PROFILE - Filters Details/Edit

General Information:

Filter Name: 3677: MS-RPC: Windows PlugPlay Request Anomaly
 Category: Application Protection - Attack Protection - Vulnerabilities
 Severity: Critical
 Class: Vulnerability

Description: This filter detects a malformed request sent to the Windows Plug and Play (PnP) RPC service. The RPC Plug and Play service, enabled by default in Windows, contains a buffer overflow vulnerability in the handling of certain RPC calls. A remote attacker can exploit the flaw to execute arbitrary code with SYSTEM privileges.
 References: Microsoft Security Bulletin MS05-039
<http://www.microsoft.com/technet/security/bulletin/MS05-039.asp>
 SecurityFocus BugTraq ID
<http://www.securityfocus.com/bid/14513>

Recommended: Block / Notify

Action/State:

Use Category Settings
 Override

State: Enabled
 Action: TS_Quarantine

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）：

IPS PROFILE - All Filters Main List

3677 Search (show all filters) per page: 100 First << >> Last 1 - 1 of 1 search results

Filter Name:	Segment:	Control:	Action:	State:	Function(s):
<input type="checkbox"/> 3677: MS-RPC: Windows PlugPlay Request Anomaly	any	Filter	TS_Quarantine	Enabled	

Edit Selected

3677 Search (show all filters) per page: 100 First << >> Last 1 - 1 of 1 search results

四、配置关键点略。