

TippingPoint IPS蠕虫攻击防护配置

1. 蠕虫攻击的过程

蠕虫攻击一般为以下三个步骤:

- 1) 扫描: 由蠕虫的扫描功能模块负责探测存在漏洞的主机;
- 2) 攻击: 攻击模块按漏洞攻击步骤自动攻击步骤1中找到的对象,取得该主机的权限(一般为管理员权限),获得一个shell;
- 3) 复制: 复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动类.

2. 防御蠕虫攻击配置

- 1) 选择"IPS >> Filter"在"Search"栏目中输入"Worm",搜索结果如图:

The screenshot shows the 'IPS PROFILE - All Filters Main List' interface. A search box contains 'worm' and the results show 1 - 10 of 44 search results. The table below represents the data shown in the screenshot:

Filter Name	Segment	Control	Action	State	Function(s)
<input type="checkbox"/> 0256. Ninda Worm Transfer (Attack Content Found)	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 0257. Ninda Worm Transfer (Email MIME Headers Found)	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 0260. HTTP_Code_Red_Worm	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 0261. HTTP_Code_Red_II_Worm	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 0274. HTTP_Code_Green_Worm	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 0275. HTTP_CRClean_Code_Red_Cleaner_Worm	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 0276. MS-SQL_Voyager_Alpha_Force_Worm_Propagation	any	Filter	Permit + Notify	Enabled	
<input type="checkbox"/> 1253. Ninda Worm Transmit: Email MIME Headers Found (tcp)	any	Category Settings	Block / Notify	Enabled	
<input type="checkbox"/> 1255. Ninda Worm Transmit: Attack Content Found (tcp)	any	Category Settings	Block / Notify	Enabled	
<input type="checkbox"/> 1350. HTTP_Apache_OpenSSL_Slapper_Worm_Worm_Transfer	any	Category Settings	Block / Notify	Enabled	

图表 1 Worm Edit

- 2) 编辑蠕虫过滤器,设置响应动作为"Block + Notify",对蠕虫进行阻断防护:

The screenshot shows the same 'IPS PROFILE - All Filters Main List' interface. The search results are the same as in the previous screenshot, but the 'Action' column for all filters has been updated to 'Block + Notify'. The table below represents the data shown in the screenshot:

Filter Name	Segment	Control	Action	State	Function(s)
<input type="checkbox"/> 0256. Ninda Worm Transfer (Attack Content Found)	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 0257. Ninda Worm Transfer (Email MIME Headers Found)	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 0260. HTTP_Code_Red_Worm	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 0261. HTTP_Code_Red_II_Worm	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 0274. HTTP_Code_Green_Worm	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 0275. HTTP_CRClean_Code_Red_Cleaner_Worm	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 0276. MS-SQL_Voyager_Alpha_Force_Worm_Propagation	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 1253. Ninda Worm Transmit: Email MIME Headers Found (tcp)	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 1255. Ninda Worm Transmit: Attack Content Found (tcp)	any	Filter	Block + Notify	Enabled	
<input type="checkbox"/> 1350. HTTP_Apache_OpenSSL_Slapper_Worm_Worm_Transfer	any	Filter	Block + Notify	Enabled	

图表 2 Worm Edit