巫继雨 2008-06-11 发表

使用Excel绘制IPS图表

1,将IPS攻击日志下载到本地,由于攻击日志保存格式为csv,而csv有一些编辑限制,所以首先将攻击日志保存为xls格式文档;

2, 然后,在Excel的第一行插入空白行,分别为各列内容设置列字段,从左到右依次为"攻击ID、攻击 时间、攻击内容、段、攻击方向、源地址、目的地址、目的端口、源端口、协议、应用层协议、严重 程度"

3,选择"数据à数据透视表和数据透视图",在弹出的向导中,直接点击"完成"按钮;



5, 下面以统计"排名前十的攻击源地址"为例, 讲解通过透视图功能生成所需的报表;

6, 首先将字段列表中"源地址"字段拖拉到左面的"将行字段拖至此处"区域,可以看到所有的攻击的源 地址将会显示在此区域中, 重复的条目将会只显示一条;

清将 页 字 段 拖 全 此 公 に 8
にき
ま 和項: 改会 次 2 2 2 2 2 2 2 2 2

7, 然后,为了得到前十的源地址,需要对源地址的攻击次数进行统计。此时将字段列表中的"攻击次数"拖拉到左面的"请将数据项拖至此处"区域;



8, 此时会看到源地址的出现次数已经进行了汇总;



9,为了找出排名前十的地址,还需要对汇总数值进行排序,鼠标选中汇总栏的任意字段,然后点击" 降序排列"按钮,此时可以看到源地址已经按照攻击次数进行了降序排列,此时我们可以轻易的获得"排 名前X位"的地址;



10, 下面,我们绘制排名前十的饼状图或柱状图;

说明:如果不习惯使用数据透视图绘制图表,可以直接将前十位的源地址和次数复制到新的工作表,然后使用"插入à图表"来独立生成图表,如下:



11, 在"源地址"上点击右键并选择"数据透视图";





12, 点击"源地址"上的倒三角符号,在弹出的列表中,首先取消"全部显示"的复选框,然后勾选前十个地址;

	- 12	-	I II I	E 18 30	······································	, 2. 13	()# ()#	·	- 18 a	安全	PRES	n
A4	•) <u>)</u>	▶ 源地	1址					No. St. Land				0
A		В	C	D	E	F	G	AC 28.10.0	rue (D) + 1511		: : : : : : : : : : : : : : : : : : :	210 I
加快况子	规胞温品	146902										
all sorth and	1.10-85											
ALL SHALL	III SAAST	50										
67 929	1 设置单元	福林大使			-				_			
029 217	37 KE-18 (E	(TTC)			1. 在	"源地力	上点	古右键:	并加度	* *		
60 190 15	#15.m)	and off's	_	-	清报.	動振荡	抑图图"		825 M O			
61, 188	1 140				×2 77	30 10 42	for partial	-	a user a			
60, 190,	更新政策	00	-					100	2	-		
122, 224	間(第Q)							- 自8	女击方向			
59, 60, 14	決定(3)								原地址			
58, 53, 11	411.0.4	-	en .					1 - E E	目的地址			
219, 153,	Mark and		w (-BE	目的端口			
122. 224.	1609 (L)							100	影澜口			
123.130.	宇铁设置	œ						- 15	外 议			
58.211.1	液粘透现	(Q)						- EL &	应用层协议			
59.36.95	10,000,55	建筑表工	1.EO					-87	"重程度			
59, 34, 19	1 10 10 10	1000						10	女击次数			
211.152.5	1 10101 1.01							1.0		-		
222. 92. 41.	228	2						-				
58, 49, 58, 1	106	2						添加到	行区域			
59, 63, 41, 1	165	2										
10.136.173	2.225	1										
59. 34. 198.	88	1										
61, 191, 55,	216	1										
Sit		383										
100000			-									
1 10 0000	/10本日本	1						- Isl				-

13, 此时,已经得到排名前十的源地址的柱状图,但不够美观,通过在图表上选择右键,可以 更改"图表类型"和"图表选项"来美化图表;



14, 下面我将生成一个饼状图,并在每块饼图上显示源地址的出现次数;在图表上点击邮件选择"图表类型",然后选择类型为三维分离饼图;



15, 在图表上点击右键选择"图表选项",然后点中"数据标志"标签项的"值"复选框,即可在各个 饼块上显示攻击次数;



16, 最终,得到的图表如下

