《黑客防线2012合订本》

图书基本信息

书名：《黑客防线2012合订本》

13位ISBN编号：9787121202902

10位ISBN编号：7121202905

出版时间：2013-6

出版社：电子工业出版社

作者：《黑客防线》编辑部

页数：456

《黑客防线2012合订本》

内容概要

本书为《黑客防线》杂志2012年杂志所刊登文章的合集，内容涉及当前系统与软件最新漏洞的攻击原理与防护、脚本攻防、渗透与提权、溢出研究，以及网络安全软件的编写、网管工具的使用等。本书涉猎范围广，涵盖目前网络安全领域的各个方面。其中不乏代表着国内网络安全的顶级技术研究。

《黑客防线2012合订本》

书籍目录

《黑客防线2012合订本》

章节摘录

版权页： 插图： 我自己写的webshell扫描工具能发现它主要是因为我把preg replace这个函数也作为了特征码，不太明白preg replace函数作用的人可能就不会认识到这一点。当然如果扫描发现了一些黑客版权特征，那基本上断定是webshell了。下图是我以前自己写的一个webshell扫描工具的效果图。 2.基于文件属性变化 除了扫描文件特征码之外，还可以结合文件变化来进行。比如html目录正常情况下不会有动态文件，但突然哪天多了一个XX.php，或者其他目录多出一个属主为nobody的文件等。一种思路就是监控文件的变化，当有变化的时候自动调用检测脚本进行检测。 3.基于网络访问特征 现在有一些IPS会将webshell.php、diy.asp、cn99.php等作为特征报警，其实是在网络上截获URL然后匹配特征进行的。顺着这个思路，如果开发一套系统对网络上的http流量进行分析，提取出所有的访问页面、参数、访问方式等信息存入数据库，当有新增的页面或页面新加一个访问参数或者请求方式由GET变为POST时就可能存在异常。但是这种方案实施和运维工作量会比较大，而且无法支持http网站（除非导入网站证书解密）。 4.基于php内核的检测 不管webshel l代码怎么变形，最终都要经过php解析引擎解析后执行，在这个时候所有的操作对你都是可见的。基于这个思路，一些牛人开始设计基于php内核的检测方式。目前还没有一款相对成熟的产品，本次某安全公司过来演示的也只是一个demo。 5.另类思路检测webshell 上传webshel l之后，黑客会进行什么操作？用webshell的浏览目录功能到处逛？还是会用到其执行命令的功能反弹一个shell？执行这些操作与正常的用户访问页面到底有什么区别？基于此，在和一些朋友的讨论下，我提出了基于进程上下文的方案，并且在真实环境下进行了测试。后面我又研究了基于系统调用的方案，并且也在真实环境下进行了测试，这里一并介绍给大家。

《黑客防线2012合订本》

编辑推荐

《黑客防线:2012合订本》由黑客防线编辑部编著，是一本涉及网络信息安全的纯技术月刊，创刊于2001年，至今已经历时12年。12年来，坚持在攻与防的对立统一中寻求技术突破的理念，积极倡导技术创新和突破，成为国内网络信息安全技术人员和相关专业在校学生不可缺少的技术月刊。

《黑客防线2012合订本》

精彩短评

1、文章内容越来越少，页码越来越少。
2、作为资料收藏，需要查查！
3、够专业，够强大，值得学习，这本书，并不是给你提供很详细的代码，只是提供一个解决思路和方案
4、一直都买，每年都买这本书，能学到不少东西
5、挺好的，原理讲解也比较详细。
6、我喜欢，一直在买作为参考书在收藏！

《黑客防线2012合订本》

版权说明