

<<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

出版时间：电子工业出版社

作者：《黑客防线》编辑部

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<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。

## 书籍目录

《黑客防线》2012合订本 目录 本月焦点 一次艰难的渗透纪实1 漏洞攻防 解密百度阅读器远程执行任意文件漏洞14 危机四伏的iWebMall多用户商城系统16 DeDeCMSv5.7最新漏洞分析18 如履薄冰的新为在线0Day漏洞分析29 解密56ican远程执行任意程序漏洞43 计算机网络安全之DLL劫持漏洞详解45 潜伏在办公室里的攻击48 优看PDF在线阅读控件远程代码执行漏洞50 WebOffice控件漏洞大曝光53 巧妙破解YesLab联网认证视频56 基于组件对象模型 (COM) 的劫持攻击技术58 手机支付宝密码存储机制分析62 UUSee2012漏洞六连发71 IE浏览器数组越界漏洞利用方法75 NOTES邮件系统漏洞发掘77 RPC漏洞挖掘79 Struts2远程执行漏洞分析之CVE—2012—0392篇83 HTML5十大威胁：隐秘攻击与漏洞潜伏86 A—PDFAlltoMP3基于SEH的漏洞利用91 危机重重的OfficeAnywhere96 惊爆UUSee网络电视2012远程溢出漏洞98 关于DarkCometRAT531的逆向分析100 AXMAN工具原理解析103 利用pvefindaddr编写飞秋漏洞利用程序107 挖掘AcReport报表远程植入命令漏洞110 Android运程监控技术 击溃360手机卫士的三大防护112 Android下访问Web服务器上传文件125 Android系统shellcode编写127 Android应用程序的补丁方法131 安卓WiFi密码破解工具编写初探141 Android环境窃听器的实现151 Android蓝牙安全通信153 Android手机一键Root原理分析160 伸向Android的核心解析NDK165 AndroidGamex木马分析报告169 Android平台下ARP欺骗的分析与实现174 Android木马分析与编写180 AndroidAPIHook之LD\_PRELOAD182 Android下APK及DEX文件解析185 移植Linux源码到Android系统环境搭建187 工具与免杀 自己动手打造APK安装器190 搜索Kernel32.dll：TEB与PEB之旅197 Windows内核调试命令利器分析199 渗透与提权 BurpSuite——SQLINJECTION203 老树开花：一个js函数引发的命案210 Linux下的MySQL提权212 PHPDISKheaderbypass & getShell215 Linux环境下的防火墙绕过技巧217 浅谈Linux下ARP入侵220 MetInfo全局变量覆盖另类突破防注入224 XSS黑盒入侵实例227 暴力破解一个ASP加密算法228 另类思路检测webshell230 由Tencent://Message协议联想到的“协议劫持” 233 外文精粹 StealthRootkits攻击技术发展趋势分析236 基于Linux内核2.6.x/3.0.x可加载内核模块的注射技术240 网络安全顾问 来自移动终端的新一代245 信息威胁技术探讨245 HardwareHack之NFC系列——门禁卡攻击248 电子渠道身份认证系统安全性分析251 摩托罗拉XOOM提权和安装backtrack5254 企业内网ISA安全认证环境搭建详解258 浅谈Windows和Linux下的嗅探攻击及防范267 揭示主流内网管控系统的脆弱性273 LinuxLKM注入攻击275 编程实现Linux环境的二进制文件反调试281 编程解析 编程实现突破Win64内核保护机制285 Linux下内核漏洞利用的几种方式290 在Win64上实现SSDTHOOK294 初步探索PE32+格式文件298 深入跟踪HelloWorld执行303 PHPHashtablecollisions简要算法分析310 远程同步CMD SHELL程序的实现312 实现Win64上的内核级InlineHook引擎316 恢复在Win64上的SSDT钩子318 Windows7注册表之SAM文件取证分析321 安博士V3Lite的一些问题324 编程实现使安博士无法访问被保护文件328 Returnil影子系统1.2的逆向分析331 对卡巴斯基安全键盘的研究337 详解Win64上的ShadowSSDT339 LinuxELF运行时内存详解343 细解使用NativeAPI编程347 利用GlibcHook打造Linux程序防火墙352 Win64上使用标准方法监控进程创建354 Win64下使用标准方法监视文件访问356 浅议MDL359 小议csrss与smss363 新思路注入DLL并绕过杀毒软件370 利用Detours实现APIHook374 在Win64上枚举消息钩子377 木马核心功能研究380 PassTrojanCut突破研究385 Windows异常处理机制387 使用Libnet实现ARP数据包发送391 ShellcodeInX64Findkernel32.dll394 ShellcodeInX64—2SearchFunctionusinghash397 Windows编程之对象与句柄402 用pcap编写网络嗅探器407 TLS反调试的前世今生411 密界寻踪 Android应用程序破解入门416 手写指令对抗IDA422 一个平板软键盘的算法分析与注册机编写428 AvKiller病毒分析432 分析一个DLL劫持下载者439

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webshell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webshell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>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>