WEB网站服务器黑客攻击安全防护托管

产品名称	WEB网站服务器黑客攻击安全防护托管
公司名称	河南刘贵商务服务有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:技术支持 发票:提供
公司地址	河南省南阳市卧龙区卧龙岗街道卧龙路经纬国际1号楼810（注册地址）
联系电话	13323693821 13140513661

产品详情

服务器的安全关系着公司整个网络以及所有数据的安全,做好网站应用服务器的安全维护是一项非常重要的工作。

互联网时代，越来越多的企业或个人站长都做起了线上业务，当网络跨数发展的同时也存在着问题，网站攻击简直防不胜防，那么当网站受到攻击的时候不要过度惊慌失措，要先静下心查看网络被攻击的原因，受到什么攻击，具体我们可以为为以下这三部分：

1、开启IP禁PING，可以防止被扫描。

2、关闭不需要的端口。

3、打开网站的防火墙。

那么有时候是因为网站被黑的原因，那么网站为什么会被黑呢，其中挂马是比较让站长头痛的事，那么一般被黑的原因可以分为两种：

1、服务器空间商的安全 导致被牵连。

2、网站程序的安全自身的程序安全漏洞被黑被入侵被挂马。有条件的话可以找专 业做安全的去看看. 公司的话可以去Sine安全看看听朋友说不错。一般都是网站程序存在漏洞或者服务器存在漏洞而被攻击了。

网站被黑解决办法：

1、在程序中很容易找到挂马的代码，直接删除，或则将你没有传服务器的源程序覆盖一次但反反复复被挂就得深入解决掉此问题了。但这不是好的解决办法。好的办法还是找专
业的程序员解决是比较直接的。

2、清马+修补漏洞=彻底解决所谓的挂马，就是heike通过各种手段，包括SQL注入，网站敏感文件扫描，服务器漏洞，网站程序0day, 等各种方法获得网站管理员账号，然后登陆网站后台，通过数据库
备份/恢复 或者上传漏洞获得一个webshell。利用获得的webshell修改网站页面的内容，向页面中加入恶意转向代码。也可以直接通过弱口令获得服务器或者网站FTP，然后直接对网站页面直接进行修改。当你访问被加入恶意代码的页面时，你就会自动的访问被转向的地址或者下载木马病毒。

如何进行服务器安全防护?

服务器是计算机的一种，它比普通计算机运行更快、负载更高、价格更贵，它是网站、游戏的基石，任何网站、游戏都需要依靠服务器来运行整个体系，因此服务器的安全防护变得非常重要，因为加强服务器安全防护，可以避免网站、游戏信息遭恶意泄露或被黑客入侵。那么如何进行服务器安全防护?以下是详细的内容介绍。

1、定期更新系统和软件补丁

不论是Windows还是Linux，任何操作系统都有漏洞，及时安装补丁，避免被不法分子恶意利用攻击。同时，需要定期安装新的操作系统，减少系统漏洞，提高服务器的安全性。

2、加强密码保护

密码保护是安全防护的第1道防线，大部分的网络攻击都是从弱口令入手。一旦网络不法分子进入了系统，之前做的安全防护工作将会大打折扣。加强对服务器系统账号和密码管理，是保证系统安全非常重要的措施。

3、定期进行备份

为防止不能预料的系统故障或用户不小心的非法操作导致重要的数据和文件丢失等情况发生，必须对服务器进行安全备份。备份很重要，除了对全系统进行每月一次备份之外，还应对修改过的数据进行每周一次备份，本地备份的同时还要进行异地备份。当发生原始数据不幸损坏、丢失等情况时，企业可以利用备份数据保证业务的运行。

4、关闭非必须的服务和端口

在服务器操作系统安装时，会启动一些不需要的服务，占用系统资源的同时，还会增加系统的安全隐患。对于不常用的服务，可以将其完全关闭。

5、监测系统日志

通过运行系统日志程序，系统会记录下所有用户使用系统的情形，包括近来登录时间、使用的账号等。日志程序会定期生成报表，企业相关人员通过对报表进行分析，可以知道是否有异常现象。

6、及时更新软件版本

可以避免你的服务器处于危险之中，使其漏洞被黑客利用并入侵，使用专业的安全漏洞扫描程序是一种保持软件实时更新的方式之一。

7、进行定期和频繁的安全检查

如果不定期开展安全检查工作，就无法知道潜藏的安全问题，从而服务器得不到基本的安全保障。定期对服务器进行安全检测，可采取漏洞扫描、渗透测试、代码审计等手段进行安全漏洞排查。