论坛中使用标签或者图片来表明言论管理员身份，言论管理员没有登录后台的权限，就类似于吧主或者版主。可以登陆后台的管理员觉得不应允许被知道，最后就不要进行发言，或者发言的时候作为普通用户进行显示。

两台DNS服务器，一台公网，一台内网，就是怕配置出错

用户密码认证不安全,改为双因素认证

数据库(加密存储)是要账号密码认证,把哈希拿出来Hash碰撞,碰撞到的就是弱密码

会对软件版本信息进行收集

离职人员账号失效处理,记录保留

内部端口限制IP访问

VLAN只出不进

wen下文件权限设置755，防止写入

审计是一种事后行为，通过对用户的行为分析，以及系统的错误分析，找到程序服务运行中的问题。

规定：

安全评估标准TCSEC（trusted computer security evaluation criteria）、TDI。CC是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。

目标要求-》实现方法-》具体要求

参照管理标准与安全标准.要用自己设计的加密算法

自动化系统,执行公司的内部标准

分层又被称为深度防御或补偿控制。通过多种策略配合来弥补一种策略的不足。

被rootkit感染的电脑，执行命令的结果是不可信的。可能是文件替换，也可能是系统调用。

避免被黑客发现的技术可以用于避免被查杀，对通信和文件也进行加密。

每天网管或者机房管理员需要每天至少一次去机房看设备的灯，即便现在已经有网络管理软件

定期将数据库漏扫系统接入vpn以后对整个系统安全巡检

超级用户也应该收到限制，比如删除了linux主机中危险的可执行程序。

员工的素质影响很大了，德勤500万数据泄漏就是因为员工坑爹了，将账号直接上传到公开的网站比如github

将企业中存储的用户，加密以后把密钥给用户，进而允许用户进行访问。

内部员工访问系统敏感信息应该变种显示，进行限制。

可信计算与可信网络没有办法在工业界推广，因为要对客户端信息做出要求。

自动注销功能是为了当你开着root账户的时候却上了个厕所。

观察：

日志管理工具，记录一般文件（文本文件之类的文件）类似git工具一样记录变化与增加。如果是其他文件则记录hash、sha-1之类的。

各种文件的md5变化，注册表与快照相比之间的变化

任务管理器-》应用历史记录

svhost进程不该出现网络访问，有流量。svchost.exe文件大小一般是5K。

如果一个服务的描述和显示的名字对不上，比如描述是Monitors USB Service Component

cd “.. "这名字看起来挺吓唬人的

信息泄露：

见过360一个极端的例子，甚至直接登录了用户私人网站的后台

经过公司分配的电脑远程登录自己的服务器，之后公司监管人员也会登进去

如果保存了的密码被清除了要你再输一遍要小心。除非是你自己清掉了。

注意上网言行

关闭不必要端口，和端口bander信息

对于爆破进行加锁

阻止2程序运行；

沙箱运行

基址随机化 (ASLR/KASLR)

不从数据页执行代码（堆和栈）

堆释放元素的时候放置一个随机数，如果被改变是可以知道的

权限：

用户组权限控制

备份文件的权限

追踪：

对软件进行逆向，然后查找类似的代码实现，发现某一个函数来自一篇中文文章，从而对目标进行可能判定

对于端口的防御：

关闭服务/程序（services.msc、组策略、注册表）----（如果不能关闭）---》防火墙设置规则（实际上也是策略组）、本地安全策略（IP安全策略，创建IP筛选器）

对空连接的防护：

因为本质是SMB的一个匿名会话，如果不需要服务的话，直接关闭服务或者禁用端口。

从组中删除Everyone成员。

启用和关闭windows功能里面可以关闭SMBv1。

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictAnonymous设置为2（win2000以后），之前只能设置为1，但是这并不能阻止空连接和对信息的查点，似乎仅仅在账号与共享卷的泄露上做了点防护。设置为2，就不能将Everyone包含在匿名访问令牌中。除了匿名访问，我们也不希望存在sid和名称之间的转化，避免user2sid工具（user2sid、sid2user进行名称与sid的互相转换。自己结合已知的RID，组装出想要的SID。不过hyena和dumpsec都可以直接查出来）。

防止重放攻击：

nonce （number once）、序号、时间戳

网络故障：

traceroute、tracert

web访问要注意DNS服务器错误 抓包检查

hostname访问 这个就本机host文件，或者局域网内host服务器

流量镜像：

通过指定的包进行重播从而对当时的攻击情况进行复现很重要。

将解密的无线的流量镜像后连接IDS接口，或者直接抓包，然后每一个固定时间周期内进行流量的分析。无线中可以使用airtun-ng将一个无线网卡变成一个虚拟隧道从而镜像，不过最简单的还是使用集线器。

串行防火墙就是在传输的路径设置上是串行的，这对防护墙的处理时间有要求。

并行防火墙指对来自内外的流量进行一次镜像，在第一时间与用户进行交互的同时在那里“慢慢”分析。这种方式也称为旁路部署。

不同部分需要防御的内容是不同的，所以有的防火墙是专门给数据库建立的。

检测系统可以对包的类型、大小、频率进行监测。

高级的流量分析工具在流量统计的时候，很友好地知道在哪个时间段内哪一个主机发了什么包最多。

工具：

入侵检测系统：snort（开源产品）

入侵检测数据集：kdd99

注册表：快照工具RegSnap、实时变化监控工具

sandbox或者vm

spybot-anti-beacon 修复windows容易受到攻击的策略，同时提供undo操作。

total unisntall、geek uninstall和reno uninstall 监视进程的行为

TCP Wrapper程序监视发送进来的包。若外部计算机试图连接，TCP Wrapper就会查看该机器是否具有连接的权限。如果有，那么访问允许。若没有，访问拒绝。该程序可以根据个人用户或网络的需求进行更改。vim /etc/hosts.allow vim /etc/hosts.deny

tripwire以及AIDE都是为每一个文件生成一个签名，需要保存在安全的地方，通过对签名的验证判断文件是否有更改（目录的位置结合文件本身的md5就能简单实现）。rpm -V（Red Hat Package Manager），使用一个确定没有问题的rpm，会比较系统中的已安装软件和为篡改软件的校验和，从而提示这个软件那些地方被更改。

通过交换机，分成一个个独立的冲突域，这样只有目标地址为特定主机或者广播包才能被转发。