聊一聊服务器的安全基线—安全小课堂第三十九期

京东安全应急响应中心 2016-12-23

安全小课堂第三十九期

安全基线，是为了明确网络上的相关设备与系统（包括操作系统、网络设备、数据库、中间件在内的所有类型的设备）达到最基本的防护能力要求而制定的一系列基准。本期我们来聊一聊服务器的安全基线。

本期邀请到网易安全专家沈明星。

文丨豌豆妹　图丨源自网络

> > > 1 < < <

豌豆妹

服务器常规的安全配置有哪些?

哆啦A梦 

安全基线，是为了明确网络上的相关设备与系统（包括操作系统、网络设备、数据库、中间件在内的所有类型的设备）达到最基本的防护能力要求而制定的一系列基准。

以Windows服务器为例，可以配置包括账号、口令、授权、补丁、防护软件、防病毒软件、日志安全要求、不必要的服务、启动项、关闭自动播放功能、共享文件夹、使用NTFS 文件系统、网络访问、会话超时设置、注册表设置等选项。

另外一个就是Unix家族，我们以Linux为例。Linux服务器相对更加安全一些，配置项也少一些，主要有账号、口令、授权、补丁、远程登录、日志、不必要的服务端口、系统banner设置、删除潜在的危险文件、FTP设置等。相信各家都有自己的安全基线标准，根据自己的业务对安全的定义略有差异，但大体上，主要还是往这些方面去考量。

> > > 2 < < <

豌豆妹

结合公司业务，常规的软件和相应的配置有哪些呢？

哆啦A梦

每个公司根据自身的技术架构差异和偏好，选择不同的操作系统、数据库、中间件来搭建公司的业务。现在互联网主要依赖于一些开源软件和实现来构建。主要用到的一些常规软件包括 MySQL、Apache、Tomcat、Nginx、LVS、Redis等等。

以MySQL为例，账号以普通帐户安全运行 mysqld，禁止MySQL以管理员帐号权限运行。应按照用户分配账号，避免不同用户间共享账号。应删除或锁定与数据库运行、维护等工作无关的账号。口令禁止使用默认密码和弱密码。授权，在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。日志，数据库应配置日志功能。补丁，系统安装了最新的安全补丁。网络连接，禁止网络连接，防止猜解密码攻击，溢出攻击和嗅探攻击，通过数据库所在操作系统或防火墙限制，只有信任的 IP 地址才能通过监听器访问数据库。连接数，根据机器性能和业务需求，设制最大最小连接数。

当然MySQL某版本还有某著名漏洞，大家都懂的。再如Tomcat，也可以从账号、口令、授权、日志、HTTP 加密协议、更改默认管理端口、错误页面重定向、目录列出、系统Banner 信息、连接数设置 、禁用非法HTTP 方法等方面进行配置。

由于用到的类似软件和中间件很多，所以这里就不去一一列举了。大家可以参考OWASP的安全基线项目：http://www.owasp.org.cn/owasp-project/jixian。

> > > 3 < < <

豌豆妹

公司网络层面上，如何结合业务做防护控制呢？

哆啦A梦

这里我想到几点。首先在网路层面的防护，除了针对服务器和服务器上的软件之外，要特别注意针对网络设备的控制。比如，现在越来越多的攻击会针对家用的路由器，而不是直接攻击终端。对IDC机房的攻击也是同样，需要做好网络设备的防护。
其次，还可以结合我们常规的漏洞扫描，在扫描器中加入安全基线扫描的功能，上面提到的一些配置是可以通过扫描器来验证，例如，若使用了弱口令，我们可以使用字典进行爆破来验证。
最后，不同的业务对安全基线的要求会不一样。比如一个金融业务的安全要求会比一个博客类业务的要求高很多，所以需要针对不同的业务制定不同基线来进行防护。

> > > 4 < < <

豌豆妹

如何实现服务器安全配置的自动化管理呢？

哆啦A梦

现在机器和设备越来越多，人肉的时代已经过去了。必须要有相应的流程和自动化工具来辅助我们做这些事。首先得需要流程和制度，需要有专业的人员来制定安全基线。
在服务器安全基线的实施方面，第一步是根据制定的安全基线制作镜像，这样就可以保证服务器的默认安全。但安全是一个过程，会随着时间的变化调整安全基线，那就需要自动化的工具来帮助进行实施，我们就使用了一些开源项目，例如puppet。也有大量的乙方安全公司会提供安全基线配置的工具，当然有的公司也会根据自身的运维和安全工具来定制自动化管理工具。

> > > 5 < < <

豌豆妹

服务器安全配置缺失的监测和检查手段有哪些呢？

现在最主流的方式，就是安全基线检测工具。工具的原理很简单，是通过在服务器上部署一个agent，搜集相关的配置信息，跟中心库中维护的安全基线标准进行比对，并进行检查，目前这种方式被大量的运用。

但是在服务器部署agent也有一定的安全风险，在有些公司推动的时候也存在一定的阻力，所以需要获得高层的支持，自上而下的进行推进，并且agent的维护和发布要相当注意。

尽管安全基线检查工具能够从技术层面对安全配置进行全面、高效的检查，但对于业务系统特有的安全问题以及业务系统管理层面的问题，仍需要结合传统的安全评估服务手段以及传统的安全检查工具（如：漏洞扫描、代码检查）来实现。