游刃基线安全系统技术白皮书

V1.2

深圳市大成天下信息技术有限公司

ShenZhen Unnoo Information Tech., Inc.

二〇〇五年五月

版权说明

商标信息

文档号：UnnooP101301
2005 年 5 月

目录

1.产品简介

1.1.概述

随着信息化进程的深入和互联网的快速发展，网络化已经成为企业信息化的发展大趋势，信息资源也得到最大程度的共享。但是，紧随信息化发展而来的网络安全问题日渐凸出，网络安全问题已成为信息时代人类共同面临的挑战，网络信息安全问题成为当务之急，如果不很好地解决这个问题，必将阻碍信息化发展的进程。

网络上的不法分子不断的寻找网络上的漏洞，企图潜入内部网络。由于用户自身网络系统的缺陷、网络软件的漏洞以及网络管理员的疏忽等等，都可能使网络入侵者有机可乘。当系统遭受了攻击，就可能造成重要的数据、资料丢失，关键的服务器丢失控制权等极其严重的后果。如果能在黑客入侵之前知道自己网络安全的情况，那么将能大大帮助管理员提前修补自己的系统，就能做到有备无患、防患未然；同时也能让企业的决策层充分了解自己企业的网络安全现状，为制定方案和相关预算起到指导作用。

游刃基线安全系统是大成科技自主开发的一款产品领先、漏洞库完备、准确性高的企业安全策略评估系统，它能为企业网络安全维护提供了强有力的保障。

1.2.公司简介

深圳市大成天下信息技术有限公司是一家专业从事网络安全产品与服务的高科技公司。凭借多年的从业经验，大成科技聚集了一批优秀的专业人才，在华南信息安全领域中具有独到的地位。

目前，大成科技的研究人员通过多年的专业安全服务经验，开发出包括游刃基线安全系统、铁卷信息监控平台等多款产品，涉及的研究领域涵盖安全评估、内容安全、接入安全等多方面，并取得多项科研技术成果。

1.3.系统要求

1、硬件环境

游刃基线安全系统运行在硬件环境为 X86 架构的台式机或笔记本电脑上。

- CPU：不低于 Pentium IV 2.2G
- 内存：不低于 512M，建议 1G
- 硬盘：不低于 50M 剩余空间，建议 200M 以上剩余空间
- 网卡：至少一块 100Mbps 以太网卡

2、软件环境

- 操作系统：Windows 2000 SP4 以上、Windows 2003、Windows XP
- 浏览器：IE5.0 以上版本

2. 系统典型应用

2.1. 部署模式

游刃在中小型网络中以平坦模式部署。游刃为网络式工作模式，只要将游刃接入网络并进行正确的配置即可正常的使用，其工作范围通常包含客户公司的整个网络地址，用户可以从任意地址登录下达扫描任务。

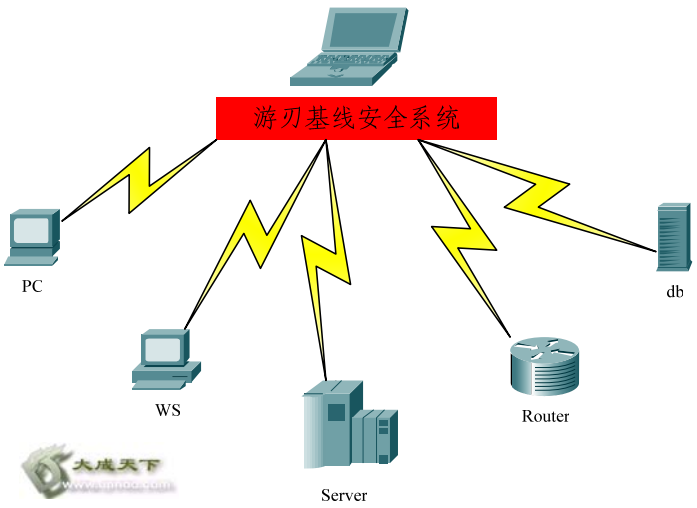

图 1：游刃基线安全系统部署模式

2.2. 典型应用

例：某金融系统于 2004 年 11 月采购游刃基线安全系统，该系统网络配置状况如下图所示：

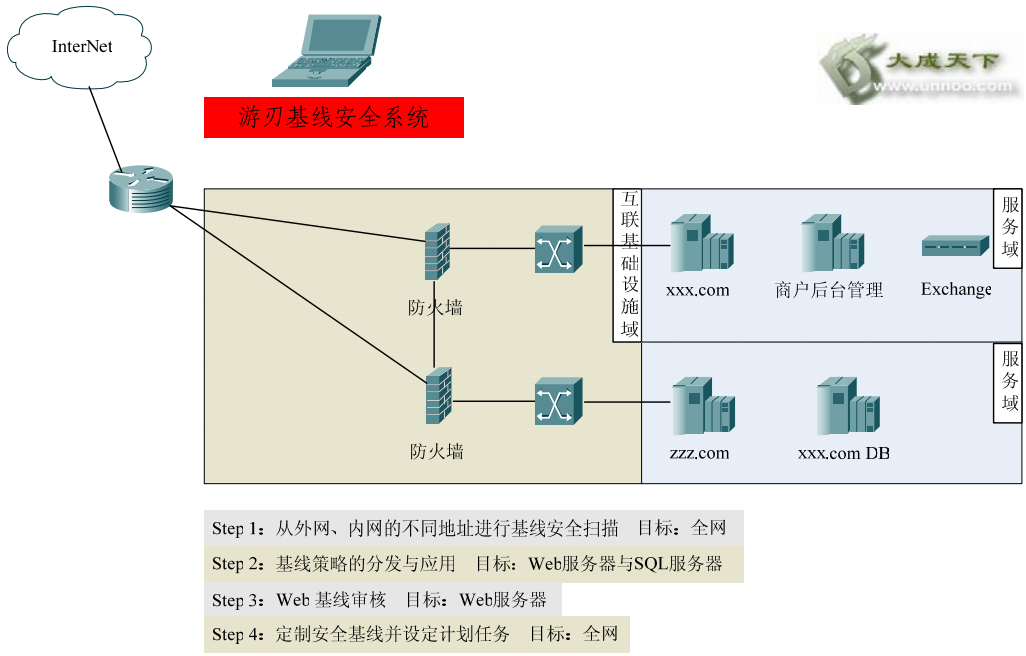

图 2：某金融系统网络拓扑图

该金融系统经营了一个网上交易系统，该系统架构为 Windows 2000 + IIS + MSSQL，系统结构简单，前台一台 App Server 连接到后台的商务后台管理（MSSQL 数据库）。在网站上运行的业务有：

- 静态的企业宣传页面；
- 企业论坛；
- XX 信息查询系统；
- MS SQL 后台数据库
- Exchange 邮件服务器；

该公司采用的基线安全管理手段包含以下三个模块：

- 基线安全扫描

  通过该扫描发现前台的邮件服务器存在 Exchange 远程缓冲区溢出漏洞，补丁尚未安装，可能造成黑客的远程攻击。

- 基线策略分发与应用

采用 Web 服务器、邮件服务器和数据库服务器的基线安全策略对主机进行加固。

- Web 基线审核

  通过 cgi 扫描和全站 SQL 注入检查，发现在该企业信息查询系统中有至少两处程序脚本存在注入漏洞。

- 补丁管理

  游刃定期对办公网络的 Windows 客户机进行补丁检查，发现有高风险补丁没有及时安装，便提示系统管理员，并且可以按照一定的安全策略断开该主机的连接。

扫描完毕后，公司将游刃的扫描结果经过审核，确定了在网络中的“合法协议”，去除了不该存在的端口/服务后，并确定该应用的版本号后，设置为当前安全基线。

明确安全基线后，通过对游刃的设置，还做到了:

- 定期在每周五凌晨 0:00 执行基线审核工作:
- 将执行结果与当前基线（或上期结果）比对后发送差异信息给系统管理员。
  - 对基线之外的端口/服务进行报警;
  - 对存在安全问题的基线内的端口/服务进行报警;
- 一旦新漏洞出现，管理员只需要重新设置安全基线，便能够快速发现网络中所有不安全的设备。

3.基本功能介绍

在木桶理论中，一个由许多块长短不同的木板箍成的木桶，决定其容水量大小的并非是其中最长的那块木板或全部木板长度的平均值，而是取决于其中最短的那块木板。要想提高木桶整体效应，不是增加最长的那块木板的长度，而是要下功夫补齐最短的那块木板的长度。

现阶段我们提出的基线安全管理，则是通过技术手段寻找出组织内部信息安全的最短板并进行修复，然后通过持续的 PDCA 过程，提高基线后进行下一轮“巡检”。

3.1. 工作流程

传统的 PDCA 流程包括了计划和设计(Plan)、建设和实施(Do)、运行和监控(Check)以及 Act(维护和改进)，这四个过程不是运行一次就完结，而是要周而复始地进行。

图 3：PDCA 模型

PDCA 具有两个特点：

- 大环带小环。如果把整个组织的工作作为一个大的 PDCA 循环，那么各个部门、小组还有各自小的 PDCA 循环，大环带动小环，一级带一级，有机地构成一个运转的体系。
- 阶梯式上升。PDCA 循环不是在同一水平上循环，每循环一次，就解决一部分问题，取得一部分成果，工作就前进一步，水平就提高一步。到了下一次循环，又有了新的目标和内容，更上一层楼。

在基线安全管理中，融入 PDCA 这种生命周期管理的方法，即从建立基线开始，进行检测和评估、查看报告并验证漏洞，并且就发现的问题进行维护修正后，进入下一轮基线构筑的过程。

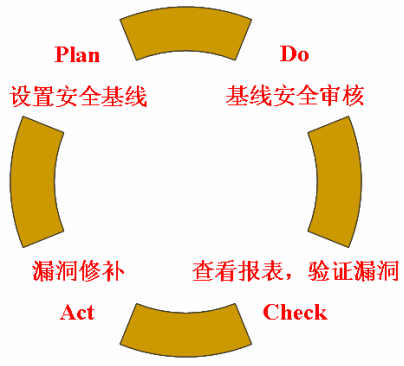

图 4: PDCA 流程在基线管理中的实际流程

3.2. 游刃基本功能

商业机构希望实现基线安全管理功能，可以采用“游刃”基线安全系统，该系统专门为基线安全管理设计，将基线安全管理简化为五个技术步骤，部署后能够渐进式地在企业安全管理中发挥作用，有效减轻系统管理员的负担。

图 5: 游刃基线安全系统

第一步：基线安全扫描与配置管理

当前网络中的漏洞扫描软件往往追求“大而全”，漏洞数据库中通常有两千甚至更多的漏洞数据，对网络安全没有足够经验的系统管理员在扫描结束后面对复杂的报告常常束手无策。

基线安全扫描则通过专家筛选，将互联网上最经常发生的攻击(例如 SANS TOP 20)、可能导致攻击者直接入侵主机的远程高风险漏洞等黑客“一击必杀”

漏洞的检查，首先**保证网络中没有远程高风险安全漏洞**。(由于安全策略可以自由选择，因此用户能够选择由专家定制的七百多条高风险漏洞，也可以选择全部近三千种攻击测试脚本。)

pg_style	(全部)		
计数项:pg_name	severity		
	高	中	总计
汇总	427	303	730
注：			
pg_style为plugin所检查的漏洞类型，包括以下几类			
style_id	style_name		
1	信息探测类		
2	网络设备与防火墙		
3	RPC服务		
4	web服务		
5	CGI问题		
6	文件服务		
7	域名服务		
8	Mail服务		
9	windows远程访问		
10	数据库问题		
11	后门程序		
12	其他服务		
13	网络拒绝服务(DoS)		
14	其他问题		

图 6: 游刃基线安全系统精选的安全漏洞数据

第二步：口令策略检查

在笔者参与的渗透测试中，约有 30%的企业是由于存在薄弱密码导致最终系统的沦陷，也正因为这样，因此有人认为：口令是信息安全永恒的主题。

口令安全策略检查将对网络中的主机、数据库、网络设备等进行全面的口令探测，探测对象包括 Windows、Telnet、SSH、SQL 等十四种不同的应用，并且针对不同行业定制密码字典。这一环节**确认组织内不存在违反安全策略的薄弱口令。**

第三步：基线策略分发与应用

这里所指的基线策略的分发与应用，指的是针对不同应用种类的 Windows 操作系统，如 OA 人员的工作站、Web 服务器、文件服务器等。根据其应用自

身的特点，可以采用向导式的基线调查方法，对口令策略、用户权限、系统日志、组设置、系统服务、文件权限、注册表权限进行优化调整，保证系统安全。

在这一步骤中，完成了主机加固的工作，**使操作系统成为纵深防御体系中的一道坚固防线**。

第四步：安全补丁检查

通过在组织内部所有需要加入管理的主机上安装“安全精灵”组件，实现对主机信息的精确收集。该组件负责搜集补丁信息并在接收到特定信号时与基线管理系统通讯，上报本机安全信息。

在“安全精灵”组件上同时具有远程管理控制功能，控制端能够对所有主机下发安全通告信息、强制安装补丁、强制离线。

这一环节部署成功后，**组织内部的安全基线水准将提升至以单机为最小单位的管理粒度**，当前最困扰系统管理员的安全蠕虫等事件的影响也将被降至最低。

第五步：其它辅助手段

游刃中还提供两款针对服务器的安全审核组件，分别是:

- Web 基线检查模块

能够检测当前流行的 SQL 注入漏洞，并包含两千多种 cgi 漏洞信息;

- 应用健壮性检查模块

包含多种应用(包括数据库)的连接测试方法，有效检验服务器的负载极限。

3.3. 大型网络中管理员的全网实施策略

- Plan 阶段：设定安全基线

首先由网络管理员对他所管理的网络进行全面的端口及应用程序版本调查，定制出网络中哪些应用/端口属于必要的应用服务端口，以此作为企业/组织内部的最优安全基线。

在实际应用中，更具可操作性的案例是采用游刃对网络进行一次全面审核，将该次审核的结果根据企业/组织的安全需求修订调整后作为企业当前安全基线。

- Do 阶段：实行基线审核

采用游刃进行常规的安全审核。

- Check 阶段：报表查询与漏洞验证

根据审核结果验证漏洞、测试修补方式并修复漏洞。

与此同时，可以将游刃的安全审核结果与安全基线进行对照，以此得出企业/组织现状与“理想状态”的差距，

- Act 阶段：漏洞修复

采取各种修补措施（补丁管理、服务管理等）进行漏洞修复工作。

漏洞修复后，可以进一步调整与优化当前的安全基线……又回到 PDCA 模型中的 Plan 阶段。

4. 主要模块描述

4.1. 漏洞知识库

作为基线安全管理系统，漏洞知识库是它的基础。漏洞知识库包含各漏洞相关信息，其中主要信息如下：

- 漏洞名称；
- 漏洞是否存在的检测方法；
- 漏洞描述；
- 漏洞详细解决方案；
- 漏洞威胁级别，如：远程可执行命令、远程信息泄露；
- CVE 编号；
- BUGTRAQ 编号；

4.2.扫描调度引擎

游刃基线安全系统调度引擎是系统最重要的模块之一，它负责完成目标的探测评估工作。相关子模块主要包括:

- 存活子模块，负责目标存活判断;
- 端口扫描子模块，负责目标开放端口探测;
- 服务判定子模块，负责目标开放端口运行服务判定;
- 操作系统类型识别子模块，负责识别目标的操作系统类型、版本、Patch号等。
- 服务－规则索引子模块，负责根据服务类型、操作系统类型到漏洞知识库中检索可能存在的漏洞项，并读入各漏洞项的检测规则。
- 规则解析子模块，负责对读入的规则进行解析，依靠规则解析结果对目标进行探测，最终将探测结果写入扫描结果数据库。

除了主扫描引擎外，游刃基线安全系统还包含多个功能引擎实现不同功能，它们包含:

- 口令策略检查引擎;
- 主机性能测试引擎;
- Web 注入检查引擎;
- 本地补丁检查引擎;

4.3.基线管理（配置管理）模块

基线管理模块能够引导用户通过第一次内网扫描的结果，创建企业/组织内部的安全基线，该基线包括存活主机、开放端口、应用版本、存在漏洞的信息。系统管理员通过对基线的管理，能够实现:

- 减少扫描结果的分析时间;
- 设备配置发生变化时及时发现;
- 新漏洞出现定制安全基线策略，可以快速发现企业存在该漏洞的设备;

4.4. 补丁管理模块

补丁管理模块可以通过两种方式实现，系统管理员可以根据自己的需要选用:

- 知晓被管理主机的管理员用户名及密码;
- 安装了游刃的“安全精灵”Agent;

前者的优点是无需在客户机安装任何软件，后者的优点是能够拥有更强大的扩展功能，例如接入管理（对存在违反安全策略的高风险的主机直接断开网络连接）等。

4.5. 系统升级模块

游刃基线安全系统的系统升级包括主程序升级和漏洞插件升级两部份，采用极其易用的向导方式，用户只需要按向导指引，三个步骤即可轻松完成升级。

大成科技保证每两周对漏洞插件进行升级，如有高风险漏洞出现，则保证48小时内研究并升级完毕。

4.6. 开放式插件接口

游刃基线安全系统用插件来描述漏洞，一个漏洞可能由一个或者多个插件描述，而一个插件也可能涵盖一个或多个漏洞。插件是用 NASL (Nessus Attack Scripting Language) 编写的。

游刃基线安全系统当前有超过 3,200 个 插件，为了便于管理，根据其相关性进行了分类，分成了若干个“插件家族”。“插件家族”以及其所包含的“插件”是系统定义好的，用户不能改变，除非用户下载了并更新了新的漏洞库。

为了方便用户，用户可以设置自己的“插件组”，“插件组”中可以包含整个的“插件家族”，也可以包含某几个插件。系统已经配置好的一些常用的“插件组”，用户还可以自定义“插件组”。在用户执行新的扫描任务时，可以直接选择定义好的“插件组”，而不必再一个一个选择插件。

同时，具备一定编程能力的用户可以采用 NASL 语言描述，对最新的漏洞自行编写插件，以满足独特的功能需求。

5. 主要特性描述

5.1. 特性描述表

表：游刃基线安全系统特性综述

产品		游刃基线安全系统
产品信息	版本	V1.0
	管理方式	专用管理软件
	所用语言	中文
	产品形态	软件
	支持的 OS	Windows NT、Windows 2000、Windows XP、Windows 2003
	部署方式	基于网络
	系统结构	单机
评估方法	推断（检查脆弱性条件）	Y
	自定义	N
扫描对象	邮件类、WEB、FTP、RPC、DNS、SNMP	Y
	DoS 服务	Y
	Finger 类	Y
	CGI 类	Y
	NetBIOS 类	Y
	木马	Y
	IP 欺骗扫描	N
	NIS 类	Y
	Proxy	Y
	数据库	MySQL、MS SQL Server、Oracle
	Windows 系列	Y
	UNIX 系列	Y
	网络设备和防火墙	Y

	国内厂商网络设备	Y
端口扫描	标准服务扫描	Y
	TCP 端口扫描	Y
	UDP 端口扫描	Y
	RPC 端口扫描	Y
	未知端口扫描	Y
	智能服务识别	Y
数据库特性	数据库漏洞数量	>2800
	脆弱性描述	清楚
	相关分析	清楚
	修补措施	详尽
	CVE\bugtraq 编号(便于网络检索)	Y
漏洞库分类	按应用分类	Y
	按端口服务	Y
	按操作系统	Y
	按威胁程度	Y
	按被利用方法	Y
提供可编程接口		Y
支持二次开发		Y
支持虚拟主机扫描		Y
模拟穿透技术		Y
扫描目标信息获取能力		强
任务应用	定制扫描策略	模板化管理
	周期性扫描	Y
	定时扫描	Y
	多主机扫描	多任务、多主机、并行
	支持断点续扫	Y
评估报告	摘要	详细
	风险等级评估	多角度

	漏洞描述及解决方案	非常详尽
	报告可修正	N
	扫描结果可查询	强
	报告导入、导出	导出
	导出为其他文件格式	HTML 文档
	输出报告模板驱动	1 个内置模板 + 自定义
	综合（跨任务）分析和查询	弱
	跨夸任务输出报表	N
支持资产管理	支持资产自动发现	Y
	风险等级和资产挂钩	Y
升级方面	升级内容	软件补丁、漏洞库
	更新方式	手动/自动
	更新频率	15 天
日志方面	日志记录功能	Y（登录、操作、异常日志）
	日志查询	Y
	定制审计策略	Y
分级用户授权管理		Y
扫描速度		2 台/分钟
生成报表速度		快
其他特性		地址簿应用与资产管理结合

5.2. 基本特性

- 渐进式扫描：根据被扫描主机的操作系统和主机应用等信息智能确定进一步的扫描流程；
- 系统稳定性高：扫描过程实时正确处理各种意外情况：如网卡故障、资源耗尽等；
- 扫描特点：扫描系统资源占用少、速度快、误报低、漏报低、稳定性高。
- 全面详尽的漏洞知识库：可检测当今网络上各种流行的安全漏洞隐患，并且知识库不断升级，使得产品随时都能拥有检测最新漏洞的能力。

- 智能端口识别技术：游刃能够智能的识别出那些开放在非标准端口的网络服务并调用针对该服务的相关插件进行扫描，能够最大限度的探测网络的安全漏洞。对于端口伪装有很好的识别能力，从而提升扫描结果的准确性和有效性。
- 模拟穿透技术：游刃采用模拟真实入侵技术来检测主机安全性，这可能对系统服务有影响，但这能保证最大限度地探测目前主机服务的安全性，并且能够探测目前可能还没有报告的安全问题。
- 广泛的用户基础：游刃的前身作为一个自由软件，发布了近三年时间，拥有广泛的用户群，在业界具有一定的知名度。
- 专家级服务：游刃由国内知名安全专家领导开发完成，并由其领导技术支持团队，为客户提供更专业，更优质的服务。

6. 系统指标

6.1. 漏洞库规范

系统漏洞库兼容 CVE 国际规范，同时提供国际 BUGTRAQ 编号。

6.2. 安全评估准确性指标

- 漏报率 ⩽5%
- 误报率 ⩽5%

6.3. 安全评估速度指标

典型情况下游刃基线安全系统扫描速度指标如下：

表：100M 局域网情况

扫描主机数量	扫描时间
1-10	<10 分钟
11-20	<20 分钟

20-40	<35 分钟
1 个通常 C 类网(%60 以上主机存活)	<3 小时

表：ADSL 拨号扫描 Internet 主机情况

扫描主机数量	扫描时间
1-10	<20 分钟
11-20	<40 分钟
20-40	<70 分钟
1 个通常 C 类网(%60 以上主机存活)	<4 小时

6.4. 网络资源占用指标

典型工作情况下带宽占用 6-20 Kb/s。

6.5. 系统资源占用指标

- 建议并行扫描的主机数：20
- 每个主机最大的线程数：50
- 运行扫描系统的资源占用：CPU 平均占用 50%（可以通过配置扫描线程及速度降低资源占用），内存平均占用 15M
- 被扫描系统的资源占用：CPU 小于 1%，内存小于 1%