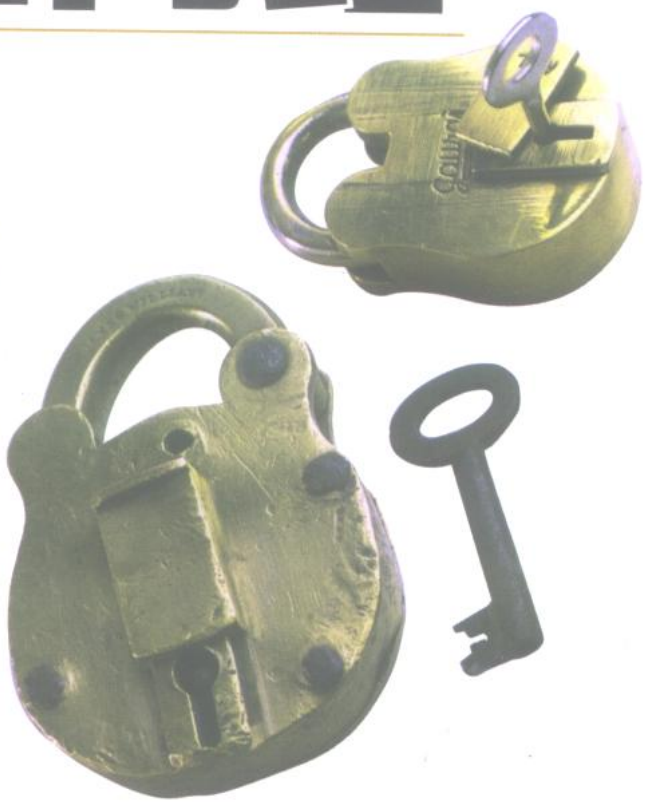
计算机网络安全技术丛书 1

System Scanner

企业网络安全维护高手



〔美〕John Shum 主编
唐晓梅 王俊辉 禄 凯 编译

本书配套光盘内容包括:
本书配套的电子书

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

21

计算机网络安全

System Scanner

企业网络安全维护高手

[美] John Shum 主编
唐晓梅 王俊辉 禄 凯 编译

本书配套光盘内容包括
本书配套的电子书

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书是“计算机网络安全技术丛书”中的一本。介绍美国ISS公司开发和研制的网络监控工具System Scanner（SS）的使用方法和技巧。

System Scanner是监控企业内部主机运行状态的“火眼金睛”。本书由7章和3个附录组成，内容包括：System Scanner基础知识，实施风险评估，锁定系统，使用报表，生成警报，管理System Scanner环境和使用策略。附录A是相关参考资料的查找方法和推荐的参考书目，附录B重点讨论了System Scanner中应用的各种策略，附录C介绍如何配置控制台。本书的最后还提供了相关术语的解释，以供读者参考。

本书内容新、描述详尽、实用性强，不仅是网络安全、网络管理和网络维护的广大从业人员必备的参考书，同时也是高等院校相关专业师生和社会相关领域业内人士不可缺少的教学、自学用书。

本书配套光盘内容包括与本书配套的电子书。

系　列　书：计算机网络安全技术丛书（1）
书　　名：System Scanner企业网络安全维护高手
文本著作者：John Shum 主编　唐晓梅　王俊辉　禄凯　编译
文本审校者：希望图书创作室
CD制作者：希望多媒体开发中心
CD测试者：希望多媒体测试部
责任编辑：苏静
出版、发行者：北京希望电子出版社
地　　址：北京海淀路82号，100080
网址：www.bhp.com.cn
E-mail: lwm@hope.com.cn
电话：010-62562329，62541992，62637101，62637102，62633308，62633309
（发行和技术支持）
010-62613322-215（门市）　010-62531267（编辑部）
经　　销：各地新华书店、软件连锁店

排　　版：希望图书输出中心
CD生产者：文录激光科技有限公司
文本印刷者：北京广益印刷厂
开本/规格：787毫米×1092毫米　1/16开本　8.125印张　166千字
版次/印次：2000年5月第1版　2000年5月第1次印刷
印　　数：0001–5000册
本 版 号：ISBN 7-900031-85-5/TP·85
定　　价：20.00元（1CD，含配套书）

编者的话

欢迎使用《System Scanner》一书。Internet Security Systems 公司是致力于 Internet 的安全性管理解决方案的全球第一流的提供者。本书配合 Internet Security Systems 公司的 System Scanner 软件的发行，专门说明 System Scanner 的使用方法和功能特点。System Scanner 是 Internet 安全系统公司推出的一种基于主机的企业安全管理解决方案。该方案提供基于主机的安全评估识别并报告安全缺陷、弱点及策略非一致性等功能；另外，系统扫描器还支持创建系统基准。当检测到与系统基准发生的任何偏差时，可自动产生报表或报警，还能够提供 Windows NT 系统的实时报警。

本书由唐晓梅、王俊辉、禄凯共同编写，全书由唐晓梅负责整理。本书适合于所有的网络工作者、大学及专业技术研究人员、Internet 服务提供商等相关人员。

目　录

第 1 章　介绍 System Scanner

引言

什么是 System Scanner（系统扫描器）？

System Scanner 是 Internet 安全系统公司推出的一种基于主机的企业安全管理解决方案。该方案提供基于主机的安全评估识别并报告安全缺陷、弱点及策略非一致性等功能；另外，System Scanner 还支持创建系统基准。当检测到与系统基准发生的任何偏差时，可自动产生报表或报警，并能够提供 Windows NT 系统的实时报警。

内部安全性评估

System Scanner 通过一个安装于每个待管理系统的代理程序，对系统安全缺陷、错误配置及策略非一致性实施检测。这些 System Scanner 代理软件允许借助中央管理系统对整个企业进行持续管理及安全策略控制。

Internet 安全系统公司概述

Internet 安全系统公司是业内领先的网络安全监控、检测及响应软件的软件供应商，该软件旨在保护企业信息系统的安全性与完整性。

本书所包含的内容

各章概述

第 1 章：介绍 ISS 和 4.0 版 System Scanner。

第 2 章：说明如何利用会话实施扫描，以及如何进行会话调度，以完成手动切断及预定的评估工作。

第 3 章：阐明系统锁定的目的，如何为文件确定基准，以及怎样为特例进行注册。

第 4 章：阐明报表类型以及如何生成这些报表。本章还将描述由 System Scanner 采集的数据在用于评估现行安全策略的报表中如何体现。

第 5 章：描述报警类型，如何产生，以及报警如何向用户报告发生针对网络的攻击行为。

第 6 章：阐明如何维护 System Scanner 工作环境。System Scanner 工作环境包括代理软件、类、扫描组以及日志文件。

第 7 章：说明确定 System Scanner 策略的目的，如何配置定制策略，以及如何将其应用到公司网络中。

附录概述

附录 A：列出了 Web 站点、书籍和其他安全方面的参考资料。

附录 B：描述 System Scanner 中所包括的策略，以及用户可根据其网络企业的安全需求创建定制策略。

附录C：阐明如何配置控制台。

节A：System Scanner

概述

System Scanner是一款用于系统安全缺陷评估产品，用于分析企业范围内网络中的设备安全性。

报表

System Scanner预先确定了有助于采集所需信息以做出安全性策略的报表。

启动安全缺陷扫描

用户可以通过以下几种途径生成报表数据：

- 确定System Scanner工作时间，从而达到自动扫描网络的目的。
- 确定扫描器是通过命令行还是用户界面启动扫描。
- 通过命令行或用户界面生成报表数据。

关于扫描

为什么实施扫描？

实施扫描能够确保系统免受损害，或至少保证在可接受数量范围内的安全性。该数量值通常由系统管理员或网络管理员决定，在系统“锁定”时使用。System Scanner代理程序在每个安装该软件的系统内部实施扫描。

什么是安全缺陷？

安全缺陷指操作系统或服务内部的安全漏洞，它使入侵者有可能获取导致非授权访问或恶意操作的信息。

如果想要了解有关单个系统安全缺陷及补救措施的更详细资料，请访问站点http://www.iss.net/xforce/中的X-Force 安全缺陷目录。

运行扫描概述

你既可以通过命令行，也可以利用GUI界面运行扫描。运用命令行需考虑的事项包括：

命令行操作：

系统提供命令行操作旨在使用户可通过命令行运行System Scanner，而不是图形用户界面。命令行允许在System Scanner网络中启动扫描与会话。

控制台命令行：控制台命令行允许你在控制台上启动会话。

代理程序命令行：该命令行允许用户利用策略在单个代理程序中运行扫描。

System Scanner的用途

检测优势

System Scanner 可完成业内的 Unix 及 Windows NT 操作系统中各种安全缺陷检测，从收集信息到发现安全缺陷，范围极广。System Scanner 可通过检查网络设备、服务及其相互关系来查找各种安全缺陷，令入侵者无机可趁。这种自动进行且全面广泛的检测相比孤立无援的管理员警惕性而言，拥有诸多优势，其中包括速度、易用性以及全面性等。

安全缺陷相关信息

System Scanner 提供有关安全缺陷的详细资料，比如易受攻击的主机、描述以及纠正措施等。它还提供利用图解说明的管理及系统运行趋势分析报表。

扫描器应用于何种网络?

除独立网络和机器以外，System Scanner 还可应用于所有基于 TCP/IP 协议的网络。

System Scanner 的日常工作

System Scanner 的日常工作包括：

- 运行网络扫描：既可以通过命令行，也可利用图形用户界面运行扫描。还可以对扫描实施调度，以达到无人值守工作。
- 结果分析：可以通过创建并检查由 System Scanner 或定制应用生成的各种报表对扫描结果进行分析；还可以利用用户界面以及 Crystal 报表工具加载以前的扫描结果并对其实施分析。

需考虑的事项

在查找系统安全缺陷时，许多为 System Scanner 所用的测试操作增加了系统操作的局限性。在规划或执行一项测试计划时，需考虑下表列出的问题：

表 1　执行一个测试计划

问　题	描　述
通知用户	在执行扫描前，需通知已扫描设备的单个用户。通过这种方法，系统拥有者就能够了解哪个扫描经过授权，从而根据扫描结果采取措施，对系统进行改善
不同的扫描时间	在一天或一个星期中的不同时间运行扫描，以增加或许在特定时间无法获得的系统访问机会
在已验证系统中运行未实施调度的扫描	在确定某个系统的安全性后，不时执行未定时扫描以维持网络安全性。仅在经过定时扫描的系统中使用未定时扫描
新系统	在安全网络中加入新系统后，尽快对新系统实施扫描。该扫描可与可靠系统及网络连接协同执行
免除扫描的系统	允许系统因特殊需要、环境或调整（比如有待升级）等理由而选择不实施扫描

安全策略的确定与执行

定义

安全策略的确定与执行意味着：

- 保证包含或解决了整个网络中的所有可应用安全缺陷。
- 确保所有系统都以一种与组织策略相一致的安全方式配置完毕。
- 及时对所有具有潜在危害的威胁实施检测、监控及响应。
- 快速修复检测到的安全缺陷。
- 为负责对付网络威胁与安全缺陷的管理人员提供及时安全报警。
- 提供准确的网络安全核查及系统运行趋势分析数据，以支持安全方案规划及评估计划。

同等安全性

如果没有充分考虑这些问题，安全方案则可能提供装饰性能效，但并不是整体解决方案。

因素

安全解决方案由以下因素组成：

- 风险分析
- 策略
- 执行
- 威胁/安全缺陷监控
- 威胁/安全缺陷响应

第 2 章　实施风险评估

引言

概述

System Scanner 通过在网络中运行扫描实施风险评估，以检测安全缺陷和安全弱点。扫描从控制台启动，并在代理系统中运行。

本章内容

本章包含的内容

表 2 提供了本章中包含的各节标题。

表 2　评估各章标题

标题	所阐述的内容
“配置会话”	• 缺省会话 • 增加会话 • 删除会话 • 定制会话 • 增加会话映射 • 删除会话映射 • 使用更新的会话命令
“利用会话实施扫描”	• 运行会话
“会话调度”	• 会话调度 • 增加调度 • 删除调度

节 A：配置会话

引言

什么是会话？

会话指网络中基于策略与代理系统相关的文件。在网络中运行扫描时需要使用会话。会话一旦准备好，用户就可利用它同时扫描几个系统。

目的

会话可用于确保在适当的系统中基于安全策略实施安全检查。

什么是会话映射?

会话映射指代理或代理级别与策略的结合。一个会话可能包括几个会话映射。有关级别的详细信息，参见“管理代理级别”。

示例

例如，在网络中的代理 1，3 和 8 上运行策略维护-1，创建一个包含下列会话映射的会话。表 3 提供了会话映射的示例。

表 3 会话映射示例

会话	会话映射
维护-1	代理 1
维护-1	代理 3
维护-1	代理 8

缺省会话

概述

System Scanner 控制台已知的每个策略都会自动创建一个与策略同名的缺省会话。

目的

利用缺省会话，可以通过向已有缺省会话中增加新代理而迅速完成整个网络的配置任务。

增加定制会话

概述

当现有缺省会话不能满足网络安全要求时，可利用控制台增加新定制会话。

操作过程

增加会话的步骤如下：

1. 在 System Scanner 启动对话框中单击管理界面。
2. 在 File 菜单中选择“New”，然后选择“Session(会话)”，新会话对话框出现。
3. 在会话名称栏中键入会话名称，接着单击“OK”。该会话则被增加到会话目录树中。

注意 在为会话命名时，确保该名称与策略名称不同。如果名称相同，可能会导致定制会话被策略的缺省会话覆盖。

4. 如果需要查看描述信息，则键入有关会话的简短描述（比如用户系统等）。报表生成后就会显示描述信息。详细资料参见“与报表协同工作”。

下一步是什么?

在运行会话前增加会话映射。参见“增加会话映射”。

定制会话

概述

定制会话是由用户创建的、不必与单一策略相关的会话。

目的

在缺省会话不能够满足系统安全要求时，System Scanner 提供创建定制会话的能力。利用定制会话，可以映射多个系统与策略的结合体。

示例

创建会话可完成以下任务：

- 在多个策略文件和一个系统间建立映射。（比如系统 1 映射所有组、所有用户和密码）。
- 在几个策略文件和几个系统间建立映射。（比如系统 1 和系统 8 映射所有用户组，系统 2 和系统 4 映射密码）。
- 在一个系统和一个策略文件间建立映射。（比如系统 2 映射所有用户）。
- 在几个系统和一个策略文件间建立映射。（比如系统 1，系统 2 和系统 3 映射所有用户组）。
- 在一个级别中的所有系统和一个策略文件间建立映射。（比如映射 Winnt 到所有用户组）。

删除定制会话

概述

利用控制台可删除过时或无用的会话，以提高 GUI 的可读性，并有助于保持控制台的实时性。

注意　已删除的会话不可能恢复。

操作过程

删除会话的步骤如下：

1. 在 System Scanner 的启动对话框中单击管理界面。
2. 扩展会话目录树，单击会话名称。
3. 在文件菜单中选择“删除”。此时会出现一个对话框，询问“你是否确定将删除会话 session name？”
4. 单击“是”，以确定删除操作。

使用更新会话命令

目的

使用更新会话命令的目的在于利用控制台自动更新缺省会话。会话信息将基于网络中的代理策略进行收集。缺省会话拥有与策略相同的名称。

注释：你必须注意确保所有代理软件处于连接状态，并正常通信。只有成功查询的会话才会包括在结果会话中。

操作过程

表4显示了运行更新会话命令的步骤。

表4 更新会话命令运行步骤

阶段	所产生结果
1	控制台查询所有代理系统以确认通信。
2	所有查询所得的代理向控制台发送其存贮的策略。
3	控制台为每个已标识的策略创建或修改会话。

注意 运行更新会话时，任何对缺省会话所作的编辑操作均失效。

操作过程

更新会话的步骤如下：

1. 在 System Scanner 启动对话框中单击管理界面。
2. 在维护菜单中选择更新会话选项。

下一步是什么？

根据从 System Scanner 网络中代理发送的的信息，控制台保留最新的会话。

增加会话映射

概述

当需要定制会话以满足特定的安全需求时，增加会话映射很有用。会话映射包括策略和代理。

先决条件

在增加会话映射时，必须首先显示该会话。

操作过程

增加会话映射的步骤如下：

1. 在 System Scanner 启动对话框中单击管理界面。
2. 扩展会话目录树，单击会话名称。
3. 对于代理到策略的映射，单击“新建”。此时会显示新会话输入对话框。
4. 对于代理，寻找并选择代理系统。
5. 选择出现在右边的策略，并单击“增加”。
6. 重复步骤5，继续增加会话映射。
7. 单击“OK”。
8. 从文件菜单中选择“保存”。

下一步是什么？

修改被保存，会话已准备就绪，可以进行扫描。

删除会话映射

概述

当需要定制会话以满足特定安全需求时，删除会话映射很有用。会话映射包括策略和代理。

先决条件

增加会话前必须先显示会话。

操作过程

创建定制会话的步骤如下：

1. 在 System Scanner 启动对话框中单击管理界面。
2. 扩展会话目录树并单击会话名称。
3. 对于代理向策略的映射，单击代理向策略映射。
4. 单击“删除”。
5. 重复步骤 4，删除其他会话映射。
6. 从文件菜单中选择“保存”。

下一步是什么？

现在，会话已删除，不能继续使用。

节 B：利用会话进行扫描

引言

分布式风险评估

分布式风险评估是 System Scanner 最强大的功能之一。利用会话，管理员可以从控制台对各种网络的扫描进行配置、运行并生成报表。

分布式风险评估如何工作

管理员可通过控制台对 System Scanner 网络中的扫描进行配置及初始化；扫描结果经加密后，发回控制台，以供查看与分析。

利用控制台，既可以对单个代理，也可以对代理组进行配置及初始化。管理员可将代理或级别置入会话中，以简化配置与远程扫描的运行工作。

级别

在决定对哪个级别进行定义以便扫描时，将代理包括在大量级别中，可为操作带来极大的灵活性。

扫描选项

实施系统扫描时，可以使用以下选项：

- 在激活状态下运行会话
- 实施会话调度

在激活状态下运行会话

先决条件

在通过控制台扫描代理之前，必须创建相应的会话，该会话在希望运行的策略与需进行扫描的特定系统间建立映射。

查看结果

扫描结果以 HTML 格式生成报表，并于扫描结束后在用户缺省浏览器中显示。若使用更多控制选项，如执行报表及技术报表等，则可以获得 Crystal 报表。

操作过程

运行扫描的步骤如下：

1. 在系统扫描启动对话框中单击“启动会话”，此时显示启动安全检查对话框。
2. 利用会话名称选择需扫描的会话。
3. 单击“启动扫描”。此时扫描开始，结果在 HTML 报表中显示。有关报表的详细资料，参见“缺省 HTML 报表”部分。

下一步是什么？

扫描结束后可生成报表，详见 “生成报表”部分。

节 C：会话调度

引言

目的

扫描调度的目的在于定期对 System Scanner 网络进行扫描，以确保安全性。已进行了调度的会话不需要监控或用户的互操作；因此，创建一个高效的调度表有助于简化安全处理并减少系统开销。

查看结果

结果必须在已调度的扫描结束后由控制台生成。详细资料参见“分析扫描结果”部分。

调度选项

扫描调度选项包括：

- 一次
- 每小时一次
- 每周一次
- 每月一次

- 每天一次
- 系统重新启动时进

理解调度控制数据

控制数据

在建立调度时，会生成调度控制数据。一旦增加一个调度，相应调度数据就会显示在窗口右边。调度控制数据以下列格式保存为 crontab 文件：[控制数据][会话名称]。

crontab 文件中控制数据部分由 5 个整形字段组成，字段间用空格相隔，以下为各字段：

- 分钟（0-59）
- 小时（0-23）
- 每月的日期（1-31）
- 每年的月份（1-12）
- 每周的日期（0-6，其中 0 代表星期日）

其中的模式可以是星号（代表所有有效值），也可以是用逗号相隔的一系列元素。一个元素既可以是数字，也可以是两个用破折号相隔的数字（代表所包含的范围）。注意，详细说明某一天可由两个字段组合完成（一个月中的日期和一个星期中的日期）。如果两个字段均由一系列元素说明，则字段都必须严格遵守该说明。比如 0 0 1,15 * 1 在每个月的第 1 天、第 15 天和每个星期一运行命令；如果仅使用一个字段说明某一天，那么另一个字段必须设为*（例如，0 0 * * 1 只在每个星期一运行命令）。

会话名称

crontab 文件中一行里的第 6 个字段是扫描所使用的策略名称。

增加调度

操作过程

增加调度的步骤如下：

1. 在 System Scanner 启动对话框中单击管理界面。
2. 在“检查”控制菜单中选择“会话调度”，此时会显示会话调度窗口，提供当前所有由控制台定义的 System Scanner 调度任务的详细信息。
3. 在“会话”菜单中单击相应会话实施调度。
4. 完成下列步骤之一：

如果想让扫描按以下选项运行	则...
运行一次	1. 单击“运行一次”。 2. 设置时间。 3. 设置日期及月份。
每小时运行一次	1. 单击“每小时运行一次”。 2. 设置整点过后的分钟数。

（续表）

如果想让扫描按以下选项运行	则...
每星期运行一次	1. 单击“每星期运行一次”。 2. 设置时间。 3. 设置每星期中的日期。
每月运行一次	1. 单击“每月运行一次”。 2. 设置时间。 3. 设置每月中的日期值。
每天运行一次	1. 单击“每天运行一次”。 2. 设置时间。 3. 如果不需要在一星期中的七天都运行扫描，则单击“哪一天”，对于不想运行扫描的日期，不设置即可。
系统重新启动时运行	1. 单击“在重新启动时运行”。 2. 单击“哪一天”。 3. 单击需运行的日期。 4. 单击“OK”。

5. 单击“增加任务”，此时会在窗口右边显示调度控制数据。
6. 单击“OK”。

下一步是什么？

生成基于会话的报表，既可以通过互操作完成，也可以在调度对话框中使用选项进行设置。在会话调度时，会创建一个名称为“_<会话>”的报表会话。详细内容参见“生成报表”部分。

删除调度

操作过程

删除调度的步骤如下：

1. 在“系统扫描启动”对话框中单击“管理界面”。
2. 在“检查”控制菜单中，选择“会话调度”，此时会显示“会话调度”窗口，提供由控制台定义的所有当前 System Scanner 的调度任务。
3. 高亮显示调度数据并删除相应条目。
4. 单击“OK”接受删除。