安全漏洞扫描服务

目录

一. 概述

1.1 基本概念

安全漏洞(security hole)

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。是受限制的计算机、组件、应用程序或其他联机资源的无意中留下的不受保护的入口点。

0-day 攻击（Zero-Day Attack）

0-day 通常是指还没有补丁的漏洞，而 0-day 攻击则是指利用这种漏洞进行的攻击。提供该漏洞细节或者利用程序的人通常是该漏洞的发现者，0-day 漏洞的利用程序对网络安全具有巨大威胁。

绿盟 RSAS（绿盟 Remote Security Assessment System）

绿盟远程安全评估系统，采用高效、智能的漏洞识别技术，第一时间主动对网络中的资产进行细致深入的漏洞检测、分析，并给用户提供专业、有效的漏洞防护建议，让攻击者无机可乘，是专业化的“漏洞管理专家”。

Open VM（Open Vulnerability Management）

开放漏洞管理工作流程平台，平台将漏洞管理的循环过程划分为漏洞预警、资产管理、漏洞分析、漏洞修复、漏洞审计五个阶段。基于这个开放平台，RSAS 将漏洞管理理念贯穿于整个产品实现过程，实现了 Open VM 的绝大部分过程。

NSIP

智能 Profile 漏洞识别技术，采用多种技术通过不同途径收集目标系统的多种信息，这些信息就是目标系统的 Profile，在进行漏洞评估过程中，Profile 不断地对中间的结果数据进行调整，保障了最后评估结果的准确性。

1.2 服务发展情况

从互联网兴起至今，利用漏洞攻击的网络安全事件不断，并且呈日趋严重的态势。每年全球因漏洞导致的经济损失巨大并且在逐年增加，漏洞已经成为危害互联网的罪魁祸首之一，也成了万众瞩目的焦点。安全漏洞扫描是一种针对系统、设备、应用的漏洞进行自动化检测、评估到管理的过程，广泛应用于信息系统安全建设和维护工作，是评估与度量信息系统风险的一种基础手段。

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，可以使攻击者在未授权的情况下访问或破坏系统。安全漏洞有很多种分类方式，按照漏洞宿主不同，可以分为三大类：第一类是由于操作系统本身设计缺陷带来的安全漏洞，这类漏洞将被运行在该系统上的应用程序所继承；第二类是应用软件程序的安全漏洞；第三类是应用服务协议的安全漏洞。近年来，针对应用软件程序和应用服务协议安全漏洞的攻击越来越多，同时利用病毒、木马技术进行网络盗窃和诈骗的网络犯罪活动呈快速上升趋势，产生了大范围的危害，由此造成的经济损失也是越发巨大。

针对 Web 应用安全漏洞的攻击也在逐渐成为主流的攻击方式。利用网站操作系统的漏洞和 Web 服务程序的 SQL 注入漏洞等，黑客能够得到 Web 服务器的控制权限，从而轻易篡改网页内容或者窃取重要内部数据，甚至在网页中植入恶意代码（俗称“网页挂马”），使得更多网站访问者受到侵害。

随着技术的不断进步，漏洞的发现、漏洞利用技术也发展到一个较高水平，从总体上来看，漏洞的发展趋势主要表现为以下几个方面：

- Windows 系统应用广泛，依然是黑客重点注意的目标。2010 年微软共发布了 106 个安全公告，修复了 247 个漏洞，比上一年多了 57 个，公告中 41 个是最高的严重级别，60 个为重要级别，没有 low 级别，其中操作系统漏洞达到 214 个。
- 随着虚拟化长足发展，基于虚拟化软件的安全漏洞挖掘及漏洞利用是最常见也是危害比较严重的。截至到目前为止，一些知名虚拟化软件的安全漏洞已经达到上百个，占据 X86 虚拟化市场绝对份额的 VMware 更是首当其冲。近些年来先后发生过如虚拟环境下共享文件夹目录遍历漏洞、VMware 的 Mac 版本 Fusion 安全漏洞导致通过 Windows 虚拟机在 Mac 主机上执行恶意代码等。

- 国际上出现大量的专业漏洞研究组织，漏洞的出现到漏洞被利用的时间在不断的缩短，同时 0-day 攻击的数量在逐渐增加。
- 利用漏洞攻击的重心由服务器端向客户端过渡，由系统层和网络层逐渐向应用层扩展；Web 应用安全漏洞造成危害日益凸显。
- 漏洞的发现、利用不仅仅局限于常见的网络设备、操作系统，而且不断的向新的应用领域扩散。
- 利用漏洞的蠕虫逐渐减少，利用漏洞攻击的手法越来越诡异，越来越隐蔽。

第一款商用漏洞评估产品诞生到现在，漏洞评估产品已有 20 多年的历史了。作为一种信息安全基础工具应用在信息系统的安全保障中，漏洞扫描产品已经成为信息安全领域中最为成熟的产品之一，同时安全漏洞扫描服务也是安全服务中基础服务项之一。

安全漏洞评估的发展大致可以分为两个阶段：第一个发展阶段的特性是安全测试工具，用户使用这类工具，尽可能模拟黑客攻击行为，为进一步分析系统的缺陷提供测试数据。代表性产品有早起的 Nmap、Nessus、Nikto 等；这个阶段模拟攻击的测试工具，围绕“探测与发现”，更多关注某个具体的漏洞，比如弱口令、操作系统的某个漏洞、CGI 的某个漏洞网路协议的某个漏洞。集中在“探测与发现”能力上，在提供给用户解决方案上存在不足；同时该阶段的漏洞评估产品基本没有考虑基于扫描结构的后期分析、统计；无法帮助用户对资产的漏洞进行方便的管理。

第二个发展阶段是安全评测与管理工具，融入了资产、风险管理等概念，为用户提供了更为全面的漏洞评估和资产管理能力，代表性产品有绿盟 RSAS、IBM ISS、McAfee Vulnerability Manager 等。这个阶段以 IT 资产为核心，侧重于漏洞生命周期管理。单靠完成检测而不能实现真正意义上的漏洞修复闭环，已经不能应对日益变化的安全漏洞形势，因此安全漏洞扫描基于漏洞扫描核心技术，并将 IT 资产与风险漏洞相结合，在尽可能准确发现网络主机的安全漏洞之余，还可以协助管理员进行漏洞修补。所以安全漏洞扫描服务是进一步加强了“探测与发现”漏洞全面性，同时增强了帮助用户“管理漏洞”侧重“修复”的能力。在发现的基础上，对每个漏洞给出详细信息和一些修补建议。

安全漏洞扫描服务是一项极具挑战的课题，是信息安全工作过程中治本的方式，只有通过对风险的控制与消除才能从根源上消除安全威胁。面临千变万化的攻击手法，单纯采取被动防御的技术手段越发显得力不从心，更多的用户开始关注风险的管理与度量，侧重在“事

前”尽量降低甚至规避风险。另一方面，国家政策和行业法规对安全风险监督的不断严格，需要采用更有效的风险管控手段进行自身安全管理以满足不断严格的合规监管要求。因此漏洞评估将在信息安全技术发展中扮演越来越重要的角色。

1.3 服务的必要性

安全漏洞扫描服务，针对系统、设备、应用的脆弱性进行自动化检测，帮助企业或者组织来侦测、扫描和改善其信息系统面临的风险隐患；侦测某个特定设备的系统配置、系统结构和属性；执行安全评估和漏洞检测；提供漏洞修补和补丁管理；是企业和组织进行信息系统合规度量和审计的一种基础技术手段。

随着企业 IT 规模的不断增大，在网络安全建设中面临千变万化的攻击手法，单纯采取被动防御的技术手段越发显得力不从心，更多的用户开始关注风险的管理与度量，侧重在“事前”尽量降低甚至规避风险。“探测与发现”漏洞全面性，同时增强了帮助用户“管理漏洞”侧重“修复”的能力。实现真正意义上的漏洞修复闭环，应对日益变化的安全漏洞形势。

漏洞扫描是确定安全漏洞修补方案的最佳手段。

参与漏洞扫描的人员具有丰富的漏洞分析和修补方面的经验，能够为客户提供更加详细、更具针对性的解决方案。

漏洞扫描产品可以帮助客户发现安全漏洞，但是只能对漏洞进行粗浅的定性和不够完备的解决方案，无法达到安全漏洞精细化管理的目标。而漏洞扫描正是对其最有效的补充。

1.4 客户收益

对于客户而言，漏洞扫描可以为其带来如下收益：

◆ 节省企业成本

漏洞扫描的过程包括现在漏洞全面检测，漏洞分析，安全评估及安全建议，无需客户另行购买漏洞扫描产品，因此，不存在设备的运行和升级维护成本、人员设备管理成本。

◆ 漏洞修补目标明确

漏洞扫描报告中明确了漏洞的修补建议，客户不再需要耗费大量的时间去分析哪些漏洞需要怎么处理，既减少了漏洞分析过程所耗费的时间，也可以将主要的精力放在漏洞的修补

上面。而且漏洞扫描报告中已经提供了关于每个漏洞确实可行的修补方案，客户一般只需要按照建议修补即可。

- 提高安全意识

周期性的漏洞扫描可以及时为客户提供近期系统中存在的安全漏洞，解决了因管理人员忙于其它事务没时间进行漏洞扫描而带来的安全管理缺失。

二. 服务的实施标准或原则

2.1 政策文件或标准

安全漏洞扫描服务将参考下列有关标准或规范进行工作。

- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）
- 《中华人民共和国计算机信息系统安全保护条列》
- GB/T 20270-2006 信息安全技术 《网络基础安全技术要求》
- GB/T 20271-2006 信息安全技术 《信息系统通用安全技术要求》
- GB/T 20272-2006 信息安全技术 《操作系统安全技术要求》
- GB/T 20273-2006 信息安全技术 《数据库管理系统安全技术要求》
- GB/T 20278-2006 信息安全技术 《网络脆弱性扫描产品技术要求》
- GB/T 20280-2006 信息安全技术 《网络脆弱性扫描产品测试评价方法》
- GB/T 21028-2007 信息安全技术 《服务器安全技术要求》
- GB/T 21050-2007 信息安全技术 《网络交换机安全技术要求》
- GB/Z 20985-2007 信息安全技术 《补丁与脆弱性管理指南》
- GB/T 20984-2007 信息安全技术 《信息安全风险评估规范》
- 《Common Vulnerabilities & Exposures 公共漏洞和暴露》
- 漏洞扫描最佳实践
- 安全服务工作规范、漏洞扫描实施规范
- ……

2.2 服务原则

在提供安全漏洞扫描服务中，将遵循下列原则。

- 保密性原则

参与安全服务项目的安全工程师会遵循保密性原则，确保客户的相关信息的保密性和安全性。同时为了确保评估人员严格按照《秘密保护管理办法》执行客户相关信息的保密工作，公司安排了专门的人员实时负责监督和纠正评估人员工作中可能出现的危害的客户信息安全的行为。

◆ 科学性原则

安全漏洞扫描服务遵循科学性原则，安全服务部会对整个安全服务项目进行科学性管理，安全监控，进度把握，以此提高安全漏洞扫描的服务质量。

◆ 规范性原则

整个服务会按照的项目实施规范进行，从客户交流，项目会议，项目资料及输出报告；从项目的项目经理，实施人员，技术支持都做到规范化管理。

◆ 专业性原则

从项目管理，具体实施，漏洞分析，安全建议，报告撰写；的安全漏洞扫描服务都是专业性的。从技术交流，方案确定，现场实施，安全分析及安全建议，在整个服务项的过程中都会体现出项目经理的专业性管理，体现出安全工程师的专业性技术；为客户提供专业的安全服务方案。

三. 漏洞扫描服务

3.1 服务范围

漏洞扫描服务可以为客户提供包括网络设备、操作系统、数据库、常见应用服务器以及WEB 应用等范围的扫描。

漏洞扫描的详细服务范围如下：

◆ 操作系统

Windows、发行版 Linux、AIX、UNIX 通用、Solaris、FreeBSD、HP-UX、BSD 等主流操作系统。

◆ 数据库

Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库。

◆ 常见应用服务

Apache、IIS、Tomcat、Weblogic 等主流应用服务，常见 FTP、EMAIL、DNS、TELENT、POP3、SNMP、SMTP、Proxy、RPC 服务等。

◆ Web 应用程序

ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 应用程序。

◆ 网络设备

常见的路由器、交换机等设备。

3.2 服务内容

安全漏洞扫描会对信息系统内的网络设备、操作系统、应用软件、中间件和服务等进行安全漏洞识别，详细内容如下：

3.2.1 网络层漏洞识别

◆ 版本漏洞，包括但不限于 IOS 存在的漏洞，涉及包括所有在线网络设备及安全设备。

- 开放服务，包括但不限于路由器开放的 Web 管理界面、其他管理方式等。
- 空弱口令，例如空/弱 telnet 口令、snmp 口令等。
- 网络资源的访问控制：检测到无线访问点，……
- 域名系统：ISC BIND SIG 资源记录无效过期时间拒绝服务攻击漏洞，Microsoft Windows DNS 拒绝服务攻击，……
- 路由器：Cisco IOS Web 配置接口安全认证可被绕过，Nortel 交换机/路由器缺省口令漏洞，华为网络设备没有设置口令，……
- ……

3.2.2 操作系统层漏洞识别

- 操作系统（包括 Windows、AIX 和 Linux、HPUX、Solaris、VMware 等）的系统补丁、漏洞、病毒等各类异常缺陷，……
- 空/弱口令系统帐户检测
- 例如：身份认证：通过 telnet 进行口令猜测，……
- 访问控制：注册表 HKEY_LOCAL_MACHINE 普通用户可写，远程主机允许匿名 FTP 登录，ftp 服务器存在匿名可写目录，……
- 系统漏洞：System V 系统 Login 远程缓冲区溢出漏洞，Microsoft Windows Locator 服务远程缓冲区溢出漏洞，……
- 安全配置问题：部分 SMB 用户存在薄弱口令，试图使用 rsh 登录进入远程系统，……
- ……

3.2.3 应用层漏洞识别

- 应用程序（包括但不限于数据库 Oracle、DB2、MS SQL，Web 服务，如 Apache、WebSphere、Tomcat、IIS 等，其他 SSH、FTP 等）缺失补丁或版本漏洞检测，……
- 空弱口令应用帐户检测。

- 数据库软件：Oracle tnslsnr 没有设置口令，Microsoft SQL Server 2000 Resolution 服务多个安全漏洞，……
- Web 服务器：Apache Mod_SSL/Apache-SSL 远程缓冲区溢出漏洞，Microsoft IIS 5.0 .printer ISAPI 远程缓冲区溢出，Sun ONE/iPlanet Web 服务程序分块编码传输漏洞，……
- 电子邮件系统：Sendmail 头处理远程溢出漏洞，Microsoft Windows 2000 SMTP 服务认证错误漏洞，……
- 防火墙及应用网管系统：Axent Raptor 防火墙拒绝服务漏洞，……
- 其它网络服务系统：Wingate POP3 USER 命令远程溢出漏洞，Linux 系统 LPRng 远程格式化串漏洞，……
- ……

3.3 服务方式

3.3.1 本地扫描和互联网扫描

本地扫描是指经过用户授权后，扫描人员达到用户工作现场，根据用户的扫描目标直接接入到用户的办公网络或业务网络中。这种扫描的好处就在于免去了扫描人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部服务器地址的威胁源或路径。

互联网扫描与本地扫描相反，扫描人员无需到达客户下场，直接从互联网访问用户的某个接入到互联网的系统并进行扫描即可。这种扫描往往是应用于那些关注互联网开放服务的用户，主要用于检测互联网开放服务的威胁源或路径。

3.3.2 单次服务和年度服务

安全漏洞扫描服务包括一次性服务和年度服务两种形式，服务地点可以选择客户现场和远程两种方式，客户可以根据需要选择适合自己的服务方式。

单次服务：适合漏洞出现不太频繁的系统。在客户提供扫描目标后，由扫描人员一次性扫描后，针对扫描结果进行输出，完成扫描后向客户提交报告，并指导客户进行漏洞的修补。

单次服务能够发现扫描时间点之前的所有安全问题，有效帮助客户确认系统当前面临的安全风险。

年度服务：适合漏洞出现较为频繁的系统。服务期限以年为单位，服务年度内帮助客户进行有限次数（每月/双月/季度/半年）的漏洞扫描工作，每次扫描均会提供详细的扫描报告，并指导客户进行漏洞修补。

3.4 服务流程

整个安全漏洞扫描服务的流程分为三个阶段：准备阶段、扫描过程和报告汇报。通过这三个阶段结合安全漏洞扫描内容和实际客户系统情况，完成安全漏洞扫描服务。

准备阶段：前期技术交流包括相关安全扫描技术、扫描原理、扫描方式及扫描条件进行交流和说明；同时商谈安全漏洞扫描服务的范围，主要是哪些主机，网络设备，应用系统等；并结合实际业务情况需求，确定扫描范围，扫描实施的时间，设备接入点，IP 地址的预留，配合人员及其他相关的整体漏扫方案。

扫描过程：依据前期准备阶段的漏扫方案，进行漏洞扫描、漏洞分析和漏洞测试，扫描过程主要是进行范围内的漏洞信息数据收集，为下一步的报告撰写提供依据和数据来源。漏洞扫描，主要采用远程安全评估系统进行范围内的安全扫描。漏洞分析，主要是对扫描结果进行分析，安全工程师会结合扫描结果和实际客户系统状况，进行安全分析。漏洞验证，对部分需要人工确定和安全分析的漏洞，进行手工测试，以确定其准确性和风险性。

报告与汇报：这个阶段主要对现场进行扫描后的数据进行安全分析，安全工程师对远程安全评估系统输出的报告，漏洞分析结果及漏洞测试具体情况进行综合梳理，分析，总结。最后给出符合客户信息系统实际情况的安全需求的安全建议。

3.5 服务报告

安全工程师在实施安全漏洞扫描服务过程中，严格按照安全服务的流程，在现场进行安全扫描方案实施漏洞扫描后，会在两个工作日（需根据扫描对象的数量进行实际调整）内出示一份漏洞扫描报告。报告名称如下：

- 《××系统安全漏洞扫描报告》

3.6 服务注意事项及措施

漏洞扫描是一项风险比较高的测试活动，扫描不当可能导致被扫描目标发生服务性能下降、影响其可用性。漏洞扫描还会尝试部分漏洞或者配置的脆弱性验证，可能会与原有的管理发生冲突，这些可以在扫描方案确定前进行沟通和交流，以此降低风险。扫描实施的时间选择，最好是避免业务高峰期和重要时期内。