铱迅信息
yxlink.com

铱迅漏洞扫描系统

产品白皮书

南京铱迅信息技术有限公司

Nanjing Yxlink Information Technologies Co.,Ltd.

注意

□本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其所提到之产品信息，所引起直接或间接的数据流失、利益损失或事业终止，铱迅信息不承担任何责任。

铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利，而无须事先通知。

本公司已竭尽全力来确保手册内载之信息的准确性和完善性。如果您发现任何错误或遗漏，请向铱迅信息反映，对此，我们深表感谢。

商标信息

铱迅信息、铱迅 Web 应用防护系统的标志为南京铱迅信息技术有限公司的商标或注册商标。本手册或随铱迅信息产品所附的其他文件中所提及的所有其他商标名称，分别为其相关所有者所持有的商标或注册商标。

目录

一、概述

1.1 漏洞的出现

在商业世界，漏洞主要是因为设计和实施中出现错误所致，造成信息完整性、可获得性和保密性受损。错误通常在软件中，也存在于各个信息系统层，从协议规格到设计到物理硬件。网络漏洞还可能是恶意用户或自动恶意代码故意为之。重要系统或网络中单个漏洞可能会严重破坏一个机构的安全态势。

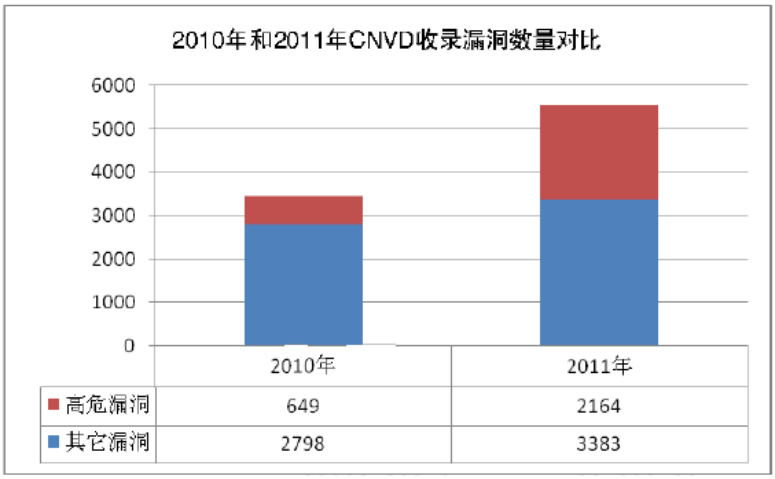
“漏洞”一词的定义是易受攻击性或“利用信息安全系统设计、程序、实施或内部控制中的弱点不经授权获得信息或进入信息系统。”这里的关键词是“弱点”。任何系统或网络中的弱点都是可防的。

1.2 漏洞的影响

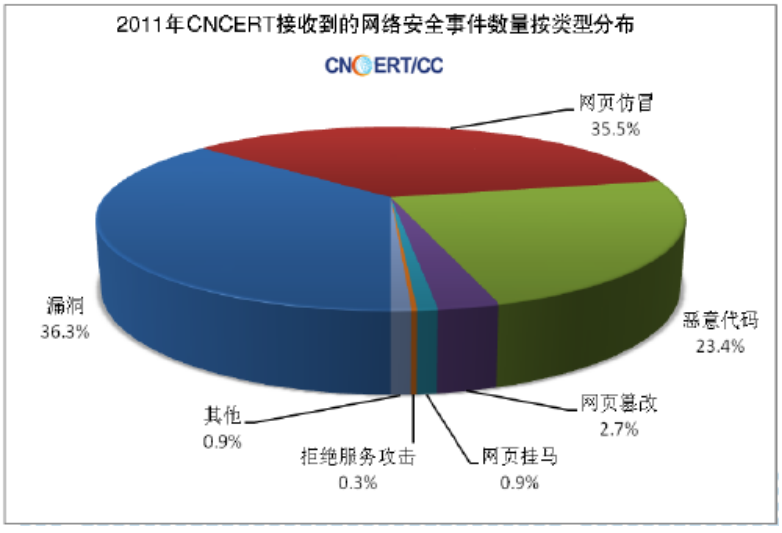
漏洞会影响到很大范围的软硬件设备，包括操作系统本身及其支撑软件，网络客户和服务器软件，网络路由器和安全防火墙等。换而言之，在这些不同的软硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

1.3 漏洞的危害

2011年，CNVD公开发布信息安全漏洞5547个，较2010年大幅增加60.9%。其中，高危漏洞有2164个，较2010年增加约2.3倍。



安全漏洞涵盖网站内容管理系统、电子邮件系统、工业控制系统、网络设备、网页浏览器、手机应用软件等类型，涉及政务、电信、银行、民航等重要部门。



网络安全性如果不能进一步提高，将不仅影响信息系统业务的开展，也会给不法分子以可乘之机。

二、产品简介

铱迅漏洞扫描系统（简称：Yxlink NVS，英文名：Yxlink Network Vulnerability Scan System），是唯一支持IP地址段批量反查域名、内网穿透扫描的专业漏洞扫描器，可支持主机漏洞扫描、Web漏洞扫描、弱密码扫描等。产品主要功能如下：

主机漏洞扫描：支持扫描操作系统漏洞、网络设备漏洞、WEB服务器漏洞、数据库服务器漏洞、邮件服务器漏洞、DNS服务器漏洞等。

Web 漏洞扫描：支持扫描 SQL 注入、跨站脚本、木马上传、代码执行、远程本地包含、信息泄露等 Web 漏洞。

弱密码扫描：支持扫描 3389 远程桌面、FTP、SSH、Telnet、Mssql、Mysql、Oracle、SMB、VNC 的弱密码，且支持自定义弱密码字典。

通过部署铱迅漏洞扫描系统，能够降低与缓解主机中的漏洞造成的威胁与损失，快速掌握主机中存在的脆弱点。

铱迅漏洞扫描系统可以广泛用于扫描数据库、文件系统、邮件系统、Web 服务器等平台。

三、铱迅漏洞扫描系统

3.1 产品功能

与入侵检测/防御系统等被动防御手段相比，漏洞扫描是一种主动的防范措施，可以有效避免黑客攻击行为，防患于未然。通过对网络的扫描，可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。

铱迅漏洞扫描系统，可提供查询每个扫描任务中，每个主机中的漏洞的数量及分类结果等详细信息。

3.1.1 主机漏洞扫描

主机系统上存储、处理和传输各种重要数据，可以说主机的安全问题是 Internet 安全的核心问题之一，是 Internet 实现安全性的关键。因此，主机系统的安全防护也是整个安全策略中非常重要的一环，铱迅漏洞扫描系统支持主机漏洞的检测。

铱迅漏洞扫描系统支持扫描缓冲区溢出漏洞、网络设备漏洞、WEB服务器漏洞、数据库服务器漏洞、邮件服务器漏洞、DNS漏洞、系统漏洞等。

缓冲区溢出漏洞：

利用缓冲区溢出攻击，可能导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，控制整个主机，进而进行各种非法操作。

通过铱迅漏洞扫描系统，可以探测主机是否存在缓冲区溢出漏洞，从而第一时间通过补丁修复，阻止黑客的溢出攻击。

网络设备漏洞：

如交换机、路由器、防火墙等网络设备本身存在安全漏洞，就可能导致设备重新加载它的操作系统。黑客就可以利用它们来在受感染的交换机和路由器上运行任意恶意代码，或者发起拒绝服务攻击。

通过铱迅漏洞扫描系统，可以第一时间发现设备本身的漏洞，在通知管理员的同时，提供相应的解决方案，防患于未然。

Web 服务器漏洞：

WEB 服务器存在多种漏洞，可能造成代码执行、缓冲区溢出、异常脚本解析等，危害严重。

铱迅漏洞扫描系统可以对 Web 服务器的多种项目进行全面的测试，并对不同危害程度的漏洞进行评估，给管理员的工作提供极大的方便。

数据库服务器漏洞：

数据库服务器漏洞一种是因为设计存在缺陷，数据库可能存在授权绕过、缓冲区溢出等漏洞，黑客可以对数据库服务器进行各种操作，最常见的是使数据库崩溃，引起拒绝服务。

铱迅漏洞扫描系统通过对数据库服务器测试，可以检测出不同版本数据库服务器的漏洞，并提供相应的解决方案，如提醒管理员及时更新新版和下载补丁等，从而防止黑客非法使用数据库造成数据泄露、更改或破坏。

邮件服务器漏洞：

如果邮件服务器存在漏洞，黑客就可利用电子邮件服务器系统的安全漏洞获得邮箱账号和密码，并通过截取通信内容，造成关键隐私数据泄露。

铱迅漏洞扫描系统对邮件服务系统进行扫描后，如果发现相关漏洞，会提醒管理员更新邮件服务器补丁，从而保证了邮件系统的安全性。

DNS 服务器漏洞：

DNS 漏洞危害性非常大，该漏洞能够让黑客在 10 秒之内发起一个“缓存毒药攻击”，轻松地伪造任何网站，比如当你输入一个正确的银行网站域名时，你可能访问到的是一个黑客伪造的站点。黑客针对缓存 DNS 服务器的漏洞，进行杠杆式攻击，然后通过劫持网站流量来牟利。

铱迅漏洞扫描系统对 DNS 测试后，会把相关信息显示给管理员。管理员通过反馈信息，可检查自己网络服务所使用的 DNS 服务器是不是还未更新，进而要求服务商更新，这样可有效防范这种攻击方式。

操作系统漏洞：

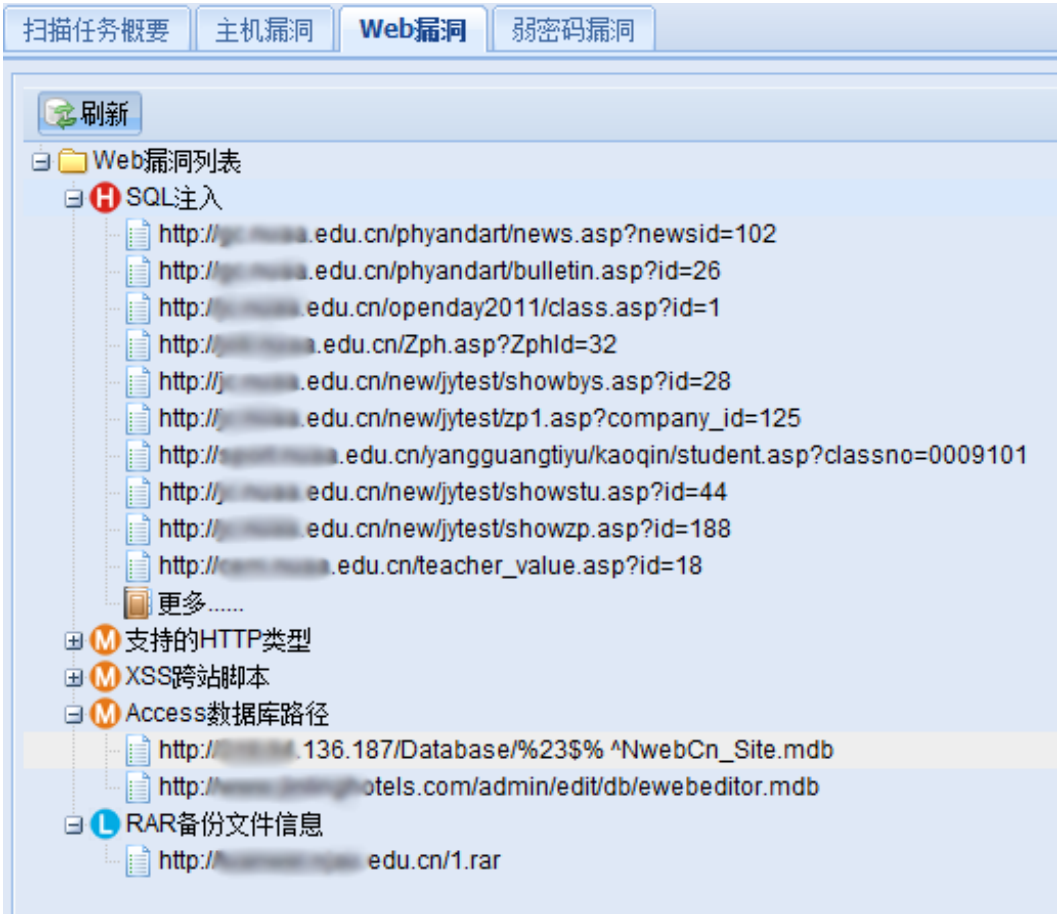
系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或错误，被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取重要资料和信息，甚至破坏系统。

铱迅漏洞扫描系统在扫描出系统漏洞后，会给管理员提供相关解决方案，提醒管理员及时更新漏洞补丁，从而完成漏洞修复。

3.1.2 Web 漏洞扫描

Web 应用程序可以运行于多种操作系统平台，由于网站开发人员在进行编码时，对于 Web 应用的安全性考虑不周到，容易留下 Web 漏洞。另外，如果管理员对于安全性重视度不够，不对已知的缺陷进行修补，攻击者就能很容易利用 Web 应用程序穿过防火墙访问 Web 服务器、数据库服务器、应用服务器等，留下安全隐患。

铱迅漏洞扫描系统支持检测 SQL 注入、跨站脚本、木马上传、代码执行、远程本地包含、信息泄露等各种类型的 web 漏洞，可第一时间显示给管理员，做到防范于未然。



Web 常见漏洞如下：

SQL 注入漏洞：

SQL 注入是通过把 SQL 命令插入到 Web 表单递交，或输入域名，或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令，是黑客经常采用的一种攻击方式。

铱迅漏洞扫描系统可以第一时间扫描出 SQL 注入漏洞，并显示给管理员，同时提醒管理员采取相关措施，禁止特殊数据的提交或将特殊提交的数据修改，从而阻止 SQL 注入攻击。

跨站脚本漏洞：

用户浏览网站时，通常会点击其中的链接。攻击者利用用户的浏览习惯，通过在链接中插入恶意代码，从而盗取用户信息。

铱迅漏洞扫描系统可以智能扫描网站中可能存在跨站漏洞，提醒管理员对跨站漏洞进行修复，阻止黑客的恶意行为。

文件上传漏洞：

如果网站存在文件上传漏洞，黑客就可以利用这些漏洞，上传黑客文件，然后黑客就可以对网站的所有文件进行任意修改。

铱迅漏洞扫描系统可以对网站的文件上传功能进行探测，并显示给管理员。

代码执行漏洞：

用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变 $PATH 或程序执行环境的其他方面来执行一个恶意构造的代码。

铱迅漏洞扫描系统可对所有输入提交可能执行命令的构造语句，进行严格的检查，从而自动快速扫出代码执行漏洞。

远程、本地包含漏洞：

远程文件包含漏洞是服务器通过 php 的特性去包含任意文件时，由于要包含的这个文件来源过滤不严，从而可去包含一个恶意文件，而黑客可以构造这个恶意文件来达到邪恶的目的。

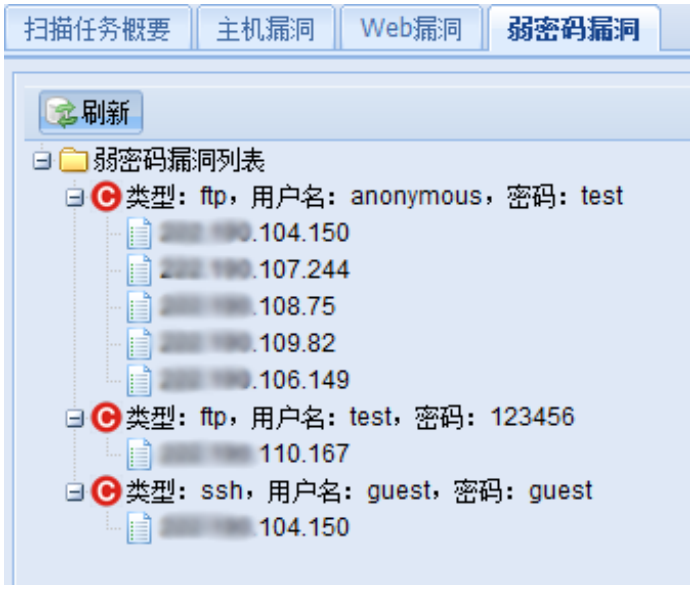
铱迅漏洞扫描系统可以检测出文件包含漏洞，并及时提供相关解决方案，提醒管理员修复相关漏洞。

3.1.3 弱密码扫描

弱密码是网络主机系统中一个普遍存在的一个严重的安全隐患,存在弱密码漏洞的计算机一直是黑客青睐的对象，通过这个漏洞，可以轻易地得到服务器的管理权限，从而威胁网站及数据的安全。

各种弱密码都会带来许多重大的安全隐患，比如系统弱口令、网站弱口令、Mssql 弱口令、Mysql 弱口令、Ftp 弱口令等。黑客采用自己生成的字典对各种密码进行暴力破解，利用弱密码直接登录后台，并在后台上传恶意代码。

铱迅漏扫扫描系统支持多种远程访问协议。与传统的单一的漏洞扫描系统相比，铱迅漏洞扫描系统利用字典文件加快破解速度，支持扫描 3389 远程桌面、FTP、SSH、Telnet、Mssql、Mysql、Oracle、SMB、VNC 的弱密码，且提供弱密码字典的自定义。

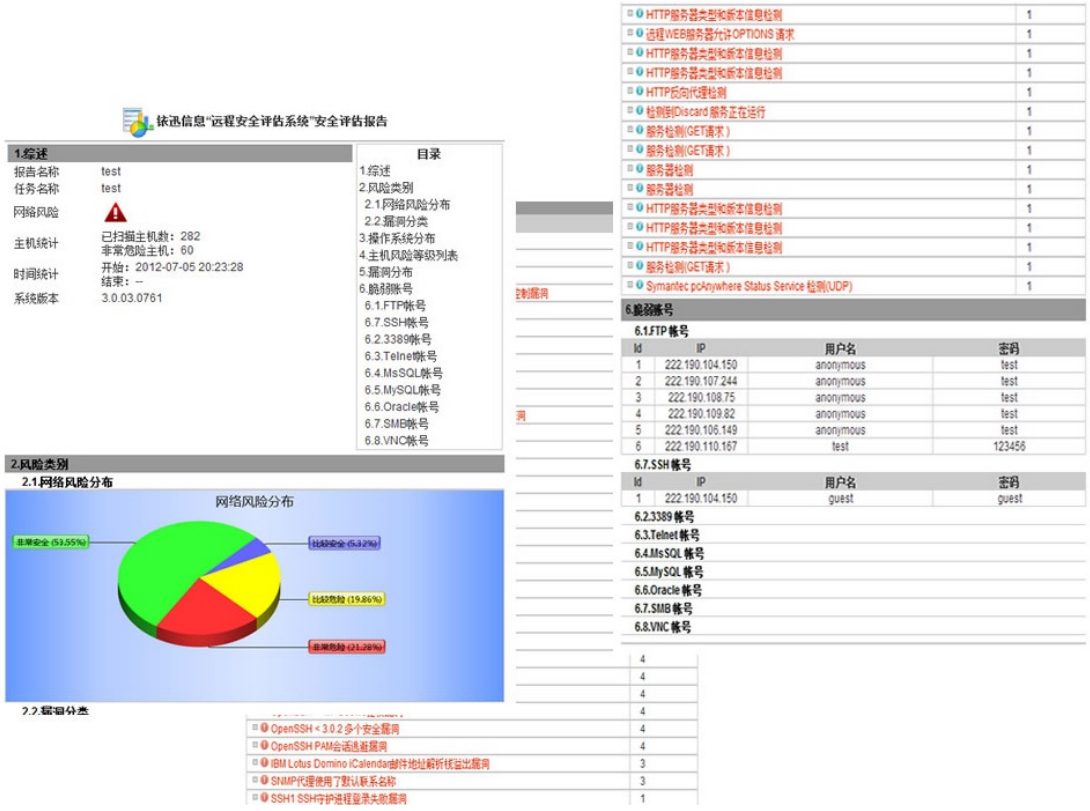


铱迅漏洞扫描系统在对网络进行扫描时，会自动扫描出网络中存在的空口令，默认口令等弱密码，并显示给管理员，提醒其修改高强度密码。

3.1.4 报表管理

铱迅漏洞扫描系统采用报表的形式对扫描结果进行分析，可提供快速报表与条件报表 2 种报表供选择，可以生产 HTML、PDF、RTF 等格式的报表文件。快速报表可以生成一次扫描任务的报表，而条件报表允许筛选指定 IP、指定漏洞类型，生成筛选后的报表。

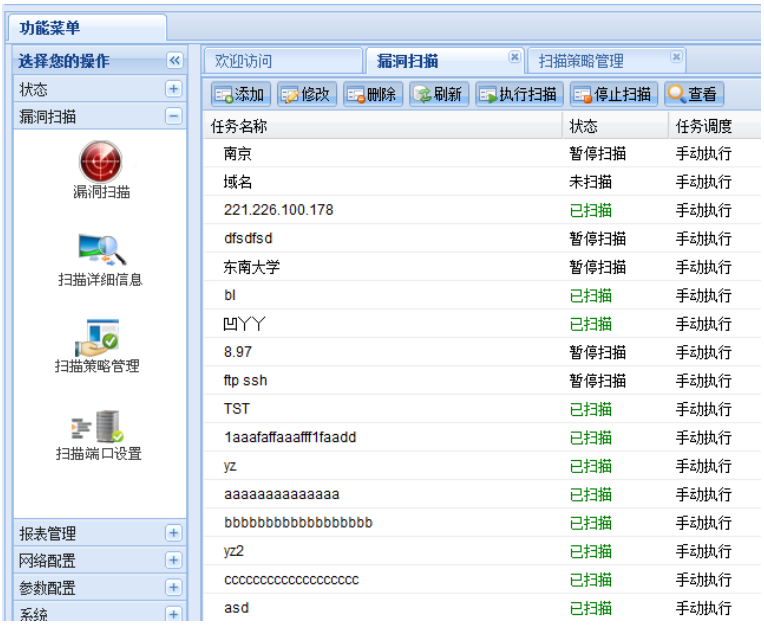
每张报表中都包含网络风险分布、不同漏洞类型的漏洞数量分布、主机风险等级列表等，方便管理员直观地对网站的安全性能进行检查和分析。



3.2 产品优势

3.2.1 批量扫描

传统的漏洞扫描产品，仅仅可以扫描指定的域名。而铱迅漏洞扫描允许扫描一个大型的 IP 地址段，通过铱迅的 DNS 域名反查系统，反查出每个 IP 地址中指向的域名，再进行扫描，大大增加扫描的效率与易操作度。



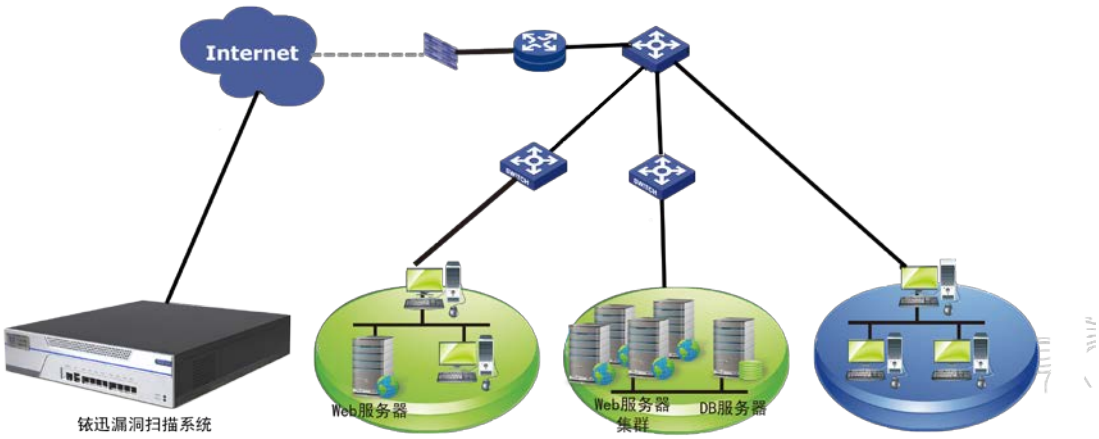
3.2.2 庞大漏洞库支撑

铱迅漏洞扫描系统拥有全面的漏洞库和即时更新能力，是基于国际 CVE 标准建立的，分为紧急、高危、中等、轻微、信息五个级别，提供超过 5 万条以上的漏洞库进行支持，可以扫描到各种隐藏的漏洞。

3.2.3 内网穿透扫描

铱迅漏洞扫描系统，不需要像传统漏洞扫描系统那样，必须在内网架上漏扫设备，才可以进行扫描。只需要利用一台内网的跳板机器，安装上铱迅漏洞扫描系统的软件，即可实现对内网所有机器的穿透扫描，也就是可以进行远程扫描。

只需要利用一台内网的跳板机器，即可进行远程扫描



3.2.4 可利用漏洞显示

铱迅漏洞扫描系统，可以结合 Metasploit （注：Metasploit 是国际著名的开源安全漏洞检测工具），提示哪些漏洞是可以被攻击者利用，这样网络管理者可以优先对于可利用的漏洞进行修补。

3.2.5 CVE、CNNVD、Metasploit 编号兼容

铱迅漏洞扫描系统，兼容 CVE、CNNVD、Metasploit 编号。符合 CVE 标准，可以更好的风险控制覆盖范围。

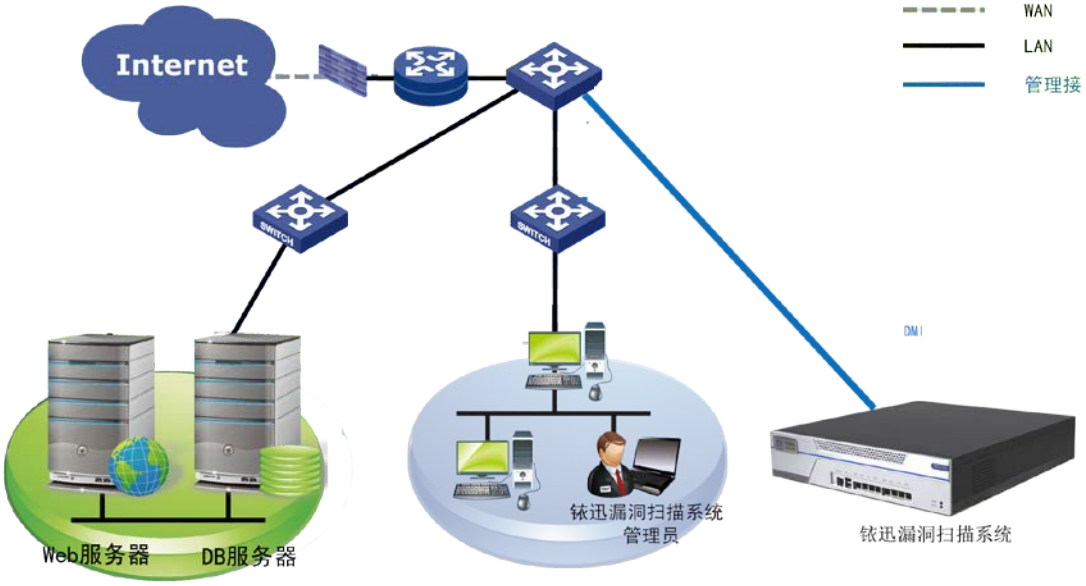
注：CVE，是国际安全组织 Common Vulnerabilities & Exposures 通用漏洞披露的缩写，为每个漏洞和暴露确定了唯一的名称。

3.2.6 远程桌面弱口令探测

铱迅漏洞扫描系统，是唯一可以提供远程桌面（3389 服务）弱口令探测功能的安全产品。如果计算机存在远程桌面弱口令，攻击者就可以直接对计算机进行控制。

四、部署方式

铱迅漏洞扫描系统，部署在任何网络可以到达的环境中都可立即工作。



铱迅信息

Yxlink

南京铱迅信息技术有限公司

江苏省南京市雨花台区玉兰路86号智汇魔方206

销售与支持热线：400 097 5557

Nanjing Yxlink Information Technologies Co.,Ltd.

206 Cube of Wisdom, No. 86 Yulan Rd., Yuhua District, Nanjing, Jiangsu, China

NJYXHVASWP011-07(01)