产品白皮书

360 漏洞扫描系统

目 录

1.产品概述 3

1.1 产品背景 3

1.2 常见安全问题 3

1.2.1 系统漏洞 4

1.2.2 WEB 漏洞 4

1.2.3 弱口令 4

1.2.4 配置核查 5

1.3 综合性漏洞扫描产品..... 5

2.产品特色 5

2.1 以“黑客”视角看待安全问题 6

3.技术优势 6

3.1 多核高性能处理 6

3.2 系统安全 6

3.3 WEB 安全 7

3.4 弱口令探测 7

3.5 配置核查 7

3.6 移动端设备 7

3.7 拒绝服务攻击 8

3.8 自动发现资产 8

3.9 漏洞验证 8

3.10 漏洞库标准 8

4.典型应用 8

4.1 拓扑图 8

4.2 总结 9

1.产品概述

1.1 产品背景

随着网络与信息技术的发展，系统漏洞、Web 安全问题一直困扰着软件、系统等开发商。2013 年，公安部发布了“计算机信息系统安全保护等级划分准则”。 2014 年，保密局针对涉密系统发布了“涉及国家秘密的信息系统分级保护技术要求”。随着我国政府越来越重视网络安全。2015 年新《国家安全法》正式颁布，明确提出国家建设网络与信息安全保障的重要性。 回顾 2015 年的安全事件，主要与系统漏洞、Web 安全事件、弱口令问题、信息泄露和移动端操作系统安全问题事件相关：

Apache 的 Struts2 漏洞问题，自从 2013 年第一个 Struts2 漏洞被曝光之后，至到 2016 年 4 月份，最新的 Struts2 的 S2-033 远程代码执行漏洞又被曝光公布。

2015 年 2 月 11 日，CMS 系统漏洞导致桔子酒店、锦江之星、速八酒店，甚至高端万豪酒店、丽思卡尔顿酒店、喜来登、洲际酒店等房客信息泄露，包括顾客姓名、身份证、手机号等大量涉及个人信息的信息泄露 同年 2 月 27 日，江苏省公安厅发布《关于立即对全省海康威视监控设备进行全面清查和安全加固的通知》。经过查询，发现海康威视设备采用了弱口令（弱口令是指使用产品初始密

码或其他简单密码）。 同年 4 月份，Android 系统的“WIFI 杀手”漏洞被曝光，黑客利用此漏洞，对开启了 WiFi 的安卓手机远程攻击，窃取手机内的照片、通讯录等重要信息，影响市面上大部分安卓设备。

1.2 常见安全问题

每次黑客攻击事件进行追溯的时候，根据日志分析后，我们往往发现基本都是系统、Web、弱口令、配置这四个方面中的其中一个出现的安全问题导致黑客可以轻松入侵的。

1) 操作系统的版本滞后，没有更新补丁，导致安全问题暴露
2) Web 问题因使用公有代码、代码编写不合规导致的安全问题，层出不穷。
3) 弱口令属于人为安全事件，复杂密码记不住，简单密码容易破解。此类因账户与口令相同的安全事件也是比比皆是。
4) 系统配置不负责流程规范，导致出现的安全，严重泄露了各类隐私数据。

1.2.1 系统漏洞

系统漏洞问题导致的安全问题，有两种起因。第一种主要原因漏洞属于未知的，属于被黑客最新发现的。此类的漏洞属于 APT 攻击范畴。第二种属于安全漏洞已经被软件厂商进行公布并提供了补丁进行修复。很多软件使用者因各种原因没有使用补丁修复。导致漏洞一直存在，并被黑客发现后利用后，被黑客窃取了重要数据并发生了安全事件。

1.2.2 Web 漏洞

Web 漏洞的范围比较广，主要涉及代码、中间件软件、数据库等软件搭建的网站环境。首先说下代码问题，代码问题主要涉及公有代码和代码编写不规范。公有代码是互联网上面发布了很多代码，一些编程软件为了高效、便捷实用了发布在互联网的代码，但是往往这类代码存在很多的安全漏洞问题，但是编程人员却无法发现。代码编写不规范是编程人员在开发过程中为了便捷，图省事。在代码编写的不规范不严谨，导致黑客从代码编写中查找漏洞。从而发生了安全事件。

中间件软件主要就是 Apache、Tomcat 这类软件，Apache 的 Struts2 频繁被曝光，而且每个漏洞是紧急的致命性的安全漏洞。 数据库的问题，主要黑客使用 SQL 语句让数据库报错，从而发现安全漏洞，黑客利用漏洞层层入侵，从而达到拖库的目标，导致大量数据泄露。

1.2.3 弱口令

弱口令多数都是人为导致的，原因在于所有设备在出厂时，为了方便用户配置和使用。往往默认密码都是十分简单或是账户和密码相同的。从人脑记忆的角度出发，复杂密码记不住。但是简单的密码是记住了，但是黑客破解的时间缩短了，而且破解也简单了。一个看似简单的账户密码，背后的安全问题就是数据泄露、黑客入侵的安全事件。

1.2.4 配置核查

系统更新了补丁，但是配置错误也会导致安全事件的发生，因此不是说系统进行补丁升级，我们的系统就十分安全了，错误的安全配置导致的安全问题，安全配置的核查工作也是十分重要的。

1.3 综合性漏洞扫描产品

从客户的角度，我们需要多方位的综合漏洞扫描产品，需要集系统漏洞、Web 漏洞、弱口令、安全配置核查于一体的综合漏洞扫描产品。360 漏洞扫描系统从最初的 3.0 版本历经多次迭代更新，最新的版本是一套从底层操作系统、上层的中间件、网站系统、代码合规、软件配置核查的综合安全漏洞扫描产品。

360 漏洞扫描系统分了 4 个方面：

- 系统扫描，针对操作系统、数据库、网络设备、防火墙等
- Web 扫描，针对 SQL 注入、跨站脚本、信息泄露等
- 弱口令检测，内置的字典，有简单密码、账户密码相同的字典库进行逐一探测
- 配置核查，主要针对操作系统、数据库的安全配置进行自动化检查

2.产品特色

2.1 以“黑客”视角看待安全问题

常见的黑客入侵事件之前，我们从网络流量中寻找问题时，都发现在入侵的前期有很多的扫描器对目标服务器、网站、中间件等系统进行漏洞扫描。黑客实际在入侵前也是使用漏洞扫描器检查攻击目标的安全问题，寻找安全漏洞从而伺机寻找薄弱环节。最后找薄弱环节进行层层突破，获取想要的资料或是数据。

360 漏洞扫描系统就是以“黑客”攻击前期的漏洞扫描器为开发视角进行产品研发的。360 漏洞扫描系统是从操作系统、数据库、网络设备、防火墙、Web 系统、弱口令、系统配置核查等多方位多视角对目标进行安全漏洞扫描检查的专业安全漏洞扫描发现产品。发现问题后为客户提供漏洞的详细报告和解决方案。

3.技术优势

3.1 多核高性能处理

360 漏洞扫描系统采用国际领先的多核处理器技术，通过自主开发的 SecOS 安全操作系统，能够高效调用多个内核处理器并行扫描漏洞，提高产品扫描性能。

在系统漏洞扫描、Web 漏洞扫描并行扫描时，SecOS 系统会自动分配 CPU、内存资源，提高扫描的速度。

3.2 系统安全

360 漏洞扫描系统针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况，网络设备漏洞情况，远程服务端口开放等情况进行综合评估，在黑客发现系统漏洞前期提供给客户安全隐患评估报告，提前进行漏洞修复，提前预防黑客攻击事件的发生。

- 操作系统：Windows、Linux、Unix 等
- 网络设备：Cisco、juniper、华为、3com 等主流厂商设备
- 数据库：Oracle、MySQL、SQLserver 等

3.3 Web 安全

360 漏洞扫描系统针对 Web 安全方面也有独到之处，Web 安全是近年来新兴的互联网安全研究方向。360 漏洞扫描系统针对 SQL 注入、XSS 跨站脚本、信息泄露、网络爬虫、目录遍历等 Web 攻击方式进行模拟黑客渗透攻击评估。 评估客户网站存在的各种 Web 安全隐患，针对网站开发中出现的安全隐患进行评估，在黑客攻击网站前期预知 Web 安全漏洞，提前告知客户问题所在，提醒客户及时修复 Web 漏洞，避免造成“网站被黑”的发生。

- 网站代码：JSP、PHP、JAVA 等代码合规性
- Web 攻击：SQL 注入、XSS 跨站脚本、目录遍历、信息泄露等主流 Web 攻击方式
- 中间件系统：Apache、Tomcat、IIS 等

3.4 弱口令探测

360 漏洞扫描系统内置有弱口令字典，针对账户和密码相同、密码相对比较简单、默认密码等问题进行自动探测，测试口令是否存在弱口令现象。提高账号防破解的安全性。破解密码主要是长度和密码的难度，密码长度和设置难度越高，黑客破解的时间越长，破解难度越大。

3.5 配置核查

360 漏洞扫描系统的配置核查功能，主要是针对操作系统、数据库、网络设备等系统的配置进行核查，检查配置是否符合标准。并可以自动启动软件执行过程的达标检测。

3.6 移动端设备

360 漏洞扫描系统不单单可以扫描 PC 端的操作系统，随着移动端设备的大趋势下。通过 WI-FI 扫描移动端的操作系统安全漏洞也属于标准的漏洞扫描配置了。针对 iOS、Android、BlackBerry 等移动端的操作系统频繁曝光的漏洞进行安全扫描。

3.7 拒绝服务攻击

360 漏洞扫描系统针对最简单、最暴力的抗拒绝服务攻击也提供测试扫描，提高操作系统、硬件设备、网站服务的大流量压力下的抗攻击能力。帮助客户排除因为遭受抗拒绝服务攻击造成的服务器宕机、设备宕机无法提供服务等安全问题。

3.8 自动发现资产

360 漏洞扫描系统提供自动发现资产功能，针对一个 IP 段进行自动漏洞扫描，自动针对在线的 IP 地址的主机进行漏洞扫描，使用 ARP、ICMP、TCP、UDP 等多种协议测试在线主机是否存活，并提供在线主机的漏洞扫描功能。

3.9 漏洞验证

360 漏洞扫描系统提供漏洞验证功能，主要是针对 GET、POST、PUT、Delete 的 SQL 注入进行自动验证和手工验证，提供简单的 SQL 注入手工验证工具。

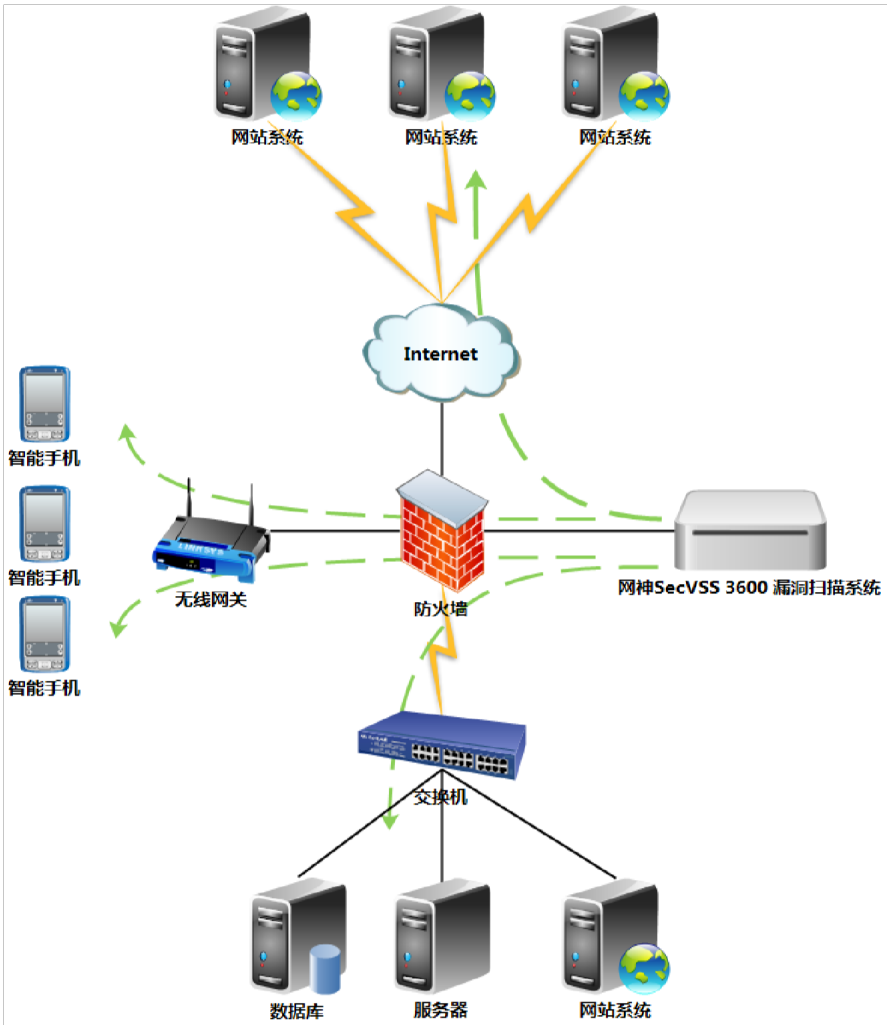
3.10 漏洞库标准

360 漏洞扫描系统兼容 CVE、CNNVD、Bugtraq ID、CVSS 等特征库标准。漏洞库提供 CVE、CNNVD 等标准的漏洞库编号，漏洞信息说明等情况。并提供漏洞的解决方案的说明。

4.典型应用

4.1 拓扑图

360 漏洞扫描系统属于旁路部署产品，在内网可以对操作系统、数据库、网络设备、防火墙等产品进行漏洞扫描，通过无线网关（WI-FI）可以对移动端设备的操作系统进行漏洞扫描。设置了 DNS 服务器可以对外网的相关网站进行 Web 漏洞扫描。



拓扑图

4.2 总结

近几年随着国家越来越重视网络信息化安全建设问题，网络安全问题已经提高到了一个前所未有的高度。国务院办公厅、公安部、工业信息化部等多部门都发布了相关的政策指引。网络问题归根结底的问题在于漏洞问题。系统漏洞、Web 漏洞、数据库泄密事件等一系列的安全问题告诉我们，漏洞是所有安全事件的罪魁祸首。

360 漏洞扫描系统就是针对漏洞问题提供技术扫描排查的，在安全事件发生之前提供漏洞扫描，提高各类系统的安全性，降低安全事件的发生，避免大多数因漏洞未修复造成的黑客攻击事件。