漏洞扫描那些事

漏洞扫描一般指扫描暴露在外网或者内网里的系统、网络组件或应用程序，检测其中的漏洞或安全弱点，而漏洞扫描器则是用来执行漏洞扫描的工具。漏洞扫描器一般基于漏洞数据库来检查远程主机，漏洞数据库包含了检查安全问题的所有信息（服务、端口、包类型、潜在的攻击路径，等等）。它可以扫描网络和网站上的上千个漏洞，提供一个风险列表，以及补救的建议。

1、下列人员会用到漏洞扫描器：

安全审计人员在进行安全审计时。

恶意攻击者或者黑客在攻击目标、获取非法访问时。

程序开发团队在发布环境中部署产品之前。

2、流行的扫描工具包含下面的功能：

维护一个包含最新漏洞的数据库。

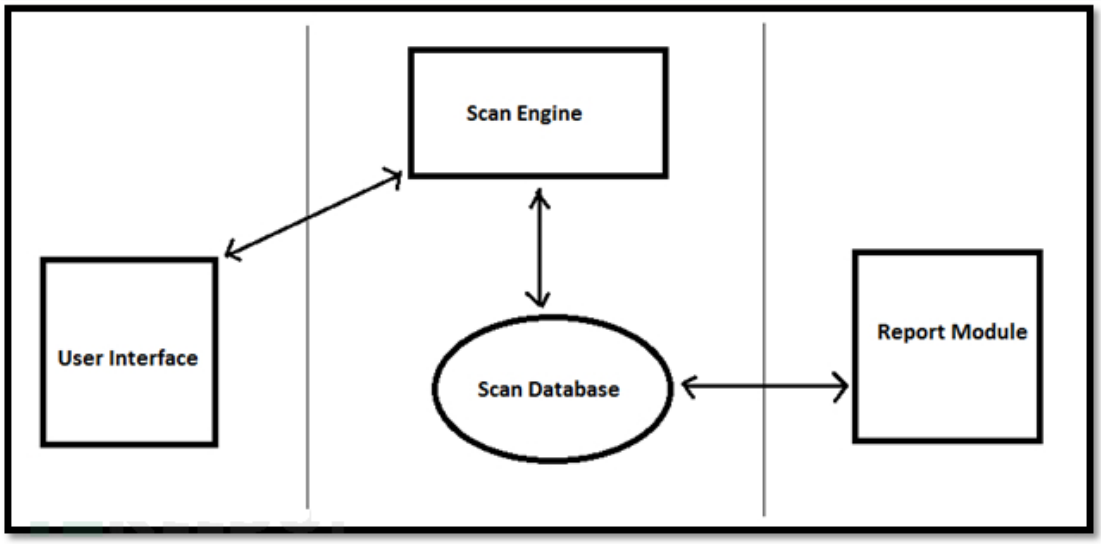
以较低的误报率检测出漏洞。

同时扫描多个目标。

提供详细的报告，包括请求和响应对。

提供修复漏洞的建议。

架构



扫描器的组件

漏洞扫描可以分成四个部分：

1、用户接口：用户通过这个接口运行和配置一个扫描。这可以是图形界面（GUI）也可以是命令行接口（CLI）。

2、扫描引擎：扫描引擎通过安装和配置的插件来执行扫描。

3、扫描数据库：扫描数据库保存了扫描器需要的数据。包括，漏洞信息、插件、消除漏洞的步骤、CVE-ID 映射（常见的漏洞）、扫描结果，等等。

4、报告模块：报告模块提供了不同的选项，可以生成不同类型的报告。比如，详细报告、漏洞列表、图形化报告，等等。

3、扫描类型

外网扫描 :有一些设备和资产是暴露在互联网的。大部分的机构都开放了 80 或者 443 端口，这样人们可以通过互联网访问他们的网站。许多管理员觉得他们实现了边界防火墙，这样他们就很安全了。但是，并不总是这样的。防火墙可以依据定义的规则和策略阻止对网络的非授权访问，但是如果攻击者找到了通过这

些端口（比如 80 或者 443）攻击其它系统的方法，防火墙就不能保护你了，因为利用这些端口，攻击者就自动绕过了防火墙，进入了你的网络。

外部扫描是重要的，它检测那些面向互联网的资产的漏洞。攻击者通过这些漏洞可以访问内网。外部扫描可以通过在互联网机器上运行漏洞扫描器来实现。最好在攻击者利用已公开的安全问题和漏洞之前，就消除它们，

内网扫描：并不是所有的攻击都来自外部网络。黑客和恶意软件也可以在内网中出现。通过以下方式，就可以访问内网：

恶意软件或者病毒通过互联网或者 USB 下载到网络中

一个可以访问内网的不满的员工

外部的黑客获取了访问内部网络的权限

因此，在内网里运行漏洞扫描器也同样重要。在内网的一台机器上运行漏洞扫描器，可以对网络中的关键组件进行扫描。重要的组件包括核心路由器、交换机、工作站、web 服务器、数据库，等等。

多久扫描一次？

每天都有很多新漏洞被发现。每个新的漏洞都会增加危险。因此，定期扫描资产非常重要。发现最新的安全问题可以帮助机构关闭安全漏洞，抵御攻击。

多久执行一次漏洞扫描并没有确定的数字。根据机构的不同而不同。

扫描的频率基于以下几点：

资产的重要性：越重要的资产扫描应该越频繁，这样就能打上最新的补丁。

曝光度 :识别和扫描那些暴露给大量用户的组件。这可以是外部和内部资产。

变动现存环境时：对现存环境的任何修改，增加新的组件和资产等，都应该进行漏洞扫描。

4、免费 vs 收费

并没有确定的答案来回答使用免费、开源的漏洞扫描器还是商业扫描器。在互联网上可以下载到许多可用的漏洞扫描器。一些是免费的，还有一些是收费的版本。免费版本的工具，比如 Burp、Nessus 等，在渗透测试常会用到。但是在一些场合 ,强制使用商业版。免费版本的漏洞扫描器可以在初步安全扫描时使用，但是他们也有一些限制：

扫描范围：免费的扫描器在扫描范围上有限制。在比较高的层级上扫描，不能覆盖到应用程序的所有部分。

精确性：可能会导致漏报，发现不了存在的安全问题。与误报相比，这个更为严重。

支持所有的攻击和输入载荷 :免费的扫描支持的攻击和输入载荷与付费版相比要少。付费版的漏洞和载荷数据库会定期更新，能检查最新的漏洞。

支持详细的报告：大部分扫描器都支持报告功能，但是免费版的扫描也许不能够生成包含有请求-响应对、修补方法、补丁下载链接等详细内容的报告。

5、全球知名漏扫

Nessus：

Nessus 是最流行的漏洞扫描器之一。它可以用于认证和非认证的漏洞扫描。除了可以进行网络漏洞扫描外，它还支持外部和内部 PCI 扫描、恶意软件扫描、移动设备扫描、策略合规性扫描、web 应用程序测试、补丁审计等。它使用超过 70,000 个插件来扫描一个目标机。

Nessus 有两个版本，免费版本和专业版本。免费版有一些限制，它不能用于专业的环境中（比如工作中），较少的插件等等。

OpenVAS：

Open Vulnerability Assessment System (OpenVAS)是由若干服务和工具组成的框架，提供全面而强大的漏洞扫描和漏洞管理功能。它是开源的，可以免费使用。它有一个客户端-服务器架构的 web 接口。server 组件用来调度扫描任务和管理插件，client 组件用于配置扫描和查看报告。

包含如下特点：

支持插件定制：OpenVAS 扫描器支持定制插件，用户可以使用 Nessus Attack Scripting Language (NASL)编写插件。

认证扫描：在认证扫描时，用户提供目标机的登录凭证，扫描器可以登录，并扫描主机上安装的组件的漏洞（Adobe reader、Wireshark 等）

导出报告：OpenVAS 有多个选项来导出报告。用户可以以 HTML、XML、TXT 和 PDF 的格式生成和下载报告。

端口扫描：OpenVAS 有多个选项进行端口扫描。包括 TCP scan, SYN scan, IKE-scan,来定位 IPSec, VPN 等.

安全检查：OpenVAS 支持安全地扫描。在这个模式下，scanner 会依据远程主机的 banner 来发送载荷，而不是发送所有的载荷。这个选项对于重要的和陈旧的主机很有用，可以防止在扫描时崩溃。

QualysGuard：

QualysGuard 是一个 Saas（Software as a Service）的私有云。可以使用基于 web 的用户界面登录，能在任何地方使用这个服务。工具包括网络发现、资产映射、漏洞检查、报告、修复跟踪。Qualys appliances 通过与云上的系统通信来进行内网扫描。

Burp Suite：

Burp Suit 是一个基于 Java 的工具，用来执行 web 应用程序安全测试。单个平台中集成了测试过程中需要的不同的工具。具有免费和商业两个版本。Burp Suit 的免费版本有如下功能：

一个拦截式代理，作为一个代理服务器可以分析和修改后台的请求和响应。

Burp Spider 能够爬取目标程序的页面和链接。

Burp Repeater 用于多次操纵和发送请求。

Burp Sequencer 用来分析 session token 的随机性和强度。

Burp Intruder 执行可定制的自动化攻击，寻找和利用漏洞。

在专业版中有一些特有的功能，包括：

一个高级的 web 应用程序扫描器，检测 web 应用程序里的漏洞。

Burp Extension 让你编写自己的插件，使用 Burp 执行复杂和定制的任务

可以保存当前状态，并在以后用它。

免费和专业版的 Burp Suit 可以在这里下载。

OWASP ZAP:

OWASP ZAP 是一个基于 Java 的跨平台开源的 web 应用程序安全检查工具。

主要功能包括：

拦截式代理：拦截式代理可以用来手动观察和处理应用程序和它的参数。它能拦截发往服务器的请求，用户可以操作 URL、隐藏的参数、协议头等等，分析应用程序的行为和安全性。同样，server 返回的响应也可以修改。

爬虫：与 Burp Suit 相同，ZAP 中的 spider 用来爬取目标应用程序的 web 页面和链接。额外功能包括支持基于 AJAX 的爬虫，应用程序会使用 JavaScript 生

成链接。对于基于 AJAX 的爬虫有一个单独的页面，spider 会在那里通过调用浏览器来探索应用程序。

主动和被动扫描：Zap 支持主动和被动扫描两种技术。在被动扫描时，工具会扫描爬虫和代理收集到的请求和响应。扫描运行在后台，因此不会影响真实的测试。在主动扫描时，扫描器会发送载荷，发现潜在的漏洞。用户可以控制主动扫描，根据扫描程度手动配置扫描器。

可以保存当前的会话，后面再用。

生成扫描报告。ZAP 支持 HTML 报告。

包括端口扫描、模糊测试等功能，支持 web Sockets。

Acunetix Web **漏洞扫描器：**

Acunetix web 漏洞扫描器是自动化的应用程序安全测试工具。它主要用于扫描 web 应用程序上的安全问题，比如 SQL 注入，XSS，目录遍历，命令注入等。用户可以用这个扫描器扫描 SANS top 20 和 OWASP top 10 的漏洞。Acunetix 有两个版本，免费和商业版。免费版试用 14 天，可以扫描所有漏洞，但是不会显示确切的位置。你可以扫描 acunetix test webiste,http://test.acunetix.com/查看详细的漏洞扫描样本。安装非常简单。主要的功能包括：

扫描器：Acunetix 的主要组件是扫描器。它是完全可定制的扫描器，用户可以根据需要配置它。用户可以在属性页定义要检查的漏洞的类型。扫描的时间基于应用程序的大小和属性页的配置情况。

漏洞检测：除了扫描常规的 web 应用程序之外，Acunetix 也能扫描基于 HTML5/JS 技术的网站。

网站爬虫：当爬虫爬取文件和目录时，我们可以配置要包含和排除的文件的类型。

子域名扫描：Acunetix 可以根据 DNS 记录搜索子域名。

调度器：Acunetix 可以制定计划扫描一个或多个网站。这个功能很有用，用户可以让它在晚上或者周末扫描。

目标寻找：用户可以扫描一个子网发现开放 80 或 443 等端口的 web 服务。

HTTP 编辑器：可以用这个工具定制请求和响应来分析特定的漏洞。它可以编码和解码参数的值。它也可以用于修改 request 参数，比如 URL、Cookie、request 数据等。

总结

漏洞扫描很快，能够节省你的时间，但是我们不能完全依赖他们。没有一个单独的工具能够发现网络或 web 应用程序中所有的漏洞。如何可以的话，使用多个自动化扫描工具来减少误报和漏报的概率。web 漏洞扫描器不能发现应用程序中与业务逻辑相关的问题。这些漏洞很严重，而且需要手工办法来发现。最好的办法是漏洞扫描器和手动测试结合起来。

如果你只拿到扫描器给出的安全问题列表，而不对它做任何工作，这是没有意义的。而且，应该由那些能够配置扫描器、理解扫描结果、明白风险和修复技术的安全工程师来实施扫描。