**测评工具清单**

|  |  |  |
| --- | --- | --- |
| 工具名称 | 工具简介 | 主要功能 |
| 远程安全评估系统 | 绿盟远程安全评估系统是绿盟科技结合多年的漏洞挖掘和安全服务实践经验，自主研发的新一代漏洞管理产品，它高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。 | 1 绿盟远程安全评估系统能够全方位检测IT系统存在的脆弱性，发现操作系统漏洞、应用系统安全漏洞、数据库系统漏洞、网络设备及安全设备漏洞，检查系统存在的弱口令，收集系统不必要开放的帐号、服务、端口，形成整体安全风险报告。 |
| 科来网络回溯分析系统 | 科来网络回溯分析系统（RAS）是一款集成大容量存储的高性能数据包采集和智能分析软硬件一体化平台，可以分布式部署在网络的关键节点，支持对物理网络和云网络流量的采集分析。RAS以关键应用为中心，实现对应用的网络访问性能、系统服务性能、应用响应性能等关键性能指标的智能分析。  同时，RAS还可实时捕获并保存网络通讯流量，具备对长期网络通讯数据进行快速数据挖掘和回溯分析能力。实现对关键业务系统中的网络异常、应用性能异常和网络行为异常的秒级发现，以及区分异常原因的智能回溯分析，提升了对关键业务系统的运行保障能力和问题处置效率。 | 全流量网络回溯分析，系统具备长时间大容量数据存储能力，能长期实时保存原始数据包，并同时保存数据流、会话及应用日志等各种统计数据；具备快速的数据检索能力，并对已发生的网络行为、应用数据和主机数据进行回溯分析；可随时分类查看及调用任意时间段的数据，当发现问题时提供一定时间范围内的回溯分析(根据设备存储空间而定)，为迅速定位问题发生原因提供了更全面的分析依据，同时为网络安全提供了强有力的数据分析保障。面向业务的安全分析与取证，RAS系统以网络中关键应用为中心，主动梳理应用的网络及应用访问行为，提供针对关键应用的异常网络访问行为发现分析，异常应用层数据分析，提高针对关键业务的网络行为的监控、审计、分析能力，提升业务系统的安全保障能力。 |
| Checkmarx静态源代码安全漏洞扫描和管理工具 | Checkmarx静态源代码安全漏洞扫描和管理工具是以色列Checkmarx 公司在分析全球静态分析技术的优缺点后,结合全球安全组织和安全专家建议而研发出的新一代源代码安全扫描工具,该工具可用于识别、跟踪和修复源代码技术上和逻辑上的缺陷，比如软件安全漏洞、质量缺陷问题和业务逻辑问题等。 | 可以从数据流分析、控制流分析、语义分析、配置分析、结构分析等五个方面全面分析软件源代码的安全问题。  数据流分析：分析程序中的数据传递过程所产生的安全问题。  控制流分析：分析程序特定时间、状态下执行操作指令的安全问题。  语义分析：分析程序中不安全的函数，方法的使用的安全问题。   配置分析：分析项目配置文件中的敏感信息和配置缺失的安全问题。  结构分析：分析程序上下文环境，结构中的安全问题。 |
| 渗透测试工具集2.7 | Nmap（"网络映射器"）是一个免费的开源（许可证）实用程序，用于网络发现和审核安全。许多系统和网络管理也发现它对于诸如网络清单、管理服务升级计划以及监视主机或服务服务升级时间等任务很有用。Nmap 使用原始 IP 数据包以新颖的方式能够在网络上拥有主机，哪些服务（应用程序名称和版本）运行什么 sesare sare、什么操作和操作系统版本，正在使用的 ilters/防火墙的数据包类型，以及其他几十个。它旨在快速扫描大型网络，但工作精细ss单主机。Nmap 在所有主要的计算机操作系统上运行，官方二进制软件包可用于 Linux、Windows 和 Mac OS X。除了经典的命令行 Nmap 可执行文件外，Nmap 套件还包括高级 gui 和结果查看器 （Zenmap）、灵活的数据传输、重定向和正文工具 （Ncat）、用于比较扫描结果 （Ndiff） 的实用程序以及生成和响应分析工具 （Nping）。 | （1）扫描主机端口，嗅探所提供的网络服务  （2）探测一组主机是否在线  （3）还可以推断主机所用的操作系统，到达主机经过的路由，系统已开放端口的软件 |
| Sqlmap是一个自动化的SQL注入工具，其主要功能是扫描，发现并利用给定的URL进行SQL注入。目前支持的数据库有MySql、Oracle、Access、PostageSQL、SQL Server、IBM DB2、SQLite、Firebird、Sybase和SAP MaxDB等。 | Sqlmap的强大的功能包括 数据库指纹识别、数据库枚举、数据提取、访问目标文件系统，并在获取完全的操作权限时执行任意命令。  （1）基于布尔类型的盲注，即可以根据返回页面判断条件真假的注入  （2）基于时间的盲注，即不能根据页面返回的内容判断任何信息，要用条件语句查看时间（3）延迟语句是否已经执行(即页面返回时间是否增加)来判断  （4）基于报错注入，即页面会返回错误信息，或者把注入的语句的结果直接返回到页面中  （5）联合查询注入，在可以使用Union的情况下注入  （6）堆查询注入，可以同时执行多条语句时的注入 |
| Acunetix Web Vulnerability Scanner（简称AWVS）是一款知名的网络漏洞扫描工具，它通过网络爬虫测试你的网站安全，检测流行安全漏洞。WVS可以检查SQL注入漏洞，也可以检查跨站脚本攻击漏洞，可以扫描任何可以通过web浏览访问和遵循HTTP/HTTPS规则的web站点和web应用程序。 | （1）它将会扫描整个网站，它通过跟踪站点上的所有链接和robots.txt 实现扫描。然后WVS就会映射出站点的结构并显示每个文件的细节.  （2）在上述的发现阶段或扫描过程之后，WVS就会自动地对所发现的每一个页面发动一系列的漏洞攻击， 这实质上是横拟黑客的攻击过程，这是一个自动扫描阶段。  （3）在它发现漏洞之后，WVS就会在"Alerts Node (警告节点）"中报告这些漏洞. 每一个报告都包含着漏洞信息和如何修复漏洞的建议.  （4）再扫一次,它会将结果保存为文件以备曰后分析以及与以前的扫描相比较，使用报告工具，就可以创建一个专业的报告来总结这次扫描. |
| Burp Suite 是用于攻击web 应用程序的集成平台，包含了许多工具。Burp Suite为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。 | Proxy——是一个拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。  Spider——是一个应用智能感应的网络爬虫，它能完整的枚举应用程序的内容和功能。  Scanner[仅限专业版]——是一个高级的工具，执行后，它能自动地发现web 应用程序的安全漏洞。  Intruder——是一个定制的高度可配置的工具，对web应用程序进行自动化攻击，如：枚举标识符，收集有用的数据，以及使用fuzzing 技术探测常规漏洞。  Repeater——是一个靠手动操作来补发单独的HTTP 请求，并分析应用程序响应的工具。  Sequencer——是一个用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具。  Decoder——是一个进行手动执行或对应用程序数据者智能解码编码的工具。  Comparer——是一个实用的工具，通常是通过一些相关的请求和响应得到两项数据的一个可视化的“差异”。 |
| 御剑后台扫描珍藏版是T00LS大牛的作品,方便查找用户后台登陆地址，同时也为程序开发人员增加了难度，尽量独特的后台目录结构。附带很强大的字典，字典我们也是可以自己修改的，继续增加规则。 | （1）扫描线程自定义:用户可根据自身电脑的配置来设置调节扫描线程  （2）集合DIR扫描 ASP ASPX PHP JSP MDB数据库 包含所有网站脚本路径扫描  （3）默认探测200 (也就是扫描的网站真实存在的路径文件) |
| AppScan，即 AppScan standard edition。其安装在 Windows 操作系统上，可以对网站等 Web 应用进行自动化的应用安全扫描和测试。  Rational AppScan（简称 AppScan）其实是一个产品家族，包括众多的应用安全扫描产品，从开发阶段的源代码扫描的 AppScan source edition，到针对 Web 应用进行快速扫描的 AppScan standard edition，以及进行安全管理和汇总整合的 AppScan enterprise Edition 等。我们经常说的 AppScan 就是指的桌面版本的 AppScan，即 AppScan standard edition。其安装在 Windows 操作系统上，可以对网站等 Web 应用进行自动化的应用安全扫描和测试。 | （1）通过搜索（爬行）发现整个 Web 应用结构  （2）根据分析，发送修改的 HTTP Request 进行攻击尝试（扫描规则库）  （3）通过对于 Respone 的分析验证是否存在安全漏 |
| Wireshark（前称Ethereal）是一个[网络封包](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B0%81%E5%8C%85" \t "_blank)分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。 | （1）数据包的过滤：抓取时过滤和抓取后的过滤  （2）数据流追踪  （3）专家信息说明  （4）数据包的统计分析 |
| Metasploit是一款开源的安全漏洞检测工具，可以帮助安全和IT专业人士识别安全性问题，验证漏洞的缓解措施，并管理专家驱动的安全性进行评估，提供真正的安全风险情报。这些功能包括智能开发，代码审计，Web应用程序扫描，社会工程。团队合作，在Metasploit和综合报告提出了他们的发现。 | （1）辅助模块  主要是为渗透测试信息搜集阶段提供大量的辅助工具，包括各种网络服务探测与扫描，构建虚假服务收集登录密码，口令的猜测与破解，敏感信息嗅探等。此外还包括一些无需获取目标系统控制权限的攻击手段，常见的如DDoS攻击等。  （2）渗透攻击模块  主要是利用发现的安全漏洞和配置弱点来对远程目标系统进行攻击，以植入和运行攻击载荷，从而获得远程目标的访问权的代码组件，根据攻击方式的不同，分为主动渗透模块和被动渗透模块。主动渗透所利用的漏洞主要位于网络服务端软件和服务承载的上层应用程序之中。被动渗透利用的漏洞主要位于客户端软件中，主要是通过诱导用户点击包含恶意代码的文件，链接等来被动的获取目标系统信息。  （3）攻击载荷模块  攻击载荷是在渗透成功之后促使目标系统运行的一段植入代码，一般都是为了帮助渗透攻击者打开目标系统上得控制会话连接。而攻击载荷模块就是集成了大量的具有针对性的植入代码，可以减少渗透攻击者的工作量。Metasploit的攻击载荷主要是分为三类：独立（Singles），传输器（Stager），传输体（Stage）。独立攻击载荷是完全独立的，自包含的可以直接植入目标系统执行的载荷，而在一些对攻击载荷的大小，运行条件有限制的情况下Metasploit提供了传输器和传输体来进行攻击。传输器代码少，短小精悍，易于传输且非常可靠，可以满足苛刻的渗透条件，然后可以通过传输器载荷进一步下载并执行传输体载荷，此时传输体载荷就不在受大小和安全防御机制的限制。  （4）空指令模块  空指令是一些对程序运行不造成影响的空操作或者无关操作。为了保证渗透攻击组件的可靠性，降低由于内存地址随机化，返回地址偏差等因素对渗透代码的影响，所以通常都需要在执行的ShellCode之前添加一段空指令区，用来作为缓冲区。  （5）编码器模块  编码器模块主要是将组装好的指令序列进行一定次数的编码，防止渗透攻击指令被检测或是阻断，或者是没有奏效。主要功能是两个：1>确保攻击载荷中不会出现一些“坏字符”，这些“坏字符”很可能导致精心构造的渗透程序不完整甚至无法执行（例如会将一些字符解读为文件尾部，从而丢失了后边的部分）2>对攻击载荷进行免杀处理，通过编码器编码，将攻击载荷的特征码进行隐藏，从而躲避入侵检测系统（IDS）和入侵防御系统（IPS）的检测和查杀。  （6）后渗透攻击模块  介绍：在Metasploit v4版本后引进，主要是支持在渗透攻击取得目标系统远程控制权之后，在受控系统中进行各种后渗透攻击动作，比如获取敏感信息，进一步拓展，实施跳板攻击等。 |
| 中国菜刀是一款专业的网站管理软件，用途广泛，使用方便，小巧实用。只要支持动态脚本的网站，都可以用中国菜刀来进行管理！程序大小：214K，在非简体中文环境下使用，自动切换到英文界面。UINCODE方式编译，支持多国语言输入显示。 | （1）文件管理：缓存下载目录，并支持离线查看缓存目录;  （2）虚拟终端：人性化的设计，操作方便;(输入HELP查看更多用法)  （3）数据库管理：图形界面,支持YSQL,MSSQL,ORACLE,INFOMIX,ACCESS，以及支持ADO方式连接的数据库。  只要往目标网站中加入一句话木马，然后你就可以在本地通过中国菜刀chopper.exe即可获取和控制整个网站目录。 |
| Struts2漏洞检测工具，支持S2-057 CVE-2018-11776 、S2-048 CVE-2017-9791、S2-046 CVE-2017-5638、S2-045 CVE-2017-5638、S2-037 CVE-2016-4438、 S2-032 CVE-2016-3081 、S2-020 CVE-2014-0094 、S2-019 CVE-2013-4316等漏洞检测。 | 检测并利用struts 2漏洞。 |
| Puma Scan是一个基于.NET框架编写的软件安全代码分析工具, | 可在团队编写代码时提供实时、连续的源代码分析支持。在使用Visual Studio工具进行开发时, 相关缺陷会实时显示为拼写检查和编译器警告, 防止将安全bug带入应用程序。Puma Scan还集成到build过程中, 以便在编译时提供安全性分析。 |
| Layer | Layer子域名挖掘机(域名查询工具)用于网站子域名查询，有服务接口、暴力破解、同服挖掘三种模式。 |
| X-Scan是国内最著名的综合扫描器之一，它完全免费，是不需要安装的[绿色软件](https://baike.baidu.com/item/%E7%BB%BF%E8%89%B2%E8%BD%AF%E4%BB%B6/298001" \t "_blank)、界面支持中文和英文两种语言、包括图形界面和命令行方式。主要由国内著名的民间黑客组织“[安全焦点](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E7%84%A6%E7%82%B9/9776672)”完成，从2000年的内部测试版X-Scan V0.2到目前的最新版本X-Scan 3.3-cn都凝聚了国内众多黑客的心血。最值得一提的是，X-Scan把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便[网管](https://baike.baidu.com/item/%E7%BD%91%E7%AE%A1/186326" \t "_blank)测试、修补漏洞。 | 采用多线程方式对指定IP地址段(或单机)进行安全漏洞检测，支持[插件](https://baike.baidu.com/item/%E6%8F%92%E4%BB%B6" \t "_blank)功能。扫描内容包括：[远程服务](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E6%9C%8D%E5%8A%A1)类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。 |
| RedHunt OS | RedHunt 操作系统的目标是通过集成攻击者的武库以及防御者的工具包来积极识别环境中的攻击，从而成为一站式安全检测商店，满足你的所有攻击仿真和攻击要求。基本设备Lubuntu-17.10.1 x64。它包含以下用于不同目的的工具：攻击仿真： Caldera, Atomic Red Team, DumpsterFire, Metta, RTA, Nmap, CrackMapExec, Responder, Zap。记录和监测：Kolide Fleet，ELK（Elasticsearch，Logstash 和 Kibana）堆栈开源智能（OSINT）：Maltego，Recon-ng，Datasploit，Thearvestor攻击信息分析：Yeti, Harpoon。 |
| [MasScan](https://www.cesafe.com/7840.html) | masscan的扫描结果类似于nmap(一个很著名的端口扫描器)，在内部，它更像scanrand, unicornscan, and ZMap，采用了异步传输的方式。它和这些扫描器最主要的区别是，它比这些扫描器更快。而且，masscan更加灵活，它允许自定义任意的地址范和端口范围。  您要扫描的IP地址/范围, 和端口号码. 一个例子以下是扫描10 Web服务器10.x.x.x网络:  masscan 10.0.0.0/8 -p80  该程序自动检测网络接口/适配器设置。 如果自动配置失败，则必须手动配置。 |
| [Invoke-ATTACKAPI](http://iphone.myzaker.com/zaker/link.php?pk=5ae67b0477ac64565b333728&b=aHR0cHM6Ly9naXRodWIuY29tL0N5YjNyV2FyZDBnL0ludm9rZS1BVFRBQ0tBUEk=&bcode=f6bab0eb&target=_new) | 这是一个开源的 PowerShell 脚本，通过自己的 API 与 MITRE ATT＆CK 框架进行交互，以收集有关攻击技术，策略等信息，点击这里获取这个脚本。 |
| [Cymulate](http://iphone.myzaker.com/zaker/link.php?pk=5ae67b0477ac64565b333728&b=aHR0cHM6Ly93d3cuY3ltdWxhdGUuY29tL3NvbHV0aW9ucy8=&bcode=8eec8680&target=_new) | Cymulate 主要是针对以下场景进行攻击模拟，例如模拟攻击 WAF、模拟攻击邮箱、DLP 攻击测试、SOC 模拟测试、邮箱测试、勒索软件测试、木马、Payload 渗透攻击测试等。这类测试的主要目的是完善产品、丰富员工的安全意识，以及相应的攻击技术能力检测和提升。举个例子，利用邮箱以及可以统计钓鱼攻击有多少用户中招。 |

**测评委托单位（签字确认）：**