# 八大常用渗透测试工具

# ****【01.Nmap】****

Nmap ("Network Mapper") 是一个自由和开放源码（许可证）的实用的网络发现和安全审计工具。Nmap是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（这是亦称 fingerprinting）。

它是网络管理员必用的软件之一，以及用以评估网络系统安全。正如大多数被用于网络安全的工具，nmap 也是不少黑客及骇客（又称脚本小子）爱用的工具 。系统管理员可以利用nmap来探测工作环境中未经批准使用的服务器，但是黑客会利用nmap来搜集目标电脑的网络设定，从而计划攻击的方法。Nmap 常被跟评估系统漏洞软件Nessus 混为一谈。Nmap 以隐秘的手法，避开闯入检测系统的监视，并尽可能不影响目标系统的日常操作。

其基本功能有三个，一是探测一组主机是否在线；其次是扫描 主机端口，嗅探所提供的网络服务；还可以推断主机所用的操作系统 。Nmap可用于扫描仅有两个节点的LAN，直至500个节点以上的网络。Nmap 还允许用户定制扫描技巧。通常，一个简单的使用ICMP协议的ping操作可以满足一般需求；也可以深入探测UDP或者TCP端口，直至主机所 使用的操作系统；还可以将所有探测结果记录到各种格式的日志中， 供进一步分析操作。

nmap运行在所有主流的计算机操作系统，和官方的二进制软件包可用于Linux，Windows和Mac OS X中，除了传统的命令行命令的可执行文件，nmap套件包括一个先进的图形用户界面和结果查看器（Zenmap），灵活的数据传输，重定向，和调试工具（NCAT），用于比较扫描结果的效用（NDIFF），和一个数据包生成和响应分析工具（nping）。

Nmap 在黑客帝国(The Matrix)中，连同SSH1的32位元循环冗余校验漏洞，被崔妮蒂用以入侵发电站的能源管理系统。它甚至出现在了十二部电影中，包括重装上阵，虎胆龙威4，与龙纹身的女孩，和最后通牒。

下载地址：<https://nmap.org/>

# ****【02.Wireshark】****

Wireshark是世界上最重要和最广泛使用的网络协议分析器。它可以让你在微观层面上看到你的网络上正在发生的事情，并且是许多商业和非盈利企业、政府机构和教育机构的标准。Wireshark发展得益于世界各地网络专家的志愿贡献，也是1998年杰拉尔德·库姆斯开始的项目的延续。

Wireshark（前称Ethereal）是一个网络封包分析软件。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。网络封包分析软件的功能可想像成 "电工技师使用电表来量测电流、电压、电阻" 的工作 - 只是将场景移植到网络上，并将电线替换成网络线。在过去，网络封包分析软件是非常昂贵的，或是专门属于盈利用的软件。Ethereal的出现改变了这一切。在GNUGPL通用许可证的保障范围底下，使用者可以以免费的代价取得软件与其源代码，并拥有针对其源代码修改及客制化的权利。Ethereal是目前全世界最广泛的网络封包分析软件之一。

下载地址：<https://www.wireshark.org/>

# ****【03.Metasploit】****

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，社会工程学。

Metasploit是H.D. Moore在2003年开发的，它是少数几个可用于执行诸多渗透测试步骤的工具。在发现新漏洞时（这是很常见的），Metasploit会监控Rapid7，然后Metasploit的200,000多个用户会将漏洞添加到Metasploit的目录上。然后，任何人只要使用Metasploit，就可以用它来测试特定系统的是否有这个漏洞。

Metasploit框架使Metasploit具有良好的可扩展性，它的控制接口负责发现漏洞、攻击漏洞，提交漏洞，然后通过一些接口加入攻击后处理工具和报表工具。Metasploit框架可以从一个漏洞扫描程序导入数据，使用关于有漏洞主机的详细信息来发现可攻击漏洞，然后使用有效载荷对系统发起攻击。所有这些操作都可以通过Metasploit的Web界面进行管理，而它只是其中一种种管理接口，另外还有命令行工具和一些商业工具等等。

攻击者可以将来漏洞扫描程序的结果导入到Metasploit框架的开源安全工具Armitage中，然后通过Metasploit的模块来确定漏洞。一旦发现了漏洞，攻击者就可以采取一种可行方法攻击系统，通过Shell或启动Metasploit的meterpreter来控制这个系统。

这些有效载荷就是在获得本地系统访问之后执行的一系列命令。这个过程需要参考一些文档并使用一些数据库技术，在发现漏洞之后开发一种可行的攻击方法。其中有效载荷数据库包含用于提取本地系统密码、安装其他软件或控制硬件等的模块，这些功能很像以前BO2K等工具所具备的功能。

下载地址：<https://www.metasploit.com/>

# ****【4.Aircrack-ng】****

Aircrack-ng是一个与802.11标准的无线网络分析有关的安全软件，主要功能有：网络侦测，数据包嗅探，WEP和WPA/WPA2-PSK破解。Aircrack-ng可以工作在任何支持监听模式的无线网卡上并嗅探802.11a，802.11b，802.11g的数据。该程序可运行在Linux和Windows上。Linux版本已经被移植到了Zaurus和Maemo系统平台, 并概念验证可移植到iPhone。

Aircrack-ng是Aircrack项目的一个分支。

下载地址：<http://www.aircrack-ng.org/>

# ****【5.Burp Suite】****

Burp Suite 是用于攻击web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。

所有的工具都共享一个能处理并显示HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

工具箱：

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”。

下载地址：<https://portswigger.net/burp/>

# ****【6.SQLMap】****

SQLMap是一款用来检测与利用SQL注入漏洞的免费开源工具，它支持对检测与利用的自动化处理（数据库指纹、访问底层文件系统、执行命令）等。

sqlmap支持五种不同的注入模式：

1、基于布尔的盲注，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内容判断任何信息，用条件语句查看时间延迟语句是否执行（即页面返回时间是否增加）来判断。

3、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在页面中。

4、联合查询注入，可以使用union的情况下的注入。

5、堆查询注入，可以同时执行多条语句的执行时的注入。

sqlmap支持的数据库有：

MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase和SAP MaxDB

可以提供一个简单的URL，Burp或WebScarab请求日志文件，文本文档中的完整http请求或者Google的搜索，匹配出结果页面，也可以自己定义一个正则来判断那个地址去测试。

测试GET参数，POST参数，HTTP Cookie参数，HTTP User-Agent头和HTTP Referer头来确认是否有SQL注入，它也可以指定用逗号分隔的列表的具体参数来测试。

可以设定HTTP(S)请求的并发数，来提高盲注时的效率。

下载地址：<http://sqlmap.org/>

# ****【7.John The Ripper】****

John the Ripper是一款免费的开源软件，是一个快速的密码破解工具，用于在已知密文的情况下尝试破解出明文的破解密码软件，支持目前大多数的加密算法，如DES、MD4、MD5等。它支持多种不同类型的系统架构，包括Unix、Linux、Windows、DOS模式、BeOS和OpenVMS，主要目的是破解不够牢固的Unix/Linux系统密码。

下载地址：<http://www.openwall.com/john/>

# ****【8.THC Hydra】****

THC Hydra是一个非常流行的密码破解，它由一只非常活跃且经验丰富的开发团队开发。THC Hydra是一个快速稳定的网络登录攻击工具，它使用字典攻击和暴力攻击，尝试大量的密码和登录组合来登录页面。攻击工具支持一系列协议，包括邮件（POP3，IMAP等），数据库，LDAP，SMB，VNC和SSH。

下载地址：http://sectools.org/tool/hydra/