工具列表：

<https://tools.kali.org/tools-listing>

1、Information Gathering（信息收集）收集目标主机的信息

2、Vulnerability Analysis（弱点分析）找出系统的薄弱点

3、Wireless Attacks（无线攻击）

4、Web Applications（web 应用程序）

5、Exploitation Tools（开发工具）

6、Forensics Tools（取证工具）

7、Stress Testing（压力测试）

8、Sniffing & Spoofing（嗅探与欺骗）

9、Password Attacks（密码破解）

10、Maintaining Access（维持访问）

11、Reverse Engineering（逆向工程）

12、Hardware Hacking（硬件黑客）

13、Reporting Tools（报告工具）

kali-linux-top10 : Top 10 Kali Linux Tools

下列工具简介源地址：

<http://www.freebuf.com/sectool/125984.html>

Metasploit是一个漏洞框架。它的全称叫做The Metasploit Framework，简称叫做MSF。Metasploit作为受欢迎的工具，不仅仅是因为它的方便性和强大性，更重要的是它的框架。它允许使用者开发自己的漏洞脚本，从而进行测试。用 Ruby 编程语言

metasploit基本用法

banner：查看版本信息

db\_driver：metasploit测试前，需要连接数据库（有的版本自动连接）db\_connect

search：查找相关模块shellcode（search name：\*\*）

use：使用模块back退出

show options：查看模块参数设置

set：设置参数信息或加载PAYLOAD（setg设置后保存）

payloads模块，也就是shellcode，就是在漏洞利用成功后所要做的事情

run：开始渗透攻击

check：测试target（目标操作系统）设置是否正确

edit：编辑当前模块

irb：ruby脚本命令行模式

.metasploit攻击方式分类

635种(exploit)溢出模块、314种(auxiliary)辅助模块、215种(payload)加载模块、27种(encoder免杀处理用)编码、8种(nops)

溢出攻击：主动溢出和被动溢出（主动攻击获取权限和监听获取权限）

<https://www.ibm.com/developerworks/cn/web/wa-metasploit/>

<http://blog.csdn.net/tan6600/article/details/46850057>

>？

显示所有的命令

Metasploit 4.5之后的版本不再包含db\_autopwn

步骤：

<http://blog.csdn.net/zxchhyg/article/details/72637596>

<https://www.cnblogs.com/zqjt/p/5431023.html>

例子：

http://www.freebuf.com/articles/web/5628.html

一．名词解释

exploit

测试者利用它来攻击一个系统，程序，或服务，以获得开发者意料之外的结果。常见的

有内存溢出，网站程序漏洞利用，配置错误exploit。

payload

我们想让被攻击系统执行的程序，如reverse shell 可以从目标机器与测试者之间建立一

个反响连接，bind shell 绑定一个执行命令的通道至测试者的机器。payload 也可以是只

能在目标机器上执行有限命令的程序。

shellcode

是进行攻击时的一系列被当作payload 的指令，通常在目标机器上执行之后提供一个可

执行命令的shell。

module

MSF 的模块，由一系列代码组成。

listener

等待来自被攻击机器的incoming 连接的监听在测试者机器上的程序

use 模块 >> 进入模块

show options

* info 模块名

Nmap是一款非常强大的实用工具,可用于：检测活在网络上的主机（主机发现）检测主机上开放的端口（端口发现或枚举）检测到相应的端口（服务发现）的软件和版本检测操作系统，硬件地址，以及软件版本检测脆弱性的漏洞（Nmap的脚本）Nmap是一个非常普遍的工具，它有命令行界面和图形用户界面。

<https://jingyan.baidu.com/article/47a29f24312010c0142399f1.html>

那么exp，就是exploit，漏洞利用的意思，注意，有漏洞不一定就有Exploit（利用)。有Exploit就肯定有漏洞。我们可以引申为利用的方式，通常是以各种代码出现的

2、NetCat是一个非常简单的Unix工具，可以读、写TCP或UDP网络连接(network connection)。它被设计成一个可靠的后端(back-end) 工具，通过与其他工具结合和重定向，你可以在脚本中以多种方式使用它。同时，它又是一个功能丰富的网络调试和开发工具，因为它可以建立你可能用到的几乎任何类型的连接，以及一些非常有意思的内建功能。NetCat，它的实际可运行的名字叫nc，是一个很早就被提供，但没有公开的事实标准的Unix工具。使用NC命令所能完成的事情令人惊讶。

netcat可以作为类似于telent的客户端,也可以监听某个端口作为服务器,还可以作为扫描工具扫描对方主机的端口,还可以用来传输文件, netcat的工作原理,其实netcat的原理很简单,它就是从网络的一端读入数据,然后输出到网络的另一端,它可以使用tcp和udp协议.之所以叫做netcat,因为它是网络上的cat,想象一下cat的功能,读出一个文件的内容,然后输出到屏幕上(默认的stdout是屏幕,当然可以重定向到其他地方).

功能详解：

<https://www.oschina.net/translate/linux-netcat-command>

？与telnet的区别

Nmap（网络映射器）是一款用于网络发现和安全审计的网络安全工具，它是自由软件。软件名字Nmap是Network Mapper的简称。

Nmap可以检测目标主机是否在线、端口开放情况、侦测运行的服务类型及版本信息、侦测操作系统与设备类型等信息。 它是网络管理员必用的软件之一，用以评估网络系统安全。

Nmap通常用在信息搜集阶段，用于搜集目标机主机的基本状态信息。扫描结果可以作为漏洞扫描、漏洞利用和权限提升阶段的输入。

业界流行的漏洞扫描工具Nessus与漏洞利用工具Metasploit都支持导入Nmap的XML格式结果，而Metasploit框架内也集成了Nmap工具（支持Metasploit直接扫描）

Nmap不仅可以用于扫描单个主机，也可以适用于扫描大规模的计算机网络

3、Nmap（网络映射器）是一款用于网络发现和安全审计的网络安全工具，它是自由软件。软件名字Nmap是Network Mapper的简称。

总结：其基本功能有：

主机发现（Host Discovery）

端口扫描（Port Scanning）

版本侦测（Version Detection）

操作系统侦测（Operating System Detection）

首先需要进行主机发现，随后确定端口状况，然后确定端口上运行具体应用程序与版本信息，然后可以进行操作系统的侦测。而在四项基本功能的基础上，Nmap提供防火墙与IDS（IntrusionDetection System,入侵检测系统）的规避技巧，可以综合应用到四个基本功能的各个阶段；另外Nmap提供强大的NSE（Nmap Scripting Language）脚本引擎功能，脚本可以对基本功能进行补充和扩展。

最基本最核心的功能

端口扫描：Nmap可以将端口识别为开放（Open）、关闭（Closed）、过滤（Filtered）、未过滤（Unfiltered）、开放或过滤（Open|Filtered）、关闭或过滤（Closed|Filtered）。默认情况下，Nmap会扫描1660个常用的端口[1]，可以覆盖大多数基本应用情况。

版本侦测：用于识别端口上运行的应用程序与程序版本。Nmap目前可以识别数千种应用的签名（Signatures）,检测数百种应用协议。而对于不识别的应用，Nmap默认会将应用的指纹(Fingerprint)打印出来，如果用户确知该应用程序，那么用户可以将信息提交到社区，为社区做贡献。

操作系统侦测：用于识别目标主机的操作系统类型、版本编号及设备类型。

Nmap目前提供1500个操作系统或设备的指纹数据库[2]，可以识别通用PC系统、路由器、交换机等设备类型。

防火墙/IDS规避和哄骗：Nmap提供多种机制来规避防火墙、IDS的的屏蔽和检查，便于秘密地探查目标主机的状况。

基本的规避方式包括：分片、IP诱骗、IP伪装、MAC地址伪装。

<http://blog.csdn.net/aspirationflow/article/details/7694274>

SQL注入是一种代码注入技术，过去常常用于攻击数据驱动性的应用，比如将恶意的SQL代码注入到特定字段用于实施拖库攻击等。SQL注入的成功必须借助应用程序的安全漏洞，例如用户输入没有经过正确地过滤（针对某些特定字符串）或者没有特别强调类型的时候，都容易造成异常地执行SQL语句。SQL注入是网站渗透中最常用的攻击技术，但是其实SQL注入可以用来攻击所有的SQL数据库。

练习网站：[www.webscanhost.org](http://www.webscanhost.org)

4、sqlmap

SQLmap是一款用来检测与利用SQL注入漏洞的免费开源工具，有一个非常棒的特性，即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）。sql自动化注入工具，可以用来检测和利用sql注入漏洞。它由python语言开发而成，因此运行需要安装python环境。

注意：sqlmap只是用来检测和利用sql注入点的，并不能扫描出网站有哪些漏洞，使用前请先使用扫描工具扫出sql注入点。

<https://null-byte.wonderhowto.com/how-to/hack-databases-hacking-mysql-online-databases-with-sqlmap-0150368/>

几年前的asp网站，基本上都有这种漏洞

定位注入的网站 利用Google Dorks字符串找到可注入的网站

inurl:item\_id=

验证网站是否可以进行SQL注入

<http://www.cinemax-prod.co.il/project.asp?item_id=10>’

<http://www.cinemax-prod.co.il/project.asp?item_id=10> and 1 = 1

<http://www.cinemax-prod.co.il/project.asp?item_id=10> and 1 = 2

如果页面返回一个SQL错误，说明页面可能存在SQL注入点；如果页面加载正常显示或者重定向到一个不同的页面，跳过这个网站，用同样的方法去测试下一个网站。

源地址：<http://drops.xmd5.com/static/drops/tips-2113.html>

2、-u : 指定目标URL

>python sqlmap.py -u "http://192.168.1.150/products.asp?id=134"

1、判断可注入的参数

2、判断可以用那种SQL注入技术来注入

3、识别出哪种数据库

4、根据用户选择，读取哪些数据

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。

支持的数据库有：MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase和SAP MaxDB

3、-b : 获取DBMS banner

4、–current-db : 获取当前数据库

>python sqlmap.py -u "http://192.168.1.150/products.asp?id=134" --current-db

5、–current-user:获取当前用户

>python sqlmap.py -u "http://192.168.1.150/products.asp?id=134" --current-user

5、aircrack-ng

<http://www.jianshu.com/p/d4da13258f35>

Aircrack-ng是一个与IEEE 802.11协议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等（无线网络的接入层协议）的数据。

Aircrack-ng主要使用了两种攻击方式进行WEP破解：一种是FMS攻击，该攻击方式是以发现该WEP漏洞的研究人员名字（Scott Fluhrer、Itsik Mantin及Adi Shamir）所命名；另一种是KoreK攻击，经统计，该攻击方式的攻击效率要远高于FMS攻击。当然，最新的版本又集成了更多种类型的攻击方式。对于无线黑客而言，Aircrack-ng是一款必不可缺的无线攻击工具，可以说很大一部分无线攻击都依赖于它来完成；而对于无线安全人员而言，Aircrack-ng也是一款必备的无线安全检测工具，它可以帮助管理员进行无线网络密码的脆弱性检查及了解无线网络信号的分布情况，非常适合对企业进行无线安全审计时使用。

包含了多款工具的无线攻击审计套装，这里面很多工具在后面的内容中都会用到，具体见下表1为Aircrack-ng包含的组件具体列表

aircrack-ng 破解WEP以及WPA（字典攻击）密钥

airdecap-ng 通过已知密钥来解密WEP或WPA嗅探数据

airmon-ng 将网卡设定为监听模式

aireplay-ng 数据包注入工具（Linux和Windows使用CommView驱动程序）

airodump-ng 数据包嗅探：将无线网络数据输送到PCAP或IVS文件并显示网络信息

airtun-ng 创建虚拟管道

airolib-ng 保存、管理ESSID密码列表

packetforge-ng 创建数据包注入用的加密包。

Tools 混合、转换工具

airbase-ng 软件模拟AP

airdecloak-ng 消除pcap文件中的WEP加密

airdriver-ng 无线设备驱动管理工具

airolib-ng 保存、管理ESSID密码列表，计算对应的密钥

airserv-ng 允许不同的进程访问无线网卡

buddy-ng easside-ng的文件描述

easside-ng 和AP接入点通讯（无WEP）

tkiptun-ng WPA/TKIP攻击

wesside-ng 自动破解WEP密钥

WEP试验:

查看网卡详细信息

>iwconfig

图4

激活网卡至监视模式

>airmon-ng start wlan0网卡名

获取附近AP (Access Point) 信息

> airodump-ng wlan0

图5

BSSID(Basic Service SetIdentifier): AP 的MAC 地址。

ESSID(The Extended Service Set Identifier): AP 的名称。

PWR(Power): 信号强度。

"-"后的数值越大表示信号越弱。

Data:当前数据传输量

CH(Channel): AP 所在的频道。

ENC(Encryption): 使用的加密算法体系。

CIPHER: 加密方式

AUTH(Authority): 认证方式

#开始抓包

>airodump-ng --ivs -w filename --bssid BSSID wlan0

--ivs设置过滤，只保存可用于破解的IVS数据报文，缩减保存的数据包大小；

-w 保存的文件名

--bssid 选中路由器的MAC

若连接着该无线路由器/AP的无线客户端正在进行大流量的交互，比如使用迅雷、电骡进行大文件下载等，则可以依靠单纯的抓包就可以破解出WEP密码。但是无线黑客们觉得这样的等待有时候过于漫长，于是就采用了一种称之为“ARP Request”的方式来读取ARP请求报文，并伪造报文再次重发出去，以便刺激AP产生更多的数据包，从而加快破解过程，这种方法就称之为ArpRequest注入攻击。

重新开一个终端。

>aireplay-ng -3 -b BBSID -h mac wlan0

-b 后跟AP的MAC地址，这里就是前面我们探测到的SSID为TPLINK的AP的MAC

-h 后跟客户端的MAC地址，也就是我们前面探测到的有效无线客户端的MAC

图六 图7

经过等待，可以在终端中看到提示：“KEY FOUND！”后面即为WPA2-PSK连接密码

6、zaproxy（OWASP Zed Attack Proxy Project）是全球最受欢迎的免费安全工具之一。它可以帮助您在开发和测试应用程序时自动查找Web应用程序中的安全漏洞。它也是经验丰富的测试者用于手动安全测试的好工具。

ZAP的核心是一个拦截代理。您需要配置浏览器以连接到您希望通过ZAP测试的Web应用程序。

<https://github.com/zaproxy/zap-core-help/wiki>

主要功能

模糊测试

主动扫描和被动扫描

手动测试：上述步骤或许找到基本的漏洞。

SSL证书欺骗

请求断点（主要通过请求断点的方法实现绕过客户端验证，拦截请求从浏览器和改变它之前提交到网站所测试的应用程序）

目录扫描

支持多种脚本语言

调用应用程序

蜘蛛（AJAX）（查询网址）

7、burpsuite

Burp Suite是用于测试Web应用程序安全性的图形工具。该工具是用Java编写的

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”。

10、Maltego

Maltego是由Paterva开发的用于开源智能和取证的专有软件。Maltego专注于提供一个用于从开放源发现数据的变换库，并以图形格式可视化这些信息，适用于链接分析和数据挖掘。

Maltego允许创建自定义实体，除了属于软件的基本实体类型之外，还允许其代表任何类型的信息。该应用程序的基本重点是分析人与人，群体，网站，域名，网络，互联网基础设施，以及与Twitter和Facebook等在线服务的关系。

它可以收集某个人的在线数据信息 –包括电子邮件地址、博客、Facebook中的朋友，个人爱好、地理位置、工作描述，然后可以一种更为有用、全面的形式展现出来。