如果你真的喜欢安全，了解下面这些工具是你通往大神之路的必备良品，快来看看都有哪些工具并学习一下吧！

这份黑客工具列表中的一部分是基于Kali Linux的，其他的工具是通过我们的社区反馈的。下面介绍了这些工具的主要功能以及教程、书籍、视频等。

端口扫描器：Nmap

Nmap是"Network Mapper"的缩写，众所周知，它是一款非常受欢迎的免费开源黑客工具。Nmap被用于发现网络和安全审计。据数据统计，全世界成千上万的系统管理员使用nmap发现网络、检查开放端

口、管理服务升级计划，以及监视主机或服务的正常运行时间。Nmap是一种使用原始IP数据包的工具，以非常创新的方式决定网络上有哪些主机，主机上的哪些服务（应用名称和版本）提供什么数据、什么操作系统、什么类型、什么版本的包过滤/防火墙正在被目标使用。使用nmap有什么好处，其中一个就是管理员用户能够确定网络是否需要打包。所有的黑客电影中都出现了nmap的身影，尤其是最近的Mr.Robot系列中。

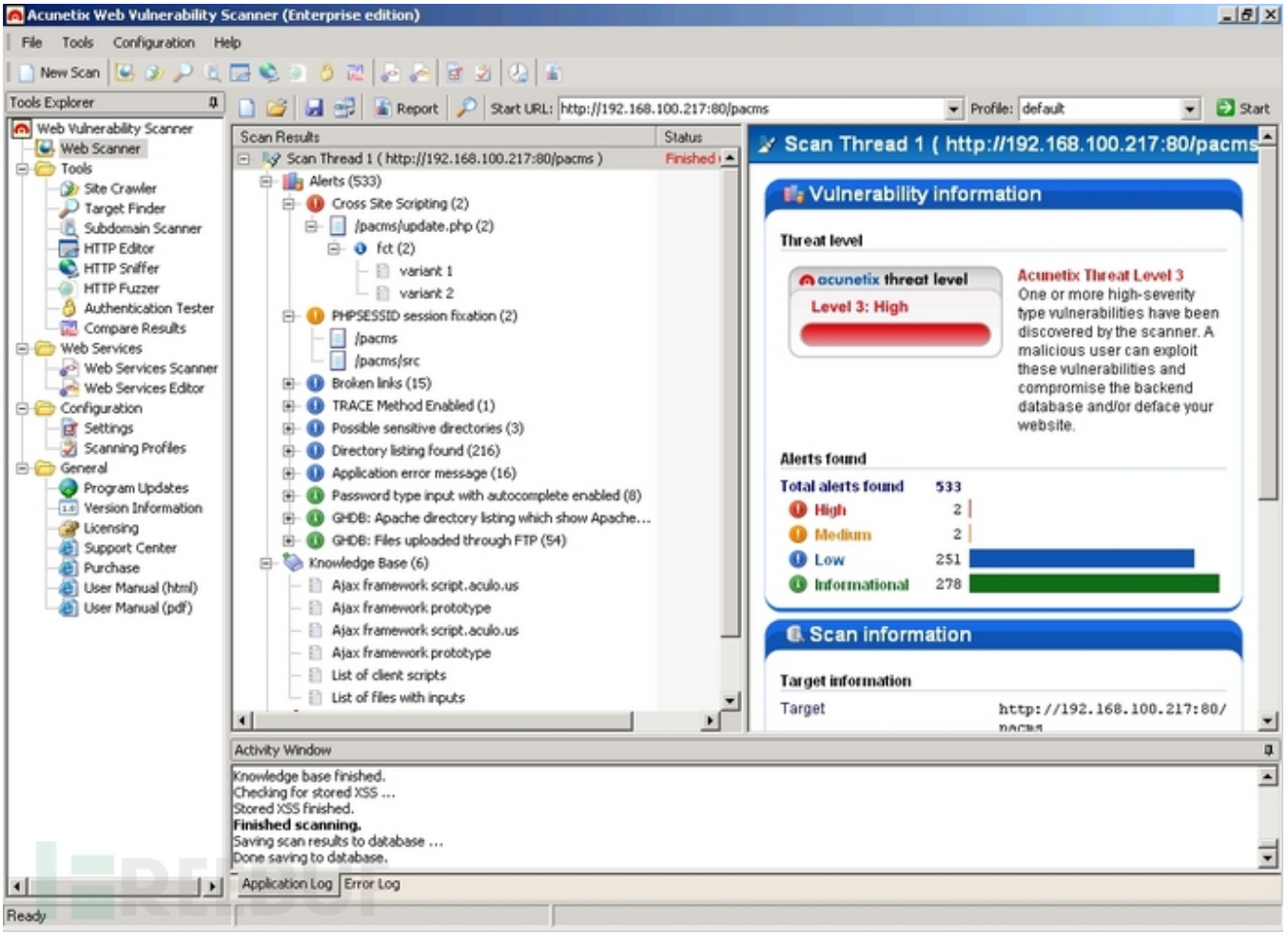
Nmap学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/category/2/nmap

书籍：https://www.concise-courses.com/books/nmap/

相似工具：https://www.concise-courses.com/hacking-tools/port-scanners/

网络漏洞扫描器：Acunetix



Acunetix是一款非常受欢迎并且非常使用的自动漏洞扫描器，Acunetix通过抓取和扫描网站和Web应用的SQL注入、XSS、XXE、SSRF和主机头攻击和其他500多个web漏洞。更新！Acunetic爱好者发布了一个100%免费的视频课程，所以你可以有效的学习如何使用这个非常棒的网络漏洞扫描器啦！更多关于Ac

unetix信息的链接以及注册Acunetix。

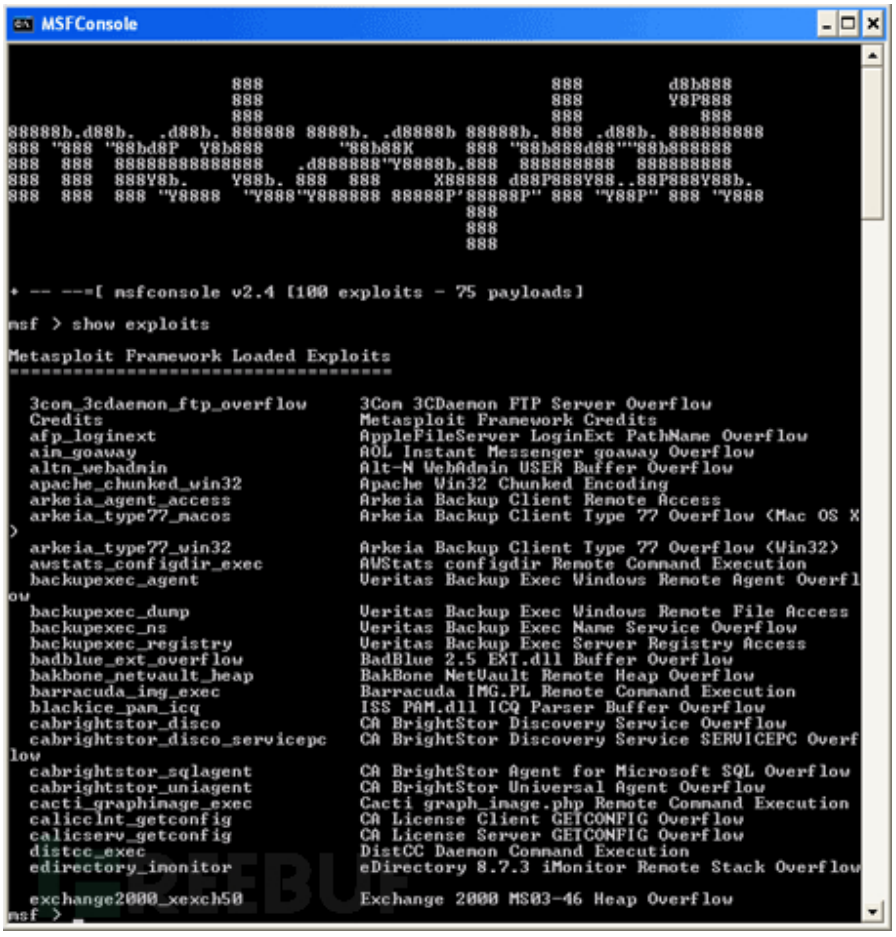
Acunetix学习资料

视频：https://www.concise-courses.com/learn/how-to-scan-for-vulnerabilities/

书籍：https://www.concise-courses.com/books/

相似工具：https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/

漏洞监测工具：Metasploit



Metasploit项目是一个非常受欢迎且受众很广的渗透测试以及攻击框架。如果你刚刚接触Metasploit，你会认为它是一个可用于执行各种任务的"黑客工具总汇"。Metasploit被专业的网络安全研究人员以及大量黑客使用，并且它被认为是研究安全的必学内容。Metasploit本质上是一个为用户提供已知安全漏洞主要信息的计算机安全项目（框架），并且Metasploit帮助指定渗透测试和IDS监测计划、战略以及

利用计划。Metasploit的优点太多，小编就不一一列举啦，希望下面的视频可以帮助你学习Metasploit。如果你是一个初学者，这里还有更多的初学者教程供你使用。

Metasploit学习资料

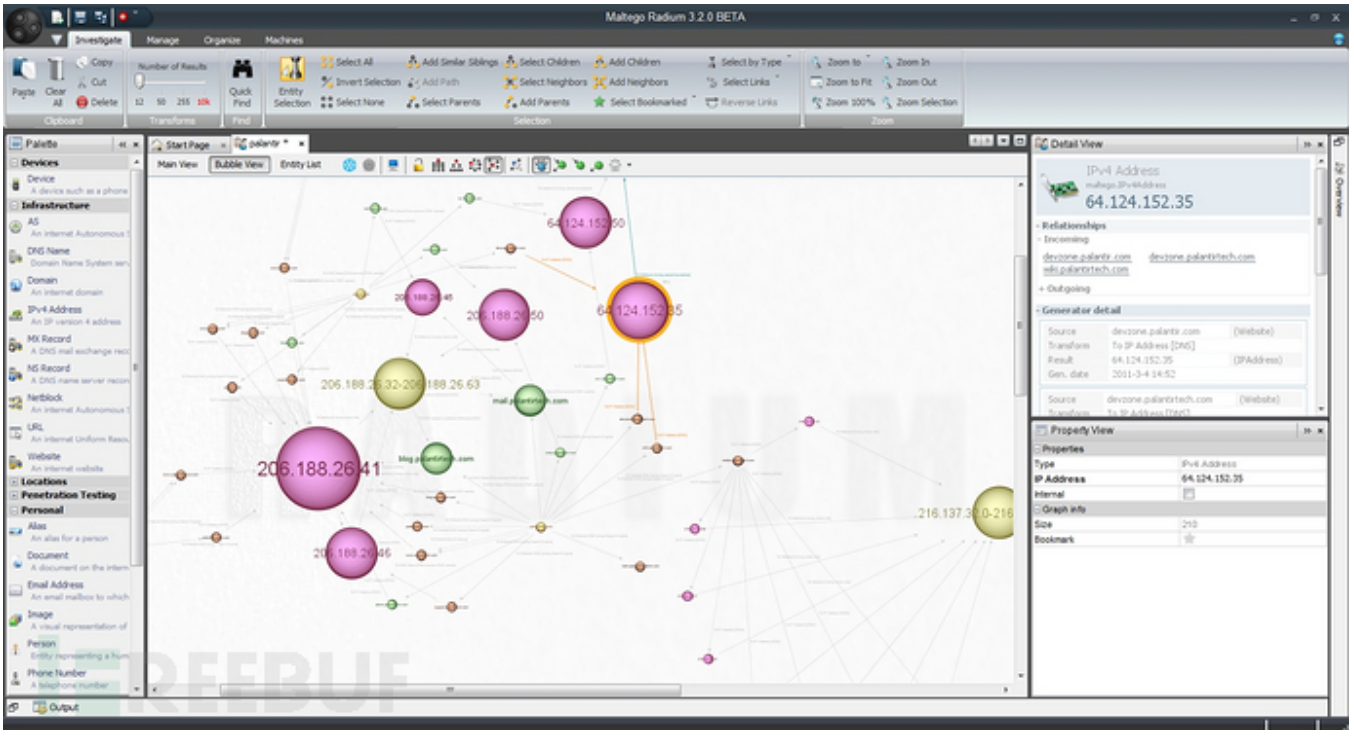
视频：https://www.concise-courses.com/hacking-tools/videos/category/3/metasploit

视频：https://www.concise-courses.com/hacking-tools/videos/category/3/metasploit

书籍：https://www.concise-courses.com/books/metasploit/

相似工具：https://www.concise-courses.com/hacking-tools/vulnerability-exploitation-tools/

取证：Maltego



Maltego跟其他取证工具不同，因为它在数字取证范围内工作。Maltego被设计用来把一个全面的网络威胁图片传给企业或者其他进行取证的组织的局部环境，它是一个平台。Maltego非常棒的一点，同时也是它非常受欢迎（因为它在Kali里排名前十）的原因是它的独特视角因为它同时提供了基于实体的网络和源，聚合了整个网络的信息-无论是网络的脆弱路由的当前配置，还是当前你的员工的国际访问，Maltego都可以定位，汇总并可视化这些数据！小编建议有兴趣的同学同时也学习OSINT网络安全数据。

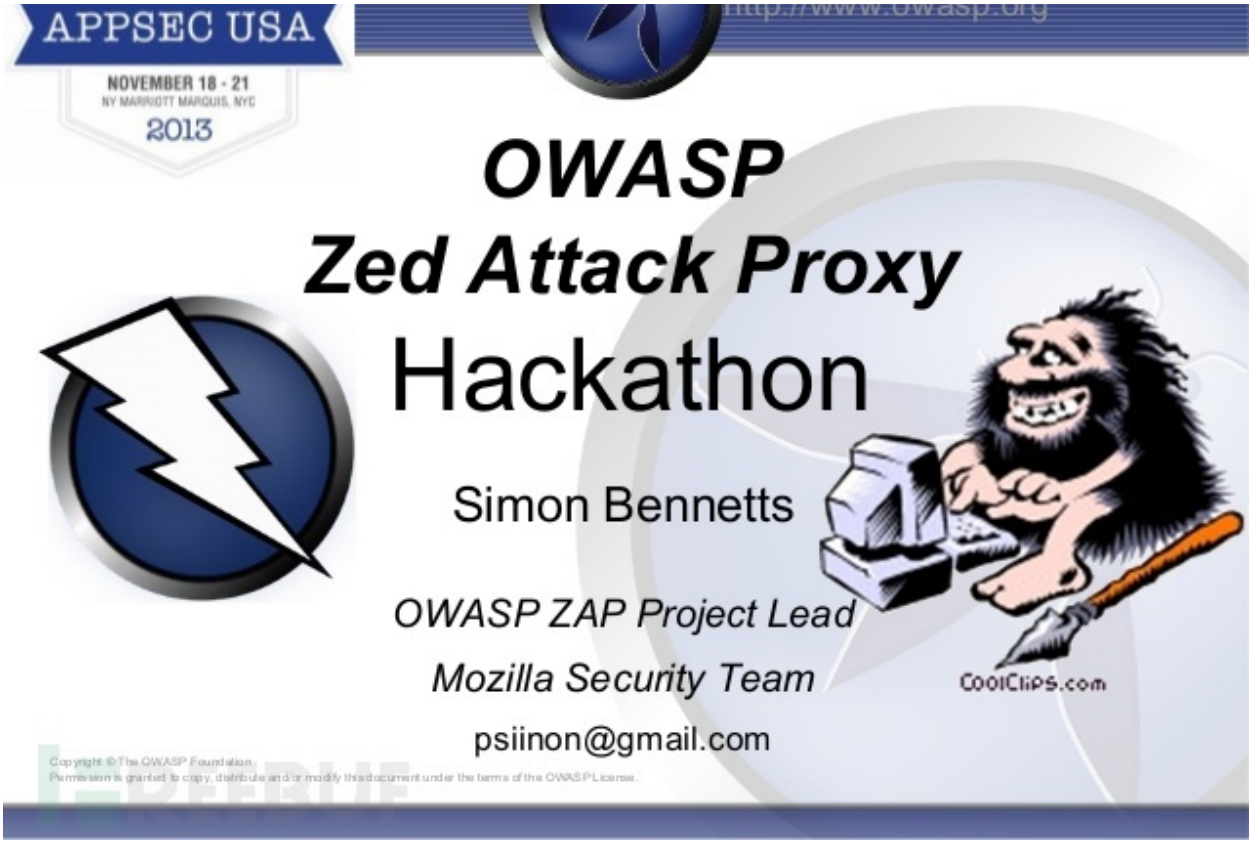
Maltego学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/category/13/maltego

书籍：https://www.concise-courses.com/books/

相似工具：https://www.concise-courses.com/hacking-tools/forensics/

网络漏洞扫描器：OWASP Zed



Zed的代理攻击(ZAP)是现在最流行的OWASP项目之一。你看到这页说明你有可能是一个经验丰富的网络安全研究人员哦，所以你可能非常熟悉OWASP。当然，OWASP在威胁列表中排名前十，它被作为学习web应用安全的指导手册。这个攻击渗透工具非常有效并且用起来非常简单。ZAP受欢迎是因为它有很多扩展支持，OWASP社区真的是一个非常棒的资源地来进行网络安全研究。ZAP提供自动扫描以及很多允许你进行专业发现网络安全漏洞的工具。好好理解这个工具并成为使用这个工具的大师非常有利于让渗透测试员的事业。如果你是一个开发者，那么这个工具会让你成为非常棒的黑客。

OWASP Zed学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/category/14/owasp-zed

书籍：https://www.concise-courses.com/books/

相似工具：https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/

手动分析包工具：Wireshark

如果说nmap排名黑客工具的第一名，那Wireshark肯定是第二受欢迎的工具。Wireshark已经存在了很长一段时间，并且他被成千上万的安全研究者用于排查、分析网络问题和网络入侵。Wireshark是个抓包工具，或者更确切的说，它是一个有效的分析数据包的开源平台。值得一提的是，Wireshark跨平台，我们本来以为它智能在GNU/Linux中运行，但是我们是错的，无论是Windows还是Linux甚至OS X都有Wireshark，还有一个类似于Wireshark的终端版本叫做TShark。这里有非常多的关于Wireshark的信息可以帮助你成为Wireshark专家。

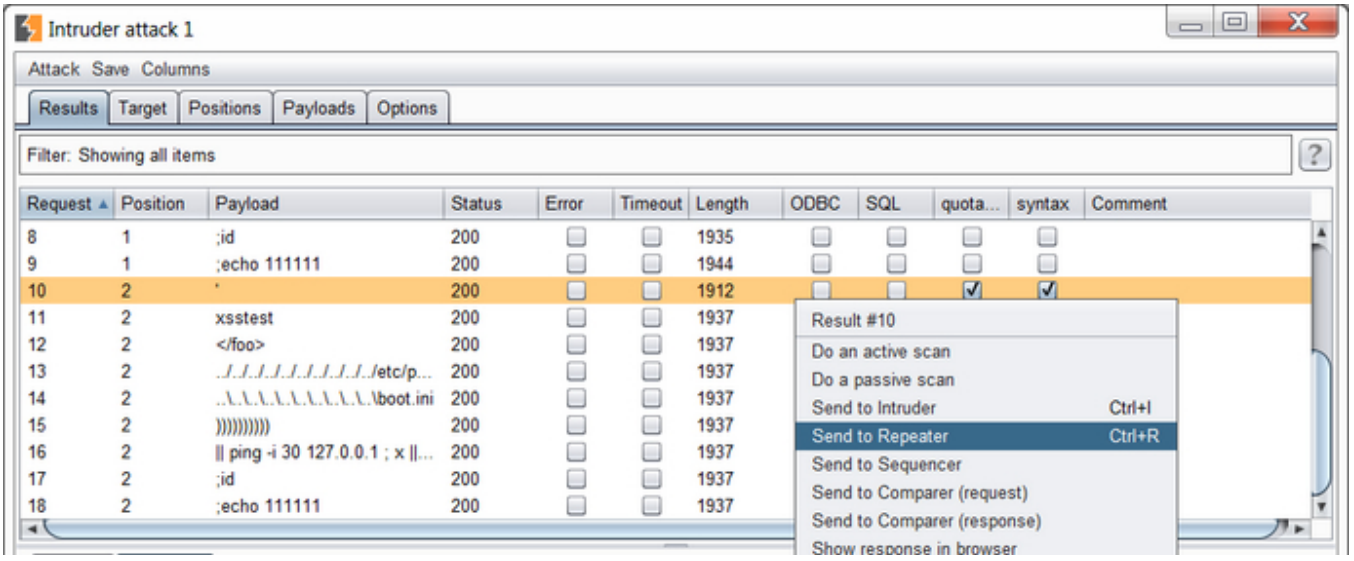
Wireshark学习资料

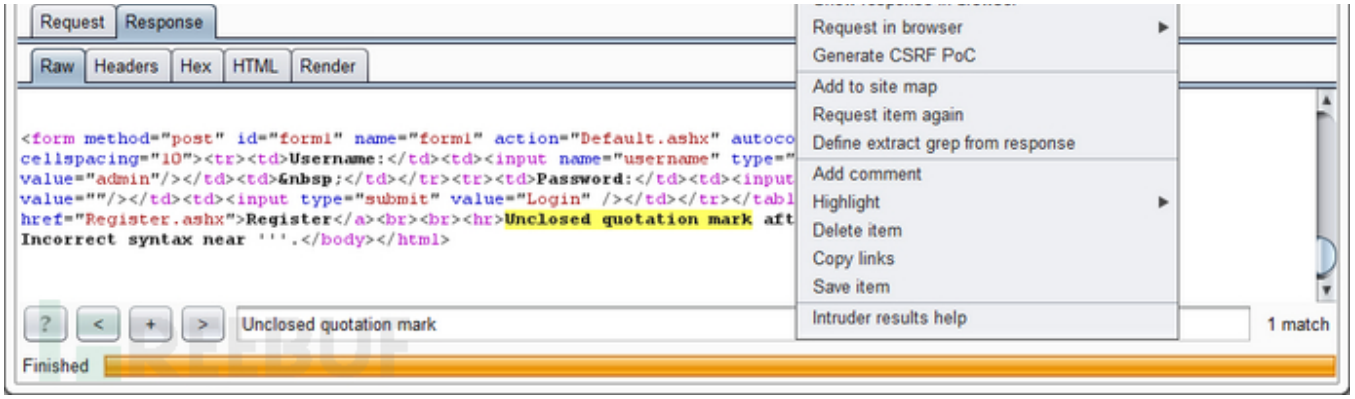
视频：https://www.concise-courses.com/hacking-tools/videos/category/16/wireshark

书籍：https://www.concise-courses.com/books/wireshark/

相似工具：https://www.concise-courses.com/hacking-tools/packet-crafting-tools/

网络漏洞扫描器：Burp Suite





Burp Suite在某种程度上很像Maltego，因为它也有一堆帮助渗透测试者和黑客的工具。Burp Suite中有两个常用应用，一个叫"Burp Suite Spider"，它可以通过监测cookie、初始化这些web应用的连接列举并绘制出一个网站的各个页面以及它的参数；另一个叫"Intruder"，它可以自动执行web应用攻击。同样，如果你是网络安全研究员或者正在进行渗透测试，Burp Suite也是一个必学工具。

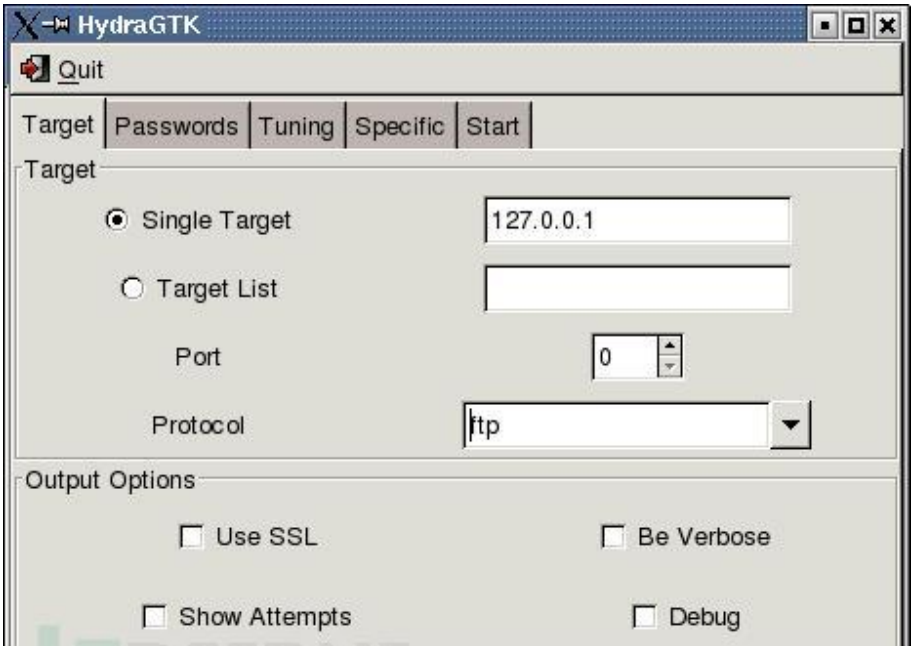
Burp Suite学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/category/7/burp-suite

书籍：https://www.concise-courses.com/books/burp-suite/

相似工具：https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/

密码破解：THC Hydra



```
hydra 127.0.0.1 ftp -l yourname -p yourpass
```

THC Hydra是一个非常流行的密码破解，它被一只非常活跃且经验丰富的开发团队开发。基本上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。

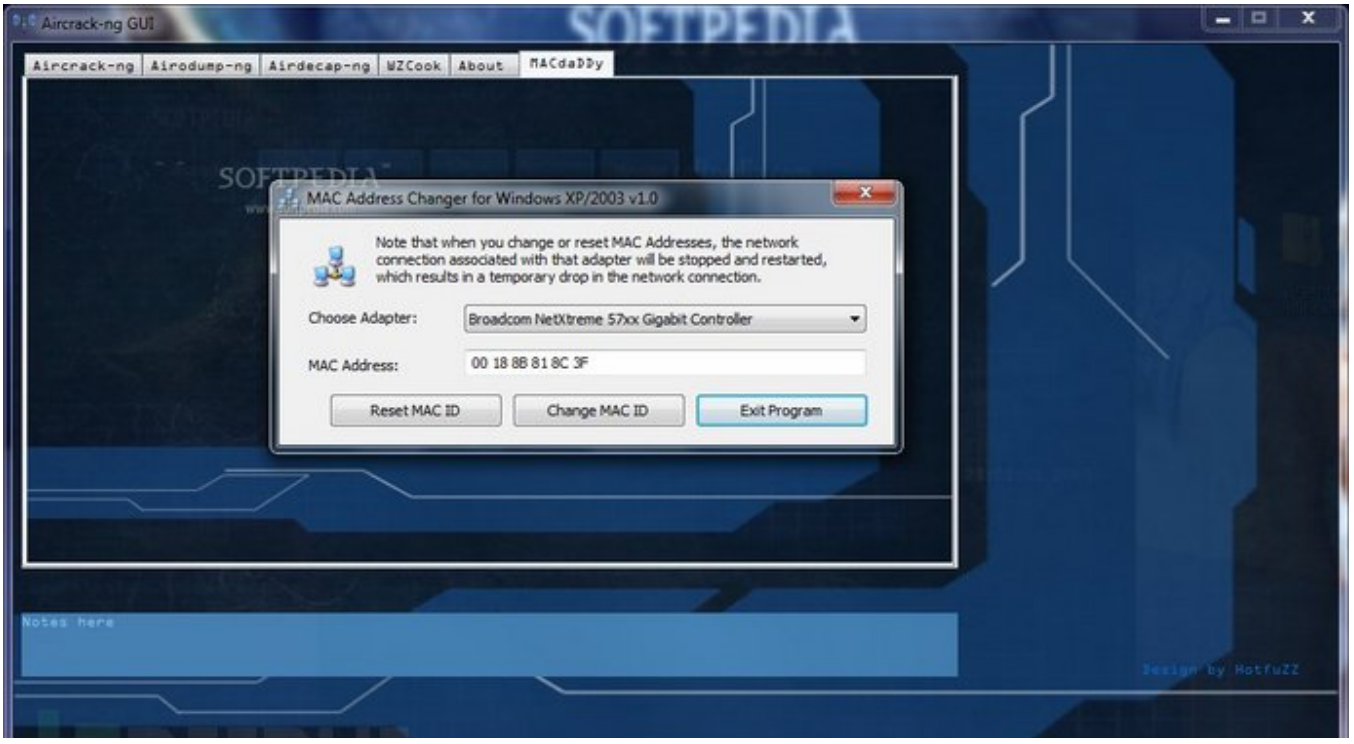
THC Hydra学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/

书籍：https://www.concise-courses.com/books/

相似工具：https://www.concise-courses.com/hacking-tools/password-crackers/

密码破解：Aircrack-ng



进行Wifi破解的Aircrack组件是攻击工具中的传奇，因为它非常有效！对于不太了解无效攻击的新手来说，Aircrack-ng是一个802.11 WEP和WPA-PSK密钥破解攻击工具并且可以在捕捉到足够数据包时恢复密钥。对于正在钻研无线网络的渗透和审计的朋友们来说，aircrack-ng将成为你最好的伙伴。Aircrack-ng利用标准FMS攻击对KoreK攻击进行了优化，并且让PTW攻击变得更有效。如果你是一个普通黑客，你可以在几分钟内破解WEP，你应该非常精通破解WPA/WPA2。如果你对无线网络攻击很感兴趣，我们强烈建议你看看Reaver，它也是一款非常受欢迎的黑客工具。

Aircrack-ng学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/category/12/aircrack-ng

书籍：https://www.concise-courses.com/books/aircrack-ng/

相似工具：https://www.concise-courses.com/hacking-tools/password-crackers/

密码破解：John The Ripper

John The Ripper（开膛手约翰）获得了最酷名字奖！大家一般把它成为"John"，它也是一款非常流行的密码破解渗透测试工具，经常被用于执行字典攻击。John the Ripper把文本字符串作为样本（来自文本文件的样本，被称为单词列表，包含在字典中找到的流行的、复杂的词汇或者之前破解时被用到的词汇），使用和加密方式相同的破解方式（包括加密算法和密钥）进行破解，然后对比加密字符串的输出

得到破解密钥。这个工具也可以用来执行变种的字典攻击。

John The Ripper学习资料

视频：https://www.concise-courses.com/hacking-tools/videos/category/1/john-the-ripper

书籍：https://www.concise-courses.com/books/

相似工具：https://www.concise-courses.com/books/

***原文地址：concise-courses，FB小编FireFrank编译，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**