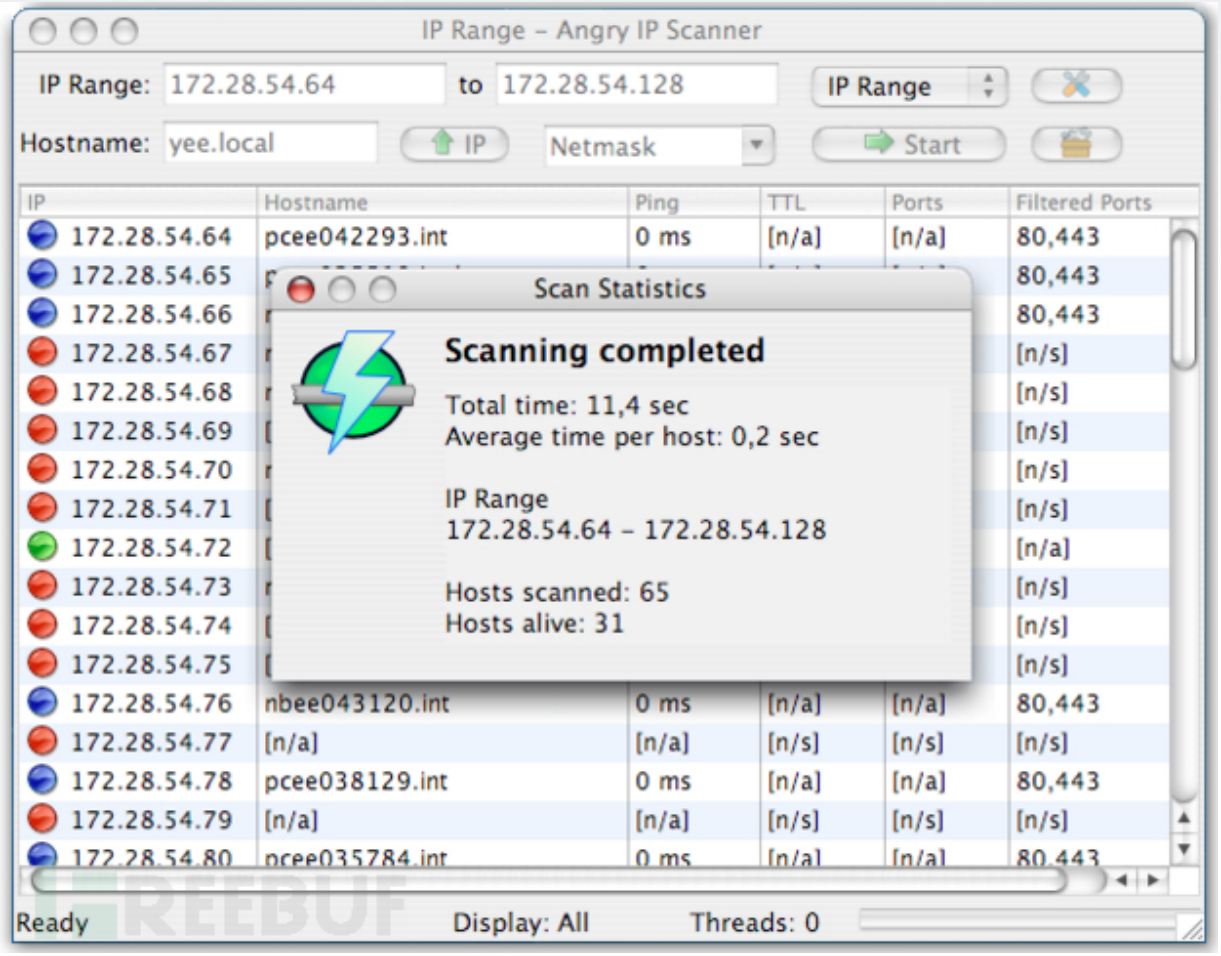
就像任何事物都有两面，黑客既可以进行恶意的攻击破坏，同样也可以通过利用自己的技术去找到系统的漏洞、缺陷等，然后通知相关企业进行修复已获得更好的防护。但无论是出于何种目的，对于黑客们而言，工具和脚本的使用都必不可少。所谓工欲善其事，必先利其器，本文将为大家整理介绍非常受欢迎的一些黑客工具，供大家挑选使用。

ANGRY IP SCANNER

黑客可以通过该工具使用人们的IP地址来对其进行跟踪并窥探其数据。其还被称作”IPScan”，即通过对IP地址和端口的扫描来找到进入用户系统的方法。它是一个开源的跨平台软件，也是目前最有效的黑客工具之一，网管、系统工程师的最爱。

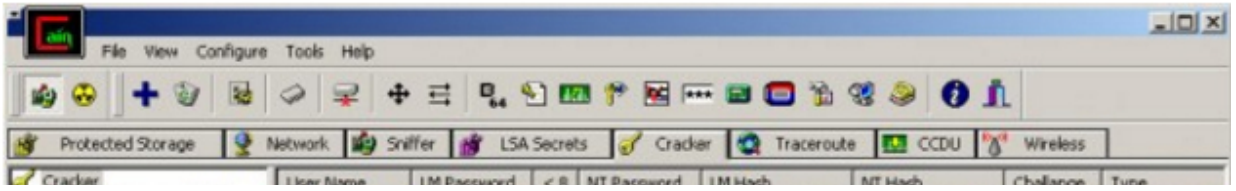


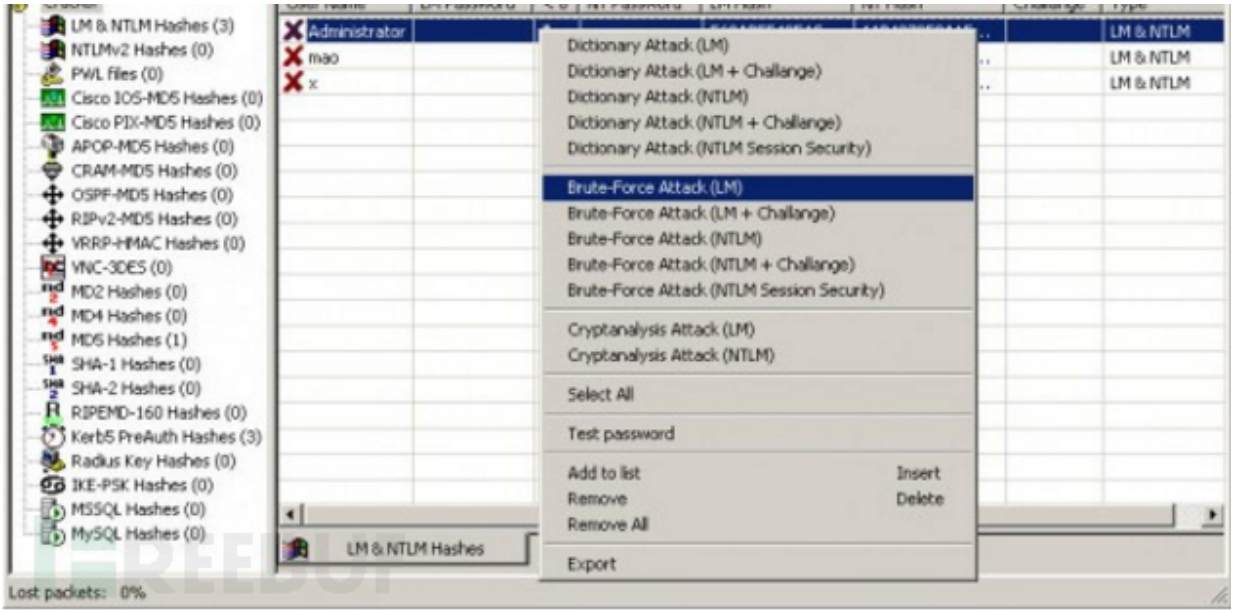
KALI LINUX

2015年8月11日， Kali Linux 最主要的一个版本 Kali Linux 2.0发布。其预装了非常多的渗透测试软件软件，并且在硬件方面也有了很大的提升，支持大量的桌面环境。.Kali Linux是一个以安全为核心理念的操作系统，你可以在任何地方运行CD和USB驱动。通过使用其预装的安全工具，你可以破解Wi-Fi 、伪造网络以及测试漏洞等等。

CAIN & ABEL

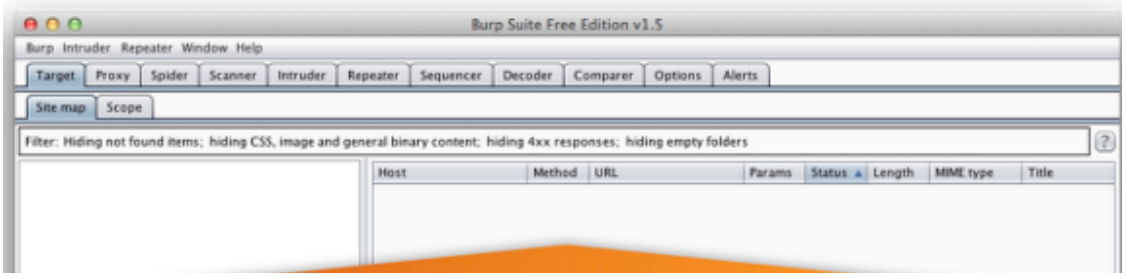
Cain & Abeld是由Oxid.it开发的一个针对Microsoft操作系统的免费口令恢复和网络嗅探测试工具。它的功能十分强大，可以网络嗅探，网络欺骗，破解加密口令、解码被打乱的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用VOIP拨打电话。





[Burp Suite Spider]

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。 Spider是其中最重要的组成部分，能够感知应用程序的网络爬虫，可以完整的枚举应用程序的内容和功能。



ETTERCAP

Ettercap是Linux下一个强大的欺骗工具，当然Windows也能用。通过它你能够用飞一般的速度创建和发送伪造的包，并发送从网络适配器到应用软件各种级别的包。绑定监听数据到一个本地端口： 从一个客户端连接到这个端口并且能够为不知道的协议解码或者把数据插进去(只有在以arp为基础模式里才能用)。这是一款非常受欢迎的工具，只要其成功运行，黑客们就可以对目标使用多种不同的攻击方式，对中间人攻击非常有帮助。

JOHN THE RIPPER

John the Ripper是一个免费开源并可以快速进行密码破解的工具，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。这款工具就像它的名字一样，更为直接且崇尚蛮力，其破解过程完全取决于用户，即只要给它时间，他总会给你一个好的结果。

METASPLOIT

Metasploit是一款开源的安全漏洞检测工具，可以帮助黑客识别安全性问题，验证漏洞的缓解措施，并对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，密码审计，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。

```
root@bt:/pentest/exploits/framework3# ./msfconsole

                  o                         8          o   o
                  8                         8              8
ooYoYo. .oPYo.   o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8    8  .oooo8 Yb..    8     8 8 8     8  8   8
8  8  8 8.        8  8    8   'Yb. 8     8 8 8     8  8   8
8  8  8 `Yooo'    8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....:::..::.....::.....:8.....:..:.....:::..::..:
::::::::::::::::::::::::::::::::::8::::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- --=[ 675 exploits - 352 auxiliary
+ -- --=[ 217 payloads - 27 encoders - 8 nops
       =[ svn r12286 updated today (2011.04.09)
```

除了以上的七款神器，另外还有七款非常值得关注： Nmap、Wireshark、Aircrack-ng、 Nessus、THC Hydra、Netcat 以及Putty。文章篇幅有限，暂不做介绍，不过都有提供下载地址哦。

***原文地址：hackread，东二门陈冠希/编译，部分内容有修改，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**