项目四

目录

[一、 实验目标 3](#_Toc116856756)

[二、 实验要求 3](#_Toc116856757)

[三、实验攻击一：DDOS攻击 3](#_Toc116856758)

[1. 实验环境介绍 3](#_Toc116856759)

[2. Kali\_1 攻击机配置 3](#_Toc116856760)

[3. Kali\_2 服务器环境配置： 4](#_Toc116856761)

[4. Windows主机环境配置 5](#_Toc116856762)

[5. 攻击机开始DDOS攻击 5](#_Toc116856763)

[6. 实验分析 7](#_Toc116856764)

[四、实验攻击二：DNS劫持 8](#_Toc116856765)

[1. 实验环境介绍 8](#_Toc116856766)

[2. Kali\_1 攻击机配置 8](#_Toc116856767)

[3. 观察正常主机是否能正常访问网页 8](#_Toc116856768)

[4. 攻击过程 8](#_Toc116856769)

[5. 攻击结果 11](#_Toc116856770)

[五、实验攻击三：网络钓鱼窃取信息 12](#_Toc116856771)

[1. 实验环境介绍 12](#_Toc116856772)

[2. 攻击过程 12](#_Toc116856773)

[六、实验攻击四：TCP会话劫持 14](#_Toc116856774)

[1. 实验环境介绍 14](#_Toc116856775)

[2. 攻击机开启ARP欺骗 14](#_Toc116856776)

[3. 靶机2开启ftp服务 15](#_Toc116856777)

[4. 攻击机开启ettercap 15](#_Toc116856778)

[5. 在靶机1上连接靶机2 17](#_Toc116856779)

[6. 攻击结果 17](#_Toc116856780)

# 实验目标

利用D501的实验环境，至少完成两种不同的攻击。

# 实验要求

1. 在报告中详细描述实验环境，如网络环境（可以是在虚拟机中构建的网络）、攻击主机和被攻击主机的配置、操作系统等。

2. 攻击工具的详细描述

3. 攻击过程的详细描述，并说明攻击效果。

# 三、实验攻击一：DDOS攻击

## 1. 实验环境介绍

VM虚拟机

Kali\_1攻击机（用来攻击服务器）

Kali\_2服务器（用来充当服务器）

Windows 10主机：（用来访问服务器）

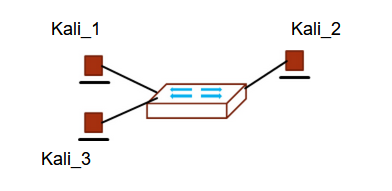


图 1 攻击一环境

## 2. Kali\_1 攻击机配置

Kali\_1，IP地址为192.168.3.85，网卡连接模式桥接模式



图表 1 攻击机的ip地址

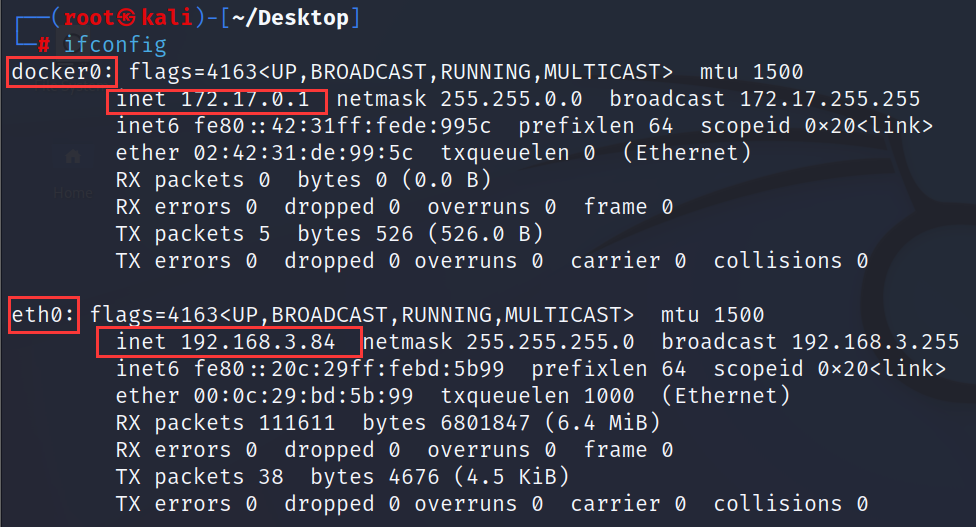
在Kali\_1上配置DDOS攻击，首先用命令git clone https://github.com/Andysun06/ddos，将工具下载到本地。然后进入该文件夹，用命令python ddos-p3.py 即可进入该工具的主界面。



图 2 DDOS工具主界面

## 3. Kali\_2 服务器环境配置：

Kali\_2，IP地址为192.168.3.84，网卡连接模式桥接模式，



在Kali\_2上配置docker环境，然后用命令docker pull sagikazarmark/dvwa将dvwa靶场搭建到本地环境。然后用命令docker run -d -p 3355:80 sagikazarmark/dvwa 将该环境搭建映射到本地的3355:80端口。

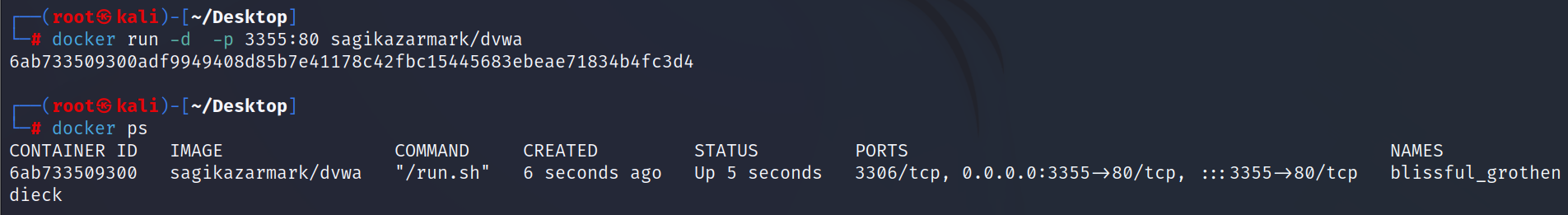


图 3 运行docker环境

## 4. Windows主机环境配置

首先用ping命令，观测是否能ping通靶场服务器（192.168.3.84）

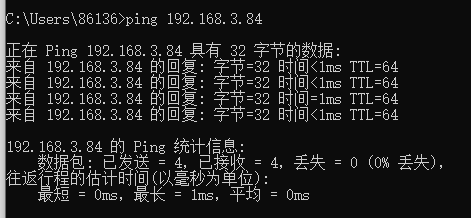


图 4 主机正常ping服务器

然后主机访问服务器搭建的dvwa靶场。访问网址为：http://192.168.3.84:3355。如下图所示，可以正常访问。

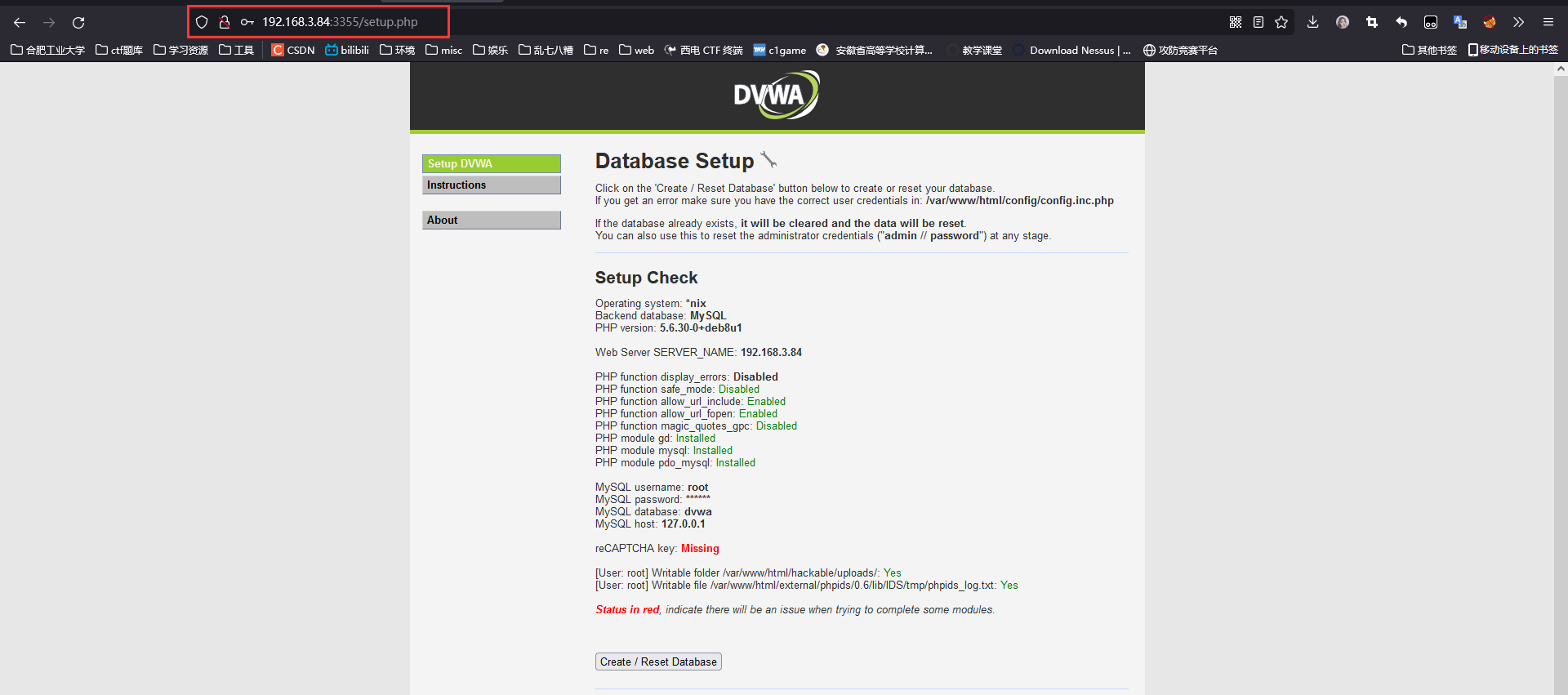
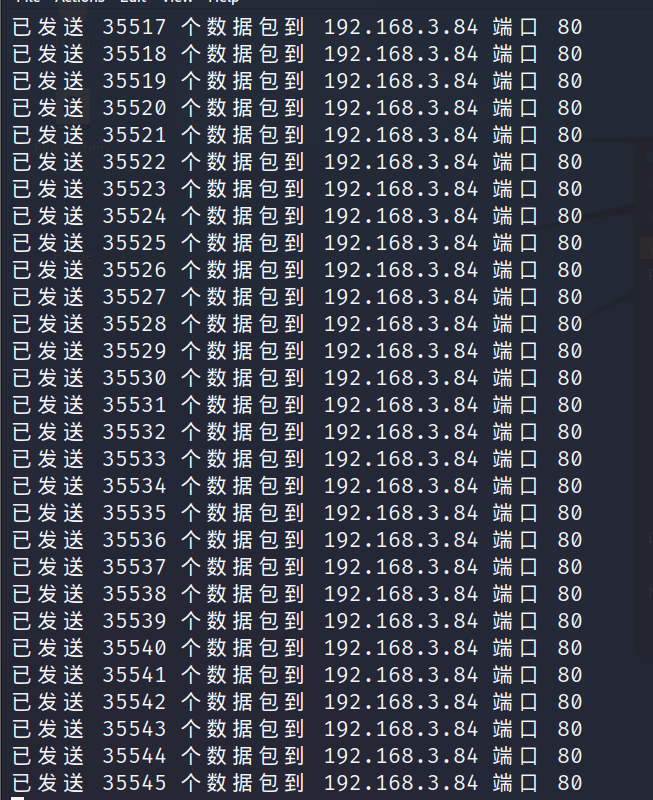


图 5 主机正常可以访问服务器

## 5. 攻击机开始DDOS攻击

攻击机Kali-hack1开始DDOS攻击，将服务器ip地址192.168.3.84输入到工具中，3355端口，攻击速率采用1000。



同时攻击机Kali-hack1用命令hping3 -S -U --flood -V --rand-source 192.168.3.84 命令则可以隐藏自己的IP地址进行IP伪装，采用多窗口并发模式。

被攻击机Kali-hack2打开Wireshark抓取ICMP流量包，可以发现大量的ip地址为被冒充机的数据包。

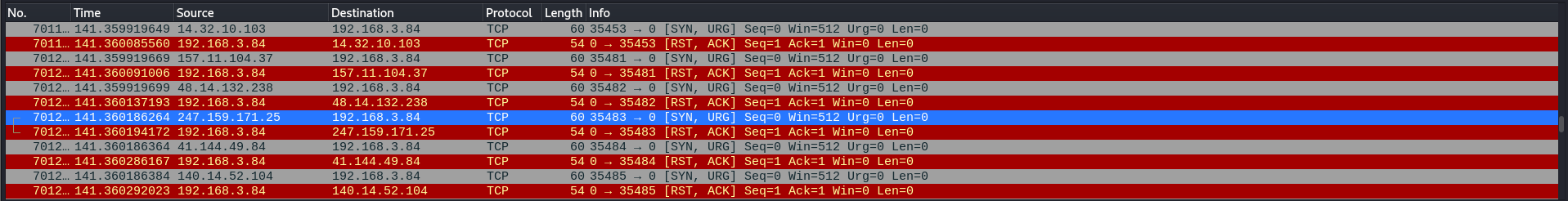


图 6被攻击机抓取的数据包

此时，在Windows10主机正常访问服务器的靶场dvwa，会发现无法返回正常的页面，服务器的资源得到了消耗。

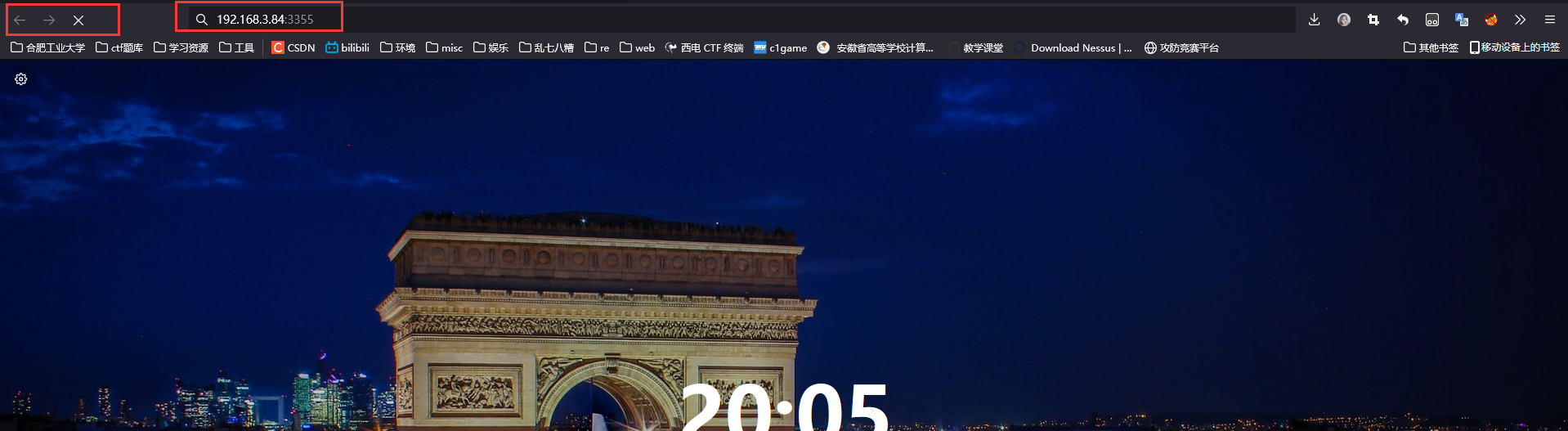


图 7 正常主机访问不到服务器的dvwa资源

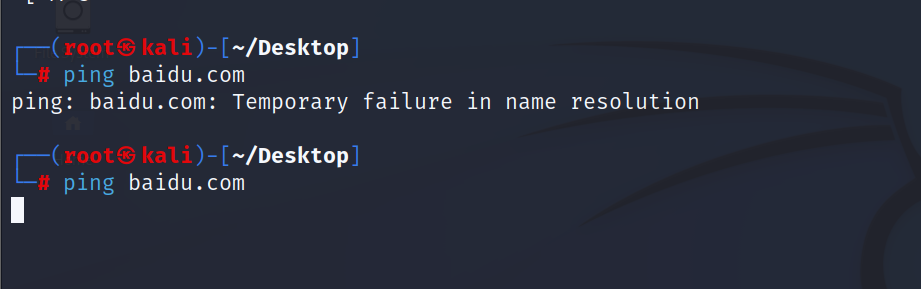


图 8 服务器被DDOS攻击后不能正常访问百度

## 6. 实验分析

1、ICMP DOS采用的是一种反弹式攻击，利用了ICMP的请求响应报文进行攻击，并能够很好的隐藏攻击者的行踪。

2、首先，攻击者选择一个有足够多主机的网络，并向这个网络的网关发送一个源地址是目标系统的ICMP请求响应广播报文。

3、其次，被选定的网关在收到广播报文后向其管辖范围内的所有主机系统发送该请求响应报文。

4、最后，所有接收到请求响应报文

# 四、实验攻击二：DNS劫持

## 1. 实验环境介绍

VM虚拟机

Kali\_1攻击机 192.168.3.85

Kali\_2正常主机 192.168.3.84

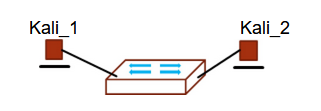


图 9攻击二环境

## 2. Kali\_1 攻击机配置

攻击机用命令systemctl start apache2开启apache服务。

攻击机设置DNS劫持的映射表：

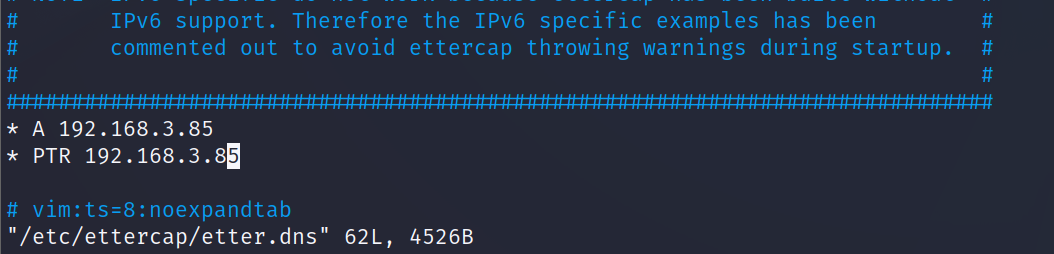


图 10 攻击机设置DNS劫持的隐射表

## 3. 观察正常主机是否能正常访问网页

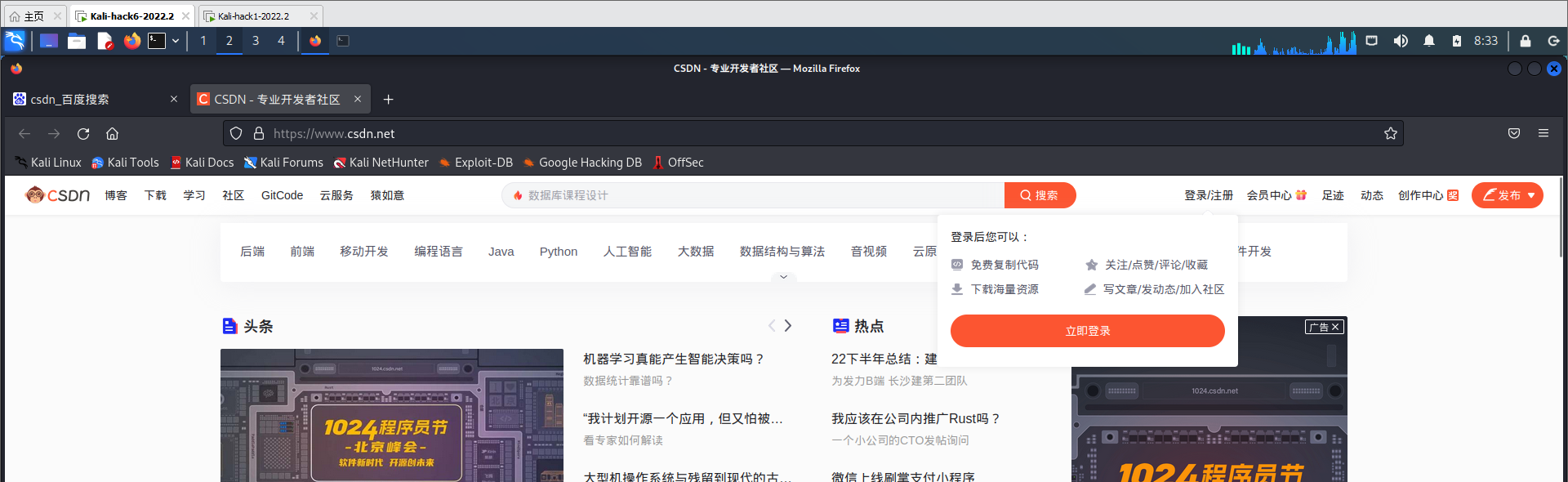


图 11正常主机能正常访问网页

## 4. 攻击过程

攻击机使用命令ettercap -G 开启ettercap软件。



图 12 ettercap主界面

然后寻找局域网内的主机：

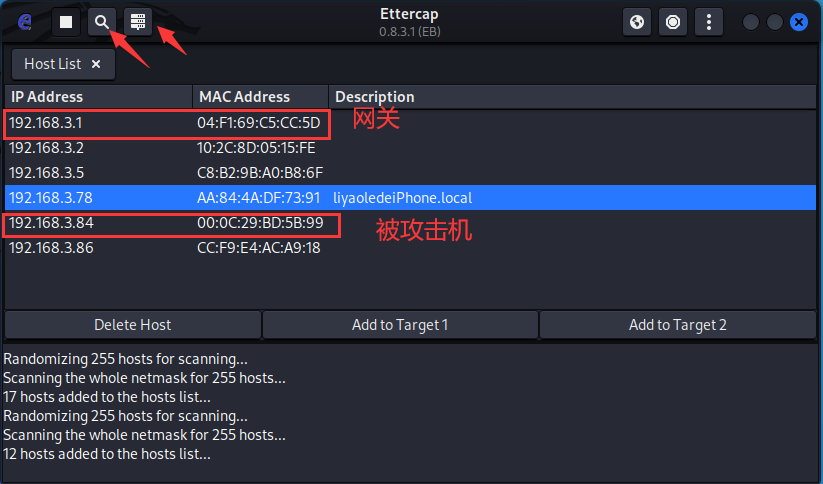


图 13 Ettercap扫描的结果

右键对应的ip地址，将网关添加到Target1,将被攻击机添加到Target2。然后点击右上角，开始ARP毒化。

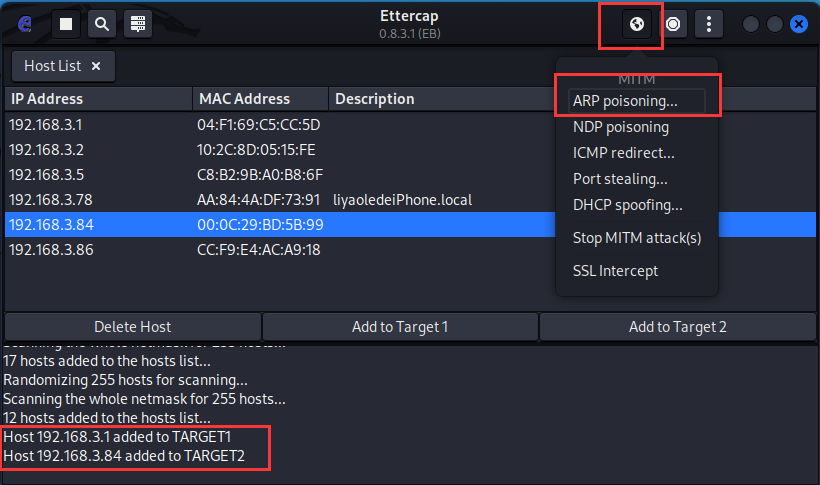


图 14 开始ARP毒化

开启dns\_spoof功能：右上角选择插件Plugins中的Magage plugins。

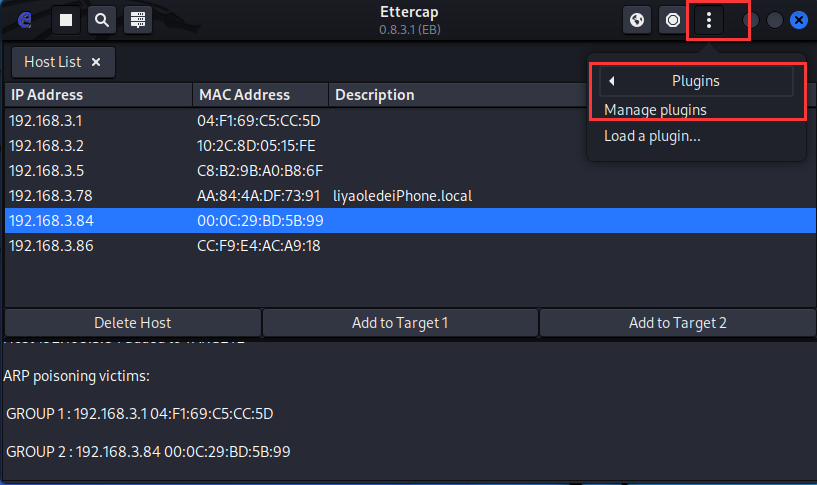


图 15 开启dns\_spoof功能（1）

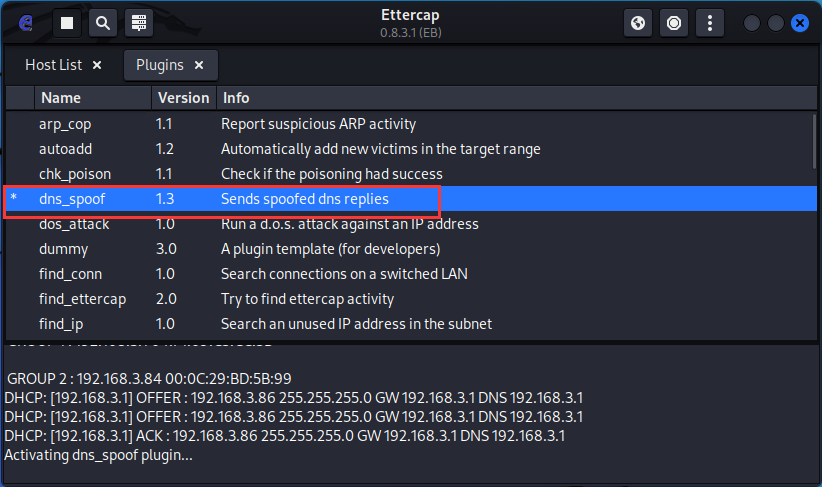


图 16 开启dns\_spoof功能（2）

## 5. 攻击结果

被攻击机ping百度，返回的ip地址却是攻击机的ip地址。

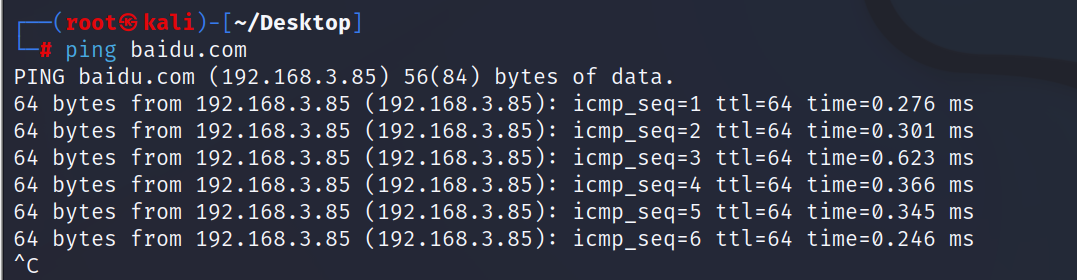


图 17 攻击结果（1）

被攻击机访问icloud.com返回的却是攻击机2的appache服务界面。至此，攻击成功。

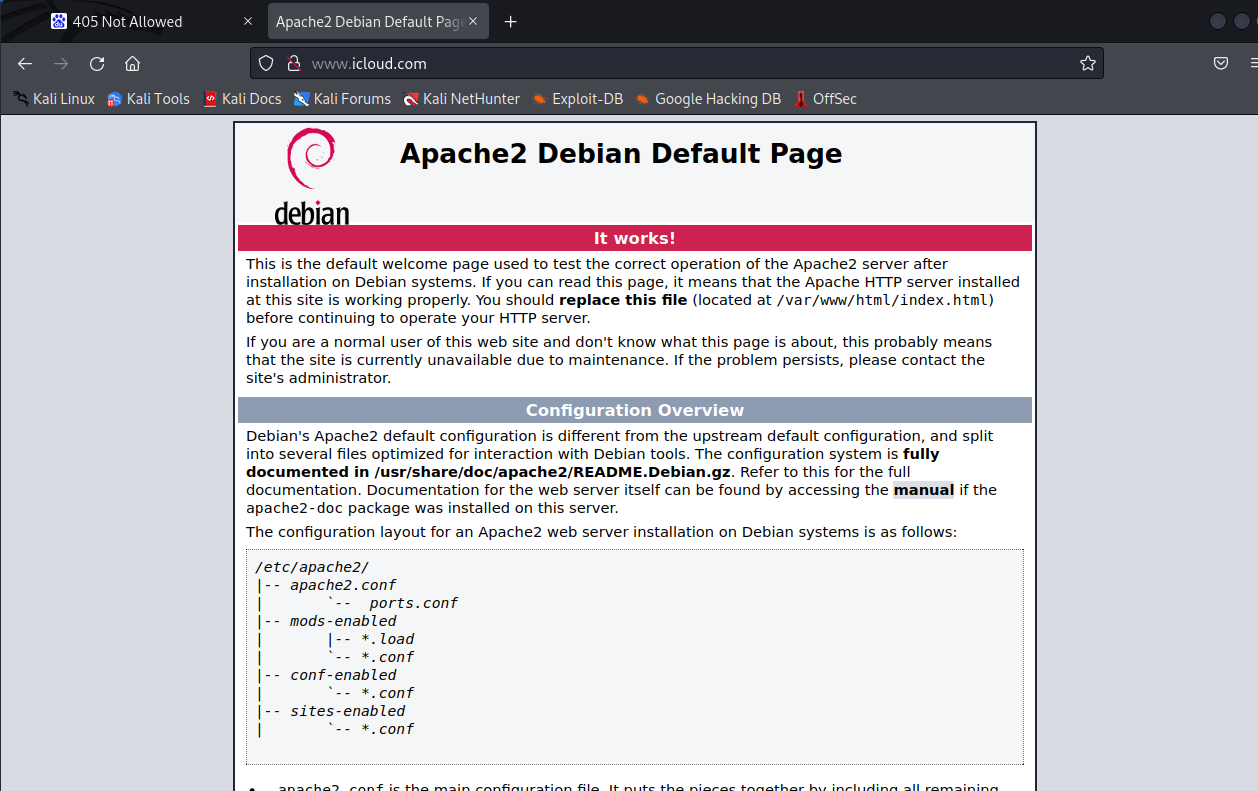


图 18 攻击结果（2）

# 五、实验攻击三：网络钓鱼窃取信息

## 1. 实验环境介绍

VM虚拟机

Kali\_1攻击机 192.168.3.85

Kali\_2正常主机 192.168.3.84

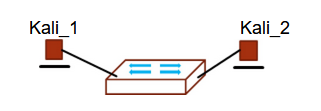
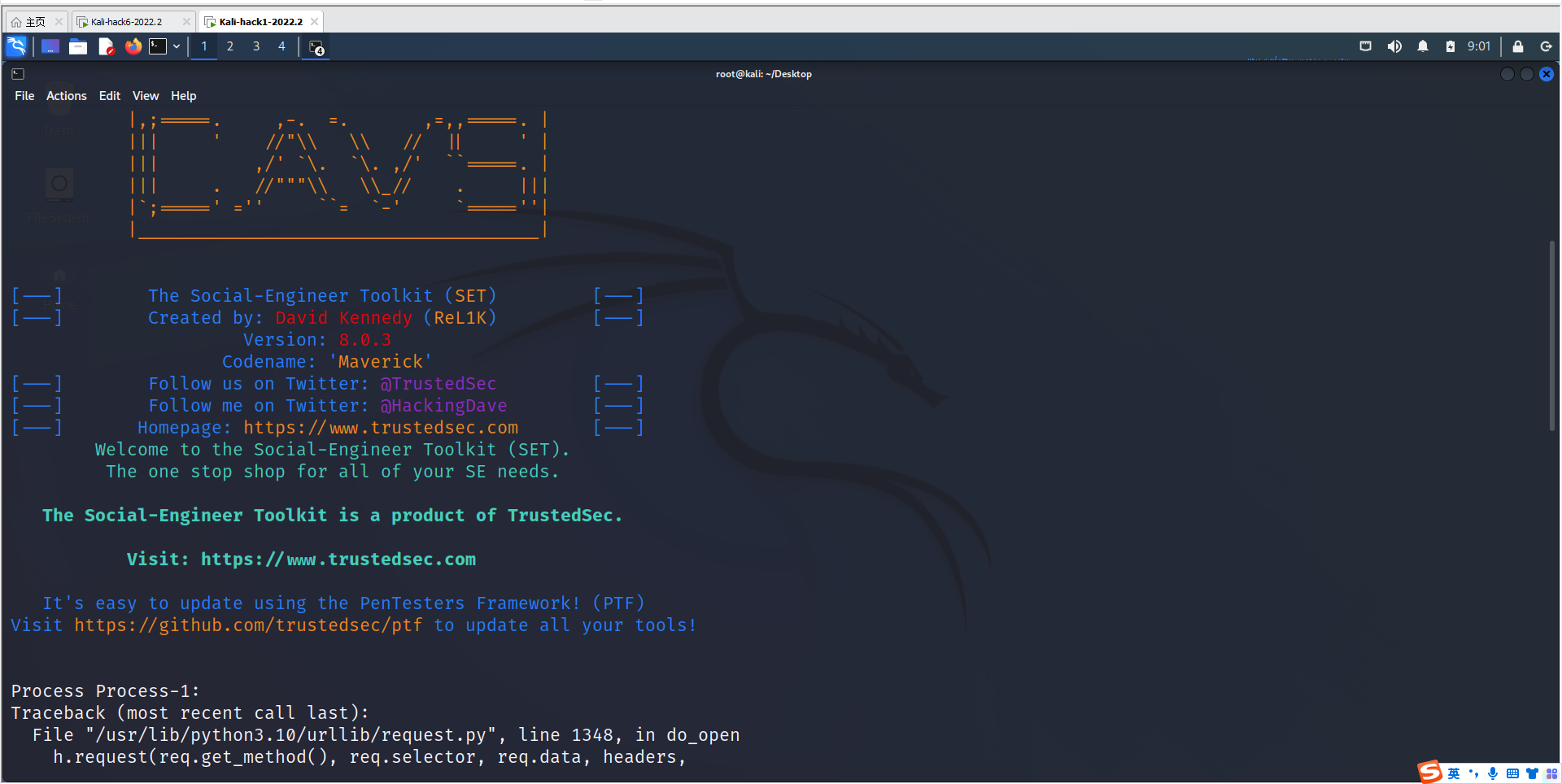


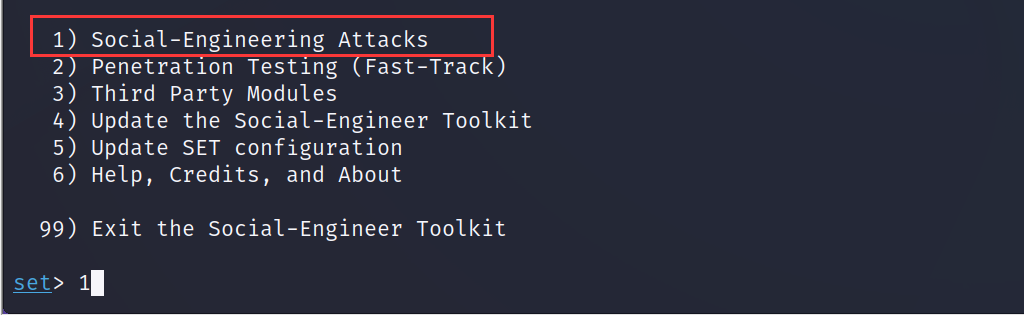
图 19攻击三环境

## 2. 攻击过程

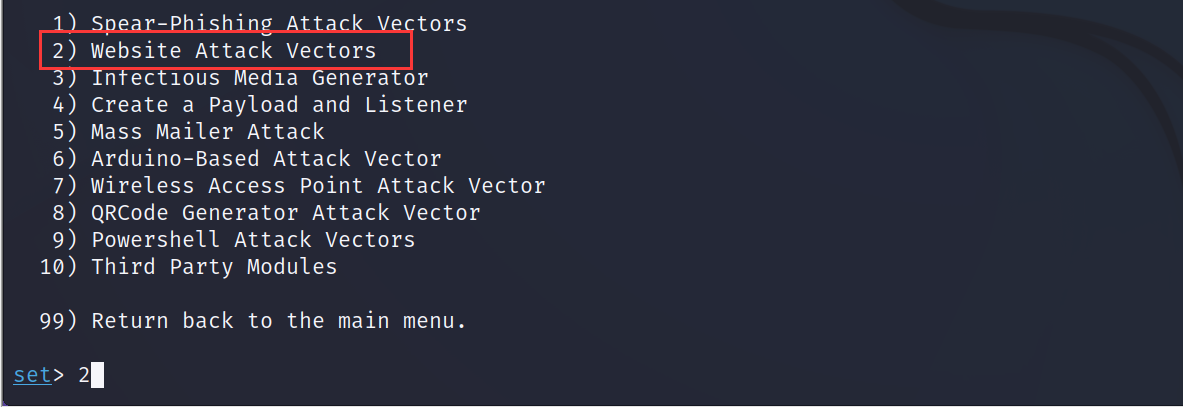
打开终端，输入命令setoolkit，显示工具菜单



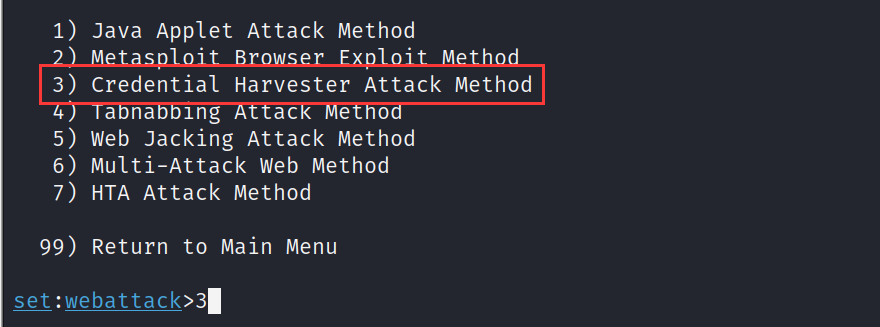
输入1，选择菜单中的Social-Engineering Attacks(社会工程学攻击) 会显示社会工程攻击的工具



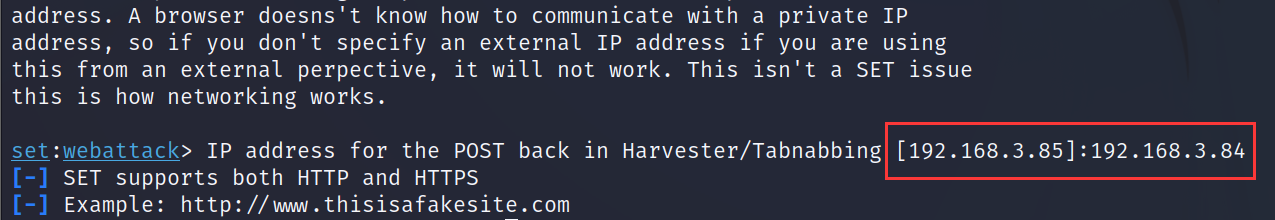
输入2，选择Website Attack Vectors网站(钓鱼）攻击向导 会列出所有的网站（钓鱼）攻击的方法供我们选择。



输入3，选择Credential Harvester Attack Method(密码收割机) 功能如其名一样



输入2，选择Site Cloner，这时会提示IP address for the POST back in Harvester/Tabnabbing[192.168.3.85(攻击机ip地址)]:192.168.3.84(输入的被攻击机的ip地址)。



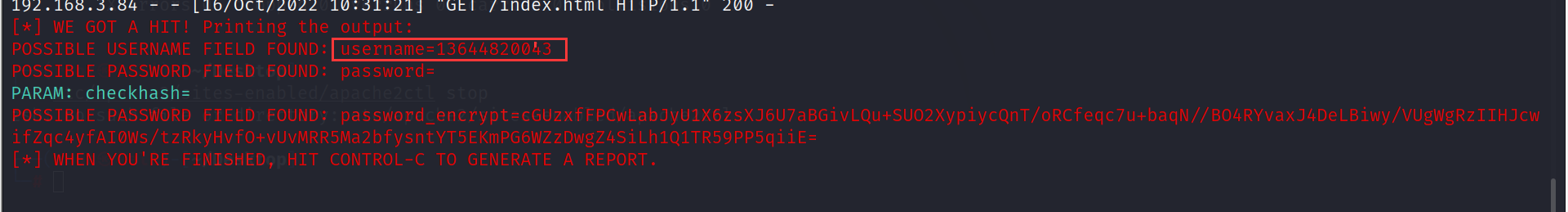
然后输入需要克隆页面的域名http://pigai.org/ (批改网为例）



在正常主机上访问攻击机的ip地址，如下图所示：



此时被攻击者如果输入正常的账号密码，就会被攻击者收集到。如下图所示：



这种方法搭配钓鱼邮箱可以起到很好的作用。

# 六、实验攻击四：TCP会话劫持

## 1. 实验环境介绍

VM虚拟机

Kali\_1靶机1（ip地址为192.168.3.84）

Kali\_2攻击机（ip地址为192.168.3.85）

Kali\_3靶机2（ip地址为192.168.3.88）

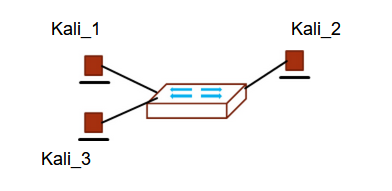


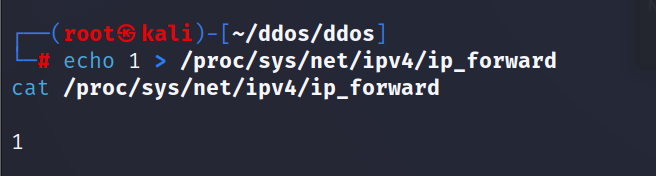
图 20 攻击一环境

## 2. 攻击机开启ARP欺骗

Kali通过ARP欺骗成为中间人，从而通过截获TCP数据包，对Kali\_1靶机1和Kali\_3靶机2之间的TCP会话进行劫持，首先在kali中设置ip路由转发。命令为：

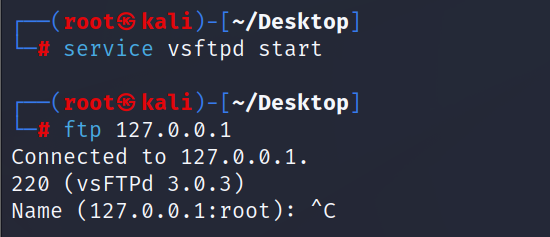
echo 1 > /proc/sys/net/ipv4/ip\_forward

cat /proc/sys/net/ipv4/ip\_forward



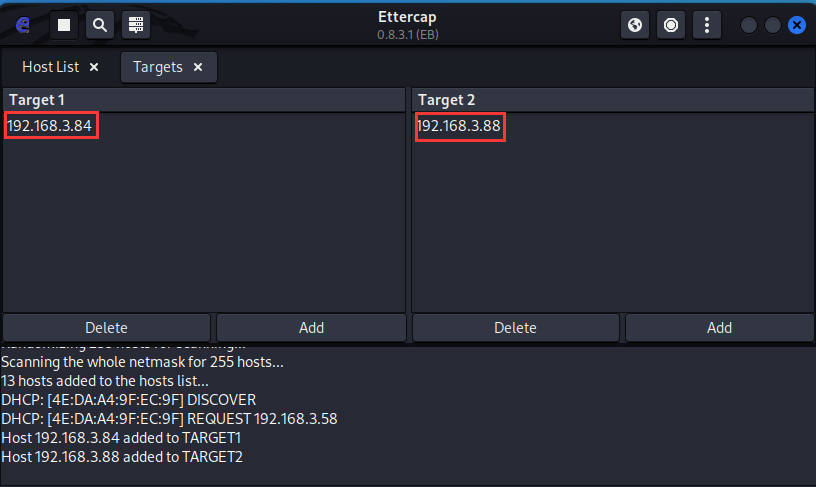
## 3. 靶机2开启ftp服务

首先用命令service vsftpd start开启ftp服务。

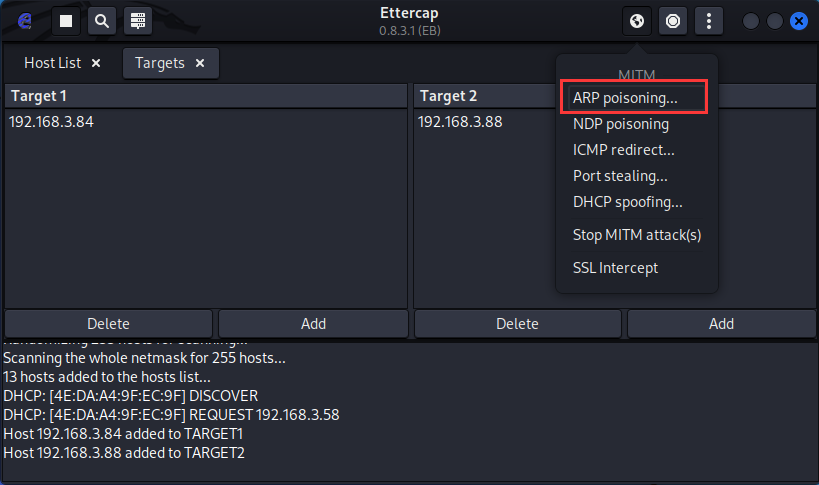


## 4. 攻击机开启ettercap

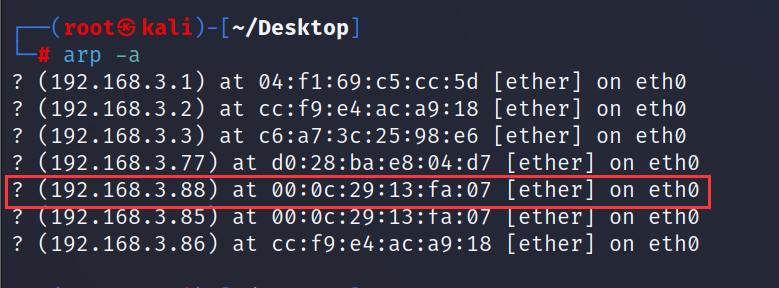
攻击机用命令ettercap -G开启ettercap软件，并将靶机1和靶机2的ip地址分别对应于Target1和Target2.

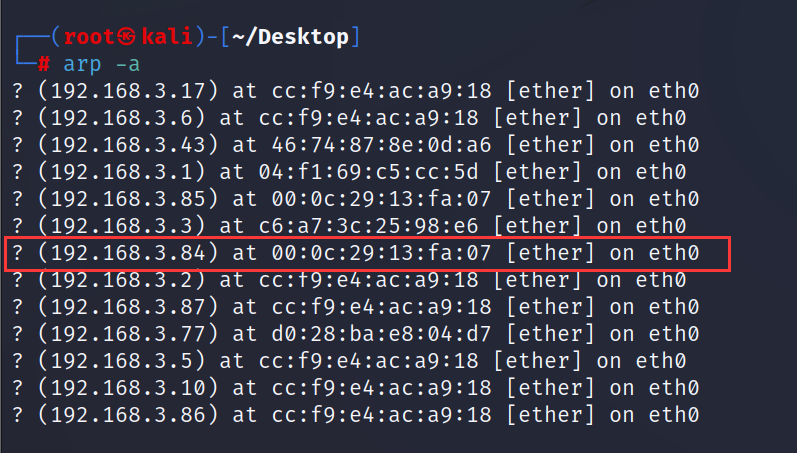


然后开启选择菜单“MITM”中的“ARPpoisoning”进行[ARP](https://so.csdn.net/so/search?q=ARP&spm=1001.2101.3001.7020" \t "_blank)欺骗，选嗅探远程连接。



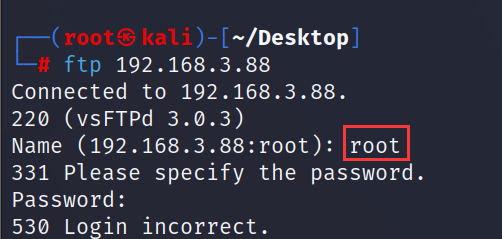
在靶机1和靶机2上使用命令arp -a查看是否被欺骗。攻击机的mac地址为00:0c:29:13:fa:07。





## 5. 在靶机1上连接靶机2

在靶机1上使用命令ftp 192.168.3.88连接远程服务器，用户名密码都是root，



## 6. 攻击结果

在攻击机的软件中右上角菜单栏中的View下的Connections找到对应的连接信息和传输的用户名密码。

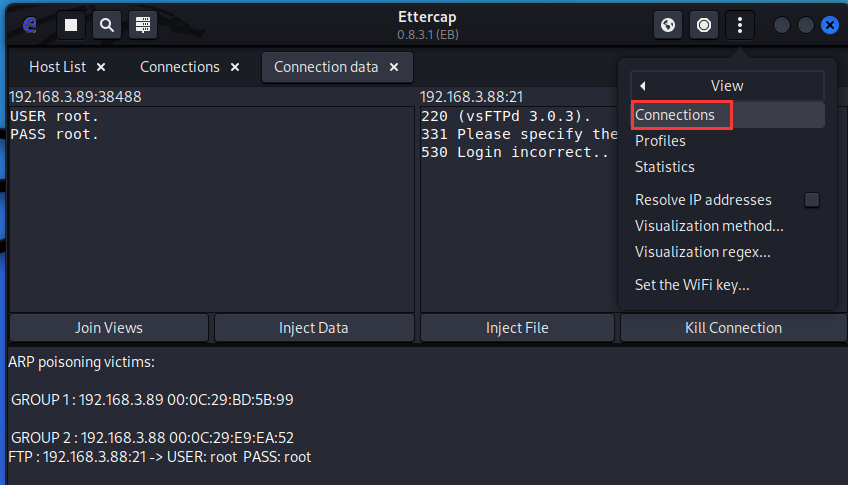


图 21 连接信息

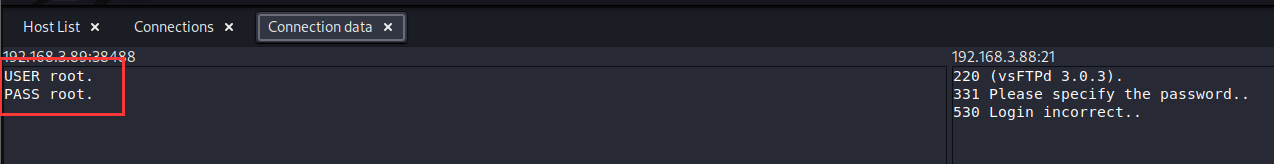


图 22 捕获的用户名和密码