**课程名称** 计算机信息安全

**实验项目名称** 实验8 使用MITMF进行键盘记录以及密码嗅探

* **一、实验任务**
  1. 在Kali环境下安装MITMF。
  2. 使用MITMF结合中间人攻击进行密码嗅探和键盘记录
* **二、实验环境**
  1. Kali
* **三、实验参考**

https://github.com/byt3bl33d3r/MITMf

https://github.com/byt3bl33d3r/MITMf/wiki/Installation

#Installation MITMf relies on a LOT of external libraries therefore it is highly recommended you use virtualenvs to install the framework, this avoids permission issues and conflicts with your system site packages (especially on Kali Linux).

Before starting the installation process:

On Arch Linux:

pacman -S python2-setuptools libnetfilter\_queue libpcap libjpeg-turbo capstone

On Debian and derivatives (e.g Ubuntu, Kali Linux etc...)

apt-get install python-dev python-setuptools libpcap0.8-dev libnetfilter-queue-dev libssl-dev libjpeg-dev libxml2-dev libxslt1-dev libcapstone3 libcapstone-dev libffi-dev file

#Installing MITMf Note: if you're rocking Arch Linux: you're awesome! Just remember to use pip2 instead of pip outside of the virtualenv

Install virtualenvwrapper:

pip install virtualenvwrapper

Edit your .bashrc or .zshrc file to source the virtualenvwrapper.sh script:

source /usr/bin/virtualenvwrapper.sh

The location of this script may vary depending on your Linux distro

Restart your terminal or run:

source /usr/bin/virtualenvwrapper.sh

Create your virtualenv:

mkvirtualenv MITMf -p /usr/bin/python2.7

Clone the MITMf repository:

git clone https://github.com/byt3bl33d3r/MITMf

cd into the directory, initialize and clone the repos submodules:

cd MITMf && git submodule init && git submodule update --recursive

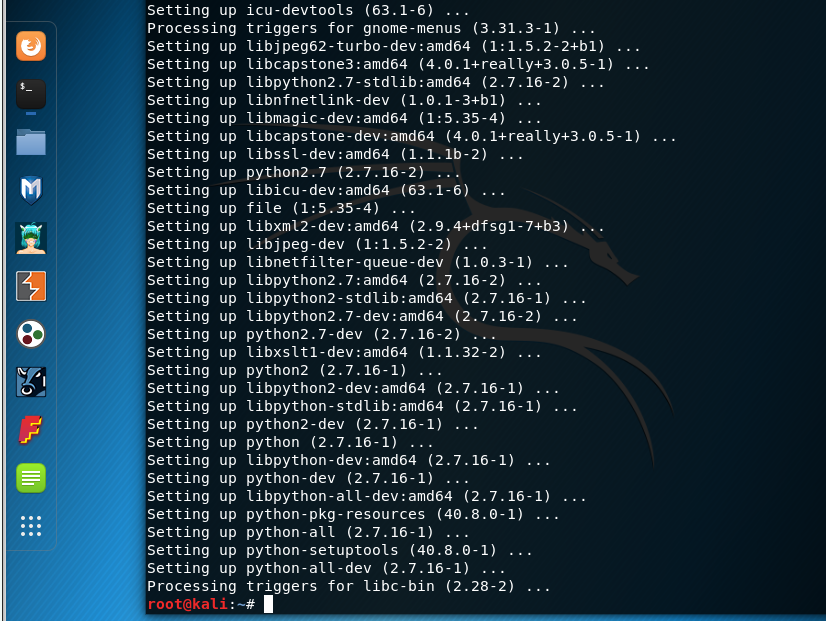
Install the dependencies:

pip install -r requirements.txt

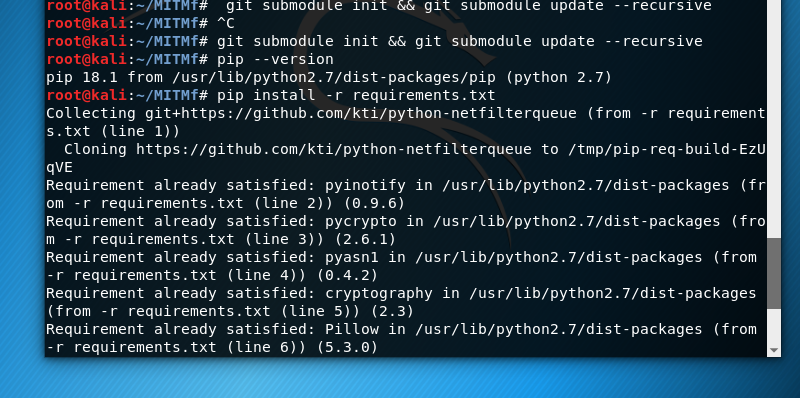
You're ready to rock!

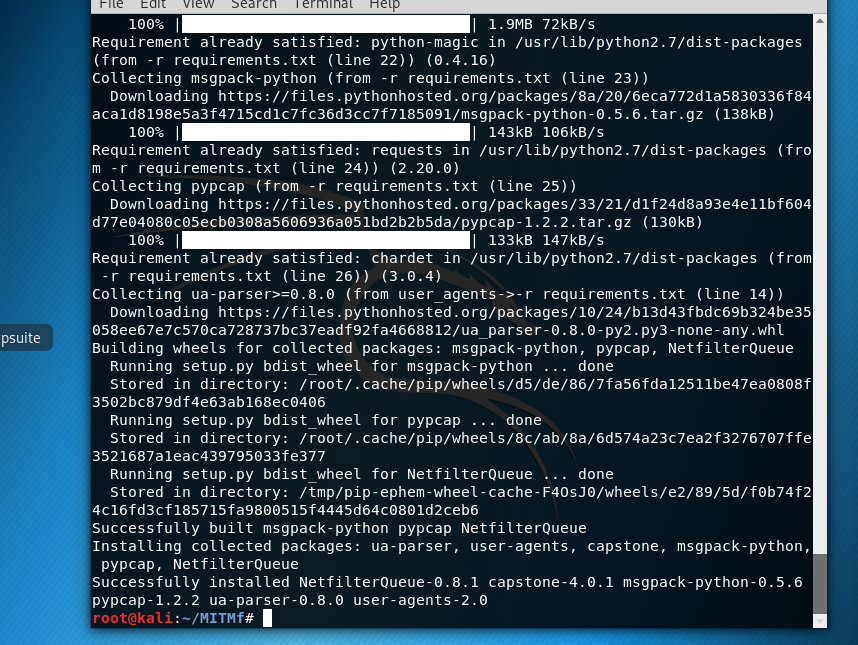
python mitmf.py --help四、写下详细实验的步骤和实验心得

安装界面：

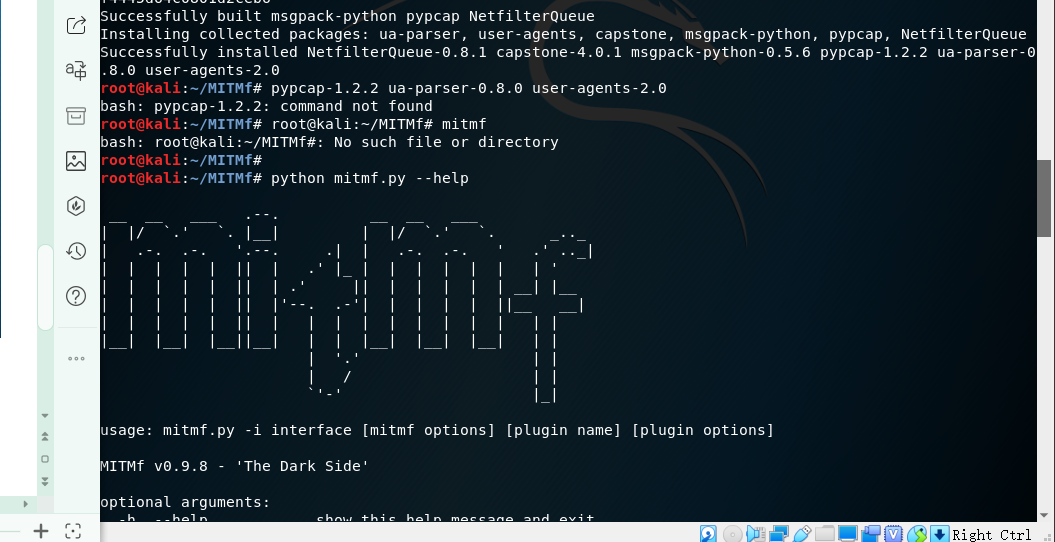


安装pip的需要文件：



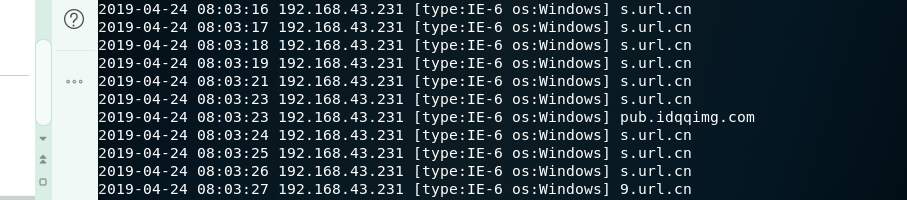


安装完毕：

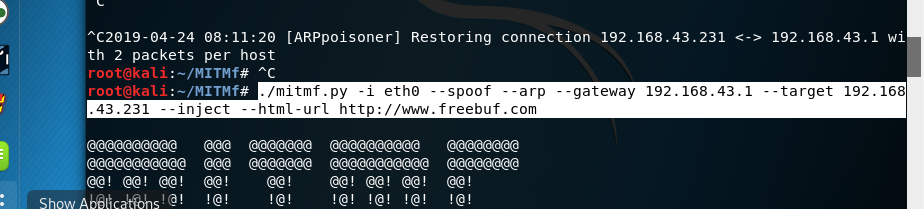


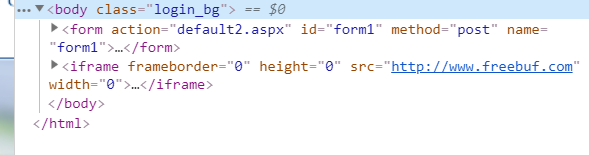
开始狂欢：

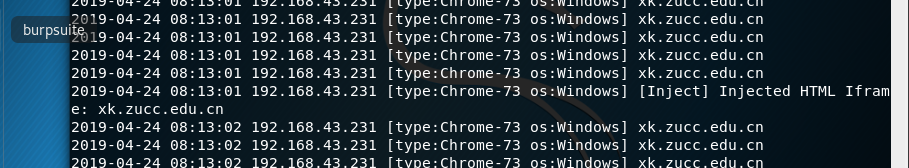
注入一个html 实验：



选课网注入成功

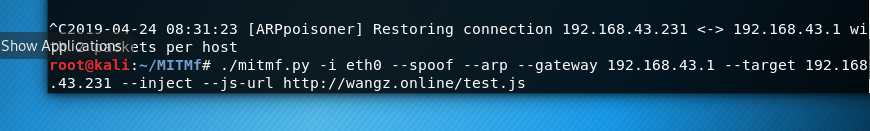


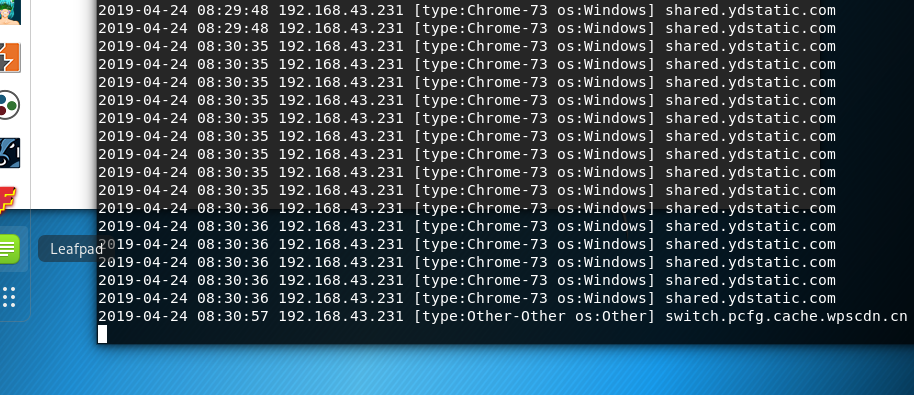


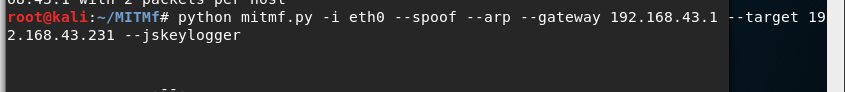


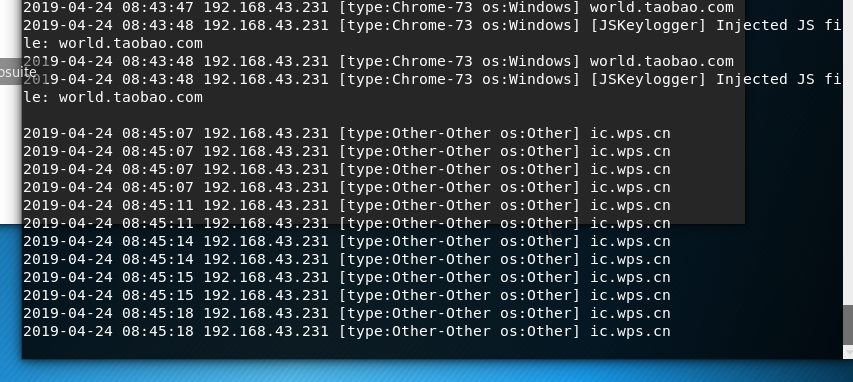
注入 js 实验：

没有成功



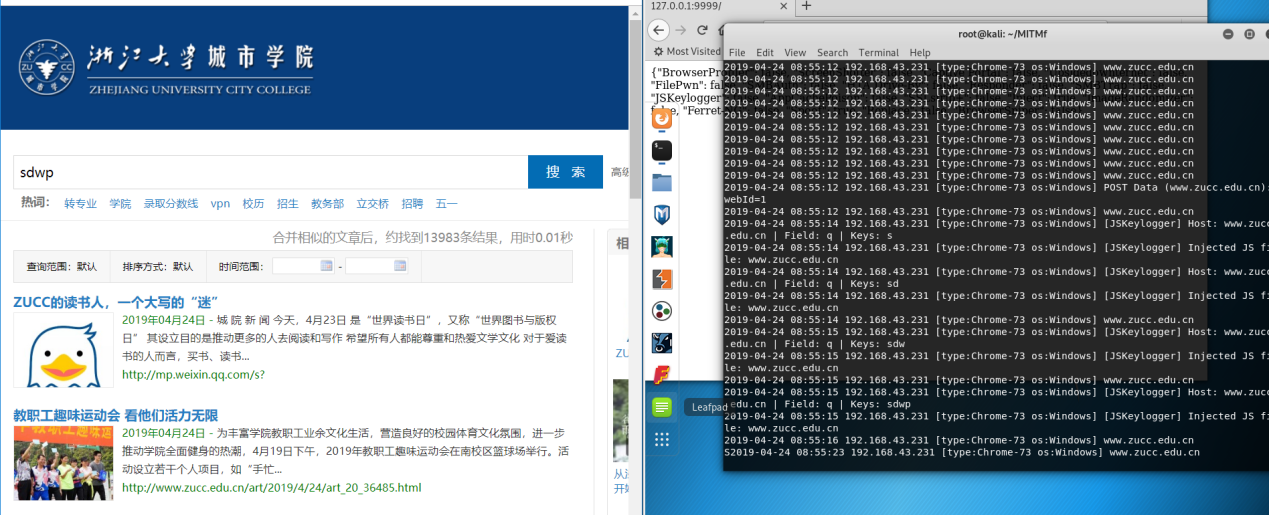






但是最后没有成功..

后来换了学校的可以成功了..



再次使用无辜的学校网址...

