网络侦查

一【实验目标】

- 了解网络侦察的基本原理
- 掌握获取网络信息的技术。

二【实验环境】

- Windows 10 操作系统
- Ubuntu 系统

三【实验原理】

网络侦察是使用技术手段，突破侦查对象计算机信息网络安全防护机制，深入其内部网络和专用网络，并进入信息系统，从中获取情报的信息和情报。主要特点是侦查方便、快捷，所获情报内容丰富，获取的信息和情报可用于后续的网络安全的渗透测试和安全加固。

Fping 是一款应用软件，适用于 linux 平台。fping 是一个向网络主机发送 ICMP echo 探测器的程序，类似于 ping，但在 ping 多个主机时性能要好得多。Fping 可以批量扫描主机,并将主机列表写在文件中。

HTTrack 是一个自由、开源的网络爬虫以及离线浏览器。用户可以通过 HTTrack 把互联网上的网站页面下载到本地计算机上。在默认设置下，HTTrack 对网站页面的下载结果是按照原始站点相对链接的结构来组织的。用网页浏览器打开这个被下载下来的网站的页面，就可以离线浏览并获得相应信息了

四【实验步骤】

实验具体操作步骤如下：

1. 进入 Ubuntu 系统，如图 1 所示。

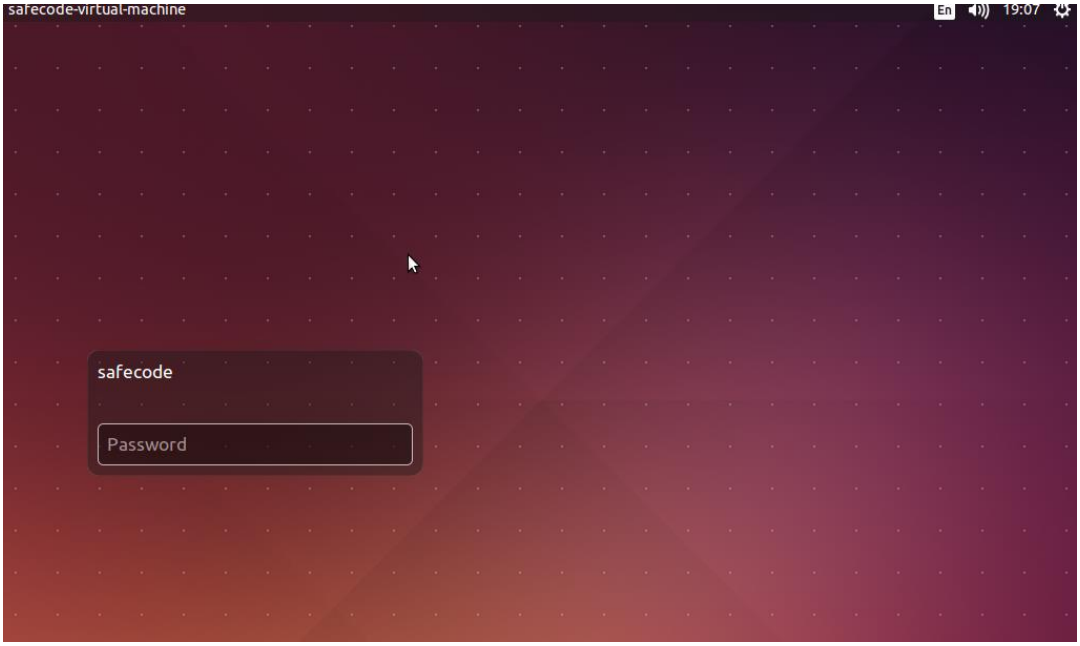

图 1

2. 输入密码【123456】。如图 2 所示

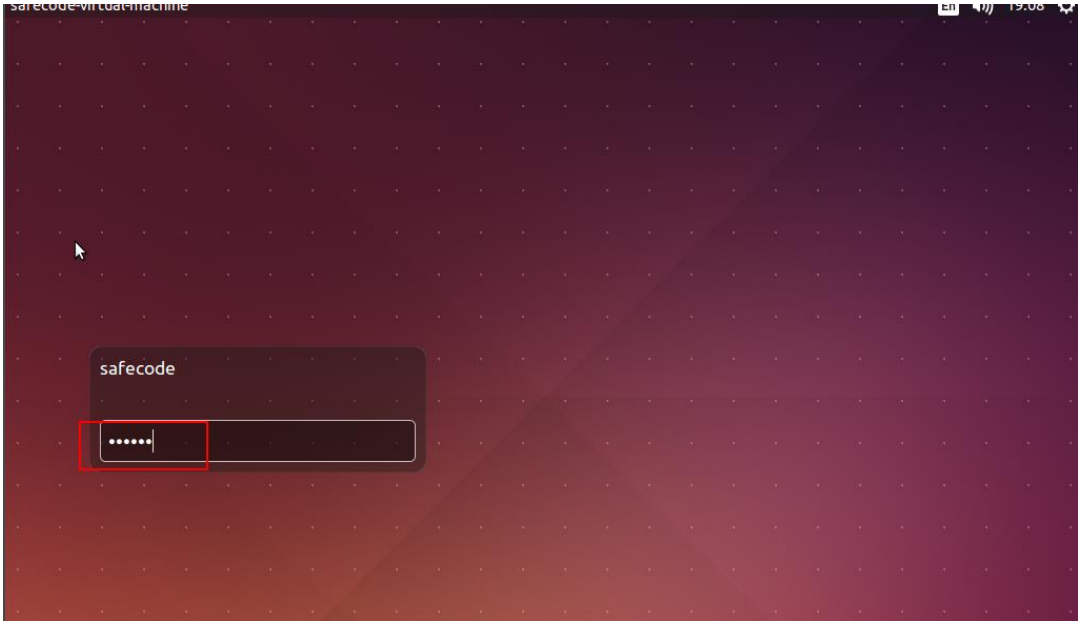

图 2

3. 登录成功后点击左侧导航栏搜索图标，输入【xterm】,开启终端，如图 3 所示。

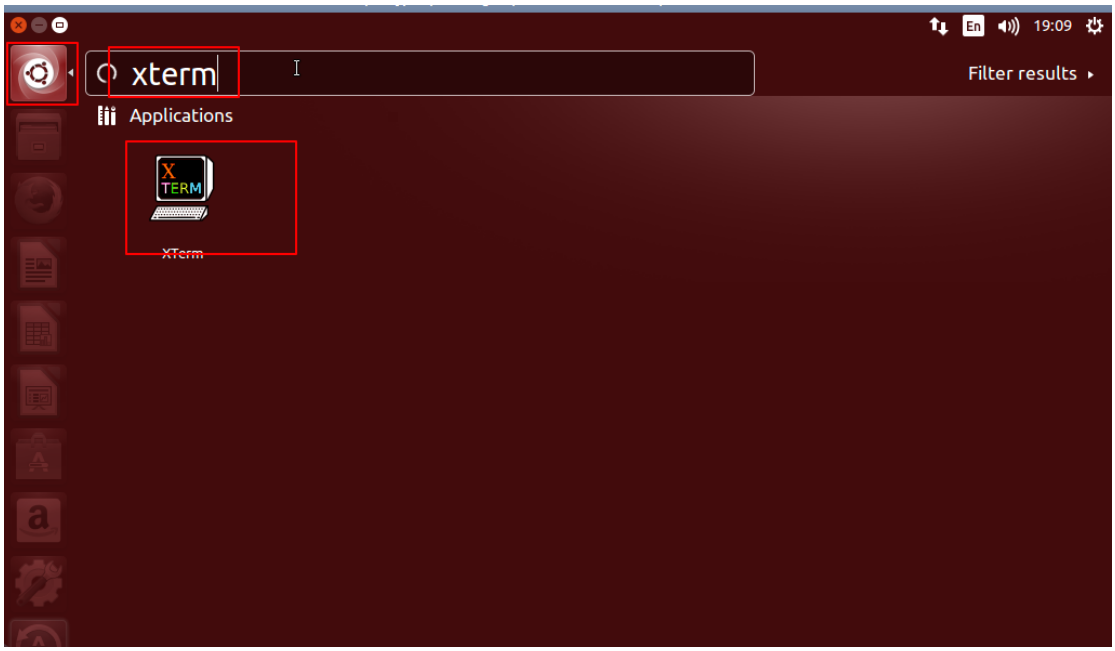

图 3

4. 在终端中输入“ifconfig”。 ifconfig 是 linux 中用于显示或配置网络设备（网络接口卡）的命令，通过此命令查看本机的 IP 地址。本机 IP 为“192.168.49.233”，以实际为准。如图 4 所示

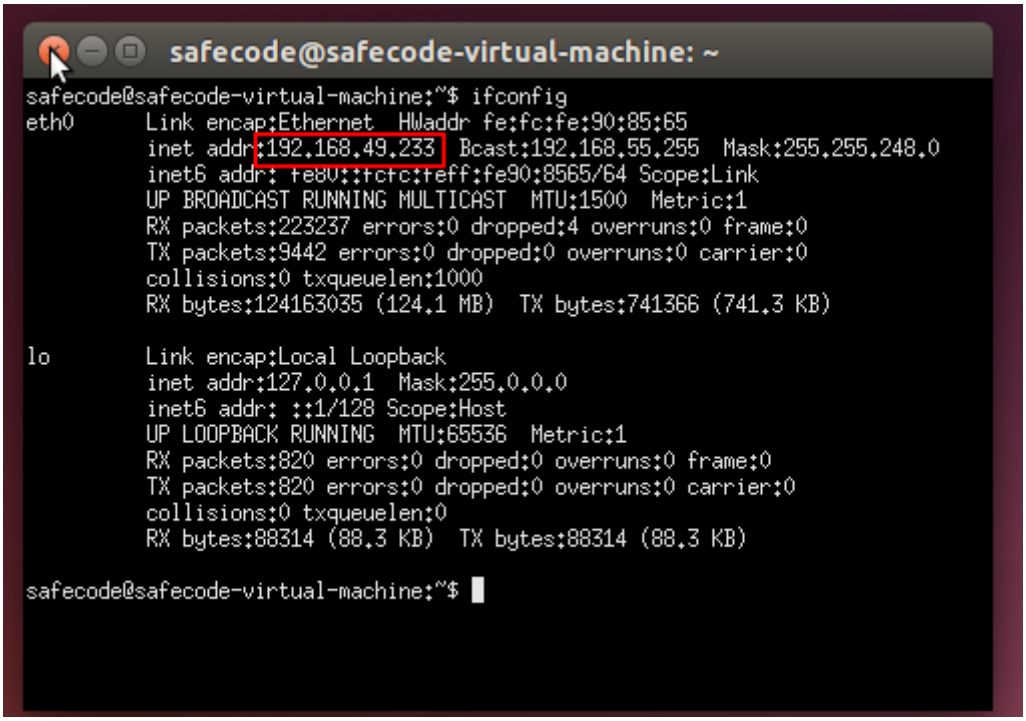

图 4

5. 通过使用 fping 可以扫描 IP 段（如果内网不通请关闭防火墙），-a 选项显示

的是目标 IP 段中的存活主机，-g 选项可以生成目标列表。输入命令【fping -a -g 192.168.49.230 192.168.49.255】，此处可以看到在整个 IP 段中的存活主机。如图 5 所示

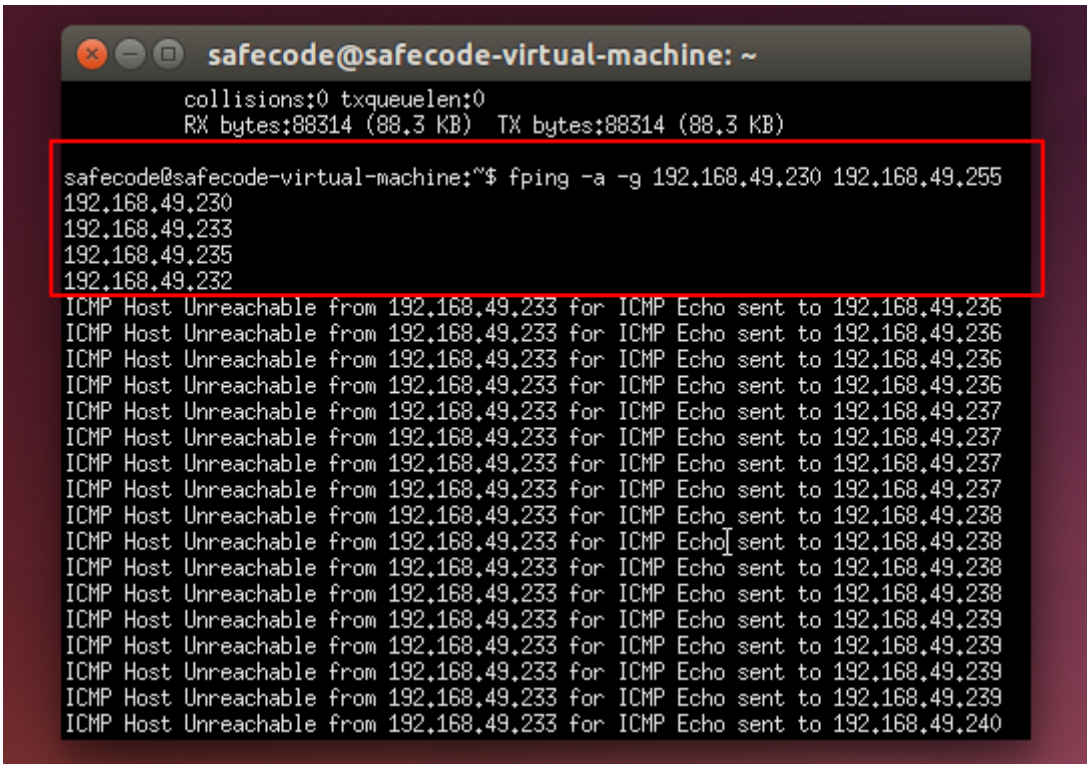

图 5

6. 进入 win10 系统，输入密码“Admin123456”，如图 6 所示。

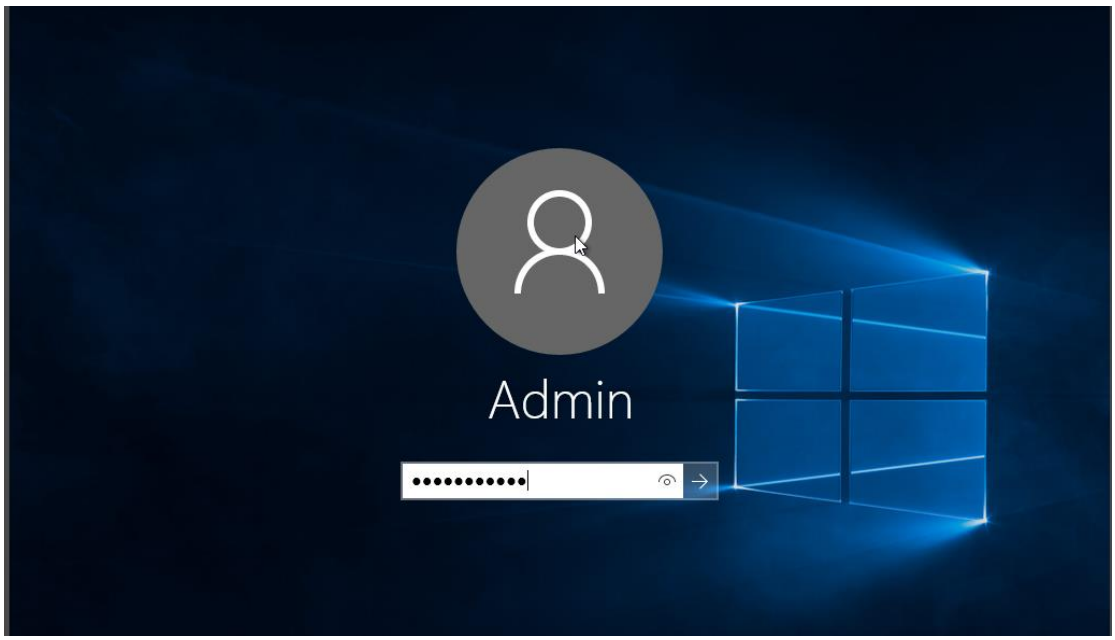

图 6

7. 点击桌面 PHPStudy，点击启动，开启目标网站，如图 7 所示。

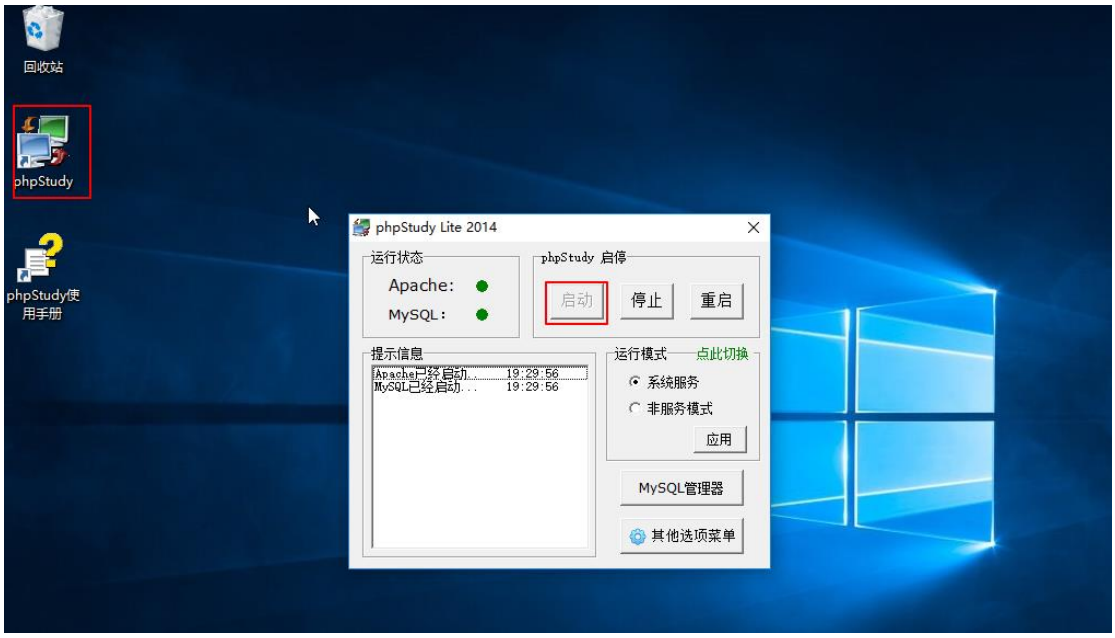

图 7

8. 进入命令提示符输入“ipconfig”，查看本机 IP 地址， 如图 8 所示。

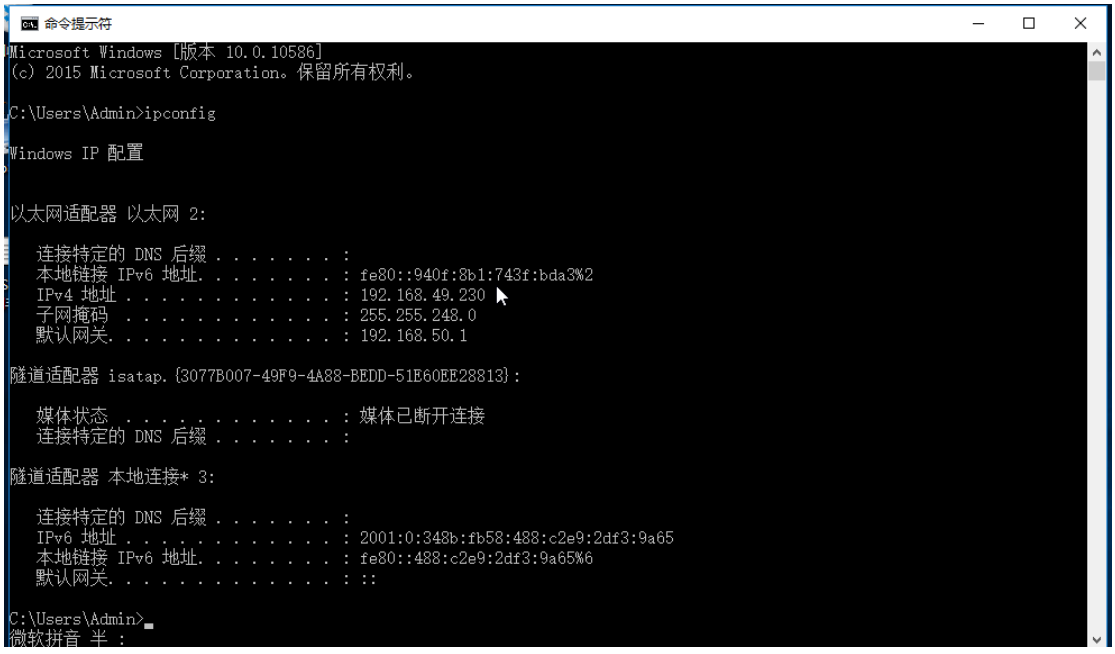

图 8

9. 使用 nmap 对存活主机 IP 192.168.49.230 进行扫描，查看目标主机开放端口，做信息收集分析。通过分析目标主机开放的端口可以发现它开放了 80 端口，意味着目标主机提供 HTTP 服务。如图 9 所示

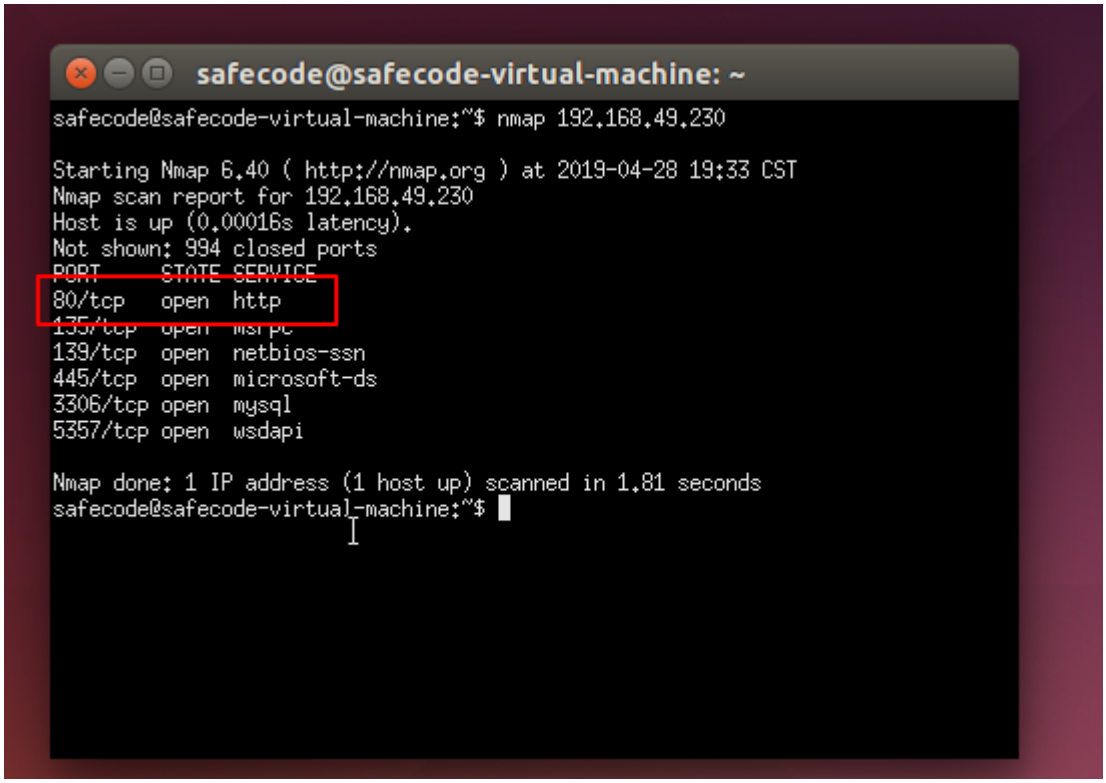

图 9

10. 通过访问目标 IP 查看目标网站。在桌面中点击左侧导航中的浏览器。如图 10 所示。

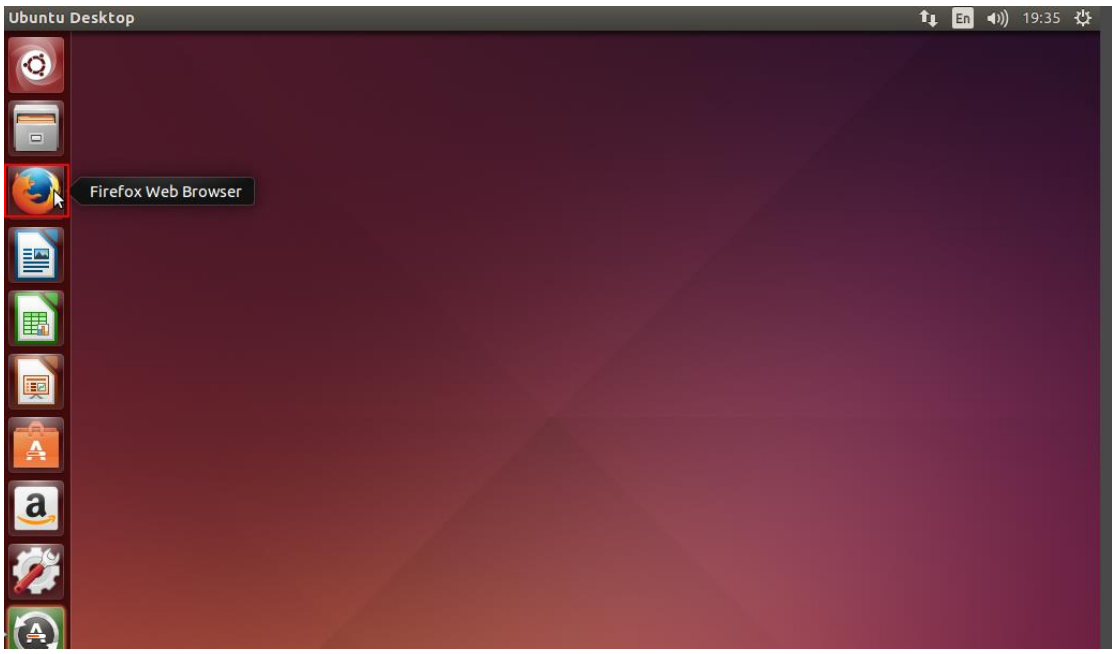

图 10

11. 在地址栏填入目标 IP 地址“192.168.49.230/dede”，点击【->】，访问目标

网站。如图 11 所示。

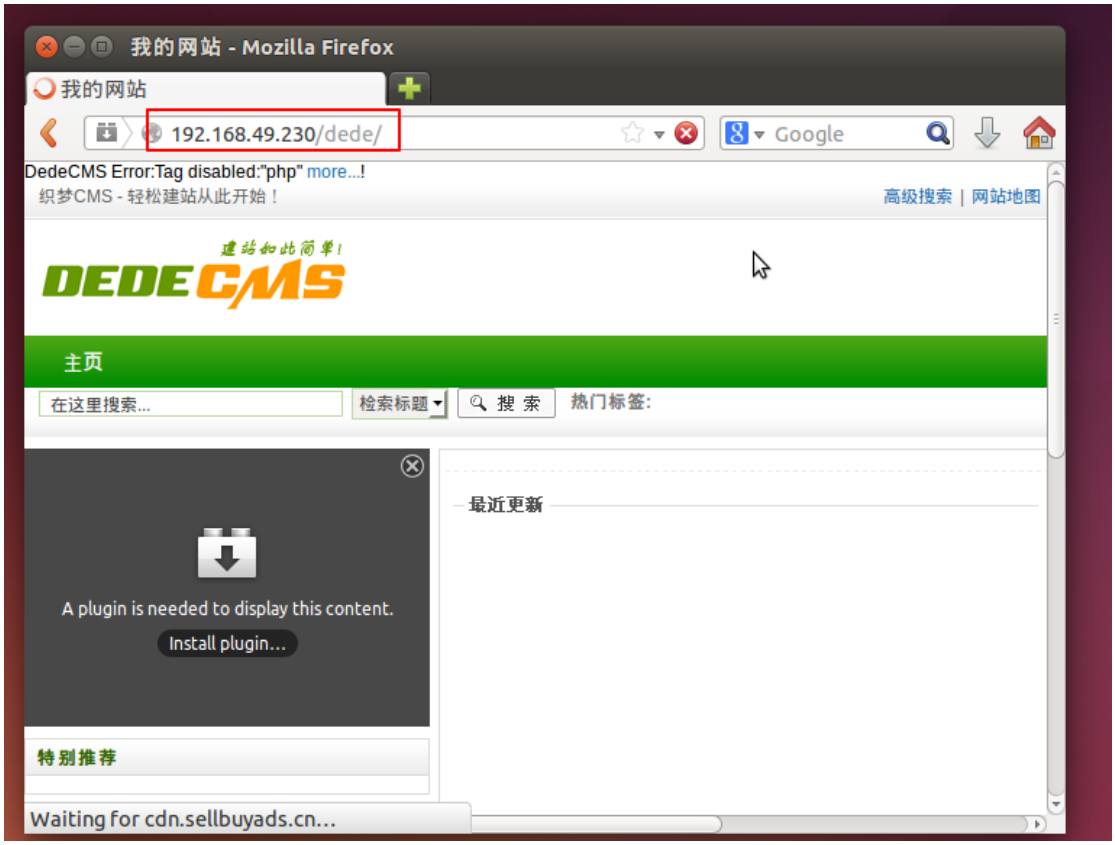

图 11

12. 可以发现目标网站可以访问，为了获取足够的信息，并且减少与目标主机的交互，可以将目标网站全部复制下来。HTTrack 是一个网站镜像工具，可以用来复制网站并存储下来。打开【终端】，并在终端中输入“httrack”命令，点击回车可以看到 httrack 的信息。如图 12 所示。

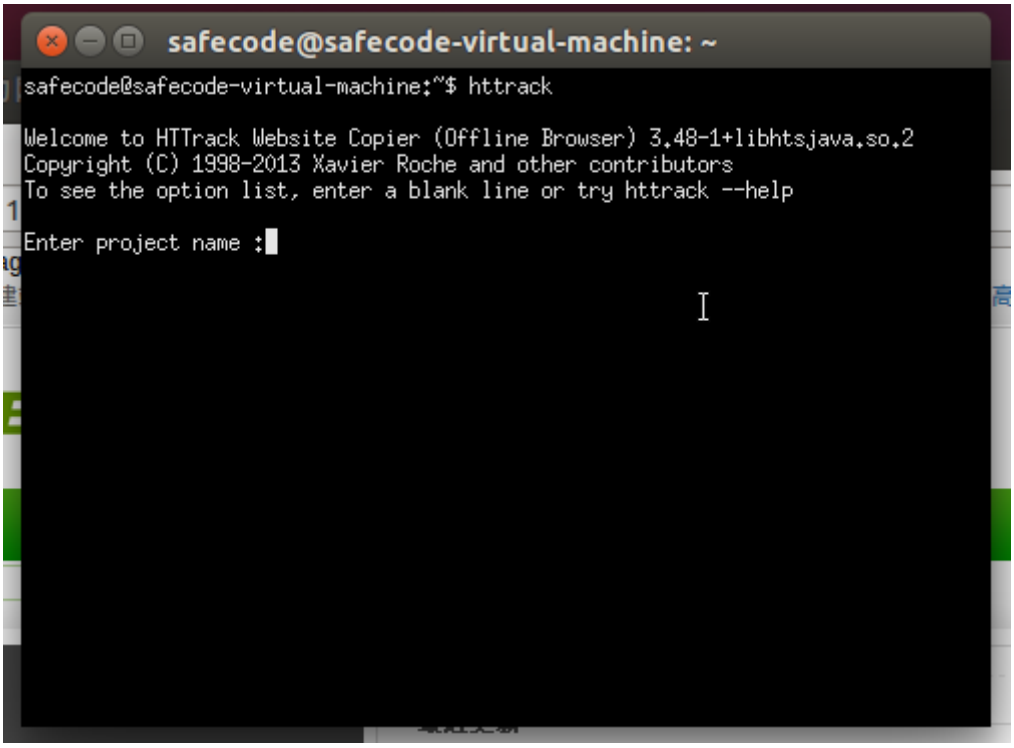

图 12

13. 在新出现的命令行中输入工程名称“test”，后面会将保存的网站信息保存到此工程中。如图 13 所示.

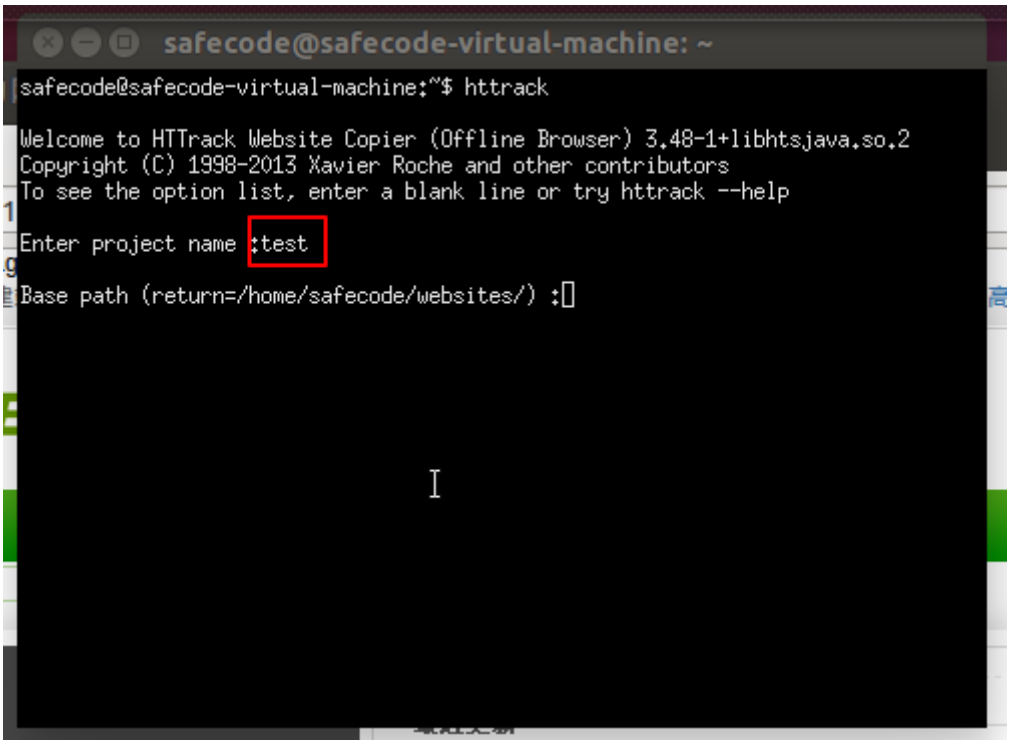

图 13

14. 在新出现的命令行中输入目标存放路径，此处默认为“/home/safecode/websites”，以 test 命名。如图 14 所示

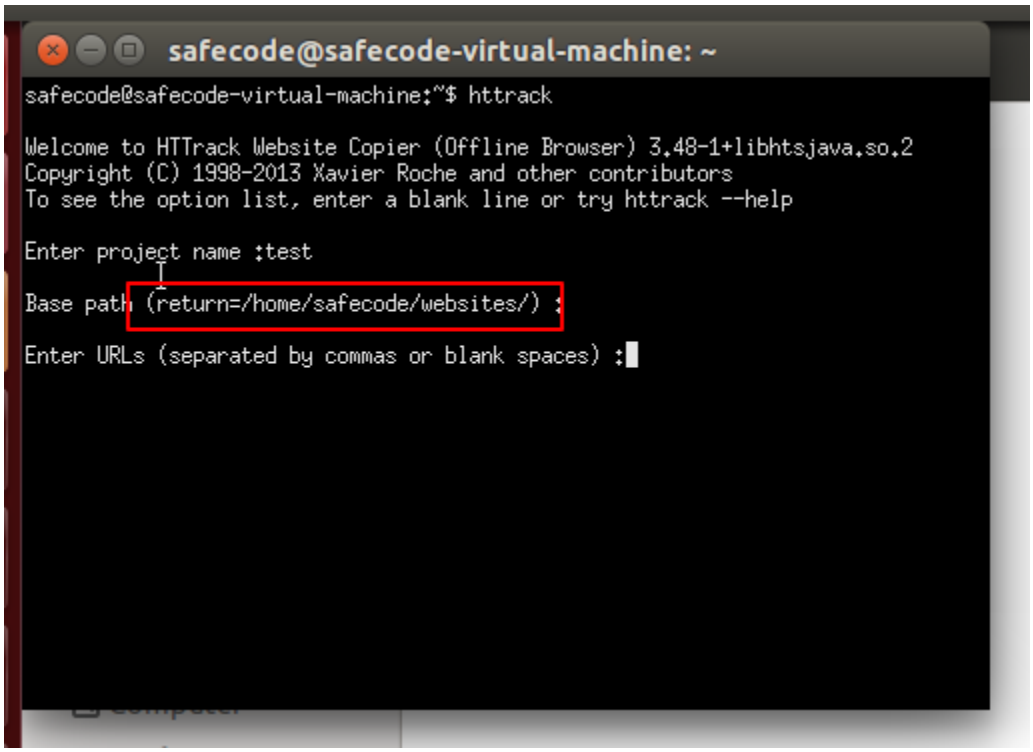

图 14

15. 输入网站 URL 此处输入“192.168.49.230/dede”，Action 输入‘1’即可，如图 15 所示。

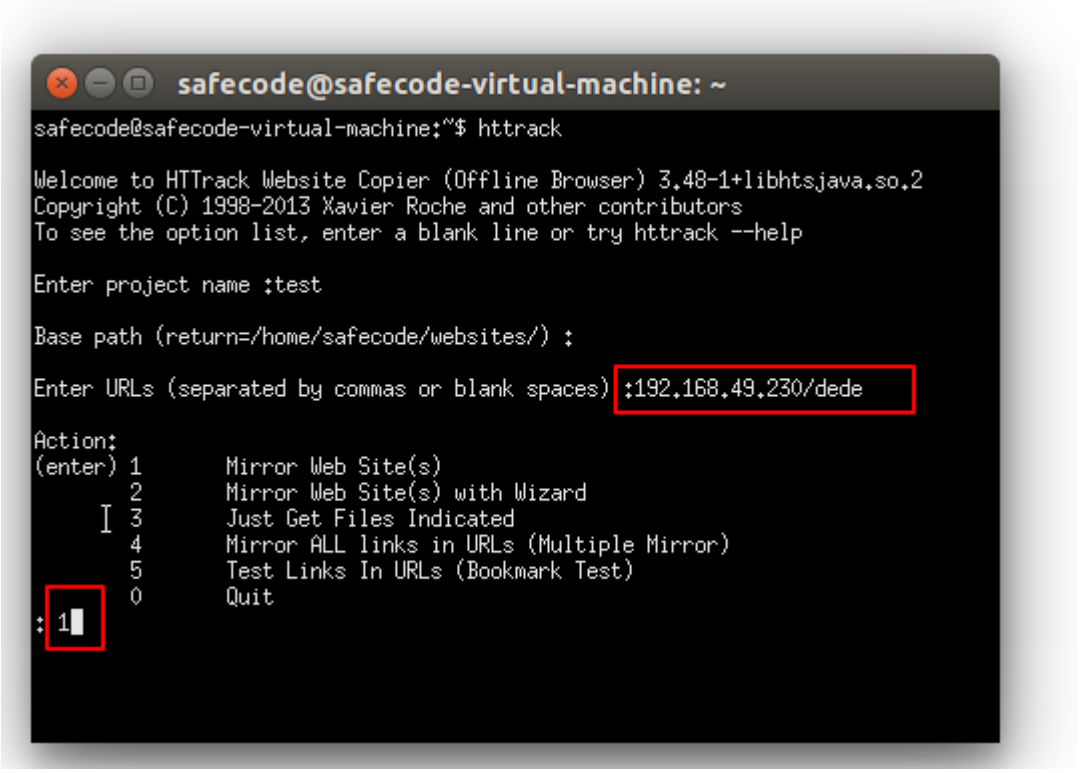

图 15

16. ‘Proxy,Wildcards,Additional’三个选项默认即可，回车跳过，如图 16 所示。

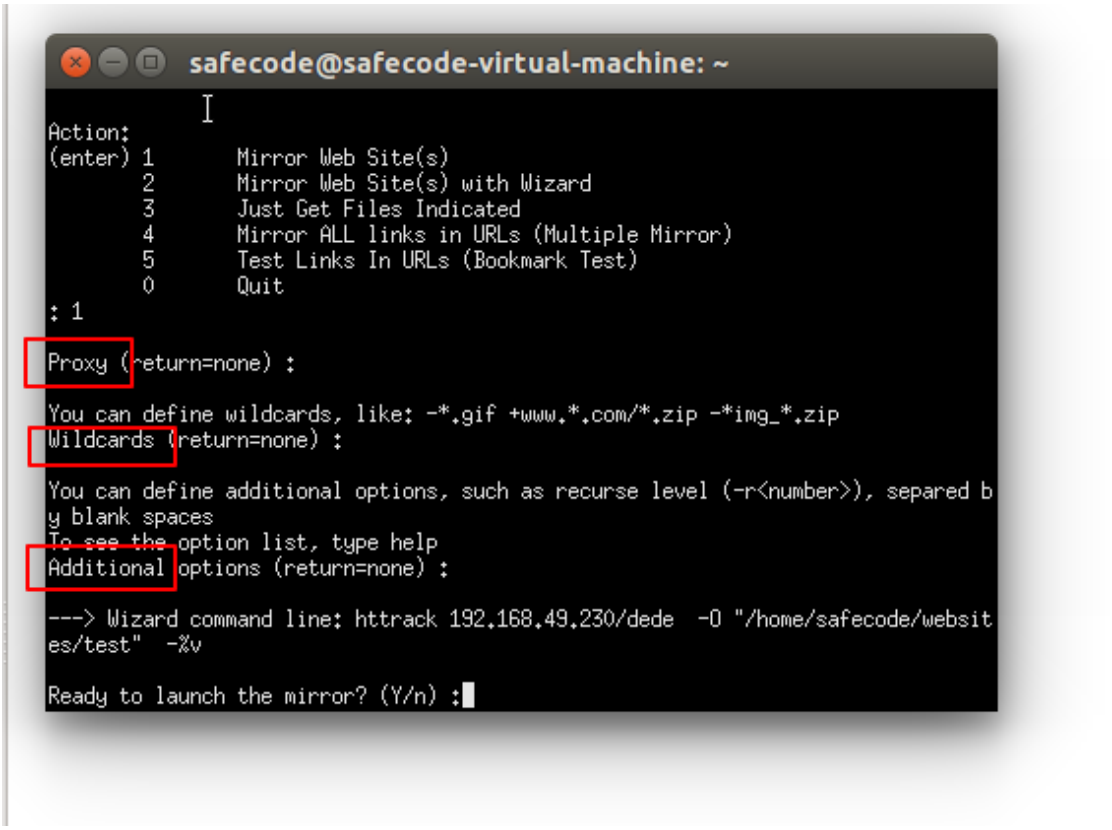

图 16

17. 输入 Y 即可开始复制网站，如图 17 所示。

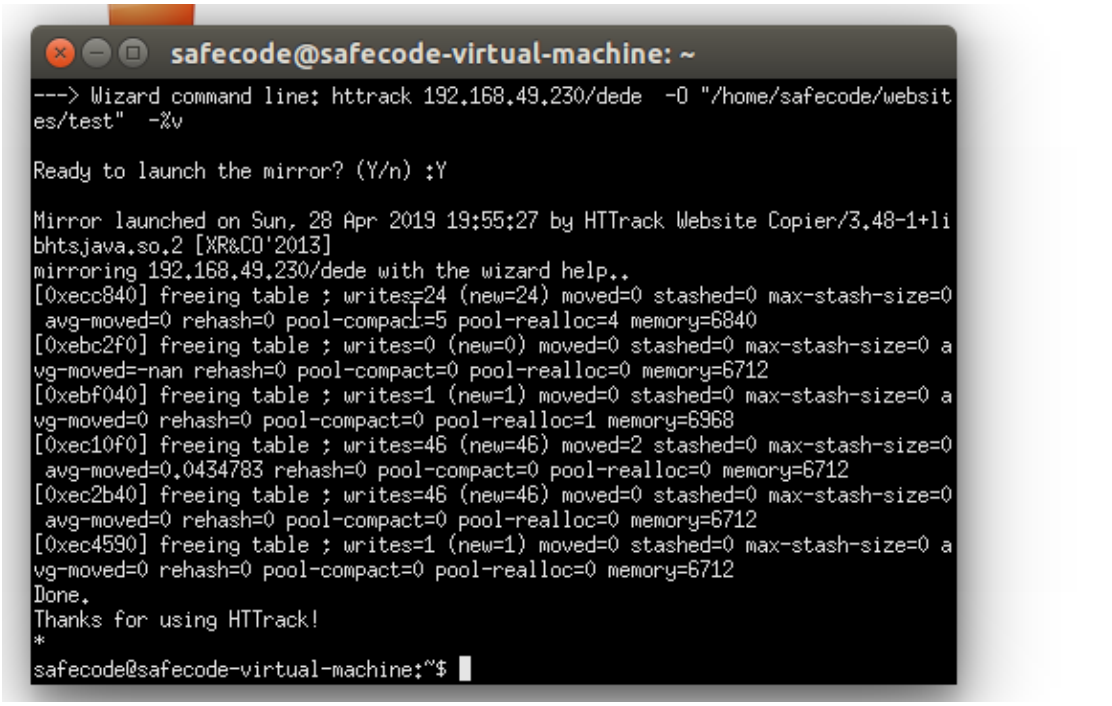

图 17

18. 复制完成后，找到复制目录，即可看到对应网站。如图 18 所示。

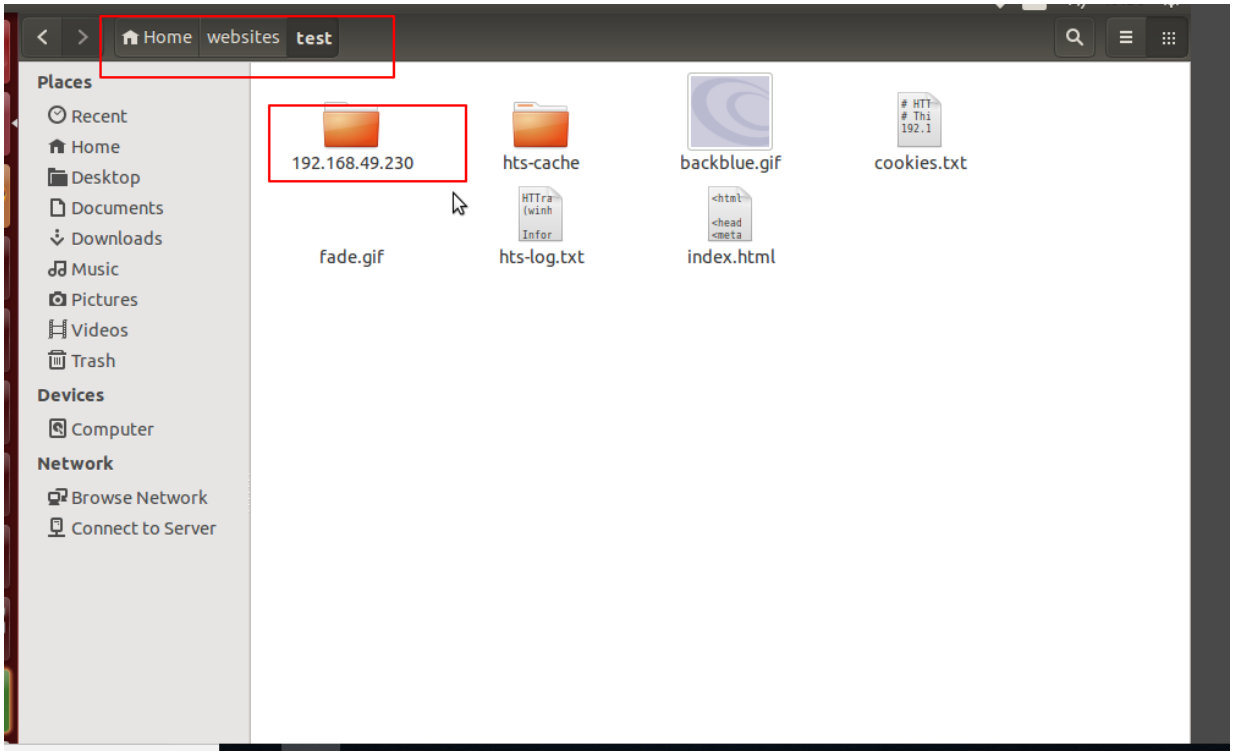

图 18

19. 进入复制网站首页，发现与目标网站一致，如图 19 所示。

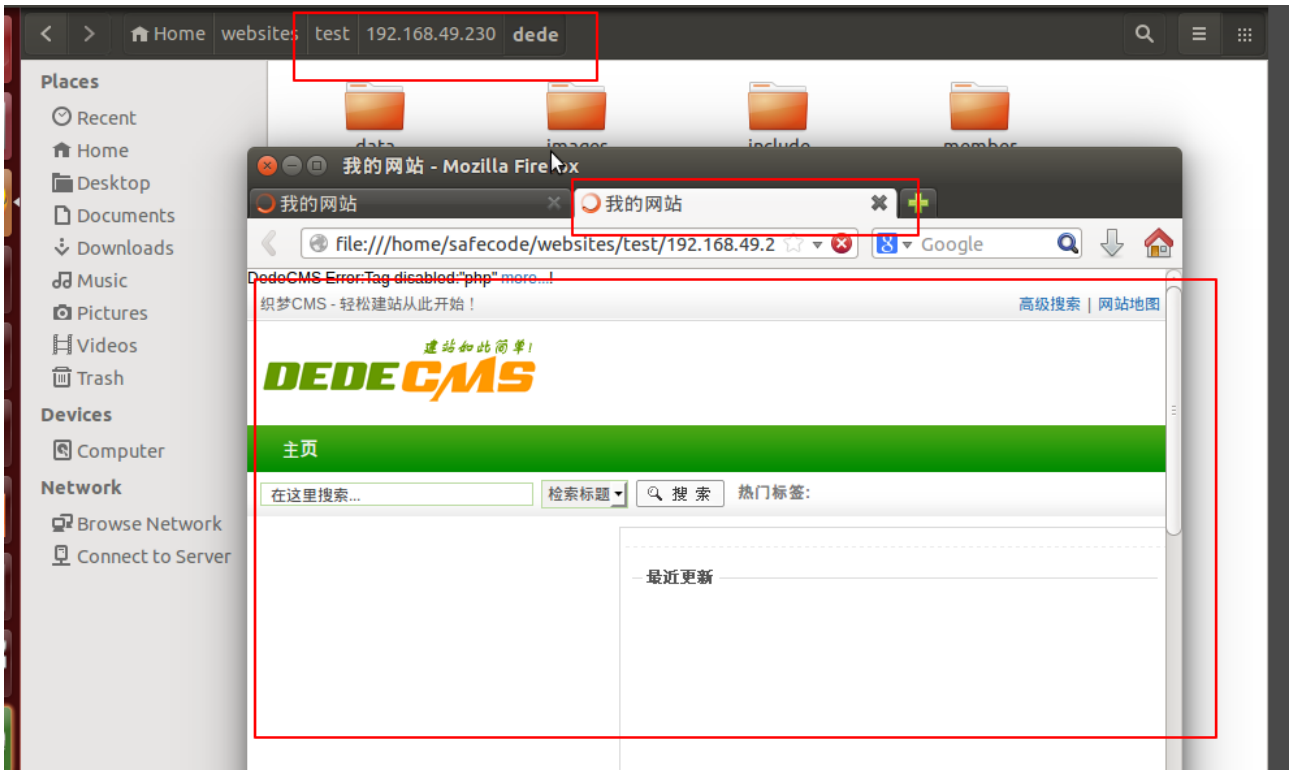

图 19

五【实验思考】

● 了解其他网络侦查手段，思考如何更全面的掌握侦查对象的信息？