

社会工程学攻击的实例化<3>

把玄幻的社会工程学攻击实例化

by:p0tt1



ID:黑客叔叔p0tt1

信息安全从业者

【RainRaid雨袭团】团队负责人

About Me


rain raid

- ★ 不做定义,去了解社会工程学攻击
- ★ 针对站点目标的思路与流程
- ★ 针对个人目标的思路与流程
- ★ 大数据,不仅仅是“大”数据
- ★ 如何将社会工程学攻击实例化
- ★ 简单的实例化案例尝试

犯罪心理&天蝎计划&.....

这些剧中团队不可或缺的人物



《犯罪心理》中值得关注的东西

他们叫做侧写师

基于真实美国联邦调查局（FBI）总部下属行为分析科部门（简称“BAU”）为背景，讲述了一班行为分析精英“侧写师”飞往全国各地，剖析最棘手的连环凶杀案件，分析凶手的心理和作案特征，并在他们再次施暴前预测出他们的下一步行动，协助当地警察捉拿凶手。

“行为分析科” (Behavioural Analysis Unit), 简称“BAU”，总部设在弗吉尼亚州的匡提科，为联邦调查局的国家暴力犯罪分析中心的一部分。

未知主体（剧中称为“Unknown Subject”——简称“Unsub”）

《天蝎计划》中唯一不太懂黑客技术的人

他在中国应该叫“张半仙”或者“神算子”



So.....

为什么总要有这样的人存在，他们在做些什么事情？

无论针对组织，团体，个体，个人目标.....

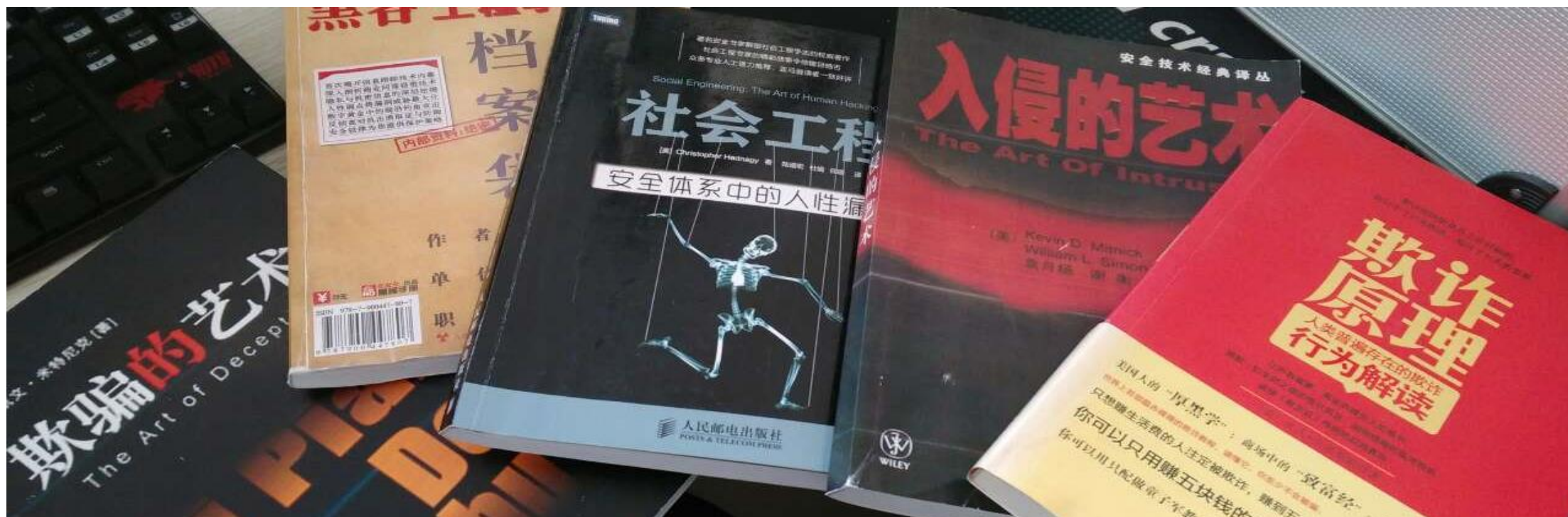
无论是用网络，机器，电话，还是肉眼.....

他们在不断的采集，收集目标信息.....

并且从繁杂的信息中验证并选择部分整理清晰的攻击思路.....

其间，或收集，或诱骗，或主动，或被动.....

这就是社会工程学攻击



一方面
我们听过很多社会工程学攻击的案例
膜拜过很多社会工程学攻击的大作品



另一方面
我们并不知道如何下手
社会工程学攻击毕竟没有可复制性

Part

01

针对站点目标的思路与流程

黑客组织Anonymous疯狂入侵中国站点思路分析

 p0tt1
  2013-01-22
  共27365人围观，发现36个不明物体
 WEB安全

关于匿名者组织的疯狂拿站和统一黑页显示时间的行为，相信大家已经见怪不怪了，但是当匿名者组织开始侵略中国网站的时候，相信大家都会坐不住了。首先，个人感觉反击的意义何在，或者说究竟有没有意义，笔者不是哲学家，思想家，不做过多探讨。但是，知己知彼确实必要的。笔者对前一段时间，国内地方GOV被疯狂秒杀的一次行动做了一次没什么技术含量的分析和猜想。

（以下敏感域名用WWW.XXX.COM略过）

首先，笔者登陆了FACEBOOK找寻了一些热议的话题：

（以下为GOOGLE翻译，英文不好，只好找谷大哥帮忙）

1. 中国3000+政务工作网站 匿名者成功获取权限
2. 匿名者再次攻击亚洲各国，宣传独立自由 在网络中
3. 亚洲强国网络安全成为匿名者的击打目标。

以上是通过匿名者为关键字模糊搜索的热议转载，基本每个热议都指向匿名者发布新闻和预告信的推特，笔者只好去推特，观看了一些匿名者发布针对亚洲和其他洲的攻击成果发布，评论中充斥着各种赞扬与羡慕，当然不乏我国网友的吐槽，也有进行技术分析的人，有一条评论中带有这样一个域名：

www.xxseo.com（化名）

接着，笔者C段了一下：

IP：

```

XXX.XXX.XXX.200
XXX.XXX.XXX.201
XXX.XXX.XXX.202
XXX.XXX.XXX.203
XXX.XXX.XXX.204
XXX.XXX.XXX.205

```

网站的时候，相信大家都会坐不住了。但是，知己知彼确实必要的。

中国国内3000+政务工作网站，匿名者组织成功获取权限，并同一时间修改了所有网站的主页。

匿名者组织再次攻击亚洲各国政务网站，宣传在网络世界中的独立与自由。

亚洲各国的网络安全成为匿名者组织的重点打击目标，各国应做好防范。

<http://www.freebuf.com/articles/web/6995.html>

用社工回溯社工

溯源攻击式从哪里开始的....

www.xxseo.com (老外评论中的一个域名)

XXX.host1068.xxseo.com.cn
XXX.host1079.xxseo.com.cn
XXX.host1081.xxseo.com.cn
XXX.host1083.xxseo.com.cn
XXX.host1093.xxseo.com.cn
XXX.host1099.xxseo.com.cn

XXX.XXX.XXX.200
XXX.XXX.XXX.201
XXX.XXX.XXX.202
XXX.XXX.XXX.203
XXX.XXX.XXX.204
XXX.XXX.XXX.205

WWW.XXX.GOV.CN

中国某省级机房

www.xxseo.com (化名)

接着，笔者C段了一下：

IP：

```
XXX.XXX.XXX.200  
XXX.XXX.XXX.201  
XXX.XXX.XXX.202  
XXX.XXX.XXX.203  
XXX.XXX.XXX.204  
XXX.XXX.XXX.205  
.....
```

以上IP全部指向中国某省级机房

OK，就这个IP段开始旁站扫描，得到无数四级域名：

```
XXX.host1068.xxseo.com.cn  
XXX.host1079.xxseo.com.cn  
XXX.host1081.xxseo.com.cn  
XXX.host1083.xxseo.com.cn  
XXX.host1093.xxseo.com.cn  
XXX.host1099.xxseo.com.cn  
.....
```

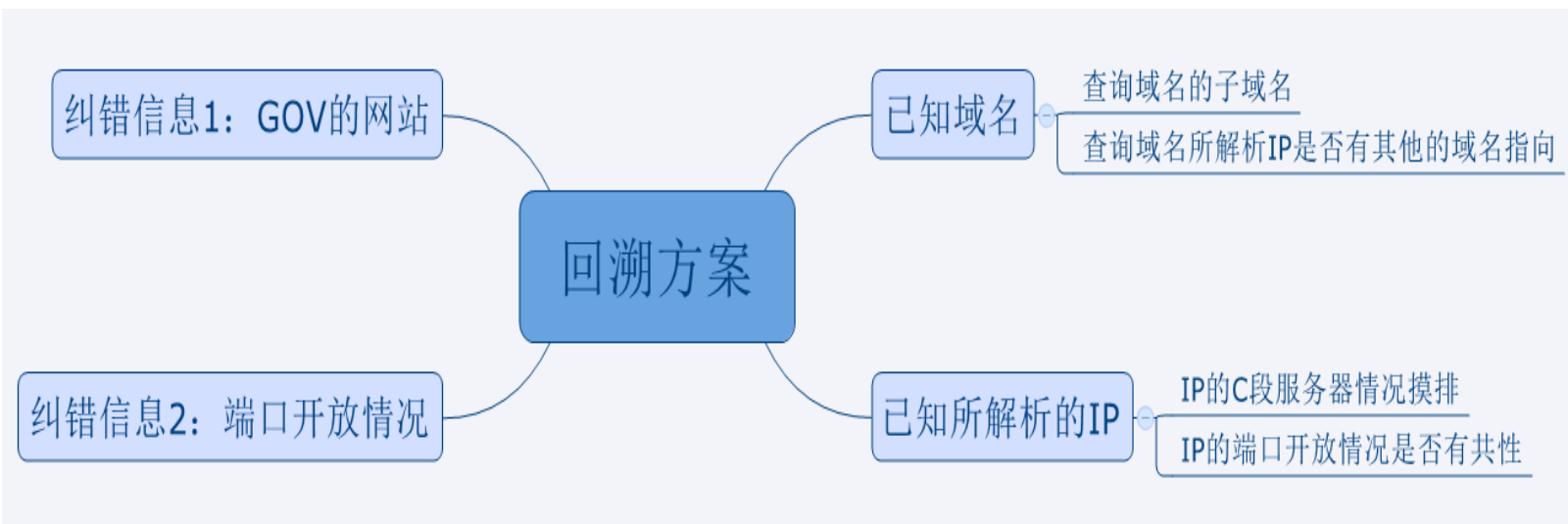
相信看到这里，大家应该明白了些什么，当然笔者还是打开验证了下

无一例外，全部是政务网站，各地GOV。

```
XXX.host1099.xxseo.com.cn
```

都是IDC机房托管的分配四级域名，实际绑定是WWW.XXX.GOV.CN

整理分类已知信息，从而得出下一步该做的事情



信息永远不会是孤立的

信息总是和其他信息所关联，或本身可以衍伸出更多的信息，这里要注意的是信息和信息类别。

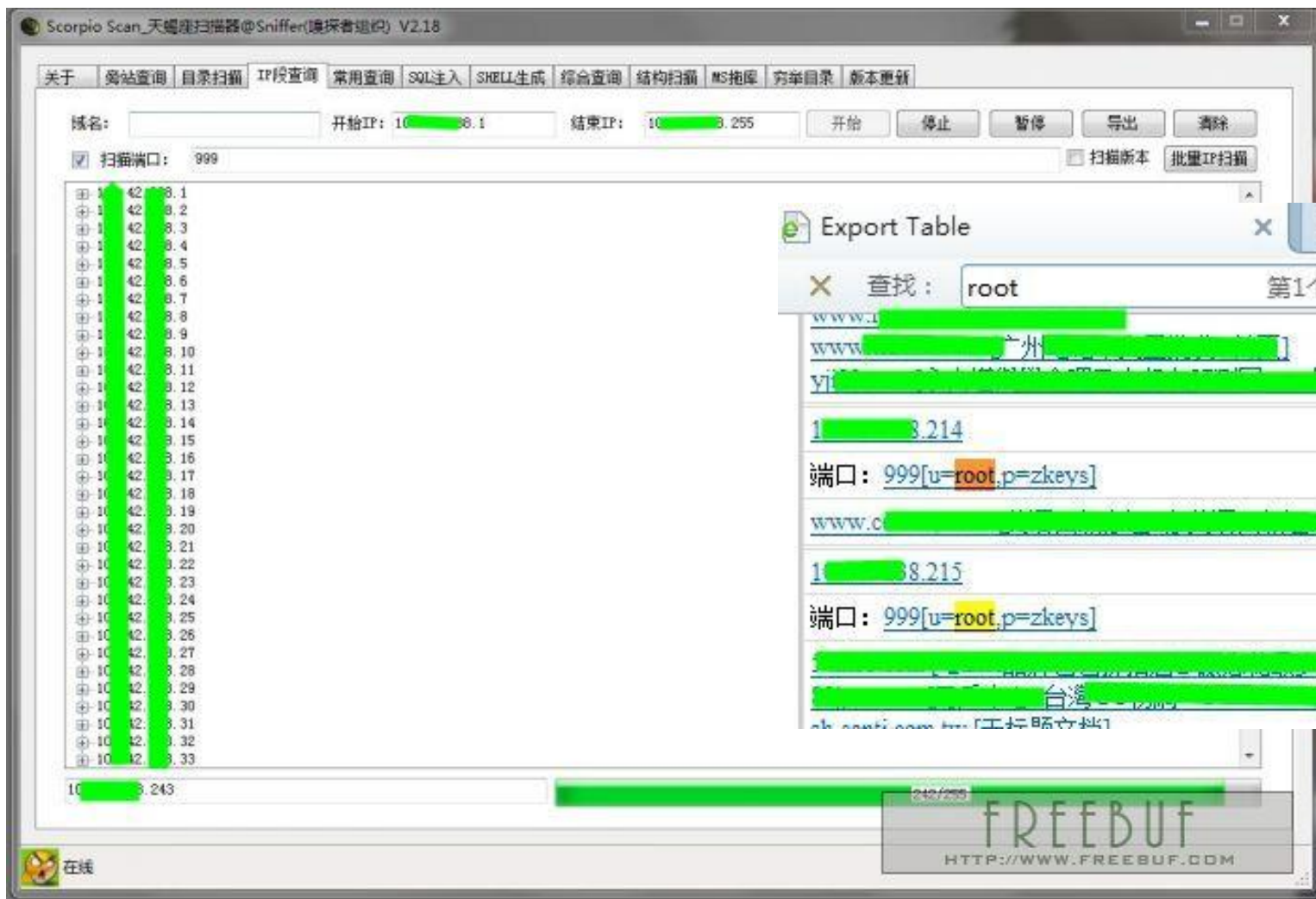


X-mind的使用

X-mind是一款跨平台的思维导图可视化程序，可以有效帮助我们整理和展现信息。

对方的攻击手法

也带有很多的社会工程学攻击的元素

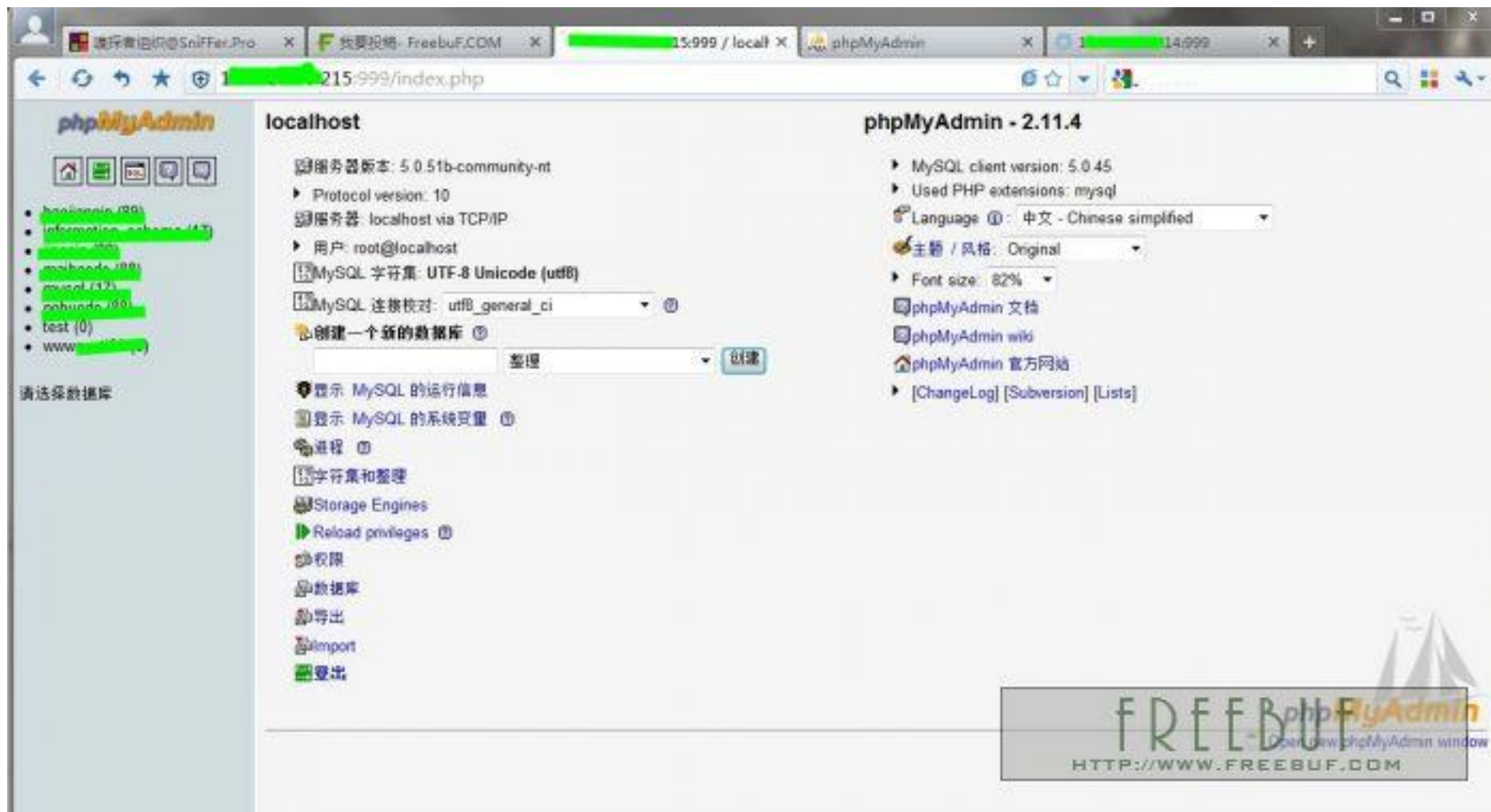


FREEBUF
HTTP://WWW.FREEBUF.COM

FREEBUF
HTTP://WWW.FREEBUF.COM

对方的攻击手法

也带有很多的社会工程学攻击的元素



对方的攻击手法

也带有很多的社会工程学攻击的元素

匿名者的攻击方案

一个制作政务网站的外包公司

公司官网 • 公司使用的业务部署程序 • 默认账号密码获取

公司的合作单位列表

发现均为GOV • IP段排查 • 全部为这个公司的几个服务器IP段

该公司制作网站服务器的端口

均开放999端口 • MySQL管理面板 • 该公司的同一套密码

批量攻击

扫描C段 • 验证是否开启999端口 • 用部署的初始密码碰撞 • 成功登录后导出webshell

公网设备

Web 服务

组件

版本

操作系统

国家

城市

端口

主机名

服务

IP 地址

模糊

组件名

版本

操作系统

国家 / 行政区名称或代码

城市名称

端口号

主机名

服务

IP 地址

模糊搜索

公网设备

Web 服务

组件

版本

网站

操作系统

国家

城市

关键词

描述

模糊

组件名

版本

网站域名

操作系统

国家 / 行政区名称或代码

城市名称

页面描述

页面关键词

模糊搜索

搜索



面对站点类型的目标，我们首先对其有一个主观上的印象，客观上的了解，这些可能来自你对其业务功能的试用，或是对其业务内容的阅读等等....



通过服务器信息查询等方法获得的信息：
服务器类型、服务器系统、服务器所在地区，IP地址段，运行的WEB服务器版本，脚本程序类型等等...



通过搜索引擎获得的信息：
旁站信息，子域名信息，WAF信息，维护部门信息，网站所属组织信息，所属组织的组织架构信息等等...

不仅仅使用传统搜索引擎

越来越多的特种搜索出现了，这些其实都基于了社会工程学。



Google
大而全的传统引擎

Fofa.so
模仿撒旦的一款，对子域名搜索支持的不错！

zoomeye.org
模仿撒旦的一款，对网络设备搜索支持的很好！

Shodan.com
鼎鼎大名的撒旦搜索，针对网络设备和工控设备甚至打印设备都能搜索。

IIS hostname:njupt.edu.cn country:CN

搜索在中国的南京邮电大学这个组织有哪些开启了IIS服务的机器.....

SHODAN IIS hostname:njupt.edu.cn country:CN Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory

Services HTTP	4	Error 202.119.236.199 Network Center Added on 04.11.2014 Nanjing Details www.ctie.njupt.edu.cn	HTTP/1.0 403 Forbidden Content-Length: 218 Content-Type: text/html Server: Microsoft-IIS/6.0 ctie: www.ctie.njupt.edu.cn X-Powered-By: ASP.NET Date: Tue, 04 Nov 2014 04:19:13 GMT
Top Cities Nanjing	3	 202.119.236.185 Network Center Added on 09.02.2014 Nanjing Details www.cw.njupt.edu.cn	HTTP/1.0 200 OK Server: Microsoft-IIS/5.0 Date: Sat, 08 Feb 2014 22:35:08 GMT X-Powered-By: ASP.NET Content-Length: 7560 Content-Type: text/html Set-Cookie: ASPSESSIONIDCSQQDRCS=APICJBCENBCBNJGLDNGBGNK; path=/ Cache-control: private
		202.119.232.8 Windows 2003 Added on 25.01.2010 Details st1.lib.njupt.edu.cn	HTTP/1.0 200 OK Content-length: 45984 X-aspnet-version: 1.1.4322 Set-cookie: ASP.NET_SessionId=4tidekmzfl51i345kjpft045; path=/ X-powered-by: ASP.NET Server: Microsoft-IIS/5.0 Cache-control: private Date: Mon, 25 Jan 2010 11:18:57 GMT Content-type: text/html; charset=utf-8

200 OK cisco country:JP

搜索在日本有哪些思科路由器暴露在公网上了.....

SHODAN 200 OK cisco country:JP Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory

Services			
HTTP	16		
SIP	13		
HTTPS	1		

Top Cities			
Tokyo	7		
Sizuoka	2		
Shirokane	1		
Mitsui	1		
Machida	1		

1.72.4.231
Ntt Docomo
Added on 28.10.2013
🇯🇵 Tokyo
[Details](#)

s804231.xgsspn.imtp.tachikawa.spmode.ne.jp

SIP/2.0 **200 OK**
Via: SIP/2.0/UDP nm;branch=foo;rport=18903;received=xxx.xxx.xxx.xxx
Contact: <sip:10.76.40.182:5060>
To: <sip:nm2@nm2>;tag=f4d7e226
From: <sip:nm@nm>;tag=root
Call-ID: 50000
CSeq: 42 OPTIONS
Accept: application/sdp, application/sdp
Accept-Language: en
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Supported: replaces, norefersub, extended-refer, timer, X-cisco-serviceuri
User-Agent: Zoiper r18164
Allow-Events: presence, kpml
Conte...

153.148.27.221
Open Computer Network
Added on 19.10.2013
🇯🇵 Tokyo
[Details](#)

p348221-omed01.tokyo.ocn.ne.jp

SIP/2.0 **200 OK**
Via: SIP/2.0/UDP nm;branch=foo;rport=17024;received=xxx.xxx.xxx.xxx
Contact: <sip:153.148.27.221:5060>
To: <sip:nm2@nm2>;tag=3556bf56
From: <sip:nm@nm>;tag=root
Call-ID: 50000
CSeq: 42 OPTIONS
Accept: application/sdp, application/sdp
Accept-Language: en
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Supported: replaces, norefersub, extended-refer, timer, X-cisco-serviceuri
User-Agent: Zoiper r**20066**
Allow-Events: presence, kpml
Con...

150.89.255.58
K-Opticom Corporation
Added on 08.10.2013
🇯🇵
[Details](#)

HTTP/1.0 **200 OK**
Date: Tue, 08 Oct 2013 15:29:17 GMT
Server: cisco-IOS

路由和交换机暴露是一件非常危险的事

当然你作为攻击方可能会很欣喜.....



Move the pointer over the ports for more information.

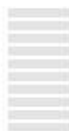
Dashboard

Switch Information

Host Name: tyo-sw-internet01
Product ID: WS-C2950-24
IP Address: 122.219.116.2
MAC Address: 00:1F:C9:3E:AD:80
Version ID:
Serial Number: FOC1216W18C
Software: 12.1(22)EA10a
Contact:
Location:

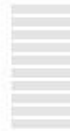
Switch Health

Bandwidth Used



0%

Packet Error



0%

[View Trends](#)

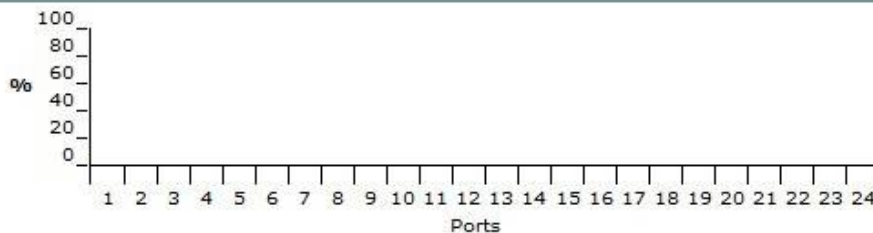
Fan



OK

Port Utilization

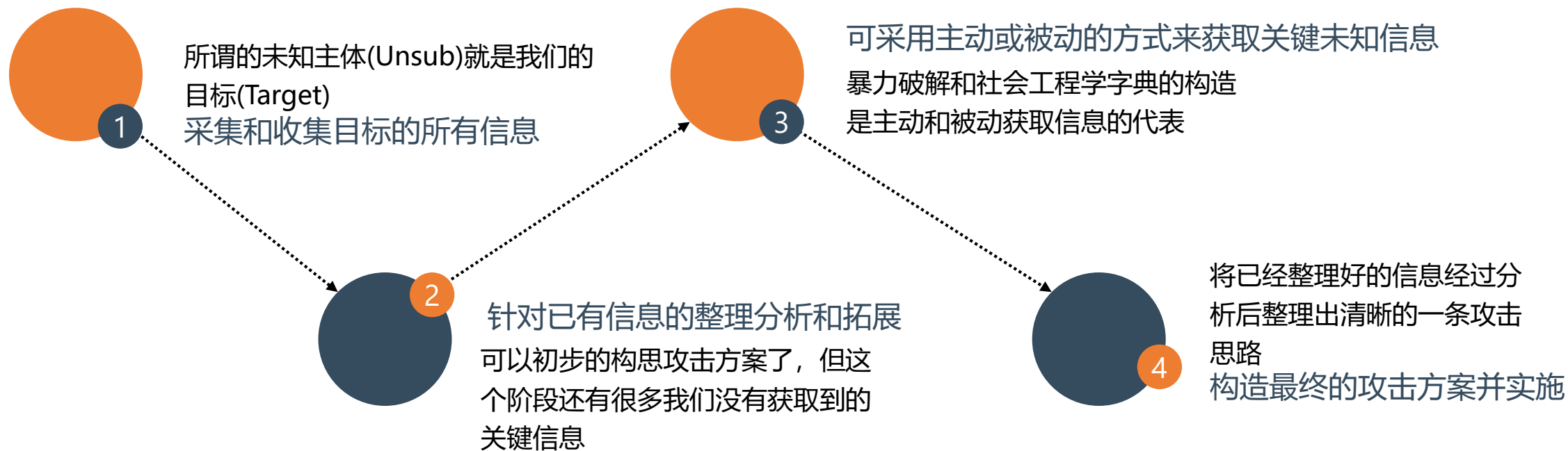
[View Trends](#) | [View Port Statistics](#)



Legend: ■ Receive ■ Transmit

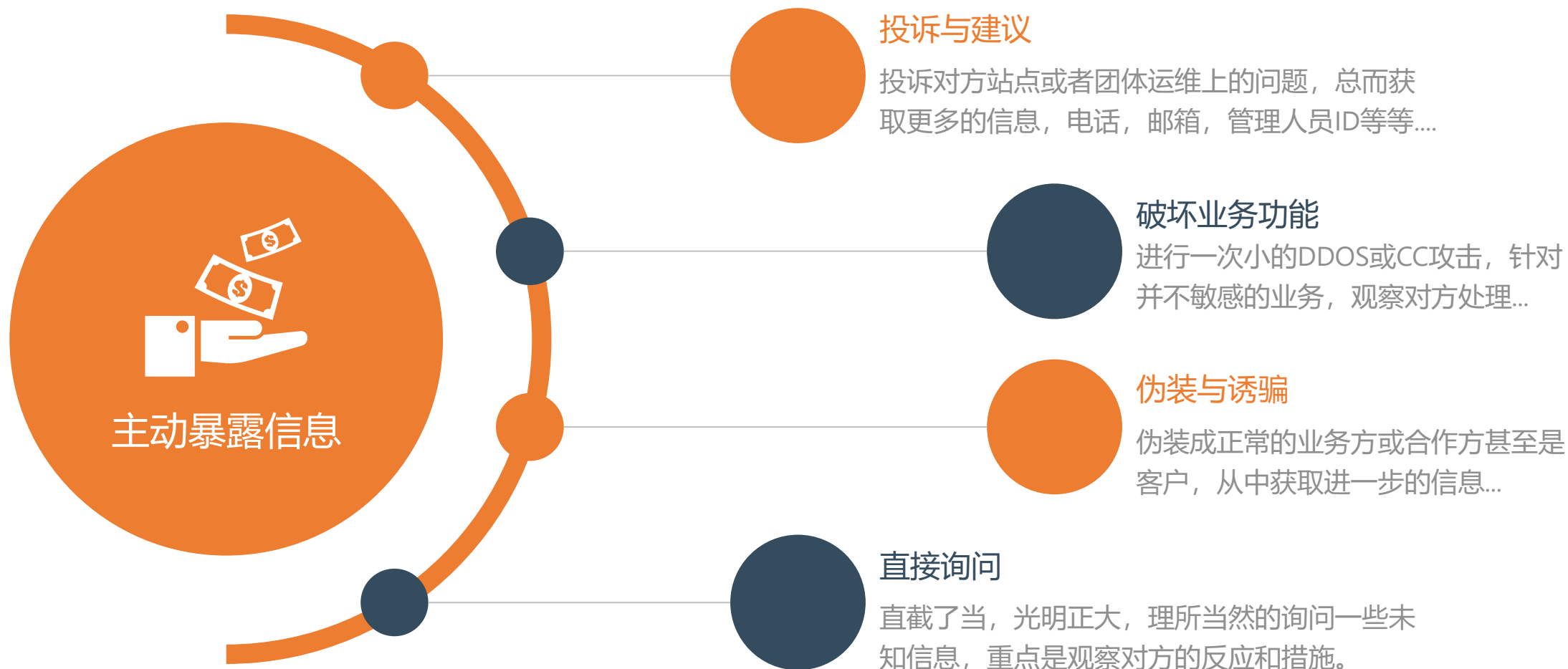
针对站点目标攻击的重点梳理

来自服务器和搜索引擎的两大信息源



小东西0x01：关于信息的主动获取

如何迫使对方主动暴露信息



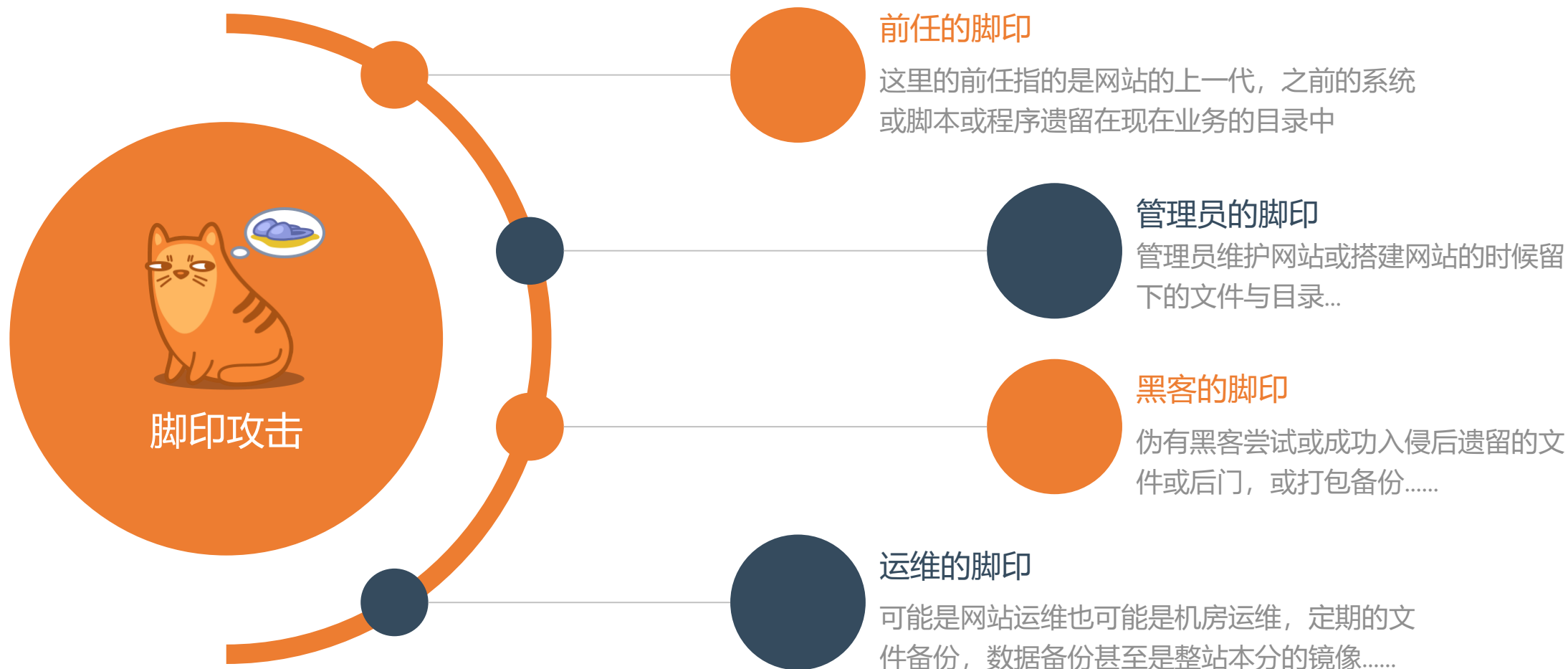
案例0x01:"M国"军事每日新闻网

最省心的一次服务器和内网渗透项目

- 1.针对站点的信息收集:获取了基本的服务器信息, 端口, IP, 建站系统, whois信息等等.....
- 2.针对该站点, 利用搜索引擎进行信息收集:获取了部分记者的邮箱, 姓名, 网站的性质和组织架构.....
- 3.留意到推特上有"M国"黑客曾宣称自己要入侵该网站发布自己对"自由"的渴望....
- 4.获取了该黑客的ID和推特账号并且对其展开新一轮的信息收集.....
- 5.从其推文和博客中得知其经常光顾"KN-Night"的一个地下IRC聊天室
- 6.加入"KN-Night"聊天, 获取更多信息, 总结了该黑客的很多惯用ID和关键词
- 7.用收集到的信息在google中搜索, 成功找到了该网站的一个/img/SlimCJ.php文件
- 8.该文件为D99 webshell,用获取到的id信息进行登录尝试, 用cjc00l成功登录webshell
- 9.巩固权限, 打包走人....黑锅有人背.....

小知识0x02: "脚印攻击"

懒人思维的逆袭



案例0x02:国内某电商测试项目

经过前面所说的信息收集方法，我们成功找到了这样一个子域名：

http://ued.*****.com/

用户体验中心，貌似是接入内网的

不过肯定不会是生产环境的内网



案例0x02:国内某电商测试项目

构造语法，和对某电商运维建站规范的熟悉

我们成功找到了这个：

`http://ued.*****.com/survey/admin/`

那么问题就来了，没有账号密码怎么办？

并且登录3次后就出现二次验证码了~



用户体验提升后台管理
USER EXPERIENCE PLAN

	用户名
	密码

登 录

案例0x02:国内某电商测试项目

社会工程学攻击的攻击方案来到这个阶段有很多方向可以做：

- 1.尝试输入admin,system,master,test等用户猜解
(这一条很明显社会工程学攻击误区)
- 2.收集用户体验中心相关人员的信息
(这也是个误区，而且很累)
- 3.直接爆破，用代理列表的方法绕过验证码
(又走回老路了~)



用户体验提升后台管理
USER EXPERIENCE PLAN

	用户名
	密码

登 录

案例0x02:国内某电商测试项目

社会工程学攻击的攻击方案的基础是依托信息资源:

1.信息是没有高低之分的

2.注重信息的多样性

PS:

实地在公司总部附近转了转,有其实中午的小饭店

我得到信息:

工牌上工号为类似手机号的字符串

穿着UED文化衫的员工工牌也是这样

某员工用手机OA APP点了几下,跟同事说下午不去了

案例0x02:国内某电商测试项目

信息收集的时候，企业介绍，联系我们，业务合作等等信息终于有用用了！

做了一个手机号的表

每个手机号只实验两次，不触发验证码

123456

654321

然后....



http://www.kouying.com/courseware/active/index.php?app=anti&type=index

文件(F) 编辑(E) 查看(V) 收藏(C) 工具(T) 帮助(H)

收藏夹

网络列表 - 苏宁易购用户体验提升计划



UED 用户体验提升后台管理
USER EXPERIENCE PLAN

登录 欢迎来到网络后台系统! 退出 重置

问卷管理 反馈信息管理 常见问题管理 账户管理

问卷列表 新增问卷 目录树管理

请输入关键词 查询 添加

ID	问卷名称	创建时间	截止时间	答卷	状态	路径	操作
183	会员会员行为习惯调研	2014-09-05	2019-12-31	402	已开放	1	查看 导出 编辑 发布路径 删除
102	苏宁易购客户满意度调研问卷	2014-09-03	2019-12-31	517	已开放	0	查看 导出 编辑 发布路径 删除
180	微票易道调研	2014-09-01	2019-12-31	0	已开放	1	查看 导出 编辑 发布路径 删除
179	苏宁易购会员满意度调研	2014-09-01	2019-12-31	980	已开放	0	查看 导出 编辑 发布路径 删除
178	数据宝调研问卷	2014-08-29	2019-12-31	187	已开放	1	查看 导出 编辑 发布路径 删除
176	易购会员调研问卷	2014-08-29	2019-12-31	1514	已开放	1	查看 导出 编辑 发布路径 删除
175	推荐给朋友及转发问卷	2014-08-29	2019-12-31	4	已开放	1	查看 导出 编辑 发布路径 删除
173	苏宁易购APP调研问卷	2014-08-27	2019-12-31	327	未开放	1	预览 导出 编辑 发布路径 删除
171	易购易购会员调研问卷	2014-08-22	2019-12-31	0	未开放	1	预览 导出 编辑 发布路径 删除
170	苏宁金融用户需求调研问卷	2014-08-22	2019-12-31	915	已开放	1	查看 导出 编辑 发布路径 删除

案例0x02:国内苏宁测试项目

人在南京就是好，账户密码不用跑！

还是因为前期的信息收集过程，我们知道该服务器的Nginx服务的版本存在文件名解析漏洞
上传点图片得到xxxxxxxxxx.jpg，访问xxxxxxxxxx.jpg/1.php 即可~

ued.suning.com/survey/admin/index.php?c=paper@a=create

搜索 smtp.uzai...

UED 用户体验提升后台管理
USER EXPERIENCE PLAN

您好, 100170009!

问卷管理 反馈信息管理 常见问题管理 账户管理

问卷列表 新增问卷 目录树管理

新增问卷

问卷标题:

问卷信息:

显示自定义内容

下一步

图片

网络图片 本地上传

上传文件: update.jpg 浏览...

确定 取消

183.57.84.91 目录(10), 文件(1)

名称	时间	大小	属性
static	2013-11-18 15:57:44	4096	0755
model	2013-11-18 15:57:43	4096	0755
sql	2013-11-18 15:57:43	4096	0755
admin	2013-11-18 15:57:45	4096	0755
lib	2013-12-18 19:22:49	4096	0755
attached	2013-11-18 15:57:45	4096	0755
tmp	2014-09-16 09:22:30	36864	0755
SpeedPHP	2013-11-18 15:57:43	4096	0755
config	2014-04-22 10:03:28	4096	0755
controller	2013-11-18 15:57:43	4096	0755
index.php	2013-11-18 15:57:43	257	0644

案例0x02:国内某电商测试项目

还得到了数据库，这又是一部分信息了，那么，我们能够继续拓展下去了~
社会工程学攻击，实际上是那些被归为APT攻击的行为主导思想。

配置 SELECT * FROM survey_user

执行成功! 返回20行

	ID	account_type	us	us	display_name	user_purview	add_time
☐ information_schema	☐ 1	-1	su	758	980f3... 緋華裊縹\$ 惹緞?	0	0
☐ test	☐ 3	0	ac	98c	b754...		1367150226
☒ ued	☐ 6	1	lv	36f	d5b7...		1385021010
☐ survey_article	☐ 7	1	13	7c8	ed3b...		1391754676
☐ survey_article_category	☐ 8	1	gu	7c8	ed3b...		1394421988
☐ survey_paper_url	☐ 9	1	13	0aa	8eb61...		1394587944
☐ survey_qes_answer	☐ 10	1	12	25f	dd7d1...		1394613492
☐ survey_qes_answer_bak_v1	☐ 11	1	nis	abc	44c5e...		1394694221
☐ survey_qes_list	☐ 12	1	13	7e2	88d6...		1394790030
☐ survey_qes_logic	☐ 13	1	12	334	11afed...		1394790041
☐ survey_qes_paper	☐ 14	1	ta	9b8	De3c6...		1394790049
☒ survey_user	☐ 15	1	13	8ff5	4aa8...		1394790056
☐ survey_visitor	☐ 16	1	12	60c	4891f...		1394790066
☐ survey_visitor_bak_v1	☐ 17	1	13	aab	30ac0...		1394790079
	☐ 19	1	xu	2bf	a9444...		1402645066
	☐ 20	1	14	dd3	81d7...		1404355249
	☐ 21	1	14	b2f	d6f49...		1404355387
	☐ 22	1	14	cbe	c7057...		1404355524
	☐ 23	1	11	f5b	e61cd...		1404370436
	☐ 24	1	zh	c7b	5fc71...		1408092921

案例0x02:国内某电商测试项目

人在南京就是好，账户密码不用跑！

获取了数据库后，我们分析了员工工号和OA账号的关系.....

成功登录了手机端（允许外网登录）的上千个账号的登录权限...

使用OA带有的临时申请内网权限（VPN）拨入苏宁内网.....

获取了内网企业通讯录，并伪造身份与他们联系....

成功从IT部门和内维部门获取了几个交换机的账号密码（还是扫描件呢）

然后成功拓扑了内网环境，并修改路由表，漫游内网....

关闭堡垒机和审计机器的监控后，开始嗅探明文密码，扩大战果

打包数据，写测试报告，走人.....

我们团队的KickCandy

我们团队想到并实践成功过的一些“馊主意”

迂回权限大

攻击CMS的厂商或者IDC机房的的公司，或者运维公司。

打击利益链

攻击广告联盟或者友情链接，站长监控平台等等

插件钓鱼

为一个毫无破绽的wordpress网站推送一款收费资源采集插件，免费试用一周

我是一个骗子

域名相似度警告，网站内容报警，服务器存储转移，DDOS攻击防御升级



Part

02

针对站点目标的思路与流程

物理攻击？那些年我们忽略掉的一些社会工程学手段

p0tt1 2013-12-17 +10 共29629人围观，发现41个不明物体

其他

周边

笔者自己也不太明白，也没资格给某种手法进行命名，暂且把这种“非主流的社工和渗透攻击结合”的方式成为物理攻击吧。

首先，做个小小的声明：文章里提到这个朋友虽然从事相关工作，但是却是正义的，也很乐于我将他知道公布出来，便是以爆料的形式。再者，文正中提到的案例确实是真实的，但请个文看官切勿对号入座，保留这层窗户纸，所有案例都已经经过法律审核，不要延伸猜想，“呵呵”一下就行了”

某天

回到了老家，百无聊赖约出了一位好友，共赴排挡，大家都不怎么会喝酒，只能是靠聊天打发时间，便有了下文，暂且叫他WSR吧。

笔者：最近社工挺流行的，真是防不胜防哈~

WSR：还好吧，不过网上的社工案例好像都还基于“调查”和“侦察”类型，不过真正发挥到极致的还是有很多没公开出来的，知道不了解才是最可怕的。

笔者：说的太玄乎了，你肯定又参与了什么吧？

WSR：很多时候，人是漏洞百出的，对人下手的话，那你就得真正面对人，不是面对电脑和几个数据库~而这方面，国内一般都被“商业间谍类型”的黑客”掌握并运用着~

笔者：那讨论讨论呗！交流交流案例！

案例1

有这样一群商业黑客，可能不能理解为传统的黑客定义了，因为他们做的事情确实有些匪夷所思，下文简称为B组织吧。

这次B组织的目标是国内数一数二的网络公司，旗下业务众多，规章制度健全，员工素质及文化成都普遍很高，管理和运营系统中的数据量异常庞大。

显然这次需要B组织进驻内网才能完成任务，但是正面渗透入侵的希望十分渺茫，在系统的渗透和检测之后，他们选择了物理攻击的途径。

B组织经过调研，了解到了该公司负责开发和运维的部门办公场所，并没有乔装打扮，只是带了个鸭舌帽背着个大点的包就堂而皇之的进入了该写字楼（难道这样比较像外卖和快递？）接着，他没有进入任何办公场所，只是在走廊尽头的大垃圾桶收集了点垃圾，塞到包里并立刻离开了，他这样每天不同的时间段来一次，持续了一周，最后两次，大楼保安居然还跟他打了招呼。



物理攻击的概念，最早使用的就是凯文-米特尼克了，电话欺骗、邮件欺骗等等



现在的物理攻击一般还仅仅是停留在wifi破解等等...



这个案例主要利用了很多人性的弱点...

<http://www.freebuf.com/news/others/20291.html>

信息收集的物理攻击体现

我们能利用的东西有很多。

不怕脏的"黑客"收垃圾：

比如：便签纸，草稿，超市小票，快递单，香烟盒，呃，居然还有一张折弯掉的3G流量卡。



美女客服寄来的优惠单

我们能利用的东西有很多。

然后美女甜甜的声音打电话：“感谢您支持，我们为您寄一份优惠单，所有物品一元包邮！”

快递单瞬间搞定了所有的流程！



计算机里，“看看”意味着什么呢？

种个木马真没那么难....

	u盘 8G特价 个性 包邮 卡通 礼品U盘 创意相机 正品 可爱优盘 美女卖u 和我联系	¥ 33.50 运费: 0.00 信用卡	广东 深圳	最近314人成交342笔 1180条评论	七天退换 消费者保障
	U盘8gb 心形钻U盘 可爱 创意u盘 个性8gu盘 女生礼品u盘 正品包邮 天猫 Tmall.com miga摩佳数码旗舰店 和我联系	¥ 91.80 运费: 12.00 信用卡	上海	最近316人成交340笔 506条评论	七天退换 正品保障
	吉他创意优u盘 8G正品特价可爱水晶 小提琴男女生情侣迷你项链个性 深圳君发电子 和我联系	¥ 36.00 运费: 0.00	广东 深圳	最近522人成交585笔 1175条评论	七天退换 消费者保障
	业王音乐宝宝优盘创意u盘可爱卡通 8gu盘8g正品特价包邮情侣个性 天猫 Tmall.com 创线记数码专营店 和我联系	¥ 29.00 运费: 0.00 信用卡	广东 深圳	最近335人成交398笔 341条评论	七天退换 正品保障



你自己求别人给你装窃听器

这次B组织选择不再露面，而是在官网收集一批邮箱，然后伪造了邮件，邮件经过邮件头文件伪造可以改成任意邮箱，于是，这些攻击邮件是京东发的。大概意思是，新品牌安卓平板电脑提前线下体验，暂不在官网发售，只给用户提前体验。这样写好处有三个，第一，这种平板肯定京东官网没有，不然露出马脚，第二，体现我们是提前用户试用，第三，买山寨货，便宜呀！！（B组织可没指望回收回来~）比如下面这些：

 三星正品 超薄 送移动电源+返现金 三星包邮送键盘9寸平板电脑 16G电容屏 WIFI上网安卓4.04双核10寸 ¥ 413.04 最近240人成交	 三星送移动电源 9寸 秒杀 10寸平板电脑 双核16G超薄电容屏掌上电脑 9寸安卓4.0 3G 现货包邮 ¥ 375.00 运费: 0.01 78条评论 最近4人成交	 包邮 超薄双摄像头9寸平板电脑 返现金! 9寸平板电脑 双摄像头超薄3G双核10寸安卓4.0 包邮 免运费 ¥ 300.00 16条评论 最近29人成交	 正版戴尔平板电脑 全网最低 购买就送硅胶保护套+键盘皮套 送键盘皮套正品戴尔9寸平板电脑超薄电容屏3G双核10寸安卓WIFI 免运费 ¥ 325.04 91条评论 最近79人成交
--	---	--	---

嗯，B组织的人们开始为这部山寨安卓平板植入安卓木马了，大家可能怀疑给安卓植入木马和多权限多功能控制有多难~那么笔者给大家提供一个 李毅吧 的帖子，请看3漏洞的视屏，赛门铁克安全专家演示的~链接是：

<http://tieba.baidu.com/p/1409914052>

接着，就是等待批量发送的攻击邮件回复了，居然有40%的人都回复申请了试用，--！搞金融的连平板都买不起么，还用的着试用？看来国人对免费的都不拒绝~总不能都给吧？那样太假，只给一个，又怕万一别人不用。所以，针对邮箱和官网的“团队简介”对比了下职位，选了一个高层领导和一个人事部的主管。把种植木马的机器寄了过去。这样两者没什么交集，而且这两种人有时间上班玩玩东西。

三天后，两个肉鸡都上线了，分别连上的wifi，一个是公司的，一个却是家里自家用的，公司的那个进行了下嗅探（不要小看安卓系统的能力，看过这篇文章的应该都玩过，<http://www.freebuf.com/articles/wireless/6279.html>），得知聊天工具是rtx，没什么戏，家里那个肉鸡呢，虽然没什么用，但是人家登陆了qq，邮箱，微信等等社交工具，当然，这些帐号密码B组织照单全收了。

剩下来，以这个员工的名义和邮箱发了一些邮件给同事，收集了跟多信息，准备绑马群发给同事。但是后来，这个员工居然是把企业邮箱（腾讯）和QQ邮箱绑定的，呃，于是导出了该邮箱附件夹，机密邮件和类似招标文档 会议记录 周报什么的，纷纷拿下，提前结束了战斗。

针对个人目标的社会工程学攻击

我们来简单的分个类

隐匿式攻击

暗中不接触不影响目标和未知主体的情况下进行的社会工程学攻击，主要以前期调研，信息分析，未知信息猜解的流程展开。

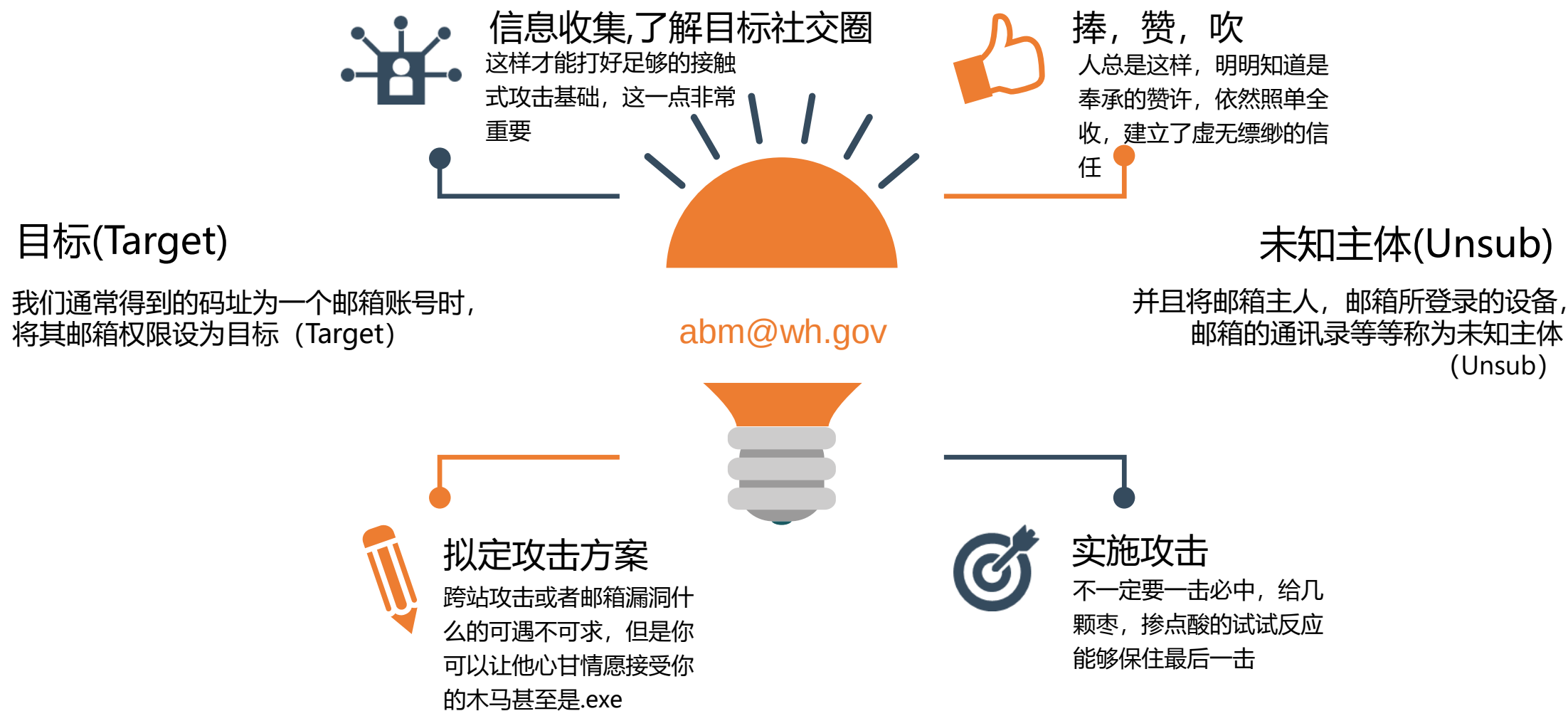
接触式攻击

主动或被动接触目标和未知主体影响或引导其暴露信息甚至未知主体主要以前期调研，信息分析，制定谋略，长短期接触交流，建立信任，展开攻击的流程所展开。



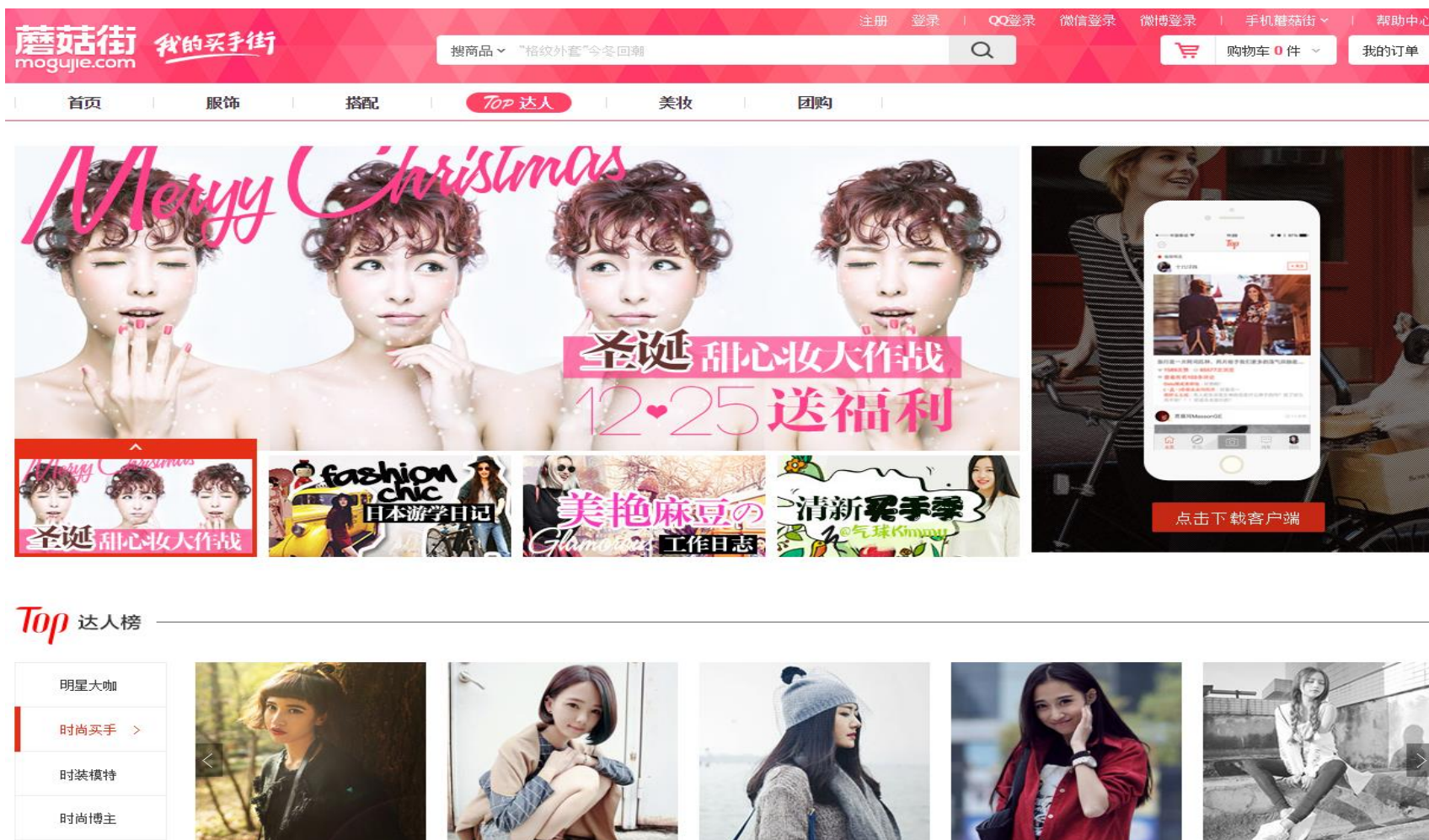
针对邮件，谈谈谋略

最常见和新手失败率最高的手法... ..



案例0x03:某网站的渗透测试

深度关注美女们的购物安全



案例0x03:某网站的渗透测试



蘑菇街没有被爆过数据泄露，但是人是最不安全的.....

谁背叛了你的信息？

Q

User	Pass	Email	Site	LoginIP
mogu jie	12bc71b74bffc24233da13c3545be51a:899b50	tuzi@mogu jie .com	Sorry	123.157.222.178
嘟嘟妹妹	a22ec04a2973042ba23df929030d4e55:b98df2	weiyibo@mogu jie .com	小米	58.68.235.84
小白（不负责	6b189e830e8d571b8550b19abc9baf35:c75e50	xiaobai@mogu jie .com	Sorry	123.157.222.182
小白（不负责	6b189e830e8d571b8550b19abc9baf35 解密	xiaobai@mogu jie .com	WSD	123.157.222.182
mogu jie	12bc71b74bffc24233da13c3545be51a 解密	tuzi@mogu jie .com	WSD	123.157.222.178
	ee5446	dyj@mogu jie .com	WSD	
01	01 ^	yaoyao@mogu jie .com ^ ^986d2018d970c7078aaa69ceafdc7f8f ^hupocz ^1 ^1900	WSD	



案例0x03:某网站的渗透测试

蘑菇街的文秘妹子，助我一臂之力.....



案例0x03:某网站的渗透测试

蘑菇街的文秘妹子，助我一臂之力.....

mail.qiye.163.com/fy3/main.jsp?sid=YApLtrDBPHiNXDhBLsBBigcScKaxdNnz&hl=zh_CN

收藏有道云笔记

蘑菇街 mogujie.com

meiying@mogujie.com [邮箱首页, 换肤, 退出]

收信 写信

收件箱 (2)

草稿箱

已发送

已删除 [清空]

垃圾邮件

病毒文件夹

通讯录

个人网盘

增值服务

企业网盘

传真服务

随身邮

易信提醒

邮件恢复

其他文件夹 [新建]

其他邮箱

早上好，美莹

你有 0 封 未读邮件，管理文件夹

邮箱容量：5G，已使用 1.29G

25.84%

邮箱服务

最近登录：01/13 22:02:58 江苏省·苏州市 最近登录异常，详情，建议立即 修改密码

蘑菇街

收信 写信

添加到个人通讯录

名称	邮箱地址
公司	
公共QQ邮箱	
人事行政部	
运营部	
研发部	
时尚消费部	
产品设计部	
垂直产品部	
财务合规部	
市场部	
客户中心	
综合产品部	
支付与金融	
TOP	
社会化产品部	
默认部门	

联系人分组 [新建组]

其他(1)

案例0x03:某网站的渗透测试

社工手法还有哪些？我们必须扩大战果！

最重要的还是信息收集：163企业邮箱,POP3协议支持

整理现有信息：萌妹子的密码和其他几个密码，企业通讯录中的700+邮箱账号

进入分析阶段：萌妹子的密码含有mogujie*****,会不会是初始或密码规则呢？

拟定攻击方案：采用九头蛇(Hydra)进行邮箱pop3登录爆破，字典为上述信息

实施攻击：

```
1 of 1 target successfully completed, 36 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-01-08 01:29:10
root@kali:/tmp#
```




吓的我都坐地上了

案例0x03:蘑菇街的渗透测试

社会工程学攻击这么方便，挖什么漏洞还.....



案例0x03:渗透测试其实也依靠着社工

大厂商尚且如此，其他的，我们该保持信心.....

漏洞盒子

首页漏洞黑板报HOT项目大厅排行榜NEW提交互联网漏洞p0tt1



p0tt1

个人中心

项目大厅

我的漏洞

账户设置

消息中心

提交漏洞

我的漏洞

所有漏洞待审阅待确认待修复已关闭已公开

项目筛选所有

漏洞标题	风险级别	状态	厂商名称	提交时间
● 蘑菇街可获取各种企业内部信息（组织架构...	高	待确认	互联网漏洞基金	2015-01-09 01:38
● 小米某登陆接口漏洞_威胁千万用户	高	已公开	小米科技	2014-10-16 14:20
● 搞定苏宁第六弹 ued用户体验提升nginx解析...	高	已公开	secsuning	2014-09-19 10:28
● 搞定苏宁第五弹 500万用户信息告急(	高	已公开	secsuning	2014-09-19 10:25
● 搞定苏宁第四弹 苏宁FOTA服务器系统(弱口令)	高	已公开	secsuning	2014-09-16 10:34
● 搞定苏宁第三弹数万VIP用户信息告急(弱口令)	高	已公开	secsuning	2014-09-16 10:32
● 搞定苏宁第二弹数万VIP用户信息告急(弱口令)	高	已公开	secsuning	2014-09-16 10:31
● 搞定苏宁第一弹(敏感信息泄露)	低	已公开	secsuning	2014-09-16 10:29
● 注册功能未做限制 可暴力注册	低	已关闭	漏洞盒子	2014-05-20 19:29
● gitub 和 新浪微博可自定义url 可导致借用网...	中	已关闭	漏洞盒子	2014-05-20 16:44

这一页PPT乱炖

讲讲很多零碎的东西，都在社会工程学攻击范畴

半主动物理攻击

物理攻击

碰瓷和求助

活动轨迹

WiFi攻击

三人成虎的下意识引导攻击

Part

03

大数据，不仅仅是“大”数据

大数据攻击不仅仅是社工库

社工库的信息都是死的，并且毫无关联性

如何让数据形成攻击：

数据中有密码

数据中有目标文件

数据中有..... 这些显然不可能！

那么数据是否能这样：

匹配使用频率最高的密码并去除弱密码

关联文件存储地址信息或目标的活动轨迹

交叉匹配，分析共性和置信度扩大战果

大数据攻击不仅仅是社工库

社工库的信息都是死的，并且毫无关联性

A流程

信息收集---》数据整理分析---》信息扩展---》最终信息整理分析---》制定攻击方案---》实施攻击方案

信息从无到有的社会工程学攻击流程

那么在拥有数据的情况下，我们的流程应该是：

固定数据拓展生成新鲜数据---》新数据归类整理---》进去A流程

大数据到底什么大?

数据量大:

大众表述和广泛认知的概念, 但是数据量大真的有用吗? 我们拿社工库来说, 1000T, 查询1小时以上后返回给你一个"null"或几十个字节的文本, 这个性价比高吗?

数据类型量大:

这个就是说数据的类型和种类繁杂, 融汇了各种各样的数据, 而不是用户名, 邮箱, 密码等等.....类型多后, 可以进行交叉比对, 简单算法或高级模型的接入后, 并建立索引, 这样才能对比出可利用信息来支撑我们的攻击方案。

基于大数据的社会工程学攻击建模

虚拟身份落地建模：

以将目标(Target)的未知主体(Unsub)还原成现实身份的攻击过程

证据链模式建模：

以将目标(Target)的已知主体 (Subject) 行动轨迹和活动方式以证据链模式串联的攻击过程

攻击开展之前：

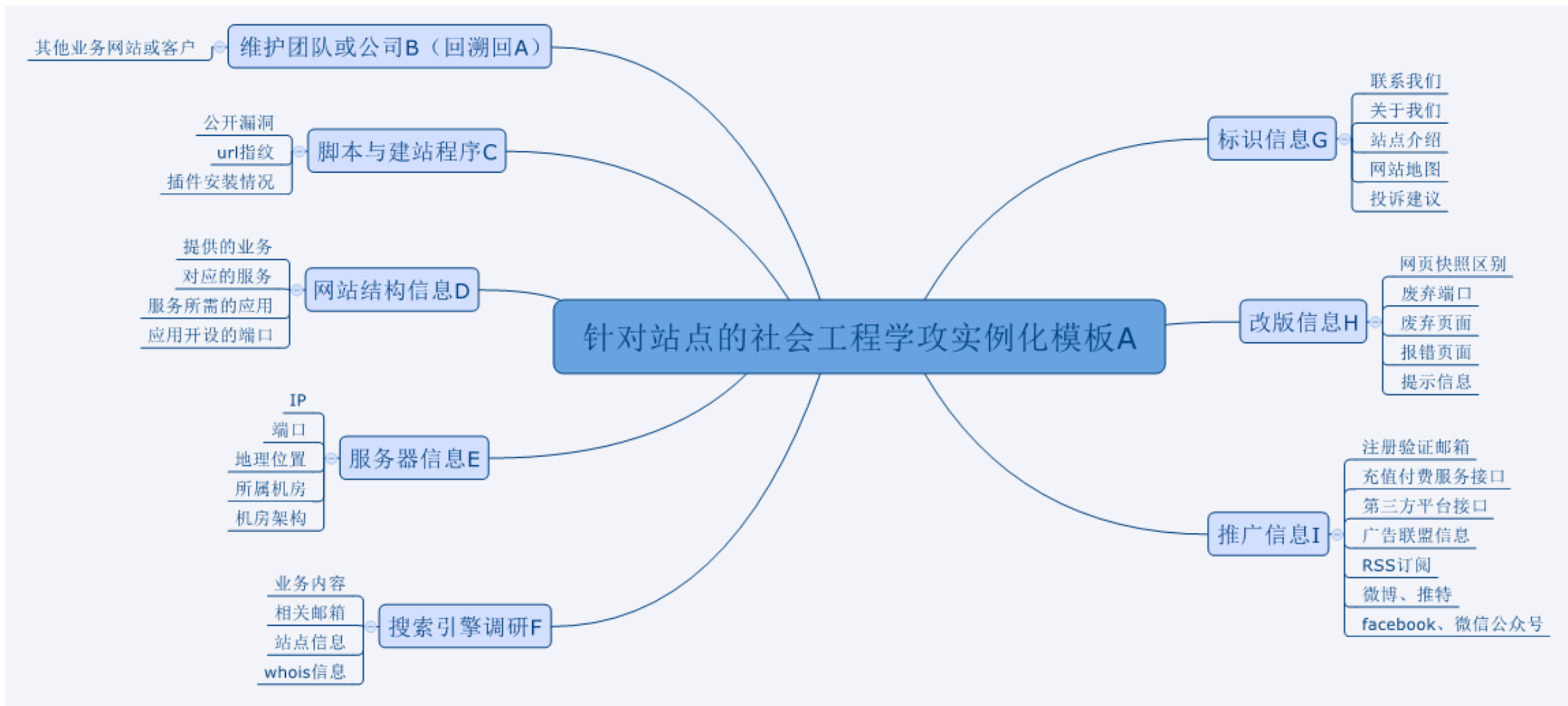
需要为本次社会工程学攻击进行定位，并将积累的经验实例化总结成的模板套入工作中

Part

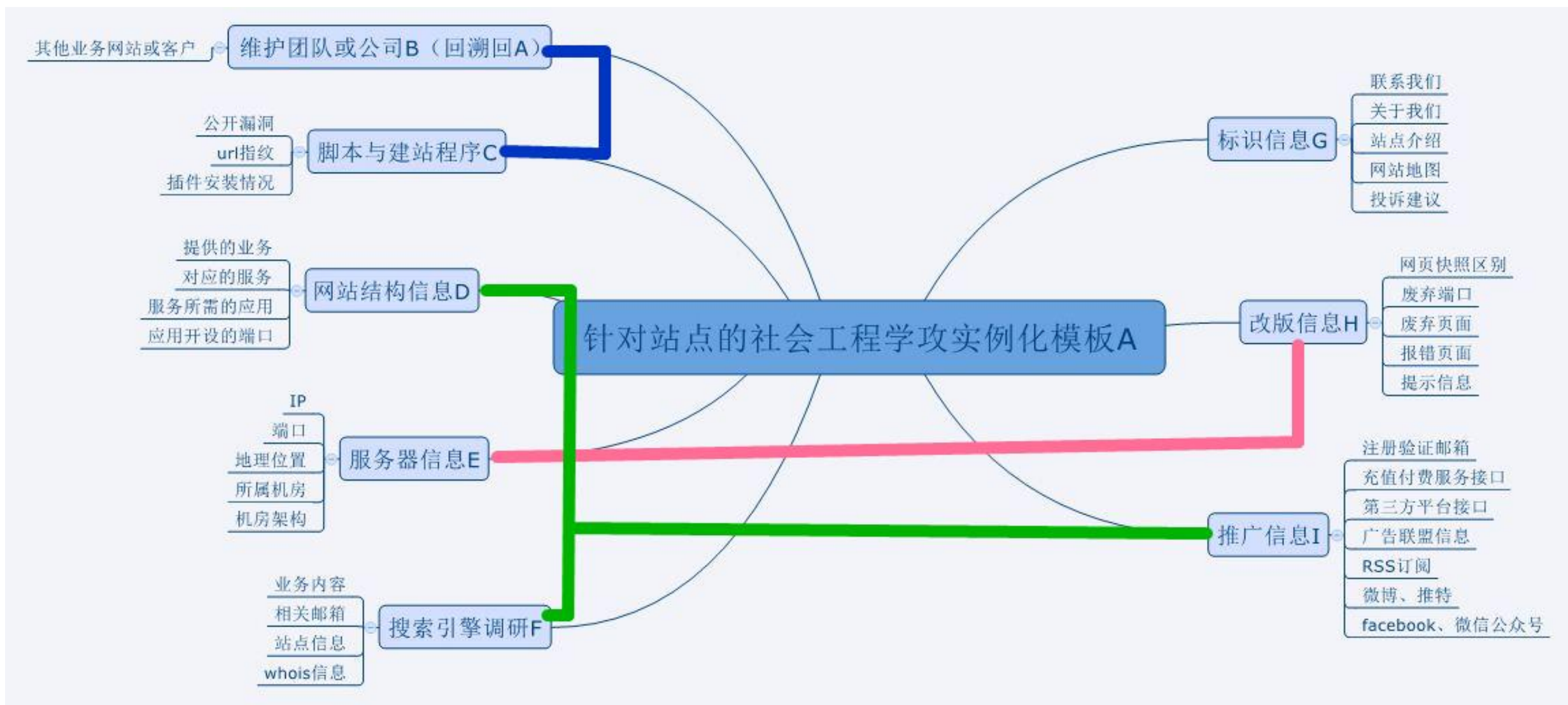
04

社会工程学攻击实例化

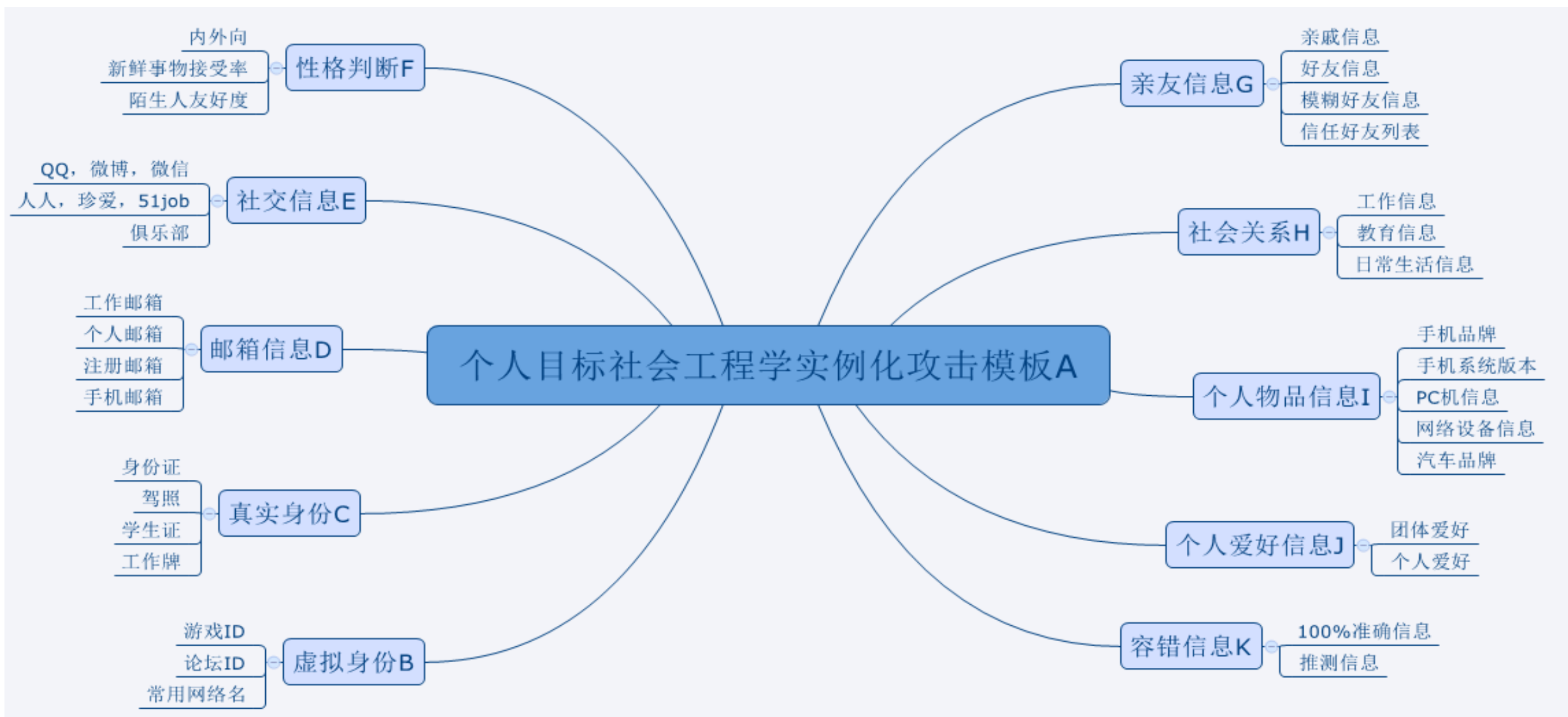
针对站点的实例化攻击模板（极简版）



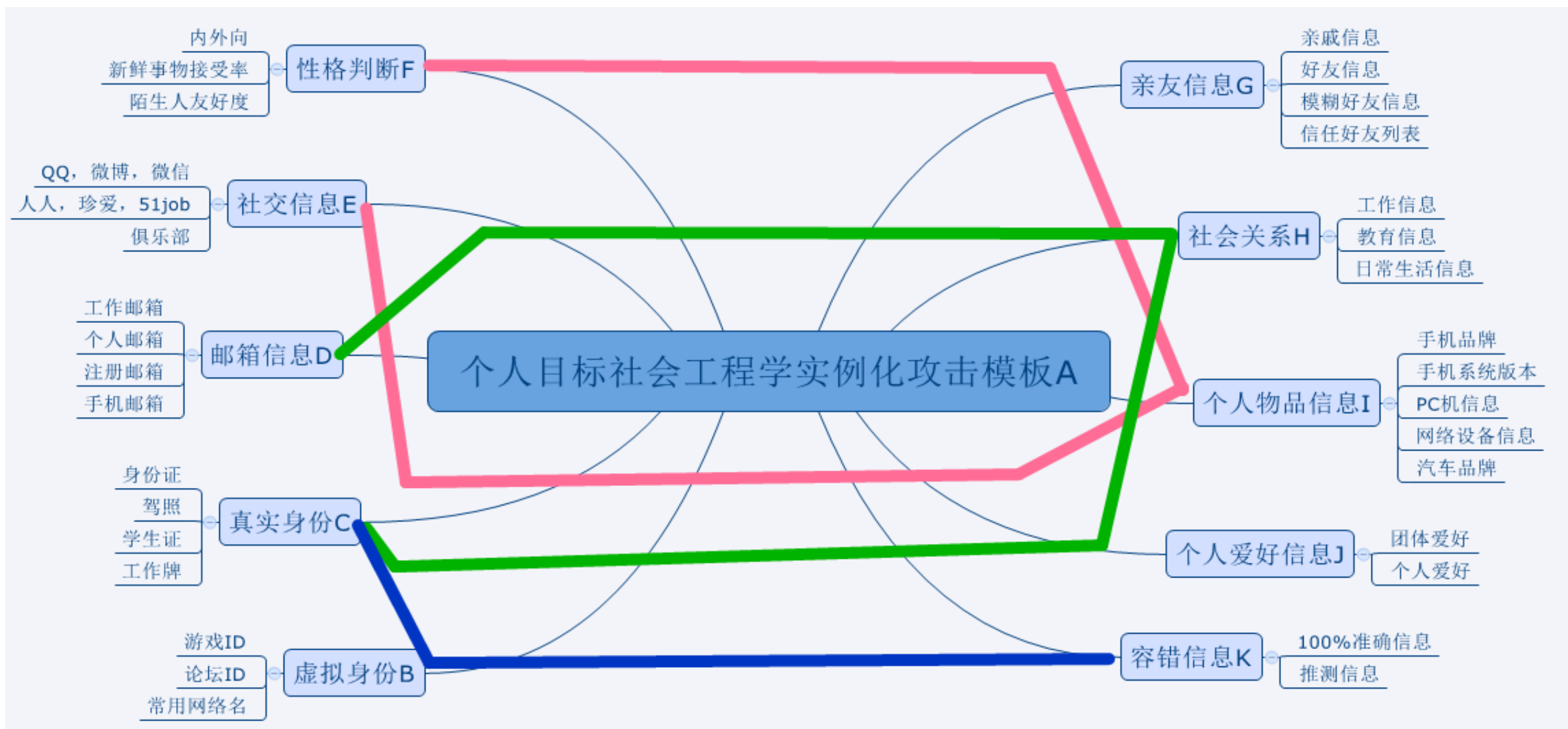
针对站点的实例化攻击模板（极简版）



针对个人目标的实例化攻击模板（极简版）



针对个人目标的实例化攻击模板（极简版）



社会工程学证据链实例化的小例子

没有应该有清晰的寻找渠道，而不仅仅停留在没有



现实容错判定条件:

GPS信息, 社交活动, 照片地标或景点, IP范围

第二层泛型拓展:

社交关系, 关注人群, @的人, 访客记录, 日志, 说说

第一层蛛网模式拓展:

社保卡, 市民卡, 火车票, 邮箱, 用户名

最终要获取或落地的信息:

身份证号, 驾照, 手机号, 户口, 姓名

谢谢大家

THANK YOU FOR YOUR ATTENTION



黑客叔叔p0tt1



p0tt1@foxmail.com