渗透那点事儿

PPTV聚力-security(向红阳)

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- PPTV聚力 安全负责人
- 微博:http://weibo.com/hongygxiang
- 议题大纲:
  - 基于运维平台渗透测试
  - 渗透需要注意的(个人观点)
  - Zenoss穿透优酷土豆内网
  - zabbix渗透搜狗&搜狐
  - LB日志在PPTV的处理

运维自动化发展很快

OWASP 中国
The Open Web Application Security Project

- 运维---自动化---标准化---模块化
  引出一系列现代化开源工具
- Zabbix
- Puppet
- Zenoss
- Openldap
- Cmdb
- Cacti
- Nagos
- CTL
- 这些东西的出现，在从运维的角度来看极大的方便了运维工作，同时也方便了广大黑客的工作

黑客之所以选择它们也有说道

OWASP 中国
The Open Web Application Security Project

- 一般情况下，这样的服务器可通往任意一个server无论内外网(做代理不错,运气好点可能直接通往办公内网)
- 脚本较多,配置文件多,里面可能会有密码(如邮件密码)
- 信息量大，IP信息,机房分布可能都在里面
- 其他,

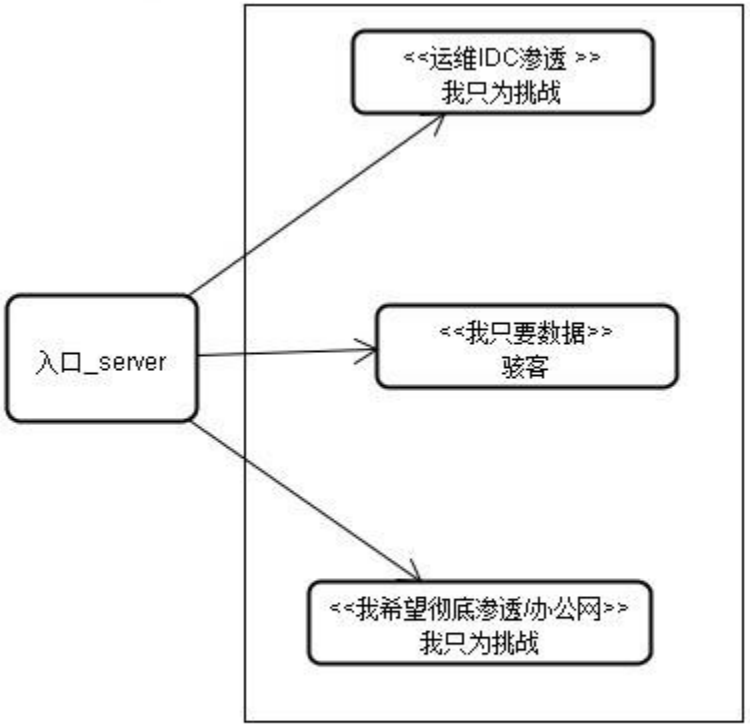
入口服务器也很讲究
(有些细节很重要)

OWASP 中国
The Open Web Application Security Project

- 入口服务器,尽量取得最高权限
- 信息收集最大化
- 仔细观察一切,根据自己的观察罗列适合此次渗透到密码字典
- 收集到的任何密码,请保留
- 你需要一个代理(内网可能用到端口转发)
- 发挥任何一个可用跳板，将信息挖掘最大化

每一次的渗透都带着相应目的

(你的目的是什么？)



目的

无论你的目的是什么，每次都渗透都会怀着相应的目的

Zenoss穿透优酷土豆内网
(我和wooyun X,D很熟)

OWASP 中国
The Open Web Application Security Project

从一个默认口令到youku和tudou内网

已公开漏洞

踩点:

```
正在 Ping youku.com [123.126.99.31] 具有 32 字节的数据:
来自 123.126.99.31 的回复: 字节=32 时间=40ms TTL=239
来自 123.126.99.31 的回复: 字节=32 时间=42ms TTL=239
来自 123.126.99.31 的回复: 字节=32 时间=46ms TTL=239
来自 123.126.99.31 的回复: 字节=32 时间=45ms TTL=239

123.126.99.31 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 40ms, 最长 = 46ms, 平均 = 43ms
```

C段入手，得到入口服务器

找到Zenoss
(你的监控系统对外了吗？)

OWASP 中国
The Open Web Application Security Project

修改默认命令
(其实很多监控工具都有这个功能)

OWASP 中国
The Open Web Application Security Project

- 可以执行任意命令，理所当然,得到了目标服务器的shell

```
bash: no job control in this shell
tty:[←[1;36mtty←[0m] jobs:[←[1;36m0←[0m] cwd:[←[1;36m/opt/zenoss←[0m]
15:59 [zenoss@a20.monitor.zenoss.b28.youku]$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:22:19:52:1b:86 brd ff:ff:ff:ff:ff:ff
    inet 211.151.50.167/24 brd 211.151.50.255 scope global eth1
    inet 61.135.196.191/24 brd 61.135.196.255 scope global eth1:1
    inet 220.181.52.168/24 brd 220.181.52.255 scope global eth1:2
    inet 220.181.185.197/25 brd 220.181.185.255 scope global eth1:3
    inet 123.126.99.77/24 brd 123.126.99.255 scope global eth1:5
    inet6 fe80::222:19ff:fe52:1b86/64 scope link
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:22:19:52:1b:88 brd ff:ff:ff:ff:ff:ff
    inet 10.103.11.20/24 brd 10.103.11.255 scope global eth0
    inet6 fe80::222:19ff:fe52:1b88/64 scope link
       valid_lft forever preferred_lft forever
tty:[←[1;36mtty←[0m] jobs:[←[1;36m0←[0m] cwd:[←[1;36m/opt/zenoss←[0m]
```

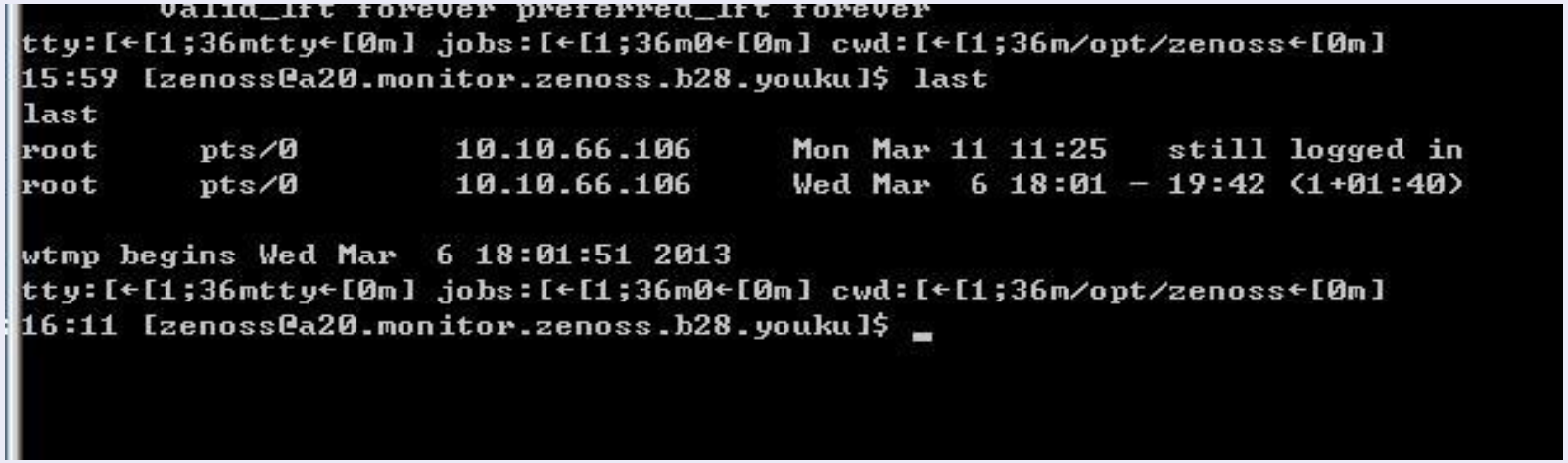
先看看我们有什么
(渗透过程中先看自己有什么,再去创造没有的)

- 信息量比较大
- 可通往所有内外网服务器
- Lib降权了,提权蛋疼了
- 没有zabbix，puppet，ldap
- 代理? Lib被降权限,开代理报错
- Zenoss特性基于python的监控系统
- 来一个python socks5代理

别小看last

OWASP 中国
The Open Web Application Security Project

- Last 记录很重要



IP 10.10.66.106,先不管他是干什么的既然是登录来源IP,肯定有点文章

接下来你该怎么办？

渗透过程中扫描是少不了的
(扫描监控,异常登录需监控)

OWASP 中国
The Open Web Application Security Project

- nmap -Sv -p 1433 10.10.0.0/16 -oX 1433log.log(当然你可以扫其他的端口)
- 1433在内网很多弱口令？
- 通过代理手动测试弱口令
- 目前为止暂未掌握有价值的密码信息
- 10.10.111.100 sa 空密码 (为什么是空口令?)
- linux+windows 渗透很方便
- 代理很不稳定(因为不是直接代理)
- 可以创造条件

接下来你会想什么？

- 远程管理卡？
- 10.105.*.* 有外网IP(用它做代理,我有root)
- 有一个方便的中转服务器很重要
  -方便信息收集
- 根据自己的所见制作适合此次渗透的密码字典

信息收集

- 10.5.*.* ？
- 1qaz2wsx
- 加域的server都在10.10.0.* 这个段，(当然，最后AD服务器确实在其中,这都是后话)
- 当然还有多很其他的
- 你的定位直接影响到这次成功与失败
- 下面该做什么？
- 找个域成员服务器?拿下权限？

域环境下面的一些特性
(你有没有这些毛病)

OWASP 中国
The Open Web Application Security Project

- 通病

1. windows特性之一有些服务运行必须管理在线,不得不说管理员也是懒的不喜欢注销在线用户,往往选择更方便的操作,直接断开(而不是注销)或许他们忘了shift后门可以直接切过去
2. AD策略域成员服务器管理员密码往往是统一的,(别说你不是的)

Hash是很容易得到的,没LM破解是困难的

找准目标,向目标出发
(域成员服务器-->域服务器)

OWASP 中国
The Open Web Application Security Project

- 10.10.0.13(域成员服务器,OA)
- 通过自己收集的密码字典获取到管理员权限(sa口令:1QAZ2wsx 乌云有)
- 10.10.0.13 直接shift后门(因为有管理员在线处于断开状态)
- 它是域管理员
- 直接连接至域服务器,再次开启shift后门

End

OWASP 中国
The Open Web Application Security Project

- PPT还没完
- 猥琐的人们有后续
- X,D提交了，
- X,D告诉大家仅供学习,研究讨论，切记别做违法犯罪的事情。

zabbix渗透搜狗&搜狐

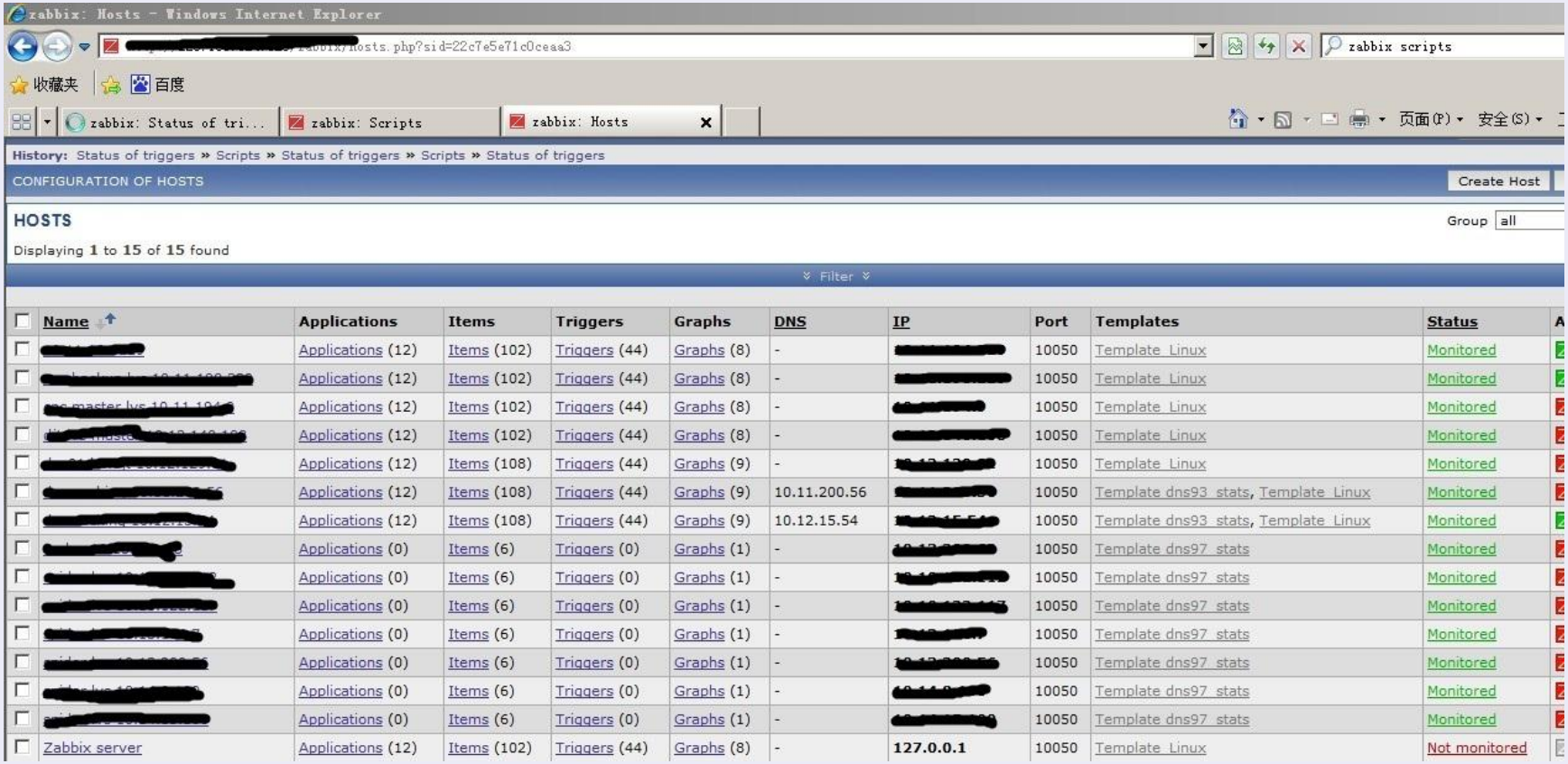
(X,D被鄙视了)

OWASP 中国
The Open Web Application Security Project

- 看我是如何利用zabbix渗透sogou&sohu内网的
- http://220.181.*.128/zabbix/
- Zabbix 对外,而且存在默认口令
- 并没有sysrun.run模块(添加了一个items直接使用system.run 跑了一个命令，没有数据返回，确定zabbix agent没有开启system.run 模块)
- 接下来你会想什么,首次发现zabbix有神一样的功能
- 请仔细阅读zabbix文档,X,D英文不好读了大半个晚上才搞定

熟悉的界面
（熟悉的东西总会有惊喜）

OWASP 中国
The Open Web Application Security Project



zabbix: Hosts - Windows Internet Explorer

[redacted]hosts.php?sid=22c7e5e71c0ceaa3

zabbix scripts

收藏夹 百度

zabbix: Status of tri... | zabbix: Scripts | zabbix: Hosts

页面(P) 安全(S)

History: Status of triggers » Scripts » Status of triggers » Scripts » Status of triggers

CONFIGURATION OF HOSTS

Create Host

HOSTS

Group all

Displaying **1** to **15** of **15** found

Filter

☐	Name	Applications	Items	Triggers	Graphs	DNS	IP	Port	Templates	Status	A
☐	[redacted]	Applications (12)	Items (102)	Triggers (44)	Graphs (8)	-	[redacted]	10050	Template_Linux	Monitored	🟩
☐	[redacted]	Applications (12)	Items (102)	Triggers (44)	Graphs (8)	-	[redacted]	10050	Template_Linux	Monitored	🟩
☐	[redacted]	Applications (12)	Items (102)	Triggers (44)	Graphs (8)	-	[redacted]	10050	Template_Linux	Monitored	🟥
☐	[redacted]	Applications (12)	Items (102)	Triggers (44)	Graphs (8)	-	[redacted]	10050	Template_Linux	Monitored	🟥
☐	[redacted]	Applications (12)	Items (108)	Triggers (44)	Graphs (9)	-	[redacted]	10050	Template_Linux	Monitored	🟥
☐	[redacted]	Applications (12)	Items (108)	Triggers (44)	Graphs (9)	10.11.200.56	[redacted]	10050	Template dns93_stats, Template_Linux	Monitored	🟥
☐	[redacted]	Applications (12)	Items (108)	Triggers (44)	Graphs (9)	10.12.15.54	[redacted]	10050	Template dns93_stats, Template_Linux	Monitored	🟩
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	[redacted]	Applications (0)	Items (6)	Triggers (0)	Graphs (1)	-	[redacted]	10050	Template dns97_stats	Monitored	🟥
☐	Zabbix server	Applications (12)	Items (102)	Triggers (44)	Graphs (8)	-	127.0.0.1	10050	Template_Linux	Not monitored	☐

Shell
(这是一个入口服务器)

- 不拿shell对不起X,D大半夜的辛苦
- 注意看红框

触发修改后的命令


ZABBIX
Monitoring
Inventory
Reports
Configuration
Administration
Dashboard
Overview
Web
Latest data
Triggers
Events
Graphs
Screens
Maps
Discovery
History: Configuration of host groups » Dashboard » Configuration of host groups » Configuration of scripts » Dashboard
LATEST DATA
Items
Filter
Show items with name like
Show items without data
Host
Name
Last check
Zabbix server
CPU (13 Items)
Zabbix server
Filesystems (25 Items)
Zabbix server
General (5 Items)
Zabbix server
Memory (5 Items)
Zabbix server
Network interfaces (6 Items)
点下这个就可以 调用命令了。
www.wooyun.org

惊喜部分

OWASP 中国
The Open Web Application Security Project

- 下面有惊喜
- Shell在手一切都有

```
/search]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether aa:aa:aa:c3:40:42 brd ff:ff:ff:ff:ff:ff
    inet [illegible]/22 brd 10.12.7.255 scope global eth0
    inet [illegible]/22 scope global secondary eth0
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether aa:aa:aa:c3:40:43 brd ff:ff:ff:ff:ff:ff
    inet [illegible]/22 brd 10.14.7.255 scope global eth1
    inet [illegible]/22 scope global secondary eth1
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether aa:aa:aa:c3:40:44 brd ff:ff:ff:ff:ff:ff
    inet [illegible]/24 brd 220.181.124.255 scope global eth2
[za[illegible] /search]$
```

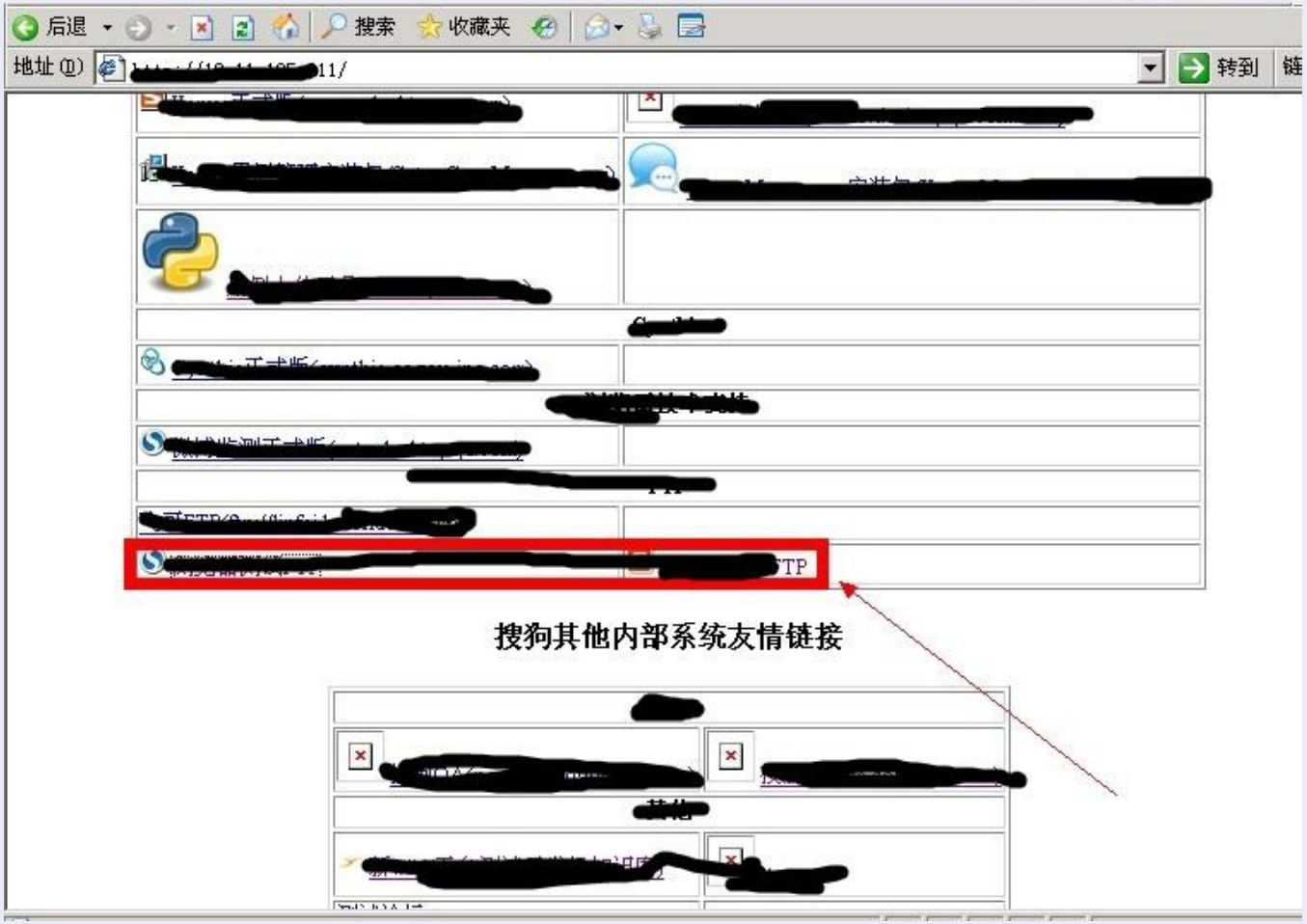
接下来？

OWASP 中国
The Open Web Application Security Project

- Root
- 代理(有外网有内网)
- 8080端口没被墙而且没被占用
- 开一个8080端口socks5代理
- 开始信息收集

内网很多东西没有认证（警惕）

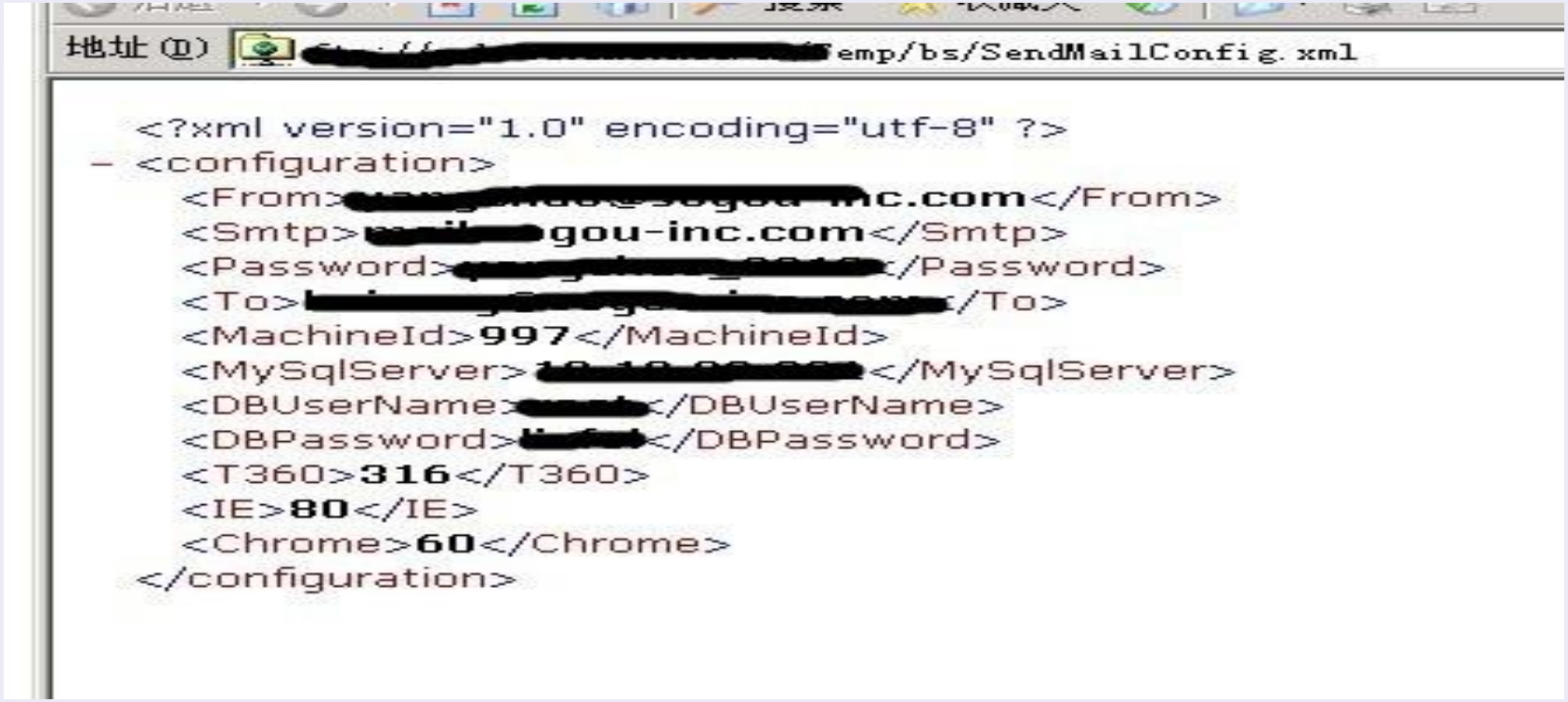
OWASP 中国
The Open Web Application Security Project



配置文件有秘密
(看别人邮箱不厚道)

OWASP 中国
The Open Web Application Security Project

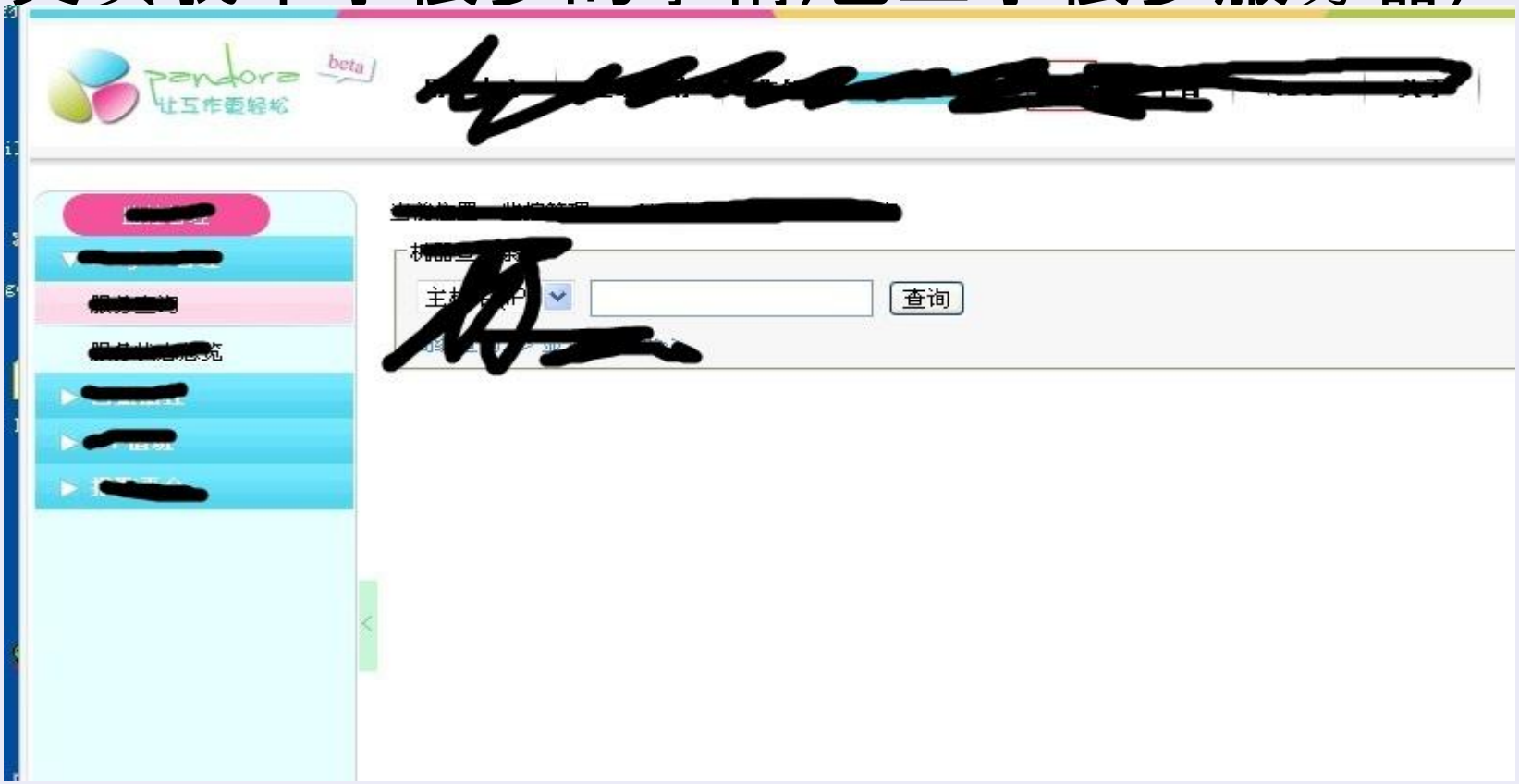
- 员工的邮箱密码,其实在过往邮件里面找到了他们常用密码(后续更精彩)



其他

OWASP 中国
The Open Web Application Security Project

- 其实我干了很多的事情,也上了很多服务器,



后续

- 有了很多信息之后,拿下域内一台域成员服

结果 | 消息

	output
1	NULL
2	主机名: SOHU-VT5KDAUSHF
3	OS 名称: Microsoft(R) Windows(R) Server 2003, Enterprise Edition
4	OS 版本: 5.2.3790 Service Pack 2 Build 3790
5	OS 制造商: Microsoft Corporation
6	OS 配置: 独立服务器
7	OS 构件类型: Multiprocessor Free
8	注册的所有人: sohu
9	注册的组织: sohu-inc
10	产品 ID: 69713-640-9722366-45937
11	初始安装日期: 2011-12-8, 14:35:37
12	系统启动时间: 283 天 11 小时 16 分 4 秒

哪些事

OWASP 中国
The Open Web Application Security Project

- 1,入口服务器

  尽量获取最高权限

  信息挖掘最大化
- 2,了解自己已有的资源,挖掘自己没有的资源
- 3，多方位思考,越是边缘性的东西越容易被忽略同时危害也不容小视
- 4,尽全力收集任何信息,无论是一个不起眼密码还是配置信息
- 5,运维系统有文章，很多安全问题被忽略
- 6,渗透测试切勿带着不法目的.

下面是花絮

OWASP 中国
The Open Web Application Security Project

- Sudoers 配置错误,方便黑客。(注意观察)

```
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DR

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
[redacted]      ALL=NOPASSWD: /sbin/ethtool
[redacted]      ALL=NOPASSWD: /usr/l[redacted].sh
```

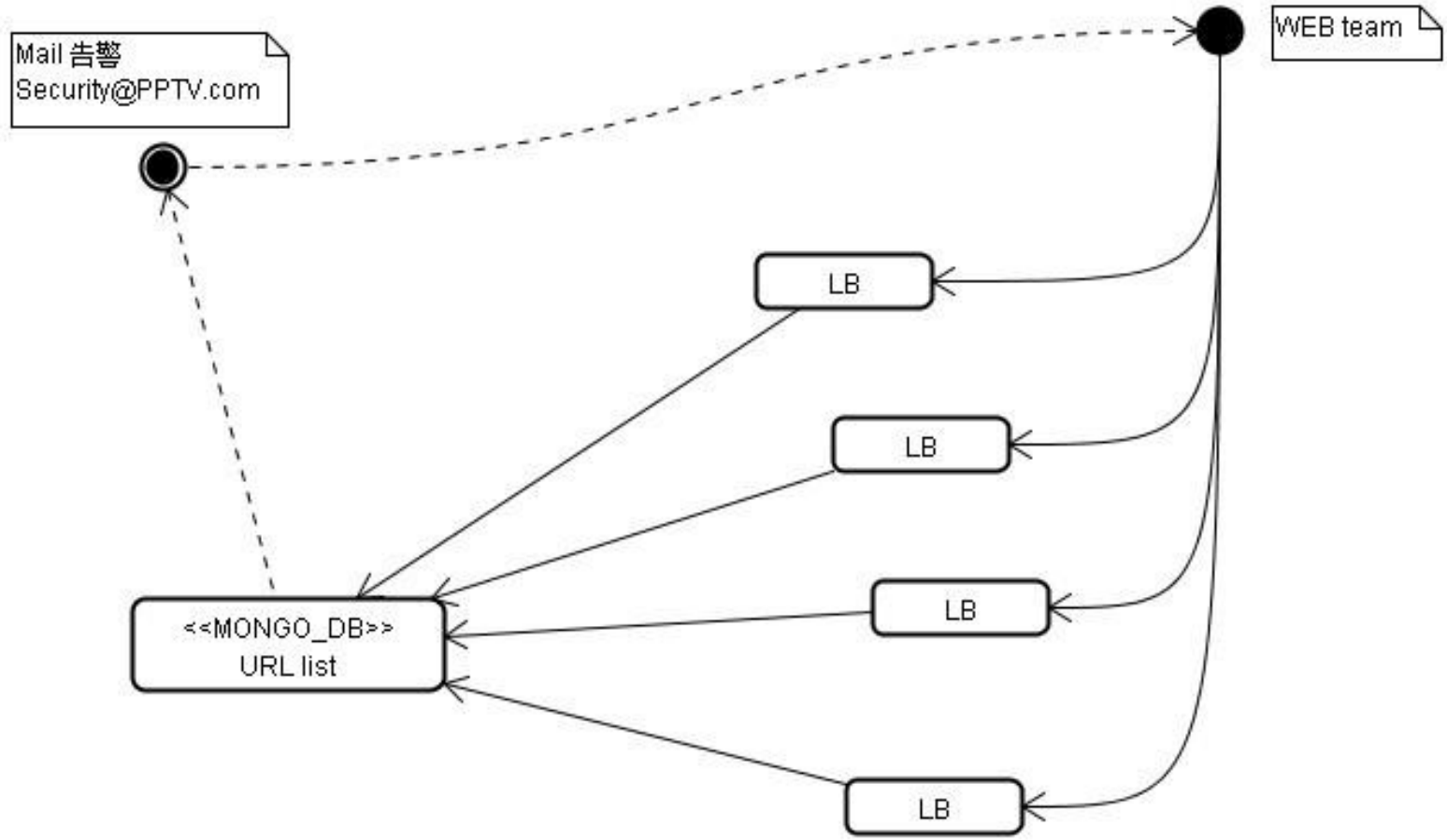
PPTV security 一小部分

(PPTV的安全架构之LB日志分析)

OWASP 中国
The Open Web Application Security Project

```
[redacted].pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20char_length(cast(count(*)%20as%
/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20char_length(cast(count(*)%20as%
/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20char_length(cast(count(*)%20as%
/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
’=’1 HTTP/1.1
.pptv.com 120.33.18.133 GET /vmei/xs?team=yellow’%20and%20(select%20ascii(substring(cast(count(*)%2
```

如何实现？


Mail 告警
Security@PPTV.com
WEB team
LB
LB
LB
LB
<<MONGO_DB>>
URL list

- The End