运维平台渗透&PPTV安全架构分享

---PPTV security –向红阳
(hongygxiang)

安全不是看你做了多少，而是看你漏了多少!

给我一个支点,我能撬起整个地球!

图片(木桶原理)

运维安全

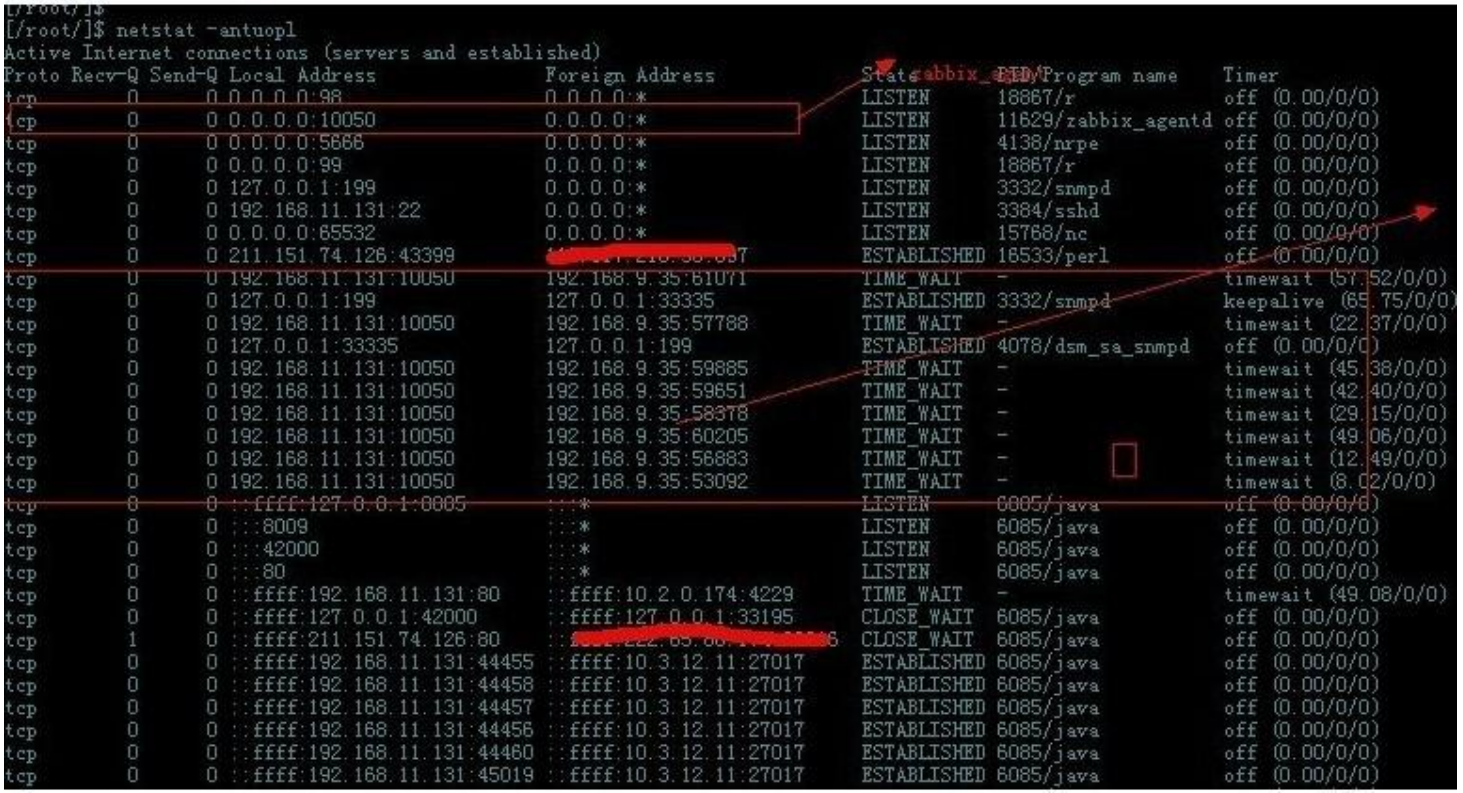
- 人是懒的，无论是运维工程师还是黑客！
- 如今运维逐步走向标准化,自动化,模块化，zabbix，puppet，open ldap，CTL，cmdb，cacti等各种开源工具，极大的方便了上规模的运维工作，节约运维成本。黑客也可以利用这些控制线上所有服务器。
- 自动化运维后面也突显了很多的安全问题,你的访问控制做好了吗?你的口令足够强吗?版本漏洞都补了吗?

原本方面运维的工具，出现问题后？

- 1、zabbix 添加监控项，执行任意命令?
- 2、puppet配置文件管理，执行任意命令?
- 3、open ldap 无敌权限?
- 4、CTL 执行任意脚本?
- 5、cmdb/cacti 等大量敏感信息泄露?
- 任意一个环节都有可能导致线上所有服务器沦陷

58.Com从web漏洞到线上所有服务器沦陷

- 漏洞源头Struts2命令执行 http://211.151.74.126/ root权限(省去了提权)



```
412  2012-03-31 15:51:35 kill 5722
413  2012-03-31 15:51:45 ps -ef | grep tomcat
414  2012-03-31 15:51:57 /opt/soft/tomcat/bin/startup.sh
415  2012-03-31 15:51:59 ps -ef | grep tomcat
416  2012-03-31 15:52:29 ps -ef | grep tomcat
417  2012-03-31 15:52:35 netstat -ntl
418  2012-03-31 15:52:57 tail -300 /opt/soft/tomcat/logs/catalina.out
419  2012-04-04 02:47:44 netstat -ntl
420  2012-04-10 19:00:42 sh /home/gx_58op.sh;exit 0
421  2012-04-11 15:54:30 cd /home/ && wget http://192.168.9.35/matl.tar.gz && tar -xvf matl.tar.gz -C /home && cd /home/matl && sh client.sh;exit 0
422  2012-04-11 17:03:21 cd /home/ && wget http://192.168.9.35/zabbix/matl.tar.gz && tar -xvf matl.tar.gz -C /home && cd /home/matl && sh client.sh;exit 0
423  2012-04-11 18:05:39 top
424  2012-04-11 18:05:42 ls
425  2012-04-11 18:05:44 ext
426  2012-04-11 18:05:45 exit
427  2012-04-12 10:22:28  rm -rf /home/matl.tar.gz* && wget http://192.168.9.35/zabbix/matl.tar.gz -P /home && tar -xvf /home/matl.tar.gz -C /home && cd /home/ma
anduan.sh;exit 0
428  2012-04-16 17:50:30 ls
429  2012-04-16 17:50:37 ls /opt/web/
430  2012-04-16 17:51:07 cd /opt/web/
431  2012-04-16 17:51:07 ls
432  2012-04-16 17:51:21 cd /opt/soft/tomcat/logs/catalina.out
433  2012-04-16 17:51:25 cd /opt/soft/tomcat/logs/
434  2012-04-16 17:51:27 ll -h
435  2012-04-16 17:51:55 ls
```

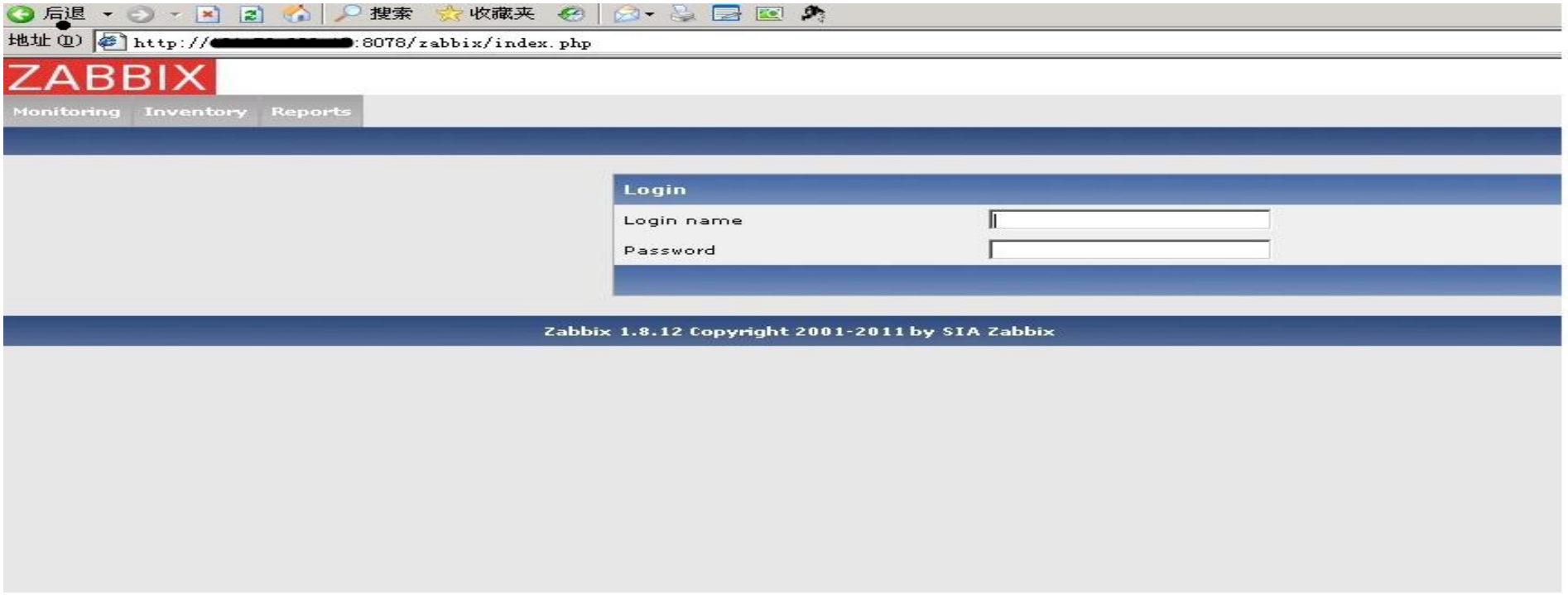
zabbix 其实端口就能看出来了，但是我curl下返回一个404，因为我不知道路径，上面history貌似告诉我了；nmap -sV -open 192.168.9.35

```
[root@CT11131 ~]#
[root@CT11131 ~]# nmap -sV -open 192.168.9.35

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2012-10-13 05:28 CST
Interesting ports on 192.168.9.35:
Not shown: 1677 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     (protocol 2.0)
80/tcp   open  http?
3306/tcp open  mysql   MySQL (unauthorized)
2 services unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprints at http://www.insecure.org/cgi-bin/ser
vicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=4.11%I=7%D=10/13%Time=50788B86%P=x86_64-redhat-linux-gnu%r
SF:(NULL,15,"SSH-2\.0-OpenSSH_5\.8\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=4.11%I=7%D=10/13%Time=50788B86%P=x86_64-redhat-linux-gnu%r
SF:(GetRequest,157,"HTTP/1\.1\x20403\x20Forbidden\r\nServer:\x20nginx\r\nD
SF:ate:\x20Fri,\x2012\x20Oct\x202012\x2021:28:38\x20GMT\r\nContent-Type:\x
SF:20text/html;\x20charset=utf-8\r\nContent-Length:\x20162\r\nConnection:\
```

- curl http://192.168.3.95/zabbix/ 返回了zabbix的登陆界面

- 机器是内网无外网IP,iptables做nat显然不太现实，最后选择了端口转发
- 推荐工具lcx(linux),或者rtcp.py(python)。


后退
搜索
收藏夹
地址(D)
http://[redacted]:8078/zabbix/index.php
ZABBIX
Monitoring
Inventory
Reports
Login
Login name
Password
Zabbix 1.8.12 Copyright 2001-2011 by SIA Zabbix


后退
搜索
收藏夹
地址(D)
http://[redacted]:8078/zabbix/srv_status.php
ZABBIX
状态统计
资产记录
系统评估
系统配置
高级配置
Dashboard | 总览 | Web | 最新数据 | 触发器 | 事件 | 图形显示 | 配置图表 | 拓扑图 | 自动发现 | 服务 |
访问记录: 审计 » 主机 » 主机组 » 主机 » 服务
IT服务
IT服务
服务
状态
Reason
SLA (最近7天)
root
Zabbix 1.8.12 Copyright 2001-2011 by SIA Zabbix

- Zabbix Default login

User:admin Pass:zabbix

名称	#	成员
admin servers	模板 (14) 主机 (3)	check http page, check ip port, hardware, http80, infolist WEB, Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50lo 10.4.10.27, 192.168.9.35, 192.168.9.35 test → ZAbbix_SERVER也在这里，这个我感觉很危险
check ip port	模板 (0) 主机 (18)	10.4.11.20, 192.168.11.11, 192.168.11.12, 192.168.11.21, 192.168.11.72, 192.168.11.79, 192.168.11.90, 192.168.11.97, 192.168.11. 192.168.11.172, 192.168.14.21, 192.168.14.208, 192.168.14.209, 192.168.14.210, 192.168.14.211
DBSERVER	模板 (4) 主机 (148)	Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 10.3.11.11, 10.3.11.12, 10.3.11.13, 10.3.11.14, 10.3.11.15, 10.3.11.16, 10.3.11.17, 10.3.11.18, 10.3.11.19, 10.3.11.20, 10.3.11.21, 1 10.3.13.16, 10.3.13.17, 10.3.13.26, 10.4.12.11, 10.4.12.12, 10.4.12.13, 10.4.12.14, 10.4.12.15, 10.4.12.16, 10.4.12.17, 10.4.12.18, 1 10.4.12.24, 10.4.12.25, 10.4.12.26, 10.4.12.27, 10.4.12.28, 10.4.12.29, 10.4.12.30, 10.4.12.31, 10.4.12.32, 10.4.12.33, 10.4.12.34, 1
Discovered hosts	模板 (4) 主机 (0)	Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load
infolist	模板 (5) 主机 (25)	infolist WEB, Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 192.168.9.42, 192.168.9.58, 192.168.9.59, 192.168.9.61, 192.168.9.92, 192.168.9.122, 192.168.9.163, 192.168.9.165, 192.168.9.170 192.168.9.175, 192.168.9.176, 192.168.9.177, 192.168.9.178, 192.168.9.179, 192.168.9.180, 192.168.9.181, 192.168.9.182, 192.168
JBOSS	模板 (4) 主机 (32)	Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 192.168.9.110, 192.168.9.111, 192.168.9.113, 192.168.9.128, 192.168.11.26, 192.168.11.27, 192.168.11.28, 192.168.11.29, 192.168 192.168.11.59, 192.168.11.60, 192.168.11.61, 192.168.11.62, 192.168.11.76, 192.168.11.77, 192.168.11.78, 192.168.11.92, 192.168 192.168.11.104, 192.168.11.105, 192.168.11.106, 192.168.11.125, 192.168.11.126, 192.168.11.127, 192.168.11.128, 192.168.11.129
L-IMC	模板 (4) 主机 (26)	Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 10.4.11.20, 10.4.11.21, 10.4.11.22, 10.4.11.23, 192.168.9.39, 192.168.9.112, 192.168.9.117, 192.168.9.118, 192.168.9.119, 192.168. 192.168.11.64, 192.168.11.86, 192.168.11.87, 192.168.11.88, 192.168.11.91, 192.168.11.120, 192.168.11.121, 192.168.11.204, 192. 192.168.11.238
OP	模板 (6) 主机 (545)	hardware, Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load, network traffic 10.3.10.15, 10.3.10.16, 10.3.10.17, 10.3.10.18, 10.3.10.19, 10.3.10.20, 10.3.10.30, 10.3.10.32, 10.3.10.33, 10.3.10.34, 10.3.10.35, 1 10.3.10.51, 10.3.10.52, 10.3.10.53, 10.3.10.60, 10.3.10.61, 10.3.11.11, 10.3.11.12, 10.3.11.13, 10.3.11.14, 10.3.11.15, 10.3.11.16, 1 10.3.11.22, 10.3.11.23, 10.3.11.24, 10.3.11.25, 10.3.11.27, 10.3.11.28, 10.3.11.29, 10.3.11.30, 10.3.11.31, 10.3.11.32, 10.3.11.40, 1
Templates	模板 (3) 主机 (0)	Linux 400processes 50load, Template FromDual.MySQL.innodb, Template Zabbix Server
tuangou	模板 (4) 主机 (26)	Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 10.3.13.13, 10.3.13.18, 10.3.13.19, 10.3.13.20, 10.3.13.21, 10.3.13.22, 10.3.13.27, 10.3.13.28, 10.3.13.29, 10.3.13.30, 10.3.13.31, 1

Tom在线,远程管理卡问题，全部核心服务器沦陷
http://www.wooyun.org/bugs/wooyun-2010-014101

```
ir -p /etc/zabbix
..
[ -f /etc/SuSE-release ]
then
  cp zabbix-1.8/misc/conf/zabbix_agentd.conf /etc/zabbix/
  cp zabbix-1.8/misc/init.d/suse/9.3/zabbix_agentd /etc/init.d/
  sed -i "s/\/opt\/zabbix\/bin/\/usr\/local\/sbin/g" /etc/init.d/zabbix_agentd
  sed -i "s/Server\=127\.0\.0\.1/Server\=172\.24\.162\.38/g" /etc/zabbix/zabbix_agentd.conf
  chkconfig --add zabbix_agentd

[ -f /etc/debian_version ]
then
 cp zabbix-1.8/misc/conf/zabbix_agentd.conf /etc/zabbix/
```

zabbix_Server


```
root@yypdtelecomweb01:/# ping -c5 172.24.162.38
ping -c5 172.24.162.38
PING 172.24.162.38 (172.24.162.38) 56(84) bytes of data.
64 bytes from 172.24.162.38: icmp_req=1 ttl=62 time=0.686 ms
64 bytes from 172.24.162.38: icmp_req=2 ttl=62 time=0.571 ms
64 bytes from 172.24.162.38: icmp_req=3 ttl=62 time=0.650 ms
64 bytes from 172.24.162.38: icmp_req=4 ttl=62 time=0.606 ms
64 bytes from 172.24.162.38: icmp_req=5 ttl=62 time=0.671 ms

--- 172.24.162.38 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.571/0.636/0.686/0.053 ms
root@yypdtelecomweb01:/#
```

- curl http://172.24.162.38/zabbix/ #返回的是zabbix登陆页

```
root@yypdtelecomweb01:/# curl http://172.24.162.38/zabbix/
curl http://172.24.162.38/zabbix/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3465  100  3465    0     0  23664      0 --:--:-- --:--:-- --:--:-- 23896
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.or
g/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>ZABBIX</title>
        <meta name="Author" content="ZABBIX SIA" />
        <link rel="shortcut icon" href="images/general/zabbix.ico" />
        <link rel="stylesheet" type="text/css" href="css.css" />
<!--[if IE 6]>
        <script type="text/javascript" src="js/ie6fix.js"></script>
        <link rel="stylesheet" type="text/css" href="styles/ie.css" />
<![endif]-->

<script type="text/javascript"> var PHP_TZ_OFFSET = 28800;</script>
<script type="text/javascript" src="jsLoader.php?ver=1.8.6&lang=en_gb"></script>

</head>
<body onload="zbxCallPostScripts();">
<table class="page_header" cellspacing="0" cellpadding="5"><tr><td class="page_h
eader_l"><a class="image" href="http://www.zabbix.com/" target="_blank"><div cla
ss="zabbix_logo"> </div></a></td><td class="page_header_r" width="100%"><a
 class="small_font" href="http://www.zabbix.com/documentation/" target="_blank">H
elp</a>|<a class="small_font" href="http://www.zabbix.com/support.php" target="_
blank">Get support</a>|<a class="small_font" href="/zabbix/?print=1">Print</a>|<
```

先启一个端口，实现一个nat功能

```
root@yypdtelecomweb01:/tmp# netstat -antuopl | grep 98
netstat -antuopl | grep 98
tcp        0      0 0.0.0.0:98              0.0.0.0:*               LISTEN
26405/rinetd     off (0.00/0/0)
tcp6       0      0 172.24.203.157:80       115.215.164.45:35980    ESTABLISHED
28818/java       off (0.00/0/0)
tcp6       0      0 172.24.203.157:7985     172.24.203.162:21201    ESTABLISHED
28818/java       off (0.00/0/0)
tcp6       0      0 127.0.0.1:9889          127.0.0.1:80            ESTABLISHED
28818/java       off (0.00/0/0)
tcp6       0      0 127.0.0.1:80            127.0.0.1:18986         ESTABLISHED
28818/java       off (0.00/0/0)
tcp6       0      0 172.24.203.157:14843    172.24.203.160:1098     ESTABLISHED
28818/java       keepalive (9.28/0/0)
tcp6       0      0 127.0.0.1:80            127.0.0.1:27987         ESTABLISHED
28818/java       off (0.00/0/0)
tcp6       0      0 127.0.0.1:18986         127.0.0.1:80            ESTABLISHED
28818/java       off (0.00/0/0)
tcp6       0      0 127.0.0.1:62981         127.0.0.1:80            ESTABLISHED
28818/java       off (0.00/0/0)
```

主机组

后退 前进 [redacted]8080/zabbix/hostgroups.php?sid=9f2604 重新载入 停止 百度 <Ctrl+K> 截取整个网页 主页 意见反馈 恢复关闭的标签页(U) 火狐

访问最多 火狐官方站点 新手上路 常用网址

Acunetix Web Scanner | Start Scan | Abort Scan | Settings | Advanced | Scanner status: Idle.

pkg_yidong_db	模板 (2) 主机 (2)	check_3306, pdk_yingdong_db 172.24.210.200, 172.24.210.201
pkg_yidong_web	模板 (2) 主机 (5)	check_port_80, pkg_yidong_web 172.24.210.11, 172.24.210.12, 172.24.210.13, 172.24.210.14, 172.24.210.21
Templates	模板 (44) 主机 (0)	Template_3COM_3824, Template_3COM_4400, Template_AIX, Template_APC_Automatic_Transfer_Switch, Template_APC_Battery, Template_App_MySQL, Template_C375 Template_Cisco_837, Template_Cisco_877, Template_Cisco_2960, Template_Cisco_PIX, Template_Cisco_PIX515E, Template_Cisco_PIX_525, Template_Dell_OpenManage Template_Dell_PowerConnect_5224, Template_Dell_PowerConnect_5324, Template_Dell_PowerConnect_6248, Template_Dell_PowerEdge, Template_FreeBSD, Template_Hibernate, Template_HPUX, Template_HP_ColorLaserJet, Template_HP_InsightManager, Template_HP_Procurve, Template_IPMI_Sun_Fire_X4100_M2, Template_ Template_Linux, Template_MacOS_X, Template_Microsoft_Exchange_2003, Template_Microsoft_Exchange_2007, Template_Microsoft_SQLServer_2005, Template_NetScree Template_Netware, Template_OpenBSD, Template_Oracle, Template_pfSense, Template_SNMPv1_Device, Template_SNMPv2_Device, Template_Solaris, Template_Standa Template_Tomcat, Template_Tru64, Template_Windows, test_oracle
test	模板 (1) 主机 (0)	test
testa	模板 (3) 主机 (1)	check_port_80, mysqlping, testa 192.168.50.14
Tomlog	模板 (4) 主机 (11)	test, tomlog_default, tomlog_default_80, tomlog_tmp log_172.24.148.177, log_172.24.148.215, log_172.24.149.241, log_172.24.180.67, log_172.24.190.49, log_172.24.190.50, log_172.24.202.50, log_172.24.202.106, log_172.24.202.131, log_172.24.202.132, log_172.24.202.180
webmail	模板 (1) 主机 (18)	webmail webmail_172.24.165.43, webmail_172.24.165.44, webmail_172.24.173.117, webmail_172.24.173.118, webmail_172.24.173.119, webmail_172.24.173.215, webmail_172.24.173.216, webmail_172.24.173.217, webmail_172.24.173.218, webmail_172.24.180.126, webmail_172.24.180.127, webmail_172.24.201.219, webmail_172.24.201.220, webmail_172.24.201.221, webmail_172.24.201.222, webmail_172.24.201.223, webmail_172.24.202.206, webmail_172.24.202.207
Windows servers	模板 (0) 主机 (0)	-
Zabbix servers	模板 (0)	192.168.14.16, Zabbix Server

远程管理卡问题

- 远程管理很大意义解决了很多运维方面各种问题，节约维护成本
- 但是你的远程管理卡有没有直接跑公网上面？
- 你的远程管理卡默认口令改了吗？
- 联想远程管理卡跳过验证漏洞!

乌云白帽子 **hongygxiang** 提交于 2012/09/10

近期机房封网 ,很多企业都使用设备上的远程管理模块并设置复杂的密码进行安全的远程管理。但乌云白帽发现某厂商设备漏洞，即使更改了远程管理密码，黑客与管理员还是能携手登陆远程服务器，我此刻又相信爱情了， 联想服务器可能都会被入侵？

漏洞过程重放：

默认口令本身是一个问题，但是联想远程管理卡还有一处问题，基本上无解，口令无论怎么改都可以绕过。

这个是一台联想自己的服务器，核心业务，什么联想网盘，等等之类的东西都在上面。访问此接口可以开启java 管理客户端 ,无需密码，管理卡的权限吗。。。至高无上了，除了拥有系统权限外，还可以控制服务器硬件，比如远程装个操作系统啥的

奇艺几百台VOD服务器沦陷
http://www.wooyun.org/bugs/wooyun-2010-010166

问题出在远程管理卡这里，默认口令没有改tty timeuot时间没有设置！下面我发一部分可能不是很全，你们自己找吧

111.1.39.231
111.1.39.230
111.1.39.98
111.1.39.100
113.57.232.116
113.57.232.117
113.57.232.113
113.57.232.118
113.57.232.114
113.57.232.112
113.57.232.119
113.57.232.111
113.57.232.115
211.161.151.77
211.161.151.89
211.161.151.80
211.161.151.83
211.161.151.86
211.161.151.92
211.161.151.74
211.161.151.68
211.161.151.95

```
root     tty2                          Wed Jun 27 20:49   still logged in
root     pts/1        repo.qiyi.domain Tue Jun 26 17:52 - 17:53  (00:01)
root     pts/1        repo.qiyi.domain Wed Jun 20 17:56 - 18:00  (00:03)
root     pts/1        repo.qiyi.domain Wed Jun 20 15:22 - 15:57  (00:34)
root     pts/1        repo.qiyi.domain Wed Jun 20 15:19 - 15:21  (00:01)
root     pts/1        repo.qiyi.domain Wed Jun 20 14:23 - 14:53  (00:29)
root     pts/1        repo.qiyi.domain Mon Jun 18 21:01 - 22:01  (01:00)
root     tty1                          Mon Jun 18 16:37   still logged in
reboot   system boot  2.6.18-164.el5   Mon Jun 18 16:37          (37+21:29)
root     tty1                          Mon Jun 18 16:28 - down   (00:04)
root     pts/0        202.108.14.9     Mon Jun 18 23:38 - 16:05  (-7:-33)
root     pts/0        202.108.14.9     Mon Jun 18 23:17 - 23:37  (00:19)
root     pts/0        202.108.14.9     Mon Jun 18 22:57 - 23:16  (00:18)
root     pts/0        202.108.14.9     Mon Jun 18 22:50 - 22:55  (00:05)
root     pts/1        202.108.14.9     Mon Jun 18 22:48 - 22:49  (00:00)
root     pts/0        202.108.14.9     Mon Jun 18 22:41 - 22:49  (00:07)
reboot   system boot  2.6.18-164.el5   Sat Jun 16 04:34          (2+11:58)
root     pts/1        :0.0             Sat Jun 16 04:24 - down   (00:07)
root     :0                            Sat Jun 16 04:24 - down   (00:07)
root     :0                            Sat Jun 16 04:24 - 04:24  (00:00)
reboot   system boot  2.6.18-164.el5   Sat Jun 16 04:22          (00:08)
reboot   system boot  2.6.18-164.el5   Sat Jun 16 04:14          (00:04)

wtmp begins Sat Jun 16 04:14:20 2012
```

```
[root@localhost ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda2              29G  3.8G   24G  14% /
/dev/sda6             211G   37G  163G  19% /data
/dev/sda3              29G   23G  4.8G  83% /var
/dev/sda1              99M   12M   83M  13% /boot
tmpfs                  16G     0   16G   0% /dev/shm
/dev/sdb              932G  807G  125G  87% /data1
/dev/sdc              932G  808G  124G  87% /data2
/dev/sdd              932G  810G  123G  87% /data3
/dev/sde              932G  807G  126G  87% /data4
/dev/sdf              932G  824G  108G  89% /data5
/dev/sdg              932G  809G  124G  87% /data6
/dev/sdi              932G  806G  127G  87% /data7
/dev/sdj              932G  807G  125G  87% /data8
/dev/sdk              932G  809G  124G  87% /data9
/dev/sdl              932G  808G  124G  87% /data10
/dev/sdh              149G  125G   24G  84% /ssd
/dev/scd0             3.4G  3.4G     0 100% /R
[root@localhost ~]#
```

那么多存活的服务器,如何确定那个为远程管理卡IP?
(需要该脚本可邮件我。)

远程管理卡https协议，curl或wget 抓返回值,得到正确返回值后保存log,

破解密码很简单,按照破解常规ssh口令破解即可,远程管理卡跑公网的应该不多,打入内网之后渗透应该是条好渠道

Wget –S http://test

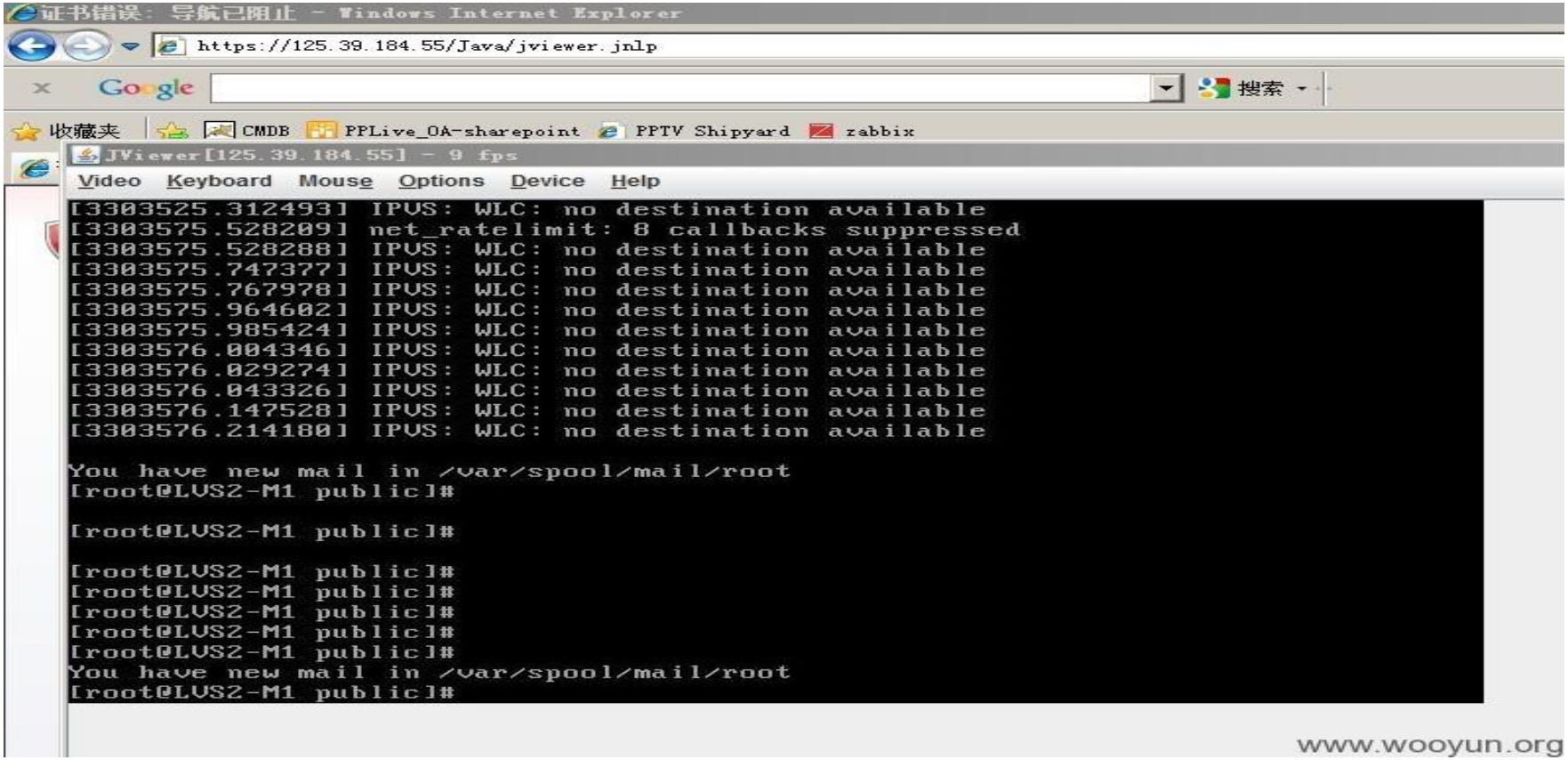
```
--2012-12-17 14:16:29--  https://
Connecting to .443... connected.
ERROR: cannot verify .140's certificate, issued by '/C=CN/ST=BEIJING/L=BEIJING/O=LENOVO/OU=LENOVO/CN=lenovo':
  Self-signed certificate encountered.
ERROR: certificate common name 'lenovo' doesn't match requested host name '.J'.
To connect to .10 insecurely, use '--no-check-certificate'.
Unable to establish SSL connection.
```

```
Mon Dec 17 14:15:28 CST 2012 .1 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default certi
ficate':
Mon Dec 17 14:15:28 CST 2012 .38 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default certi
ficate':
Mon Dec 17 14:15:28 CST 2012 .7 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default certi
ficate':
Mon Dec 17 14:15:28 CST 2012 .8 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default cert
ificate':
Mon Dec 17 14:15:28 CST 2012 .9 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default cert
ificate':
Mon Dec 17 14:15:28 CST 2012 5 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default certif
icate':
Mon Dec 17 14:15:27 CST 2012 9 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default certifi
cate':
Mon Dec 17 14:15:28 CST 2012 .7 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default cert
ificate':
Mon Dec 17 14:15:28 CST 2012 .1 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default cert
ificate':
Mon Dec 17 14:15:28 CST 2012 .3 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default cert
ificate':
Mon Dec 17 14:15:28 CST 2012 2 '/C=US/ST=Texas/L=Round Rock/O=Dell Inc./OU=Remote Access Group/CN=iDRAC6 default cert
ificate':
```

利用联想远程管理卡漏洞成功入侵联想核心服务器

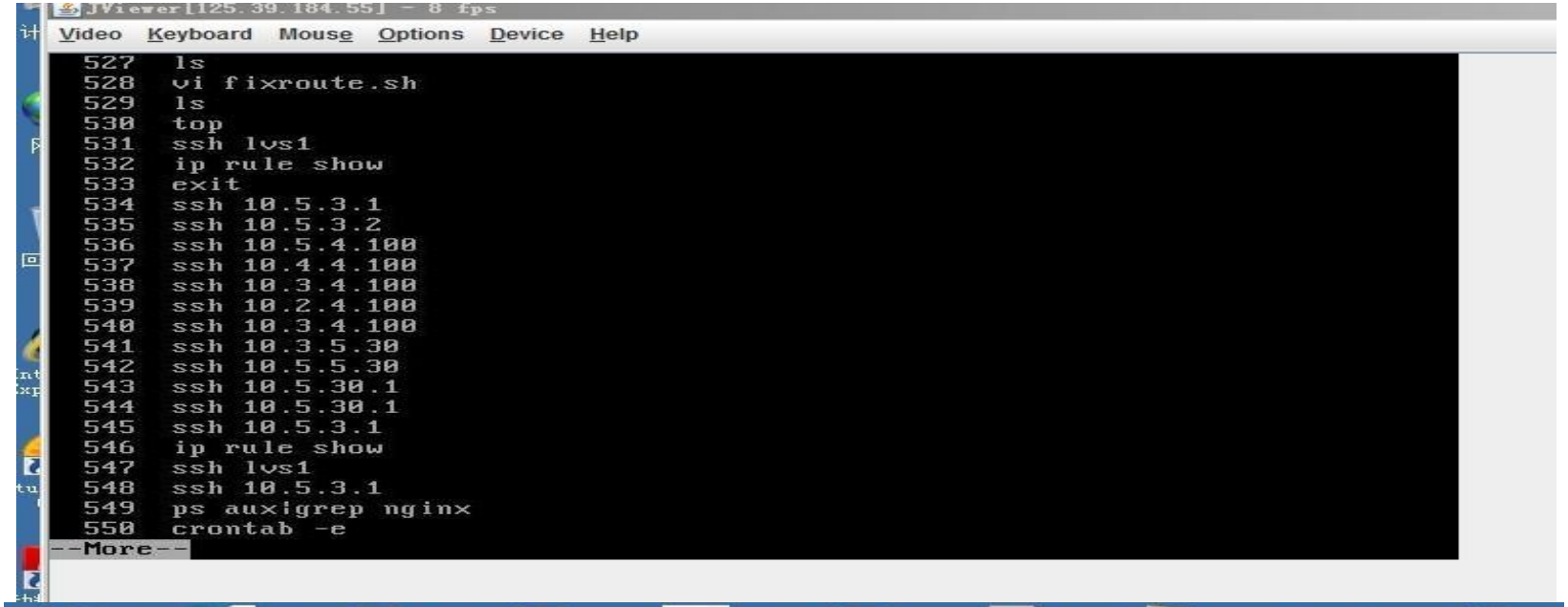
http://www.wooyun.org/bugs/wooyun-2010-012007

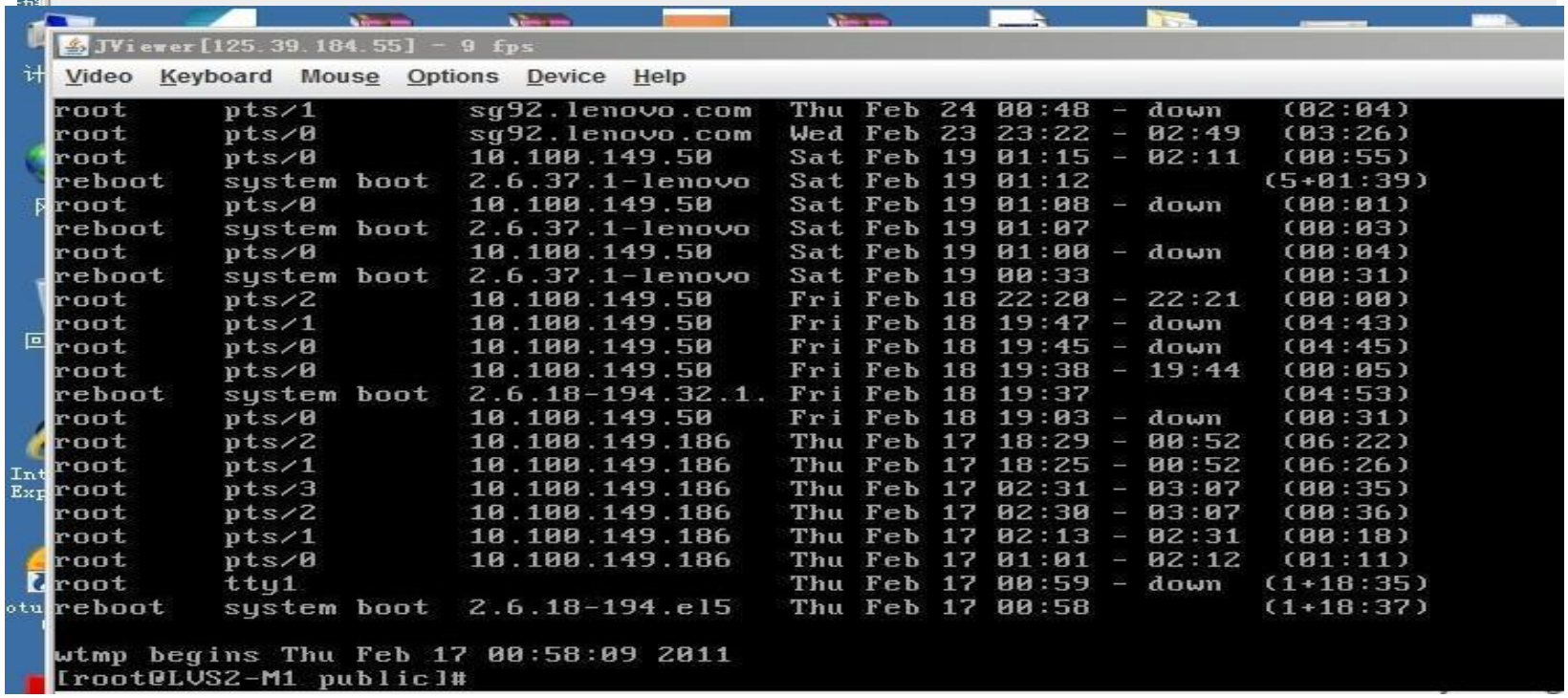
https://125.39.184.55/Java/jviewer.jnlp (简单跳过验证) 加上tty time没有设置直接直接获取到root 如下图:



很多人都是一样,使用了远程管理卡登陆之后不退出的,当这种情况遇到联想的远程管理卡漏洞,那就很无敌了(还是建议设置tty timeout 10分钟左右)

这个问题应该是联想忽略的一个问题,联想已出pach 但是更新此path比较麻烦估计没有几个人更新的


JViewer[125.39.184.55] - 8 fps
Video Keyboard Mouse Options Device Help
527 ls
528 vi fixroute.sh
529 ls
530 top
531 ssh lvs1
532 ip rule show
533 exit
534 ssh 10.5.3.1
535 ssh 10.5.3.2
536 ssh 10.5.4.100
537 ssh 10.4.4.100
538 ssh 10.3.4.100
539 ssh 10.2.4.100
540 ssh 10.3.4.100
541 ssh 10.3.5.30
542 ssh 10.5.5.30
543 ssh 10.5.30.1
544 ssh 10.5.30.1
545 ssh 10.5.3.1
546 ip rule show
547 ssh lvs1
548 ssh 10.5.3.1
549 ps aux|grep nginx
550 crontab -e
--More--


JViewer[125.39.184.55] - 9 fps
Video Keyboard Mouse Options Device Help
root pts/1 sg92.lenovo.com Thu Feb 24 00:48 - down (02:04)
root pts/0 sg92.lenovo.com Wed Feb 23 23:22 - 02:49 (03:26)
root pts/0 10.100.149.50 Sat Feb 19 01:15 - 02:11 (00:55)
reboot system boot 2.6.37.1-lenovo Sat Feb 19 01:12 (5+01:39)
root pts/0 10.100.149.50 Sat Feb 19 01:08 - down (00:01)
reboot system boot 2.6.37.1-lenovo Sat Feb 19 01:07 (00:03)
root pts/0 10.100.149.50 Sat Feb 19 01:00 - down (00:04)
reboot system boot 2.6.37.1-lenovo Sat Feb 19 00:33 (00:31)
root pts/2 10.100.149.50 Fri Feb 18 22:20 - 22:21 (00:00)
root pts/1 10.100.149.50 Fri Feb 18 19:47 - down (04:43)
root pts/0 10.100.149.50 Fri Feb 18 19:45 - down (04:45)
root pts/0 10.100.149.50 Fri Feb 18 19:38 - 19:44 (00:05)
reboot system boot 2.6.18-194.32.1. Fri Feb 18 19:37 (04:53)
root pts/0 10.100.149.50 Fri Feb 18 19:03 - down (00:31)
root pts/2 10.100.149.186 Thu Feb 17 18:29 - 00:52 (06:22)
root pts/1 10.100.149.186 Thu Feb 17 18:25 - 00:52 (06:26)
root pts/3 10.100.149.186 Thu Feb 17 02:31 - 03:07 (00:35)
root pts/2 10.100.149.186 Thu Feb 17 02:30 - 03:07 (00:36)
root pts/1 10.100.149.186 Thu Feb 17 02:13 - 02:31 (00:18)
root pts/0 10.100.149.186 Thu Feb 17 01:01 - 02:12 (01:11)
root tty1 Thu Feb 17 00:59 - down (1+18:35)
reboot system boot 2.6.18-194.el5 Thu Feb 17 00:58 (1+18:37)
wtmp begins Thu Feb 17 00:58:09 2011
[root@LVS2-M1 public]#

入侵种代理或squit代理的灵活运

- 入侵的过程当中会遇到多种多样的情况，下面的这种比较多见，
- Web漏洞直接得到后端server的权限,后端server为内网无法访问互联网,想端口转发或其他的操作都拒绝访问，这个时候，代理会起到很大的作用。

PPTV安全架构

整体架构；

1、LB日志实时分析

2、核心服务器跳板机机制

3、ossec agent 监控

4、open ldap 登陆策略

5、系统日志分析

LB日志实时分析

- LB日志实时分析,(每个LB每天几百G的日志压缩前，从中分析出可能会纯在入侵行为的日志并发送告警邮件)
- LB实时日志直接进入mogoDB,匹配安全正则(如:裸日志含有”20%select%20”等、、、)
- 实时日志分析在mongoDB完成，历史日志进入hadoop

LB访问日志实时监控,发现注入,命令执行,上传等问题

- 访问日志实时进入mongoDB匹配安全正则发现潜在威胁.历史日志直接进入hadoop.

正在被攻击。
攻击访问都是 500.

124.160.184.11 kuainv.pptv.com - [13/Sep/2012:11:11:17 +0800] "GET /play/209/?aid=love&gid=dl%27%3b%20waitfor%20delay%20%270%3a0%3a4%27%20--%20 HTTP/1.0" 500 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" "211.144.198.146, 124.160.184.12" "0.003" "10.203.101.108:9000" "500" "0.003"
124.160.184.11 kuainv.pptv.com - [13/Sep/2012:11:11:17 +0800] "GET /play/209/?aid=love&gid=dl%22%3b%20waitfor%20delay%20%270%3a0%3a4%27%20--%20 HTTP/1.0" 500 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" "211.144.198.146, 124.160.184.12" "0.004" "10.203.101.108:9000" "500" "0.004"
124.160.184.11 kuainv.pptv.com - [13/Sep/2012:11:11:18 +0800] "GET /play/209/?aid=love&gid=/..//..//..//..//..//..//..//etc/passwd%00 HTTP/1.0" 500 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" "211.144.198.146, 124.160.184.12" "0.005" "10.203.101.106:9000" "500" "0.005"
124.160.184.11 kuainv.pptv.com - [13/Sep/2012:11:11:18 +0800] "GET /play/209/?aid=love&gid=%2fetc%2fpasswd HTTP/1.0" 500 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" "211.144.198.146, 124.160.184.12" "0.004" "10.203.101.107:9000" "500" "0.004"
124.160.184.11 kuainv.pptv.com - [13/Sep/2012:11:11:18 +0800] "GET /play/209/?aid=love&gid=..%2f...%2f..%2f.%2f..%2f...%2f..%2f.%2f..%2f...%2f..%2f.%2f..%2f...%2f..%2f.%2f..%2f...%2f..%2f.%2f..%2f...%2f..%2f.%2f..%2f...%2f..%2f.%2fetc%2fpasswd HTTP/1.0" 500 0 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" "211.144.198.146, 124.160.184.12" "0.005" "10.203.101.106:9000" "500" "0.005"
124.160.184.11 kuainv.pptv.com - [13/Sep/2012:11:11:18 +0800] "GET /play/209/?aid=love&gid=invalid../../../../../../../../../etc/passwd/./ "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" "211.144.198.146, 124.160.184.12" "0.005" "10.203.101.106:9000" "500" "0.005"

已成功执行sleep,

Tty timeout&远程卡系统层面统一修改密码

```
tty |grep pts >/dev/null
if [[ $? -eq 0 ]];then
        export TMOUT=3600
else
        export TMOUT=1200
fi
```

- Tty timeout统一设置时间10分钟,
- 统一使用ipmitool 修改远程管理卡口令

服务器启动时间少于5分钟实时告警

(这些主要应对远程管理带来的危害)

核心服务器跳板机制

cas统一认证

- 应对可批量管理服务器的后端服务统一加强各方面安全需求，采用跳板机制，拒绝运维网直接登陆服务器现象，user login严格控制。
- Cas统一认证，拒绝zabbix,等后端服务，后台使用默认口令，弱口令等

Zabbix和puppet配合使用实时查找webshell,rootkit后门检测

- 实时监控(任何websehll,变异web后门及时发现)

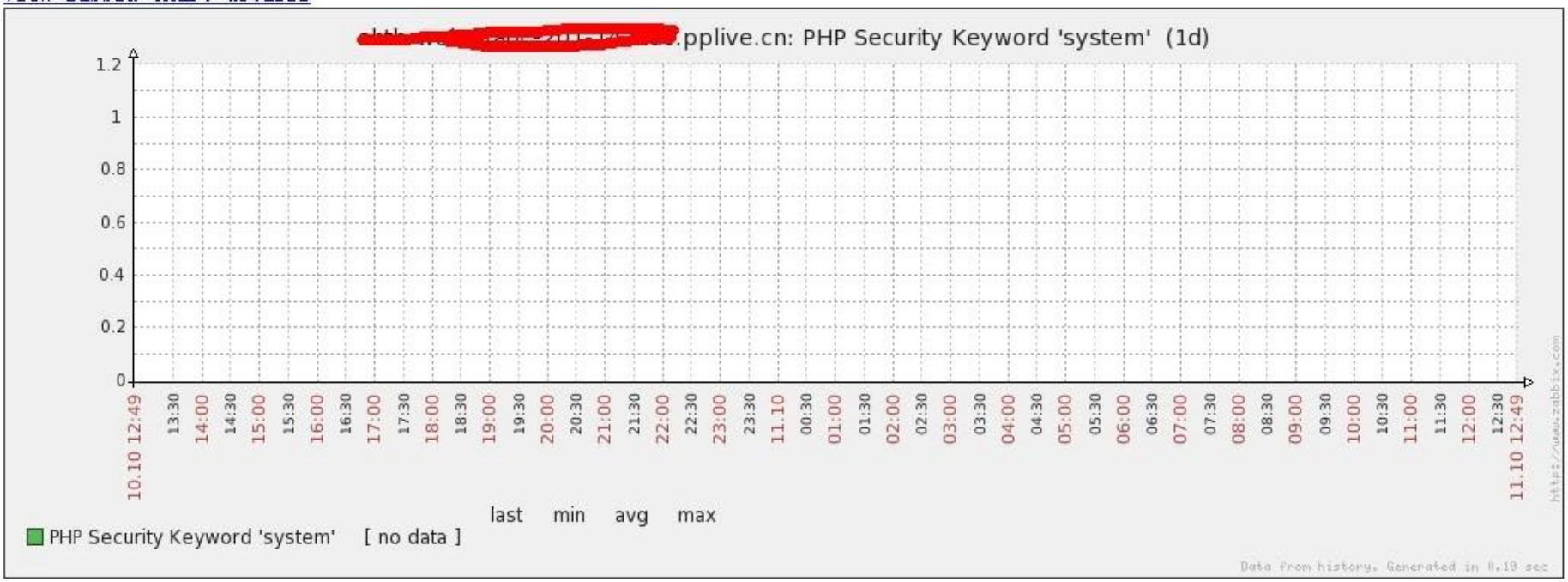
Host: [redacted].pplive.cn

IP: [redacted]

Issue: Keyword system in PHP

Date: Thu Oct 11 12:49:20 2012

View zabbix chart details



发件人： zabbix
发送时间： [redacted]年10月31日 18:24
收件人： [redacted]
主题： [Notify][P2]rkhunter find issue

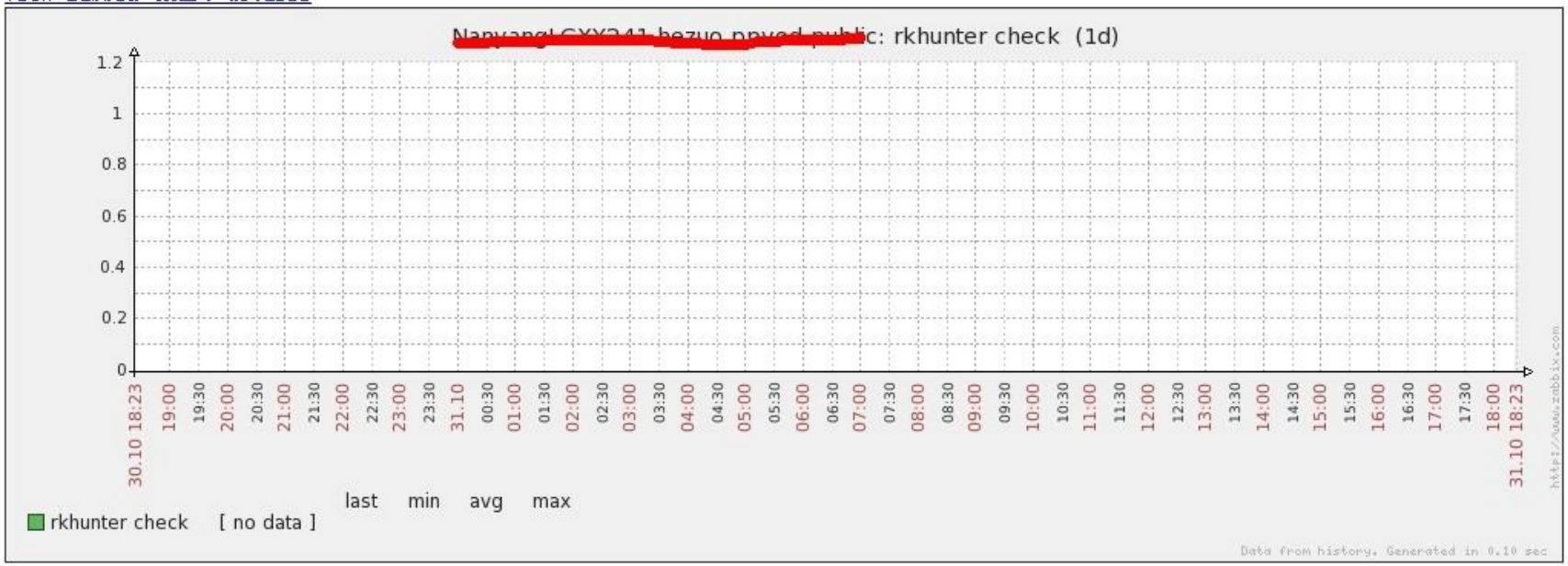
Host: [redacted]vod.public

IP: [redacted]

Issue: rkhunter find issue

Date: Wed Oct 31 18:23:29 2012

View zabbix chart details



ossec agent 监控

- Ossec 目前涵盖端口(匹配黑白名单)监控,rootkit监控,关键文件监控(/bin/* 等),user login&sudo动作告警(匹配黑白名单)等、、、其他常规监控，实时告警

新端口开放21端口定义在黑名单。原则该服务器不应该开放21端口

Open ldap

- 明细open ldap 分组,防止跨越权限访问服务器,
- 自助密码服务,首次登陆修改密码,密码要求满足复杂度需求

系统日志分析

服务器,交互机,防火墙

- 配合日志分析查找可能存在的问题,如:密码暴力破解(交互机ACL可能存在问题)
- 一天一报告，全面排查可能存在的问题
- 用色标记(一部分)

- End