安全排查与防御

1. 常见安全漏洞分析
2. Web安全应急
3. Windows基础加固
4. Linux基础加固
5. 常见可疑情况排查

常见Web安全漏洞分析

① SQL注入

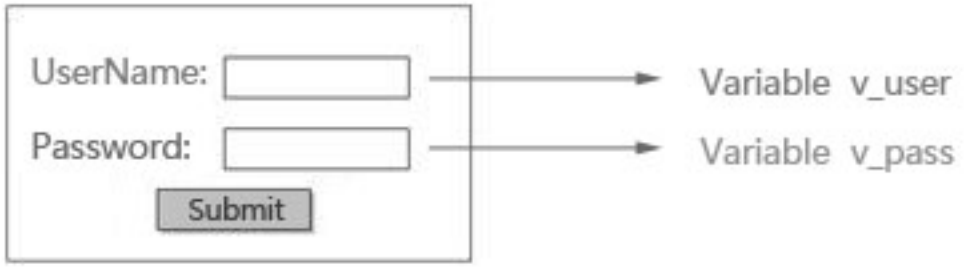
② 跨站脚本

③ 文件上传

④ CMS漏洞

⑤ 文件泄露

SQL注入漏洞



select * from user where user_name='admin' and password='123456';

```
"select * from user where user_name='"
+ v_user +
"' and password='"
+ v_pass +
"'."
  ';
```

select * from user where user_name='admin' and password='1' or '1'='1';

SQL注入漏洞

```
<?php
setcookie("TestCookie","test");
$s = $_GET['id'];
echo $s;
$con =
mysql_connect("localhost","root","testi
ng");
if (!$con)
{
  die('Could not connect: ' . mysql_error());
 }
mysql_select_db("empirecms51", $con);
$result = mysql_query("SELECT * FROM
phome_enewsuser where userid=".$s);
echo $result;
mysql_close($con);
?>
```

危害限制

1. 漏洞消除
2. 限制危害更多的数据
3. 限制攻击者的活动范围

- ✓ 代码层修复
- ✓ 安全防护
  - ✓ 代码层修复
  - ✓ 安全防护
- ✓ 数据库独立
- ✓ 数据库权限限制
- ✓ Web目录限制
- ✓ 系统安全加固

危害限制

1. 漏洞消除
2. 限制危害更多的数据
3. 限制攻击者的活动范围

- ✓ 代码层修复
- ✓ 安全防护
  - ✓ 代码层修复
  - ✓ 安全防护
- ✓ 数据库独立
- ✓ 数据库权限限制
- ✓ Web目录限制
- ✓ 系统安全加固

SQL注入漏洞可能出现的位置

a) 表单提交，主要是POST请求，也包括GET请求。

b) URL参数提交，主要为GET请求参数。

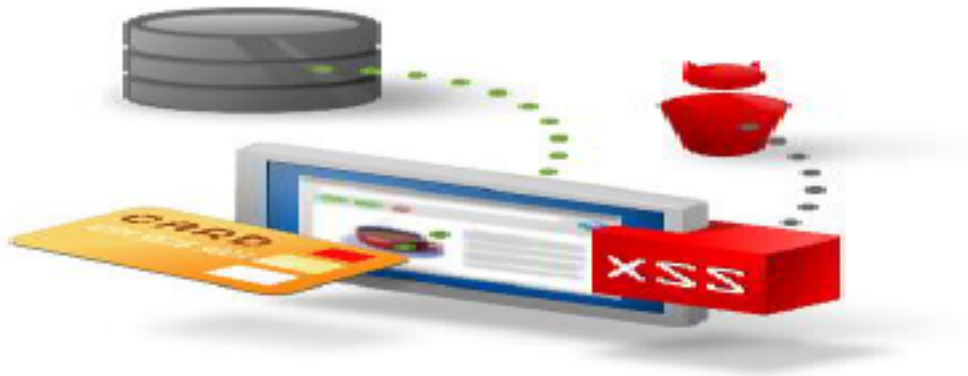
c) Cookie参数提交。

d) HTTP请求头部的一些可修改的值，比如Referer、User_Agent等。

跨站脚本漏洞

【案例：XSS漏洞实践】

通过利用盲打工具展示XSS漏洞的巨大危害




```
<?php
setcookie("TestCookie","test");
$s = $_GET['id'];
echo $s;
$b = $_POST['post'];
echo $b;echo "</br></br>";
echo "Referer:";
echo $_SERVER["HTTP_REFERER"];
echo "</br></br>";
echo "Cookies:";
echo $_SERVER["HTTP_COOKIE"];
?>
```

跨站脚本漏洞

HttpOnly

检查输入/输出

XSS Filter

安全编码函数

富文本过滤

```
<?php
header("Set-
Cookie:cookie=knownsec;httponly",false);
?>
response.setHeader("Set-
Cookie","cookiename=value;
Path=/;Domain=domainvalue;Max-
Age=seconds;HttpOnly");
```

http://www.stripesframework.org/display/stripes/XSS+filter

文件上传漏洞

【案例：上传漏洞实践】

介绍三种常见的文件上传漏洞，通过实例展示文件上传漏洞的巨大危害。

文件泄露漏洞

【案例：上传漏洞实践】

介绍三种常见的文件上传漏洞，通过实例展示文件上传漏洞的巨大危害。

Web安全应急

Web应急响应目标

危害抑制

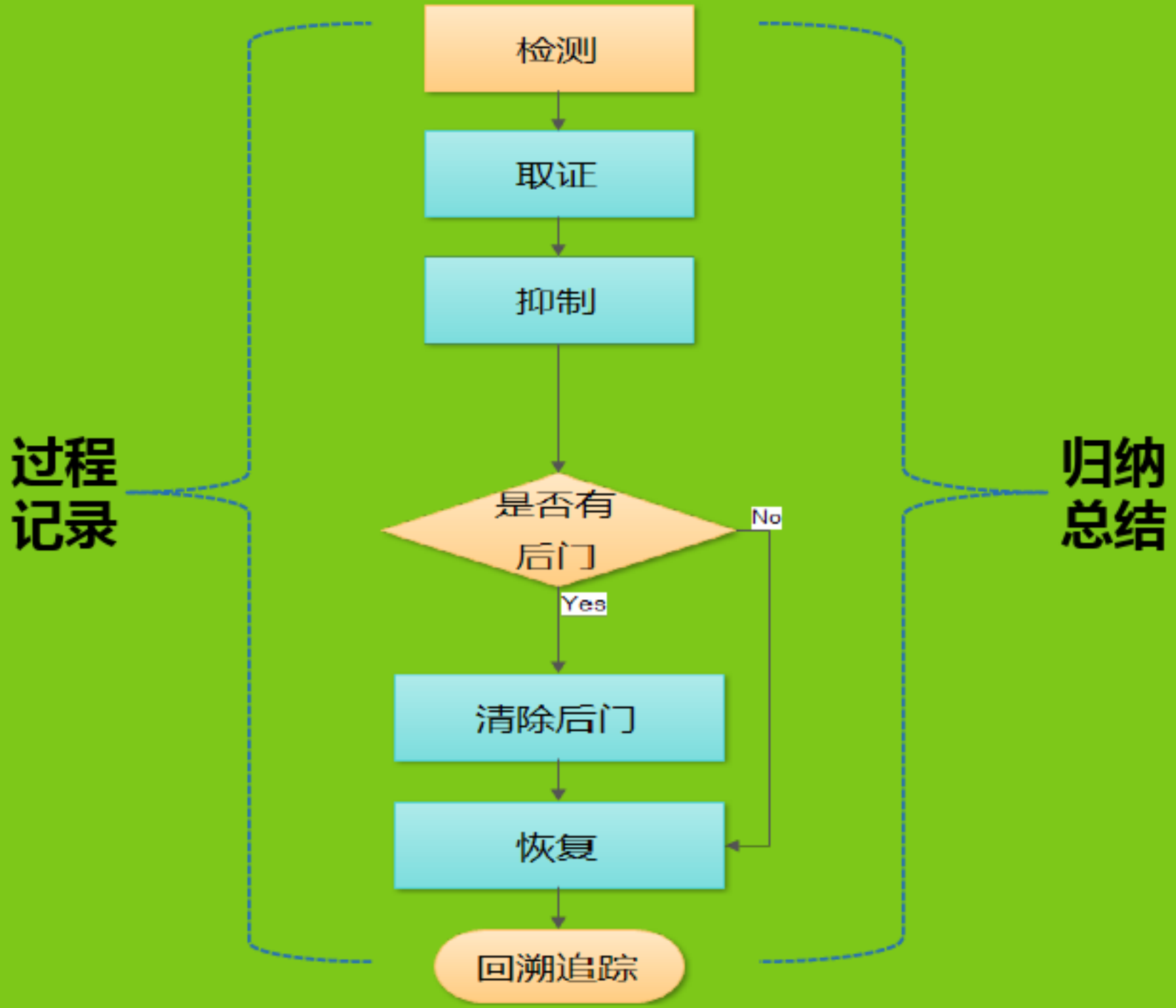
后门清除

确保恢复

亡羊补牢

追究责任

归纳总结


检测
取证
抑制
是否有后门
No
Yes
清除后门
恢复
回溯追踪
过程记录
归纳总结

Web安全应急主要技术点

Web日志：

a) IIS类型日志

b) Apache日志

系统日志：

a) 安全日志

b) 历史命令

c) 应用程序日志

d) 系统日志

Web安全应急主要技术点

#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2015-05-05 01:01:15
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status
2015-05-05 01:05:02 W3SVC1 10.211.55.6 POST /test.cer - 80 - 10.211.55.4 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
2015-05-05 01:05:07 W3SVC1 10.211.55.6 POST /test.cer - 80 - 10.211.55.4 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
2015-05-05 01:05:09 W3SVC1 10.211.55.6 POST /test.cer - 80 - 10.211.55.4 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0

Web安全应急主要技术点

```
10.211.55.2 - - [05/May/2015:15:50:16 +0800] "GET /upfile/x.php?file=default.css&version=3.2.2 HTTP/1.1"
200 2892
10.211.55.2 - - [05/May/2015:15:50:16 +0800] "GET /upfile/x.php?file=functions.js&version=3.2.2 HTTP/1.1"
200 18115
10.211.55.2 - - [05/May/2015:15:50:16 +0800] "GET /upfile/x.php?file=favicon.ico&version=3.2.2 HTTP/1.1"
200 318
10.211.55.2 - - [05/May/2015:15:50:25 +0800] "POST /upfile/x.php HTTP/1.1" 302 -
10.211.55.2 - - [05/May/2015:15:50:25 +0800] "GET /upfile/x.php?server=localhost&username=root HTTP/1.1"
200 4705
10.211.55.2 - - [05/May/2015:15:50:25 +0800] "GET
/upfile/x.php?server=localhost&username=root&script=connect HTTP/1.1" 200 111
```

HTTP协议介绍

- HTTP 报文首部（字段）
  - Referer、cookie、user-agent、host、date、via
- HTTP方法
  - GET、Post、Put
- HTTP状态码
  - 200、201、302、403、404、500

HTTP报文首部（字段）

URL:http://news.baidu.com/

请求标头 | 请求正文 | 响应标头 | 响应正文 | Cookie | 发起程序 | 计时

键	值
请求	GET / HTTP/1.1
Accept	application/x-ms-application, image/jpeg, application/xaml+xm...
Referer	http://www.baidu.com/
Accept-Language	zh-CN
User-Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Tri...
Accept-Encoding	gzip, deflate
Host	news.baidu.com
DNT	1
Connection	Keep-Alive
Cookie	BAIDUID=89D0B75A86D8C19BB7975F66DB50107D:FG=1; BDREFER=%7Burl...

常见HTTP响应状态码

URL:http://news.baidu.com/

请求标头 | 请求正文 | 响应标头 | 响应正文 | Cookie | 发起程序 | 计时

键	值
响应	HTTP/1.1 200 OK

URL:http://news.baidu.com/images

请求标头 | 请求正文 | 响应标头 | 响应正文 | Cookie | 发起程序 | 计时

键	值
响应	HTTP/1.1 302 Found

URL:http://www.knownsec.com/admin

请求标头 | 请求正文 | 响应标头 | 响应正文 | Cookie | 发起程序 | 计时

键	值
响应	HTTP/1.1 403 Forbidden

URL:http://app.chinaz.com/admin

请求标头 | 请求正文 | 响应标头 | 响应正文 | Cookie | 发起程序 | 计时

键	值
响应	HTTP/1.1 404 Not Found
Date	Sun, 23 Dec 2012 06:18:04 GMT
Server	Apache/2.2.17 (CentOS)
Content-Length	283
Keep-Alive	timeout=3, max=300
Connection	Keep-Alive
Content-Type	text/html; charset=iso-8859-1

WEB扫描日志

- 2012-03-07 01:45:50 192.168.100.29 POST /blood/regweb/admin/adminindex.aspx - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 500 0 0
- 2012-03-07 01:45:50 192.168.100.29 GET /blood/regweb/admin/email - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 404 0 2
- 2012-03-07 01:45:50 192.168.100.29 POST /blood/regweb/admin/adminindex.aspx - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 500 0 0
- 2012-03-07 01:45:50 192.168.100.29 POST /blood/regweb/admin/adminindex.aspx - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 200 0 0
- 2012-03-07 01:45:50 192.168.100.29 GET /blood/regweb/admin/adminindex.000 - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 404 0 2
- 2012-03-07 01:45:50 192.168.100.29 GET /blood/regweb/admin/mailman - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 404 0 2
- 2012-03-07 01:45:50 192.168.100.29 POST /blood/regweb/admin/adminindex.aspx - 80 - 106.3.242.195 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0) 500 0 0

SQL注入攻击日志

- 2012-03-11 16:56:42 192.168.100.29 POST /lptScore/cjcx_result.asp |12|80040e07|将_varchar_值_'考生'_转换为数据类型为_int_的列时发生语法错误。 80 - 124.128.255.229 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CLR+2.0.50727;+Media+Center+PC+5.0;+.NET+CLR+3.0.04506;+.NET+CLR+1.1.4322) 500 0 0
- 2012-03-11 16:56:42 192.168.100.29 POST /lptScore/cjcx_result.asp |12|80040e07|将_varchar_值_'管理'_转换为数据类型为_int_的列时发生语法错误。 80 - 124.128.255.229 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CLR+2.0.50727;+Media+Center+PC+5.0;+.NET+CLR+3.0.04506;+.NET+CLR+1.1.4322) 500 0 0

Web登陆日志

- 60.13.40.96 - - [08/Mar/2012:19:45:09 +0800] "GET /sofprogecslive/tools.jsp?o=vLogin HTTP/1.1" 200 646 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET4.0C; 360EE)"
- 60.13.40.96 - - [08/Mar/2012:19:45:16 +0800] "POST /sofprogecslive/tools.jsp HTTP/1.1" 302 - "http://www.XXXxx.cn/sofprogecslive/tools.jsp?o=vLogin" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET4.0C; 360EE)“

文件上传日志

- 221.204.135.94 - - [24/Feb/2012:18:14:42 +0800] "GET /sofprogecslive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogecslive/&fsAction=createFile&fileName=tools.jsp HTTP/1.1" 200 2801 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)"
- 221.204.135.94 - - [24/Feb/2012:18:14:42 +0800] "GET /sofprogecslive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogecslive/tools.jsp&fsAction=open HTTP/1.1" 200 3757 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)"

文件上传日志

- 221.204.135.94 - - [24/Feb/2012:18:14:47 +0800] "POST /sofprogecslive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogecslive/tools.jsp&fsAction=save HTTP/1.1" 200 2846 "http://www.XXXxx.cn/sofprogecslive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogecslive/tools.jsp&fsAction=open" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)"

一些应急过程中的工具

- 取证工具：
  - Ghost、Windows PE、Linux CD
- 日志分析：
  - Log Parser 2.2//微软出品，质量和功能一流 | LogView.exe//分析大型日志首选
  - MyEventViewer.exe//分析系统日志 | Grep//全能王
- 日志切割：
  - Split | cat | dd | head | tail | awk
- 过程验证：
  - Nc | Curl | Wget | SQLmap | Hackbar

UnxUtils

应急过程中的一些注意事项

日志存放路径

Windows：

① 安全日志：%systemroot%\system32\config\SecEvent.EVT

② 系统日志：%systemroot%\system32\config\SysEvent.EVT

③ 应用程序日志：%systemroot%\system32\config\AppEvent.EVT

④ Web日志：%systemroot%\system32\logfiles\w3svc1\

⑤ 计划任务：%systemroot%\schedlgu.txt

⑥ 防火墙： %systemroot%\pfirewall.log

Linux：

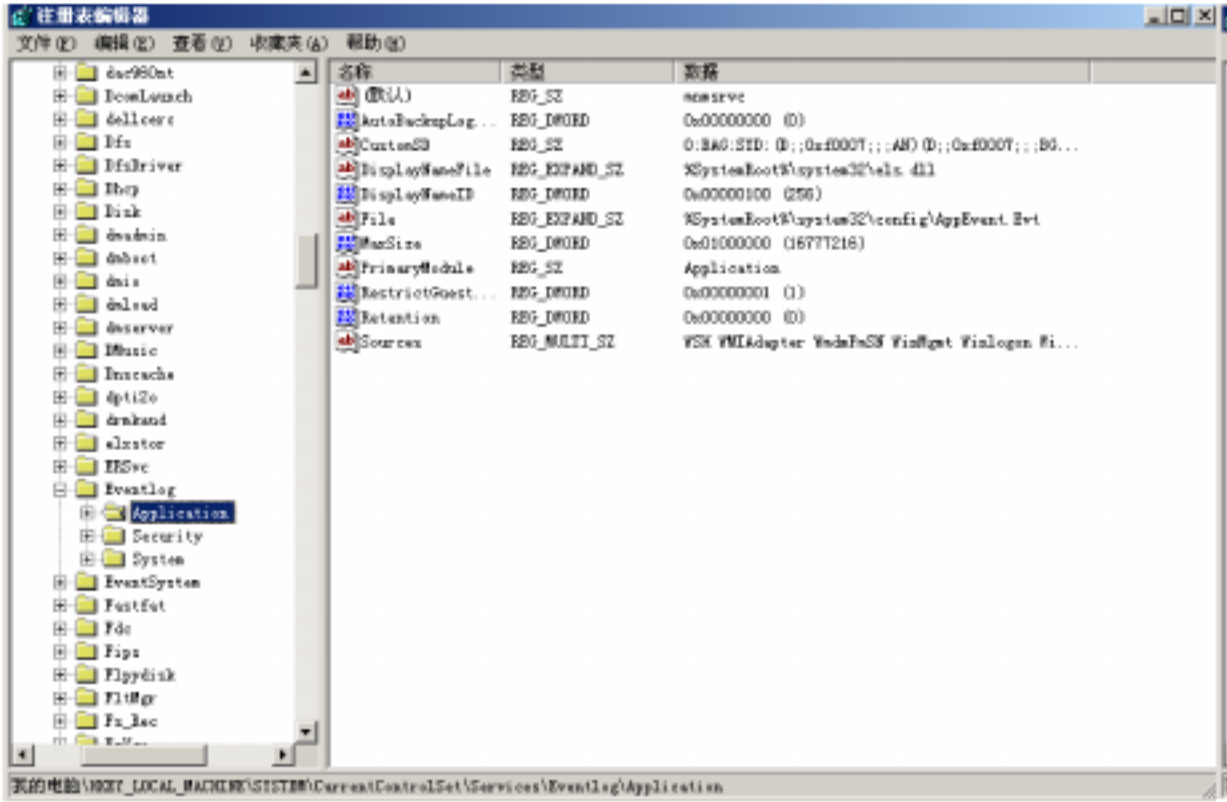
① 安全日志：/var/logs/secure*

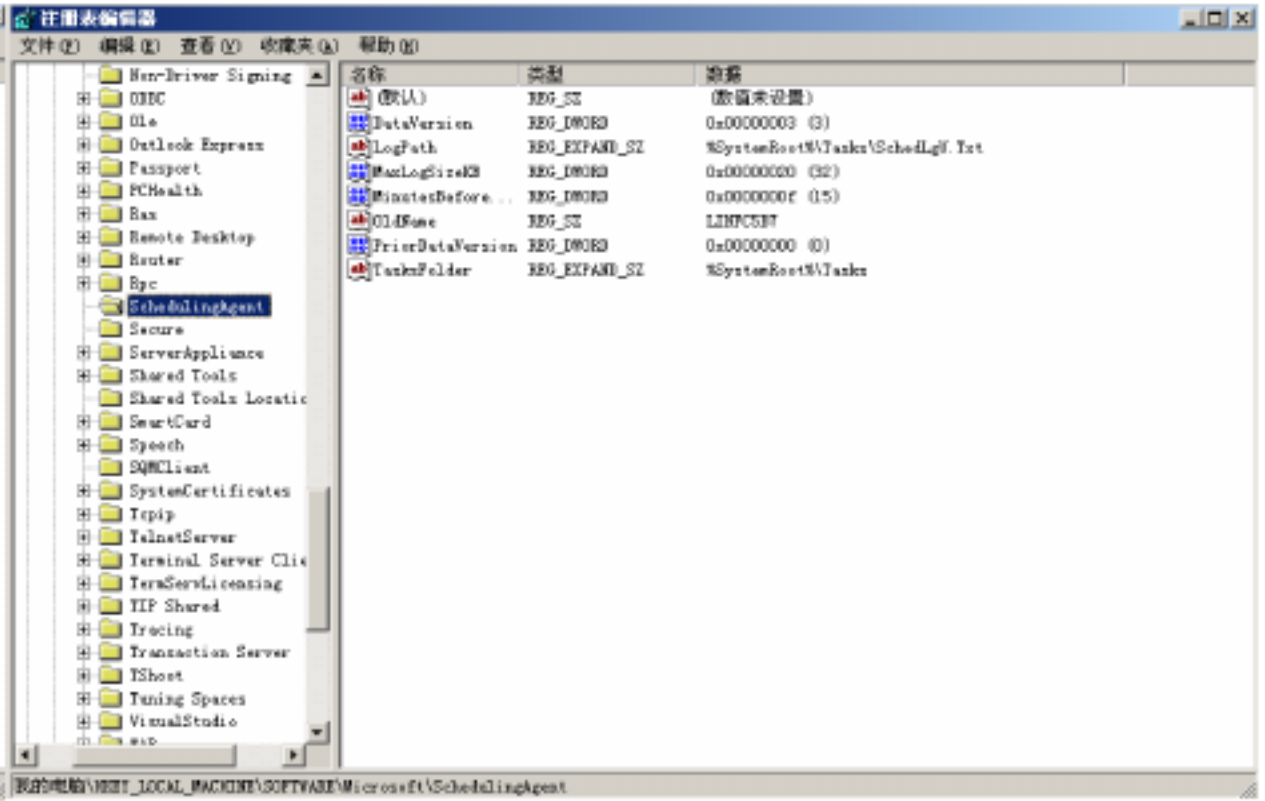
② History

③ Lastlog

④ wtmp

日志存放路径


注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
Application
Security
System
名称 类型 数据
(默认) REG_SZ
AutoBackupLog... REG_DWORD
CustomSD REG_SZ
DisplayNameFile REG_EXPAND_SZ
DisplayNameID REG_DWORD
File REG_EXPAND_SZ
MaxSize REG_DWORD
PrimaryModule REG_SZ
RestrictGuest... REG_DWORD
Retention REG_DWORD
Sources REG_MULTI_SZ
我的电脑\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application


注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
SchedulingAgent
名称 类型 数据
(默认) REG_SZ (数值未设置)
DataVersion REG_DWORD 0x00000003 (3)
LogPath REG_EXPAND_SZ %SystemRoot%\Tasks\SchedLgU.Txt
MaxLogSizeKB REG_DWORD 0x00000020 (32)
MinutesBefore... REG_DWORD 0x0000000f (15)
OldName REG_SZ LINFC587
PrevDataVersion REG_DWORD 0x00000000 (0)
TasksFolder REG_EXPAND_SZ %SystemRoot%\Tasks
我的电脑\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent

history记录时间

```
root@ubuntu:~# ls -la
ls: 初始化月份字符串出错
总用量 20
drwx------  2 root root 4096  6月  9 23:20 .
drwxr-xr-x 22 root root 4096  6月  9 23:05 ..
-rw-------  1 root root  322  6月 10 18:09 .bash_history
-rw-r--r--  1 root root 3106  2月 20  2014 .bashrc
-rw-r--r--  1 root root  140  2月 20  2014 .profile
root@ubuntu:~#
```

```
root@ubuntu:~# history |head -10
    1  wget http://127.0.0.1
    2  ls
    3  cd /home
    4  ls
    5  cd linf/
    6  ls
    7  ls -la
    8  exit
    9  halt
   10  stat /bin/ls
root@ubuntu:~#
```

日志存放路径

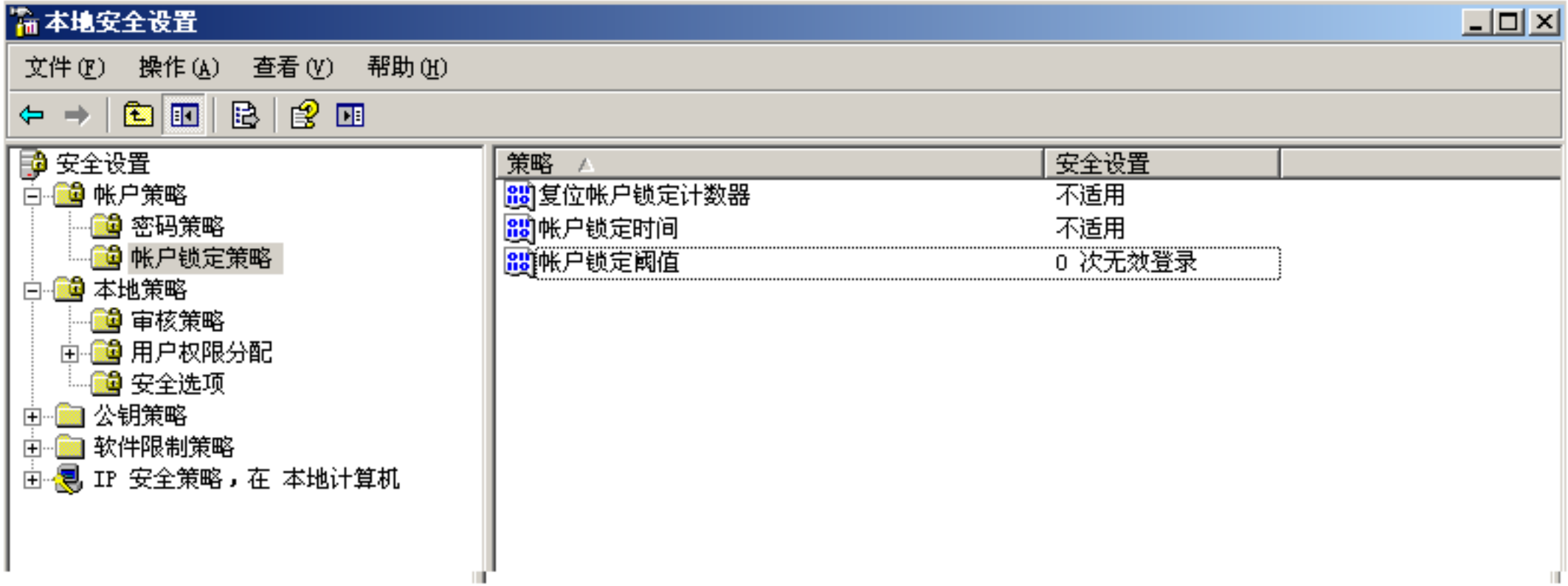
```
root@ubuntu:~# export HISTTIMEFORMAT="%F %T `whoami` "
root@ubuntu:~# echo 'export HISTTIMEFORMAT="%F %T `whoami` "' >> /etc/profile
root@ubuntu:~# history
    1  2015-06-12 08:24:48 root wget http://127.0.0.1
    2  2015-06-12 08:24:48 root ls
    3  2015-06-12 08:24:48 root cd /home
    4  2015-06-12 08:24:48 root ls
    5  2015-06-12 08:24:48 root cd linf/
    6  2015-06-12 08:24:48 root ls
    7  2015-06-12 08:24:48 root ls -la
    8  2015-06-12 08:24:48 root exit
    9  2015-06-12 08:24:48 root halt
   10  2015-06-12 08:24:48 root stat /bin/ls
   11  2015-06-12 08:24:48 root stat /
   12  2015-06-12 08:24:48 root echo *
   13  2015-06-12 08:24:48 root cd /home
   14  2015-06-12 08:24:48 root ls
```

Windows基础加固

常见可疑情况排查

- 密码
  - 密码强度
- 防火墙
  - 入站规则
  - 出站规则
  - 应用程序控制
- 服务
  - 远程桌面管理
  - Web服务

密码策略


本地安全设置
文件(F) 操作(A) 查看(V) 帮助(H)
安全设置
帐户策略
密码策略
帐户锁定策略
本地策略
审核策略
用户权限分配
安全选项
公钥策略
软件限制策略
IP 安全策略，在 本地计算机
策略
安全设置
复位帐户锁定计数器
不适用
帐户锁定时间
不适用
帐户锁定阈值
0 次无效登录

防火墙


高级安全 Windows 防火墙
文件(F) 操作(A) 查看(V) 帮助(H)
本地计算机 上的高级安全 Win
入站规则
出站规则
连接安全规则
监视
防火墙
连接安全规则
安全关联
主模式
快速模式
本地计算机 上的高级安全 Windows 防火墙
高级安全 Windows 防火墙为 Windows 计算机提供网络安全。
概述
域配置文件
Windows 防火墙已关闭。
专用配置文件
Windows 防火墙已关闭。
公用配置文件是活动的
Windows 防火墙已关闭。
Windows 防火墙属性
入门
计算机之间的身份验证通信
创建连接安全性规则指定使用 Internet 协议安全性(IPSec)对计算机之间的连接进行身份验证和保护的方式和时间。
连接安全规则
查看和创建防火墙规则
创建允许或阻止连接指定程序或端口的防火墙规则。还可以仅在以下情况下允许连接：对连接进行身份验证，连接来自授权用户、组或计算机。默认情况下，阻止入站连接(除非这些连接匹配允许它们的规则)，允许出站连接(除非这些连接匹配阻止它们的规则)。
入站规则
出站规则
查看当前防火墙以及 IPsec 策略和活动
查看有关当前应用的防火墙与连接安全性规则和活动网络连接的安全关联的信息。
监视
操作
本地计算机 上的高级...
导入策略...
导出策略...
还原默认策略
诊断/修复
查看
刷新
属性
帮助

服务

① 账户隔离

② 权限控制

③ 应用程序池应用

④ 目录定制

⑤ 扩展定制

Linux基础加固

常见可疑情况排查

✓SSH服务

①限制登录IP

②禁止root远程登录

③设置用户超时退出

✓关键文件备份

✓日志加固与备份

常见可疑情况排查

- 网站打不开了？
- 服务器是否已经被控制？
- 服务器出现大量连接数？
- 服务器大量发数据包？

常见可疑情况排查

常见可疑情况排查

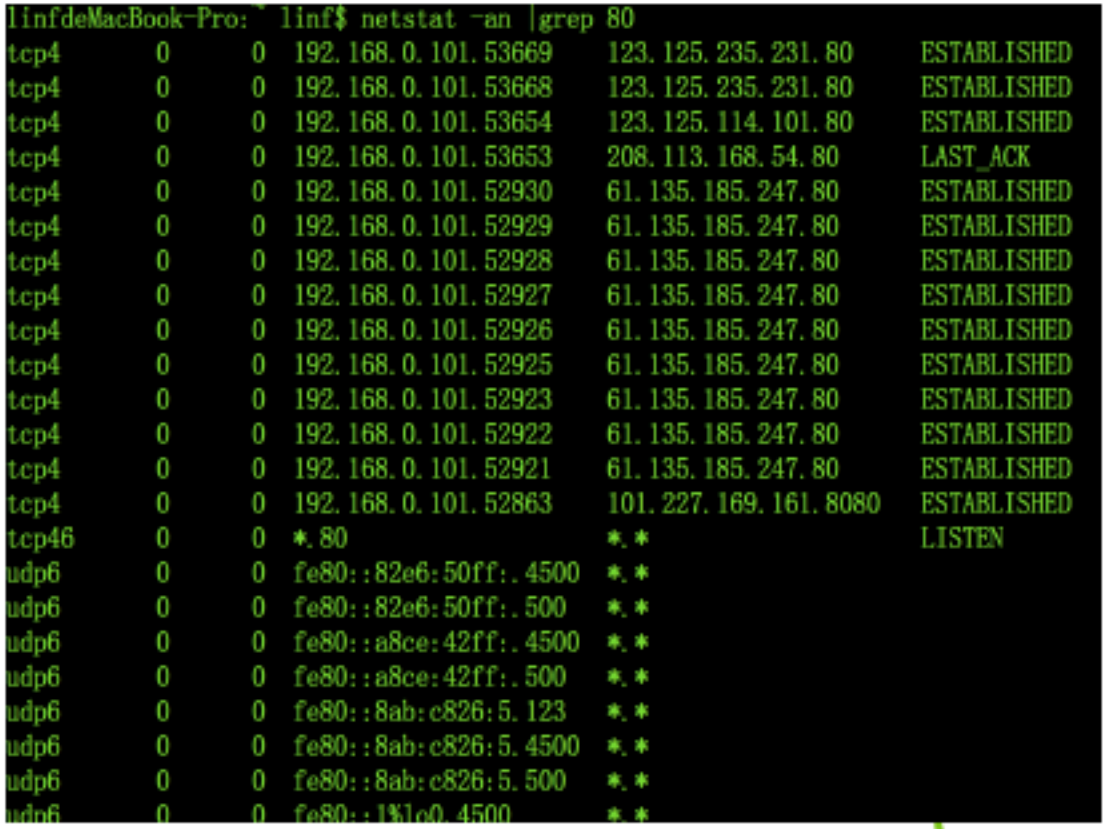
- 网站打不开了？
- 服务器是否已经被控制？
- 服务器出现大量连接数？
- 服务器大量发数据包？

网站打不开


主机域名绑定
修改密码
设置首页
主机状态设置
虚拟目录
isapi筛选器
重启网站
网站辅助功能
错误页面定义
站点重定向
mime类型
脚本错误设置
脚本映射
站点同步
ASP.NET版本
网站文件管理
在线上传
恢复备份
RAR文件解压
RAR压缩
超级替换
文件删除
预装软件
网站安全管理
安全设置
读写权限
ip限制
文件保护
目录保护
查杀病毒
木马清除
网站情报系统
访问统计
流量分析
WWW日志下载
FTP日志下载
查看网站
防盗链接

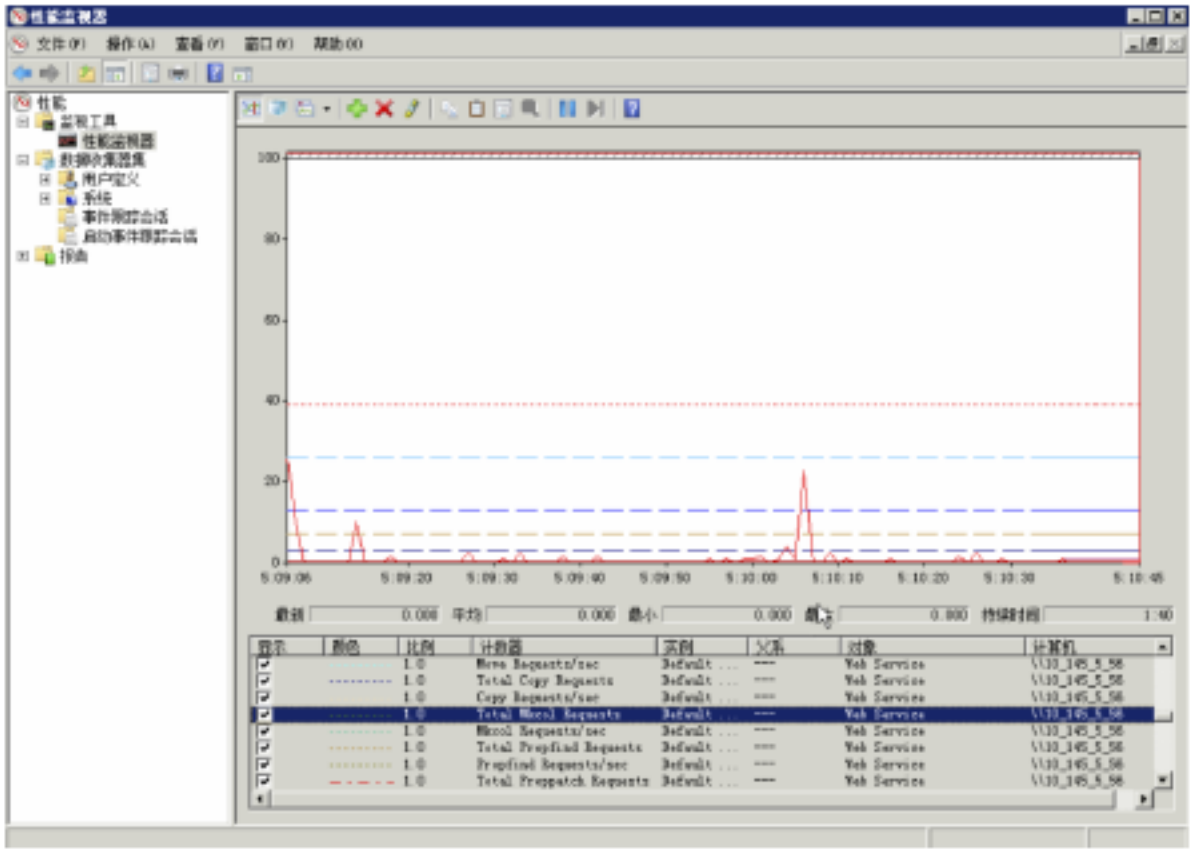
网站打不开——连接数查看

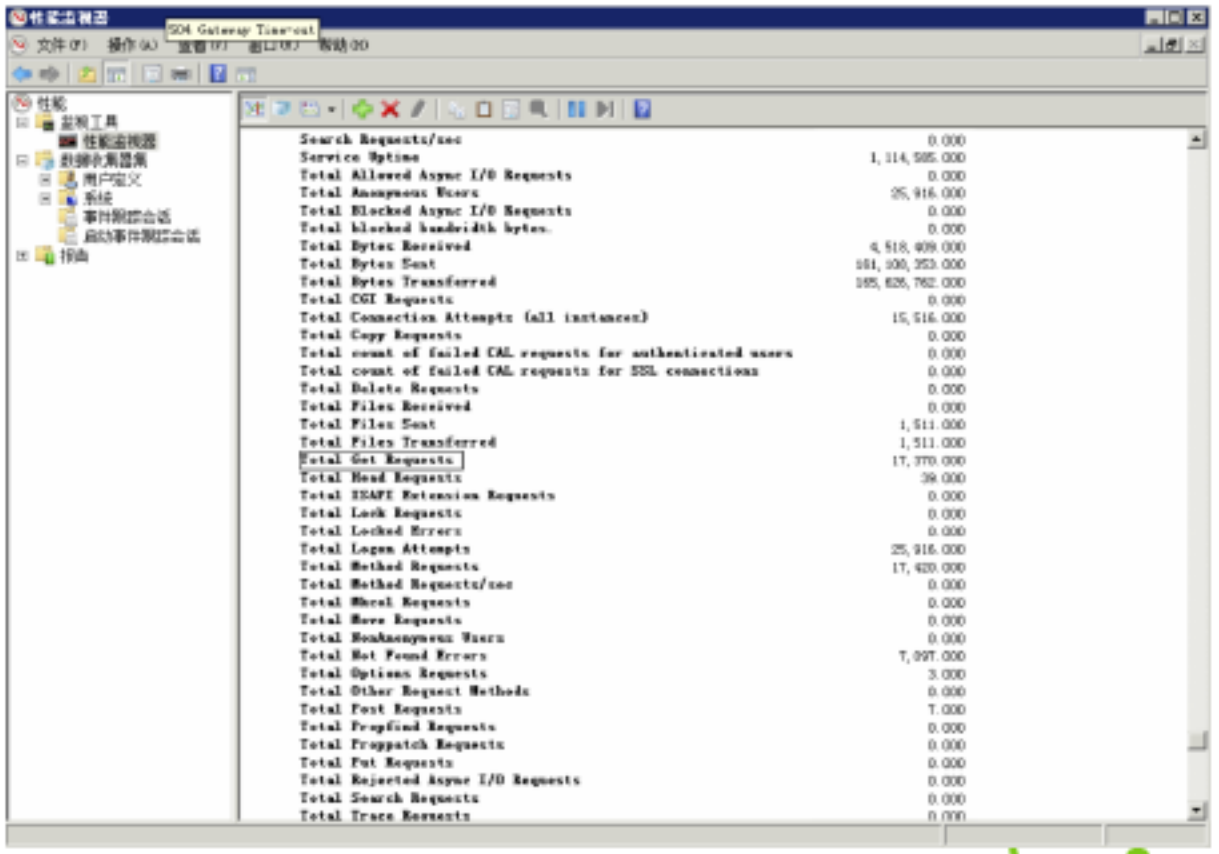
通过网络连接来判断



网站打不开——连接数查看

通过性能检测器



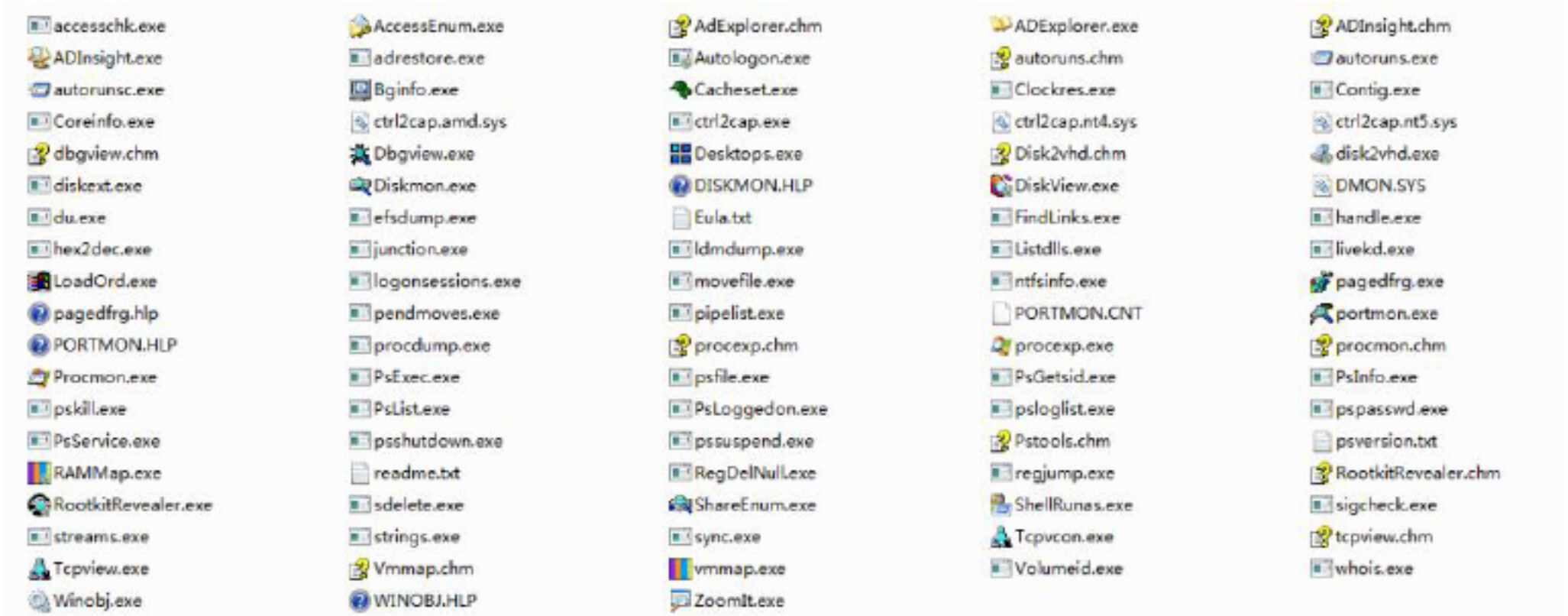


服务器是否被控制

根据异常现象决定检查手段

服务器是否被控制

根据异常现象决定检查手段



推荐资料

- 《HTTP权威指南》
- 《web前端黑客技术揭秘》
- 《黑客攻防技术宝典：Web实战篇(第2版)》

Q&A

THANKS