



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

UserName: → Variable v_user
Password: → Variable v_pass

```
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);
$result = mysql_query("SELECT * FROM
phome_eneuser where userid= ".$s);
echo $result;
mysql_close($con);
?>
```





危害限制

1. 漏洞消除

✓ 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

✓ 代码层修复

✓ 安全防护

2. 限制危害更多的数据

3. 限制攻击者的活动范围





危害限制

1. 漏洞消除

✓ 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

✓ 代码层修复

✓ 安全防护

2. 限制危害更多的数据

3. 限制攻击者的活动范围





SQL注入漏洞可能出现的位置

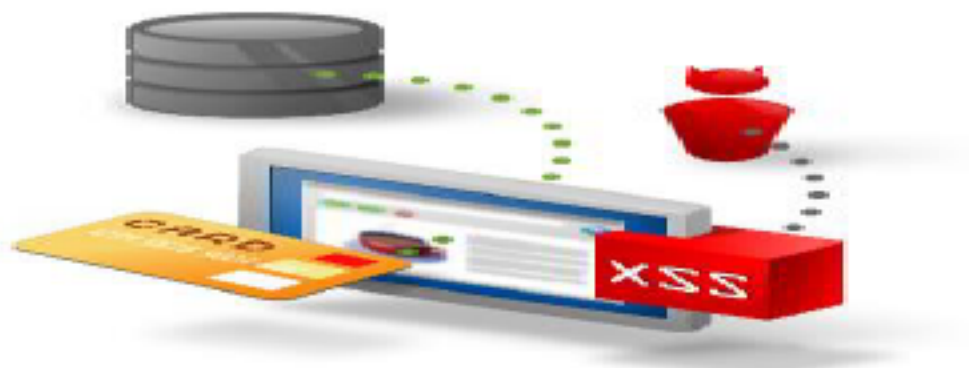
- a) 表单提交，主要是POST请求，也包括GET请求。
- b) URL参数提交，主要为GET请求参数。
- c) Cookie参数提交。
- d) HTTP请求头部的一些可修改的值，比如Referer、User_Agent等。



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","cookie=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

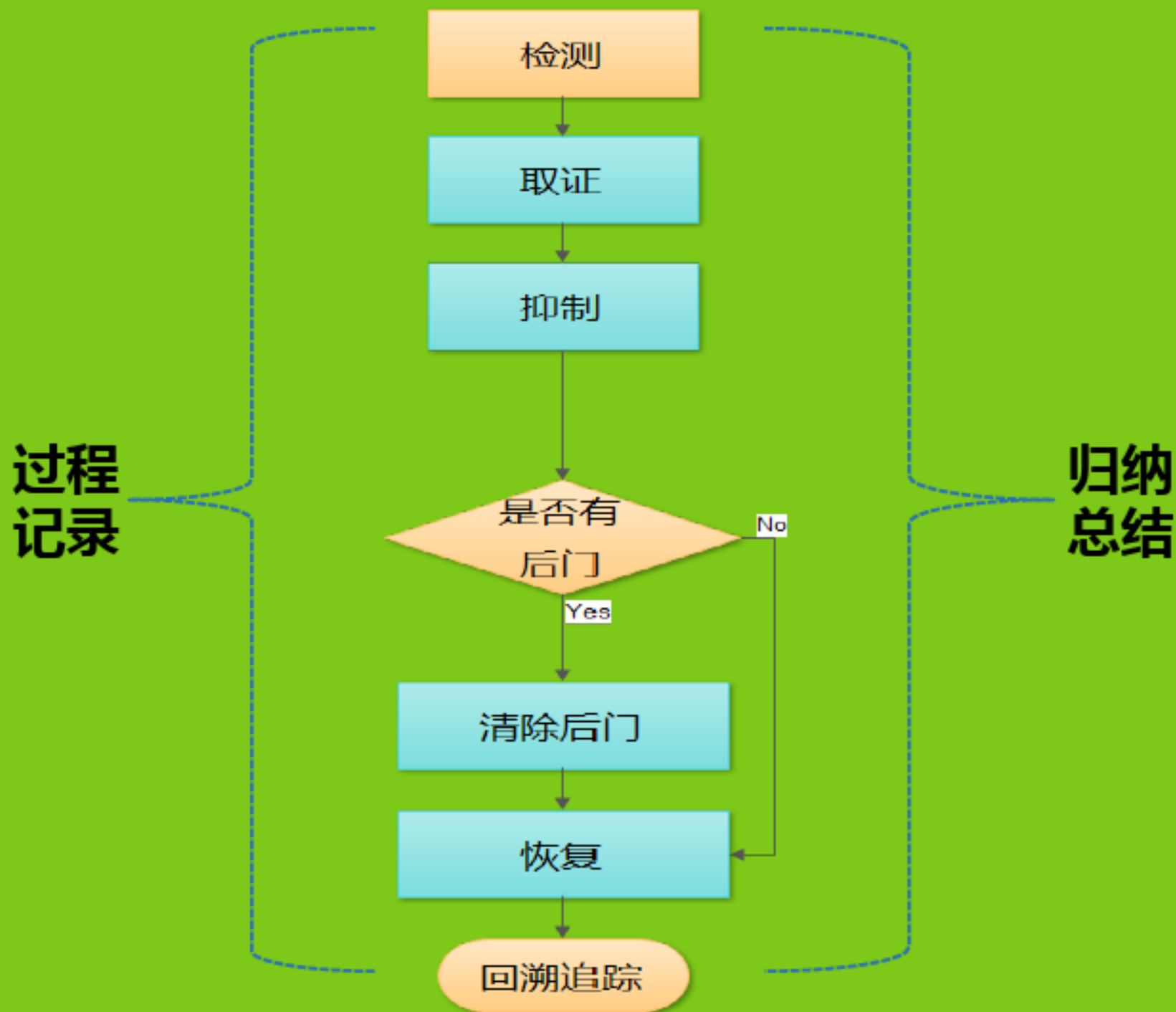


追究责任



归纳总结







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+xml...
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=89DOB75A86D8C19BB7975F66DB50107D:FG=1; BDREFER=%7Bur1...





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 /sofprogeclive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogeclive/&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 /sofprogeclive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogeclive/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 /sofprogeclive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogeclive/tools.jsp&fsAction=save HTTP/1.1" 200 2846 "http://www.XXXxx.cn/sofprogeclive/live/file/60b9f77f135a02553ea7ffe/aa.jsp?action=filesystem&curPath=/usr/server/webapp/sofprogeclive/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%\schedlg.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

The image displays two side-by-side screenshots of the Windows Registry Editor. The left screenshot shows the tree view expanded to 'Eventlog' > 'Application', with the right pane showing a list of registry values. The right screenshot shows the tree view expanded to 'SchedulingAgent', with the right pane showing a list of registry values.

名称	类型	数据
(默认)	REG_SZ	mscsrv
AutoBackupLog...	REG_DWORD	0x00000000 (0)
CustomSD	REG_SZ	0:8A0:SID: (0);0x00007; ;AM (0);0x00007; ;B0...
DisplayNoneFile	REG_EXPAND_SZ	%SystemRoot%\system32\els.dll
DisplayNoneIP	REG_DWORD	0x00000100 (256)
File	REG_EXPAND_SZ	%SystemRoot%\system32\config\AppEvent.Evt
MaxSize	REG_DWORD	0x01000000 (16777216)
PrimaryModule	REG_SZ	Application
RestrictGuest...	REG_DWORD	0x00000001 (1)
Retention	REG_DWORD	0x00000000 (0)
Sources	REG_MULTI_SZ	VSX VMIAadapter VndrPaSF WinRgt Winlogn Fi...

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\SchedLgfl.Txt
MaxLogSizeKB	REG_DWORD	0x00000000 (0)
MinutesBefore...	REG_DWORD	0x0000000f (15)
OldName	REG_SZ	LNTFCSEF
PriorDataVersion	REG_DWORD	0x00000000 (0)
TaskFolder	REG_EXPAND_SZ	%SystemRoot%\Tasks





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  9 23:20 .
drwxr-xr-x 22 root root 4096 6  9 23:05 ..
-rw----- 1 root root  322 6 10 18:09 .bash_history
-rw-r--r-- 1 root root 3106 2 20 2014 .bashrc
-rw-r--r-- 1 root root  140 2 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

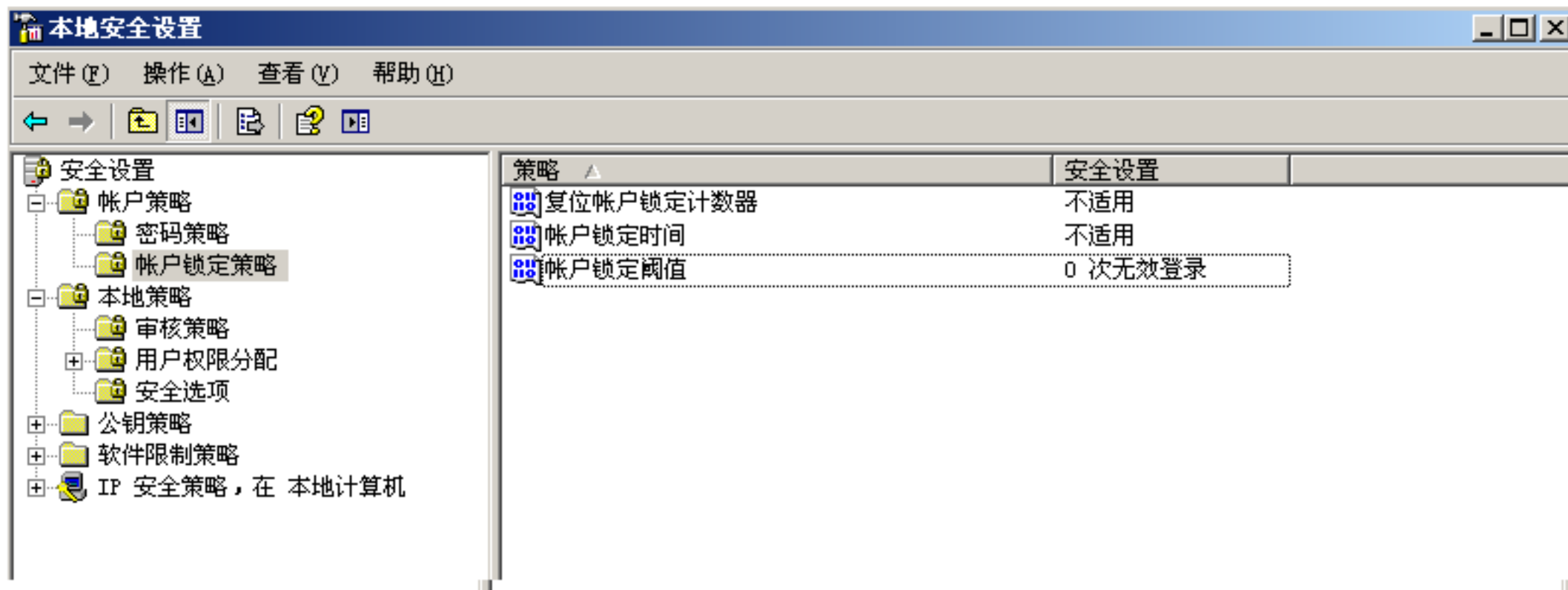


常见可疑情况排查

- 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



The screenshot shows the 'Local Security Settings' window in Windows. The left pane shows the tree view with 'Account Lockout Policy' selected. The right pane displays the following settings:

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





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 iisapi筛选器 重启网站

网站辅助功能

错误页面定义 站点重定向 nines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 BAE文件解压 BAE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

```
管理员: 命令提示符
C:\Users\Administrator>netstat -ano

活动连接

协议 本地地址 外部地址 状态 PID
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING 1272
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 656
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING 372
TCP 0.0.0.0:1026 0.0.0.0:0 LISTENING 744
TCP 0.0.0.0:1027 0.0.0.0:0 LISTENING 792
TCP 0.0.0.0:1028 0.0.0.0:0 LISTENING 2084
TCP 0.0.0.0:1032 0.0.0.0:0 LISTENING 468
TCP 0.0.0.0:1033 0.0.0.0:0 LISTENING 460
TCP 0.0.0.0:1723 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING 4284
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 2248
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING 4856
TCP 0.0.0.0:36000 0.0.0.0:0 LISTENING 3468
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING 4
TCP 10.145.5.56:80 114.111.166.70:4005 ESTABLISHED 4
TCP 10.145.5.56:80 114.111.166.70:4007 ESTABLISHED 4
TCP 10.145.5.56:80 114.111.166.70:4008 ESTABLISHED 4
```

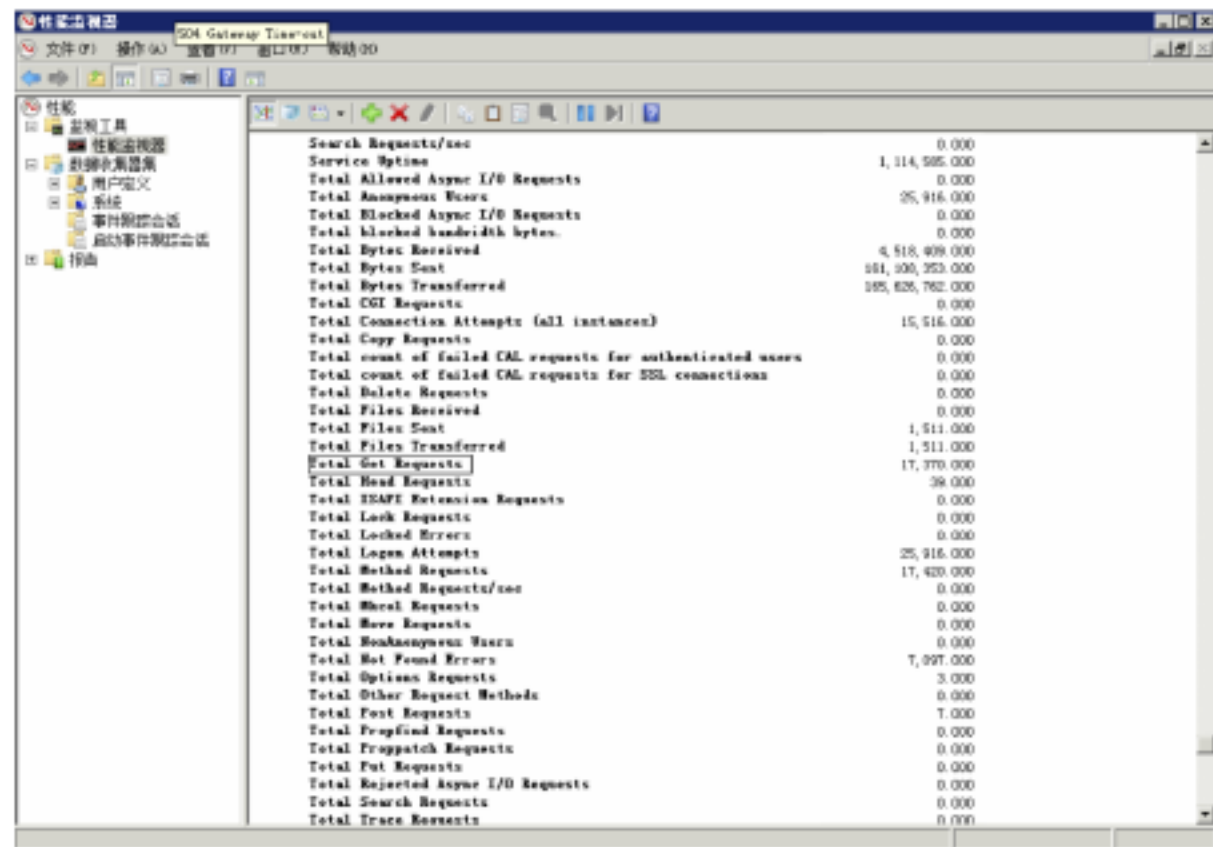
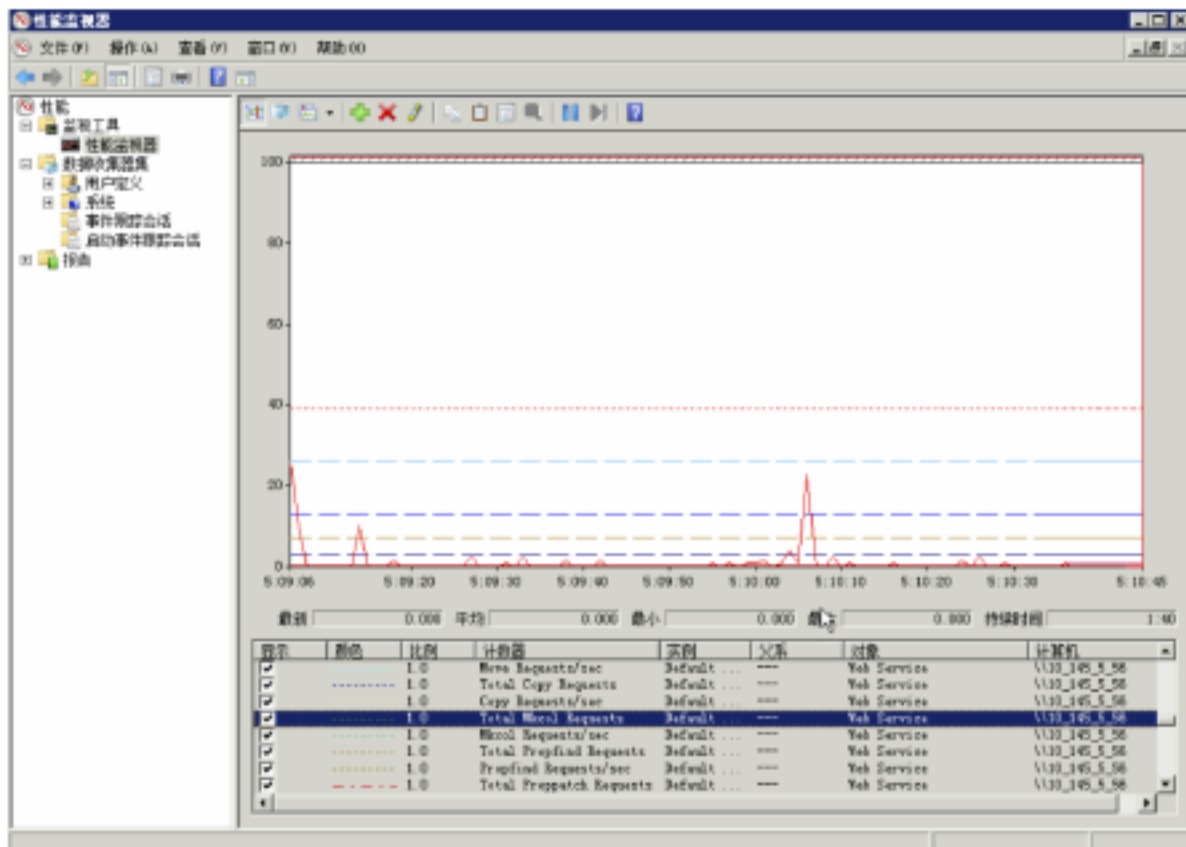
```
linfdeMacBook-Pro:~ linf$ netstat -an |grep 80
tcp4 0 0 192.168.0.101.53669 123.125.235.231.80 ESTABLISHED
tcp4 0 0 192.168.0.101.53668 123.125.235.231.80 ESTABLISHED
tcp4 0 0 192.168.0.101.53654 123.125.114.101.80 ESTABLISHED
tcp4 0 0 192.168.0.101.53653 208.113.168.54.80 LAST_ACK
tcp4 0 0 192.168.0.101.52930 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52929 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52928 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52927 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52926 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52925 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52923 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52922 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52921 61.135.185.247.80 ESTABLISHED
tcp4 0 0 192.168.0.101.52863 101.227.169.161.8080 ESTABLISHED
tcp46 0 0 *.*.80 *.* LISTEN
udp6 0 0 fe80::82e6:50ff::4500 *.*
udp6 0 0 fe80::82e6:50ff::500 *.*
udp6 0 0 fe80::a8ce:42ff::4500 *.*
udp6 0 0 fe80::a8ce:42ff::500 *.*
udp6 0 0 fe80::8ab:c826:5.123 *.*
udp6 0 0 fe80::8ab:c826:5.4500 *.*
udp6 0 0 fe80::8ab:c826:5.500 *.*
udp6 0 0 fe80::1%1c0.4500 *.*
```





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

- accesschk.exe
- ADInsight.exe
- autorunsc.exe
- Coreinfo.exe
- dbgview.chm
- diskext.exe
- du.exe
- hex2dec.exe
- LoadOrd.exe
- pagedfrg.hlp
- PORTMON.HLP
- Procmon.exe
- pskill.exe
- PsService.exe
- RAMMap.exe
- RootkitRevealer.exe
- streams.exe
- Tcpview.exe
- Winobj.exe

- AccessEnum.exe
- adrestore.exe
- Bginfo.exe
- ctrl2cap.amd.sys
- Dbgview.exe
- Diskmon.exe
- efsdump.exe
- junction.exe
- logonsessions.exe
- pendmoves.exe
- procdump.exe
- PsExec.exe
- PsList.exe
- psshutdown.exe
- readme.txt
- sdelete.exe
- strings.exe
- Vmmap.chm
- WINOBJ.HLP

- AdExplorer.chm
- Autologon.exe
- Cacheset.exe
- ctrl2cap.exe
- Desktops.exe
- DISKMON.HLP
- Eula.txt
- ldmdump.exe
- movefile.exe
- pipelist.exe
- procexp.chm
- psfile.exe
- PsLoggedon.exe
- pssuspend.exe
- RegDelNull.exe
- ShareEnum.exe
- sync.exe
- vmmap.exe
- ZoomIt.exe

- ADExplorer.exe
- autoruns.chm
- Clockres.exe
- ctrl2cap.nt4.sys
- Disk2vhd.chm
- DiskView.exe
- FindLinks.exe
- Listdlls.exe
- ntfsinfo.exe
- PORTMON.CNT
- procexp.exe
- PsGetsid.exe
- psloglist.exe
- Pstools.chm
- regjump.exe
- ShellRunas.exe
- Tcpvcon.exe
- Volumeid.exe

- ADInsight.chm
- autoruns.exe
- Contig.exe
- ctrl2cap.nt5.sys
- disk2vhd.exe
- DMON.SYS
- handle.exe
- livekd.exe
- pagedfrg.exe
- portmon.exe
- procmon.chm
- PsInfo.exe
- pspasswd.exe
- psversion.txt
- RootkitRevealer.chm
- sigcheck.exe
- tcpview.chm
- whois.exe



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 