目录 | Content

1 Web Hack

2 Windows Hack

3 Linux Hack

Web Hack

SQL 注入

跨站（XSS）

上传漏洞

逻辑错误

用户认证

错误信息

容器及框架

安全工具

Web Hack / SQL 注入

http://site/news.php?*id=1* ▶ Select * from table_name where *id=1*

http://site/news.php?*id=1'* ▶ Select * from table_name where *id=1'*

Web Hack / SQL 注入

```
mysql> describe users;
+----------+---------------+------+-----+---------+-------+
| Field    | Type          | Null | Key | Default | Extra |
+----------+---------------+------+-----+---------+-------+
| id       | int(5)        | NO   |     | NULL    |       |
| username | varchar(100)  | NO   |     | NULL    |       |
| desc     | varchar(1000) | NO   |     | NULL    |       |
+----------+---------------+------+-----+---------+-------+
3 rows in set (0.00 sec)

mysql> select * from users where id=1;
+----+----------+---------------+
| id | username | desc          |
+----+----------+---------------+
|  1 | Tom      | Yes.I'm here. |
+----+----------+---------------+
1 row in set (0.00 sec)

mysql> select * from users where id=1 union select 1,2;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql>
mysql> select * from users where id=1 union select 1,2,3;
+----+----------+---------------+
| id | username | desc          |
+----+----------+---------------+
|  1 | Tom      | Yes.I'm here. |
|  1 | 2        | 3             |
+----+----------+---------------+
2 rows in set (0.00 sec)
```

http://site/news.php?*id=1*

http://site/news.php?*id=1 union select 1,2*

http://site/news.php?*id=1 union select 1,2,3*

Web Hack / SQL 注入 / 防御

检查/限制：id 参数的类型（int）

（参考：security.database.sql-injection.php）

http://site/news.php?*id=1 union select 1,2,3*

使用 ESAPI

（参考：OWASP ESAPI Project）

限制：id 传入程序的长度

（参考：security.database.sql-injection.php）

Web Hack ／跨站（XSS）

XSS Phishing

Web Hack / 跨站（XSS） / 防御

- 转义 而非 过滤
- 检查外部引用
- OWASP ESAPI

Web Hack / 上传漏洞

常见三种不彻底的检查方式

JavaScript
本地检查

HTTP
内容（头部）检查

服务器端
文件类型检查

Web Hack / 上传漏洞

常见三种不彻底的检查方式

JavaScript
本地检查

```
<script type="text/javascript">
var validFilesTypes = ["png", "jpg", "jpeg", "gif"];

function ValidateFile() {
var file = document.getElementById("<%=FileUpload1.ClientID%>");
var filePath = file.value;
var ext = filePath.substring(filePath.lastIndexOf(".")  + 1, filePath.length).toLowerCase();

var isValidFile = false;
for (var i = 0; i < validFilesTypes.length;  i++) {
   if (ext == validFilesTypes[i]) {
   isValidFile = true;
  break;    }  }

if (!isValidFile)  {
alert("无效的文件。请上传文件扩展名为：\n\n"  + validFilesTypes.join(",  "));
}

return isValidFile;
}
</script>
```

Web Hack / 上传漏洞

常见三种不彻底的检查方式

HTTP

内容（头部）检查

```
POST
http://site/upload.php?action=save&amp;formID=Form&amp;objID=pic&amp;rnd=2015/5/25%2023:
28:59 HTTP/1.1
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Content-Type: multipart/form-data; boundary=---------------------------7df1d91e0234
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Content-Length: 90759
Host: site
Pragma: no-cache
Cookie: JSession=B43DA7E6760C2EA28DB5822D2421C89F;
----------------------------7df1d91e0234
Content-Disposition: form-data; name="file";; filename="c99.php";
Content-Type: text/plain

<?php
//Starting calls
if (!function_exists("getmicrotime")) {function getmicrotime() {list($usec, $sec) = explode(" ",
microtime()); return ((float)$usec + (float)$sec);}}
error_reporting(5);
@ignore_user_abort(TRUE);
.............................
```

Web Hack / 上传漏洞

常见三种不彻底的检查方式

服务器端
文件类型检查

c99.php + wallpaper.jpg = wallpaper.php;.jpg

mime_content_type(“wallpaper.php;.jpg”) = image/jpeg

Web Hack / 上传漏洞 / 防御

- 任何JS检查都不可信任
- 任何局部检查都不可信任
- 可写则不可执行、可执行则不可写

Web Hack / 逻辑错误

- 权限逻辑错误
- 业务逻辑错误

Web Hack / 逻辑错误

- 权限逻辑错误

1

http://site/private_msg.php?*id=1*

http://site/private_msg.php?*id=100*

Web Hack / 逻辑错误

- 权限逻辑错误

2

http://site/download.php?*file=/upload/abc.rar*

http://site/download.php?*file=../../../../../../etc/passwd*

Web Hack / 逻辑错误

- 权限逻辑错误

3

http://site/file.php?id=3&*type=view*

http://site/file.php?id=3&*type=edit*

Web Hack / 逻辑错误

- 业务逻辑错误

正常的

[USER] -> A -> B -> C

危险的

[USER] -> A -> C

[USER] -> C -> B

[USER] -> C

Web Hack / 逻辑错误 / 防御

更早期、更完整的**安全设计**能力

Web Hack / 用户认证

- 口令破解
- 找回口令

Web Hack / 用户认证

- 找回口令

密码重置信

发件人：[redacted]n.net>

时间： 2012-04-24 13:02:08

收件人：n[redacted]om.com

进入[redacted]网

亲爱的[redacted]ki：

您申请重新设置在[redacted]网的登录密码，请点击下面的链接地址，打开页面完成密码设置操作：

请点击以下链接登陆：

http://p[redacted]net/[redacted]tPwdLink.php?Data=f0be7fc54bb91ef387c21d829c4df2e63bb08572c65583940f2ec56c3d0cae6ac34eb57e70300e8c376e0ad67a01e3d34ced0d6bf34fafd7497e4b3f1067eee47055f4bcc4e0d60f5e68322f291de4b225fb0042f5e2ebb28ce42bf8b093ed06e66c59656d94c2487ec6da4025fba80b

如果以上链接无法点击，请将上述地址复制到您的浏览器地址栏,打开页面即可。

Web Hack / 用户认证

- 找回口令

首页 收件箱 联系人 [收件箱] ...

查看信头 打印 编码 上一封 下一封

[redacted]找回密码

发件人： serv[redacted].com

时间： 2011-08-24 11:09:42

收件人： [redacted]m.com

您好：[redacted]
请您点击以下链接修改您的[redacted]密码：http://www[redacted]o.com/account/GetPassword/?code=reset&uid=12662650&id=GRFUES
您可以通过该链接地址，修改您的[redacted]密码，请您在收到此邮件后尽快进行修改密码操作（请不要超过60分钟）。
【注意】本邮件为系统自动发送的邮件，请不要回复本邮件。
[redacted]管理团队.

Web Hack / 用户认证 / 防御

- 业务**安全设计**能力
- 多个业务环境下，用户泄漏的**信息不可交叉**

Web Hack / 错误信息

异常 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 收藏夹

地址(D) http://[redacted]/search.jsp?keyword='

消息提示

org.springframework.jdbc.UncategorizedSQLException: StatementCallback; uncategorized SQLException for SQL [SELECT ID, TITLE, to_char(NOTICE) NOTICE, PUBLISH_DATE FROM C_NOTICE_view where ismessage=0 and(NOTICE like '%"%' or TITLE like '%"%')]; SQL state [HY000]; error code [22835]; [BEA][Oracle JDBC Driver][Oracle]ORA-22835: Buffer too small for CLOB to CHAR or BLOB to RAW conversion (actual: 70728, maximum: 4000) ; nested exception is java.sql.SQLException: [BEA][Oracle JDBC Driver][Oracle]ORA-22835: Buffer too small for CLOB to CHAR or BLOB to RAW conversion (actual: 70728, maximum: 4000)

more >>

Web Hack / 错误信息

Web Hack / 错误信息 / 防御

- 自定义HTTP 500 错误信息内容
- 用户反馈信息尽量模糊

Web Hack / 容器及框架

- Apache / Nginx / IIS
- Tomcat / WebLogic / WebSphere
- Struts2 / Spring / Hibernate
- Laravel / Flight / Yii / ThinkPHP
- ……
- ……

Web Hack / 安全工具

扫描器

- AppScan / AWVS / Nikto / W3AF
- Wapiti / SQLMap

防御

- Mod_Security / ISAPI Filter

日志分析

- grep / awk
- LogParser

目录 | Content

1 Web Hack

2 Windows Hack

3 Linux Hack

Windows Hack

用户

文件系统

端口与服务

安全策略

系统日志

安全工具

Windows Hack / 用户

SID Security Indentifers

SID 是 Windows 操作系统对用户的唯一识别标识

Windows Hack / 用户

SID Security Indentifers

S-1-5-21-227282834-4902751233-3986278212-500

SID-修订信息-颁发机构-子机构信息-相对ID（系统内）

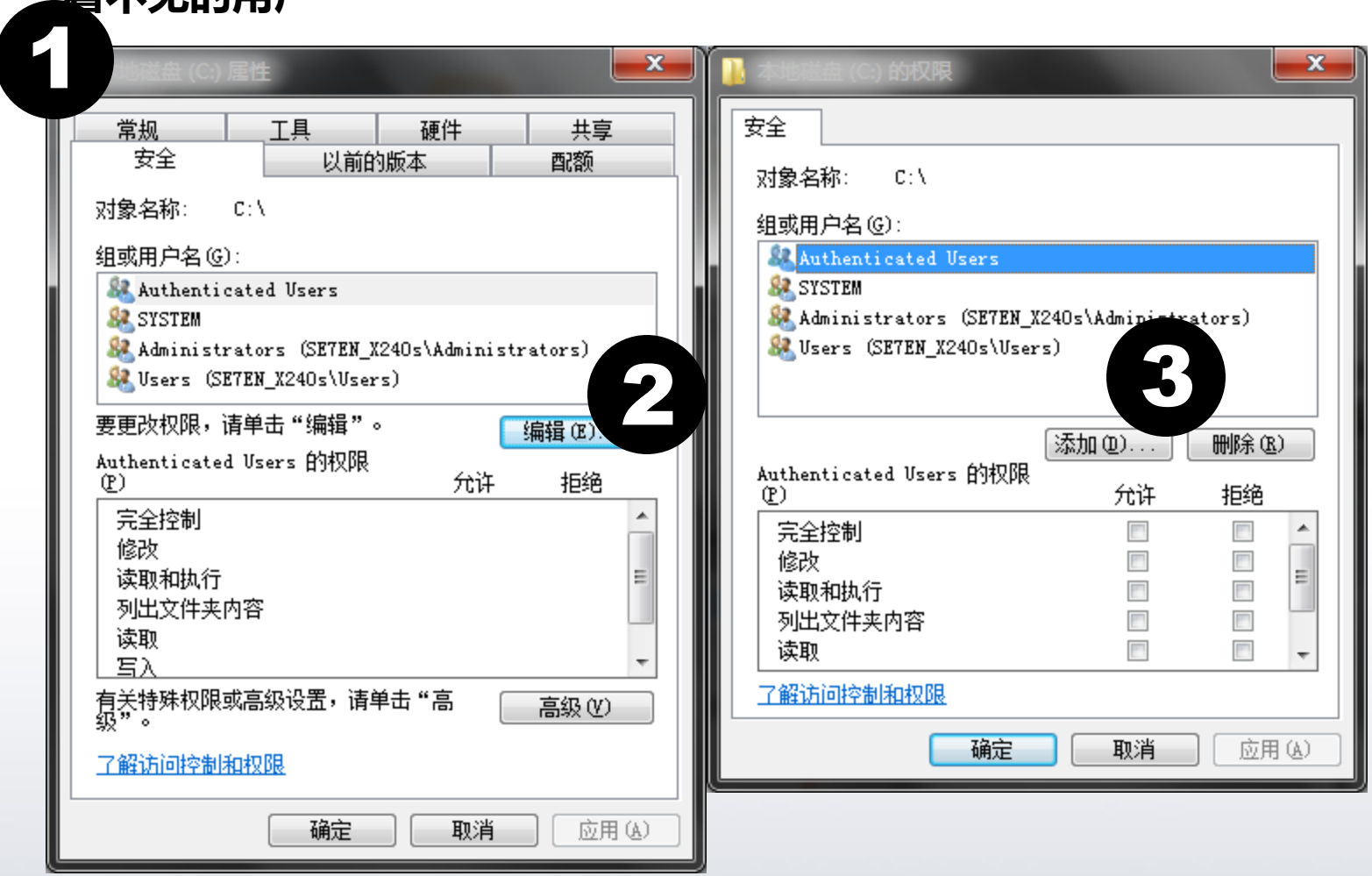
Windows Hack / 用户

命令 ： wmic useraccount get caption,sid

```
C:\Users>wmic useraccount get caption,sid
Caption                 SID
Comp\Administrator      S-1-5-21-2256973234-4228750033-3446299212-500
Comp\Guest              S-1-5-21-2256973234-4228750033-3446299212-501
Comp\HomeGroupUser$     S-1-5-21-2256973234-4228750033-3446299212-1002
Comp\python             S-1-5-21-2256973234-4228750033-3446299212-1000
```

Windows Hack / 用户

看不见的用户

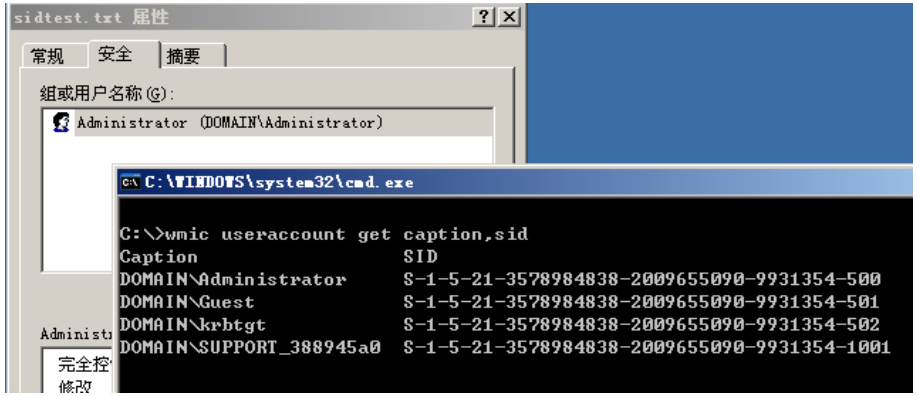


Windows Hack / 用户

看不见的用户

Windows Hack / 用户

SID 与用户名不相关及SID的不可复制性



Windows Hack / 文件系统

ACL

messages 属性

常规 | 共享 | 安全 | 自定义

组或用户名称(G):

- Administrators (PYTHON\Administrators)
- CREATOR OWNER
- SYSTEM
- Users (PYTHON\Users)

添加(D)... 删除(R)

Administrators 的权限(P)	允许	拒绝
完全控制	☑	☐
修改	☑	☐
读取和运行	☑	☐
列出文件夹目录	☑	☐
读取	☑	☐
写入	☑	☐

特别权限或高级设置，请单击“高级”。 高级(V)

确定 取消 应用(A)

messages 的高级安全设置

权限 | 审核 | 所有者 | 有效权限

要查看有关特殊权限的详细信息，请选择一个权限项目，然后单击“编辑”。

权限项目(T):

类型	名称	权限	继承于	应用于
允许	Administrators ...	完全控制	D:\	该文件夹，子文件...
允许	SYSTEM	完全控制	D:\	该文件夹，子文件...
允许	CREATOR OWNER	完全控制	D:\	只有子文件夹及文件
允许	Users (PYTHON\U...	读取和运行	D:\	该文件夹，子文件...
允许	Users (PYTHON\U...	特殊	D:\	该文件夹及子文件夹

添加(D)... 编辑(E)... 删除(R)

☑ 允许父项的继承权限传播到该对象和所有子对象。包括

☐ 用在此显示的可以应用到子对象的项目替代所有子对象

进一步了解访问控制。

ACE

messages 的权限项目

对象

该权限是从父对象继承来的。

名称(N): rators (PYTHON\Administrators) 更改(C)...

应用到(O): 该文件夹，子文件夹及文件

权限(P):	允许	拒绝
完全控制	☑	☐
遍历文件夹/运行文件	☑	☐
列出文件夹/读取数据	☑	☐
读取属性	☑	☐
读取扩展属性	☑	☐
创建文件/写入数据	☑	☐
创建文件夹/附加数据	☑	☐
写入属性	☑	☐
写入扩展属性	☑	☐
删除子文件夹及文件	☑	☐
删除	☑	☐

☐ 将这些权限只应用到这个容器中的对象和/或容器上(T) 全部清除(L)

确定 取消

Windows Hack / 文件系统

NTFS 下的 EFS 加密

Windows Hack / 文件系统

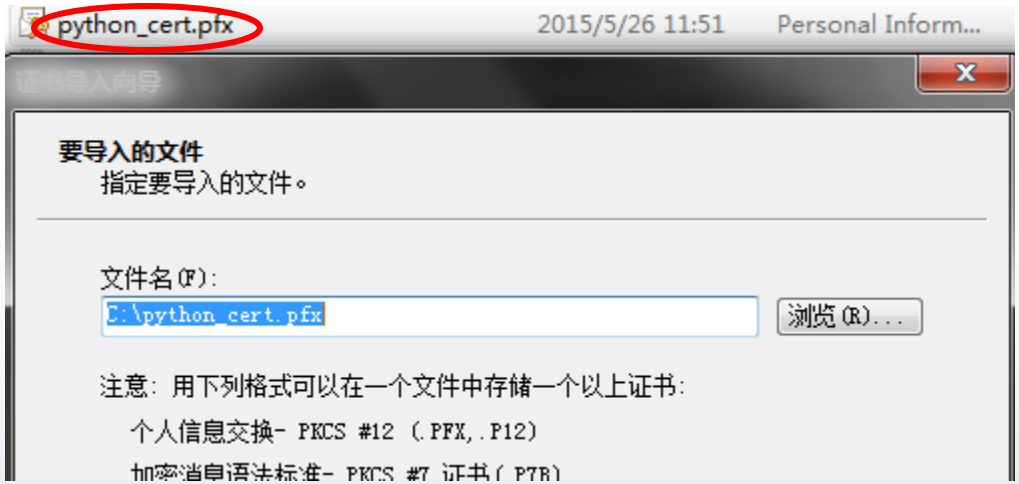
C:\>cipher

清单 C:\
不加密新加到此目录的文件。

U alipay
U CFLog
U Downloads
U Program Files
U Program Files (x86)
U Python25
U Python27
U SWTOOLS
U Temp
E test.txt
U TimeEventNSIS.log
U UpdateChromeLinksLogs
U Users
U Windows

C:\>cipher /x
请输入备份 PFX 文件名。
python_cert.pfx
请键入密码来保护 .PFX 文件:
请重新键入密码来进行确认:

成功备份了 EFS 证书。



EFS 加密 与 EFS 证书备份

Windows Hack / 端口与服务

SMB/CIFS 与 NTLM

VMware Virtual Ethernet Adapter: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

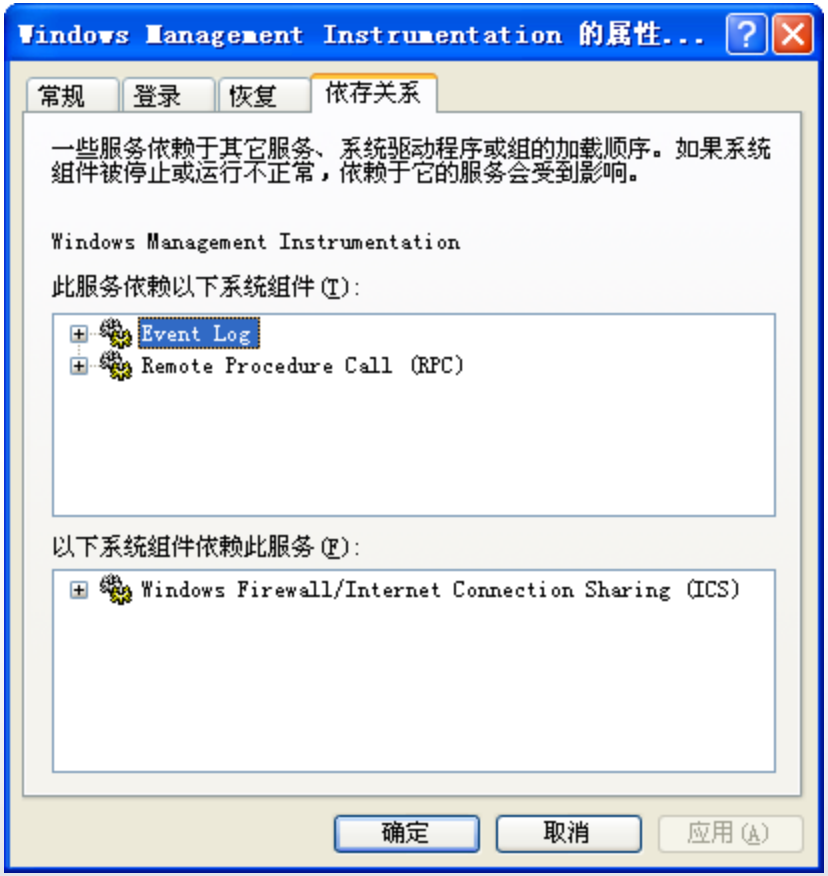
Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	1.1.1.7	1.1.1.101	TCP	2038 > netbios-ssn [SYN] Seq=0 Len=0 MSS=1460
2	0.000543	1.1.1.101	1.1.1.7	TCP	netbios-ssn > 2038 [SYN, ACK] Seq=0 Ack=1 Win=17520
3	0.000571	1.1.1.7	1.1.1.101	TCP	2038 > netbios-ssn [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.000616	1.1.1.7	1.1.1.101	NBSS	Session request, to *SMBSERVER<20> from MBB<00>
5	0.000963	1.1.1.101	1.1.1.7	NBSS	Positive session response
6	0.001005	1.1.1.7	1.1.1.101	SMB	Negotiate Protocol Request
7	0.002478	1.1.1.101	1.1.1.7	SMB	Negotiate Protocol Response
8	0.002644	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
9	0.005477	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
10	0.005818	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
11	0.006520	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
12	0.006747	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
13	0.007310	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
14	0.007502	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
15	0.007994	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
16	0.008172	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
17	0.008733	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
18	0.008919	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
19	0.009402	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
20	0.009575	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
21	0.010052	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied
22	0.010223	1.1.1.7	1.1.1.101	SMB	Session Setup AndX Request, User: DREAM\administrato
23	0.010691	1.1.1.101	1.1.1.7	SMB	Session Setup AndX Response, Error: Access denied

```
⊞ Ethernet II, Src: vmware_c0:00:01 (00:50:56:c0:00:01), Dst: vmware_ca:52:87 (00:0c:29:ca:52:87)
⊞ Internet Protocol, Src: 1.1.1.7 (1.1.1.7), Dst: 1.1.1.101 (1.1.1.101)
⊞ Transmission Control Protocol, Src Port: 2038 (2038), Dst Port: netbios-ssn (139), Seq: 241, Ack: 110, Len: 97
⊞ NetBIOS Session Service
⊟ SMB (Server Message Block Protocol)
  ⊞ SMB Header
  ⊟ Session Setup AndX Request (0x73)
```

Windows Hack ／端口与服务

WMI（Windows Management Instrumentation）



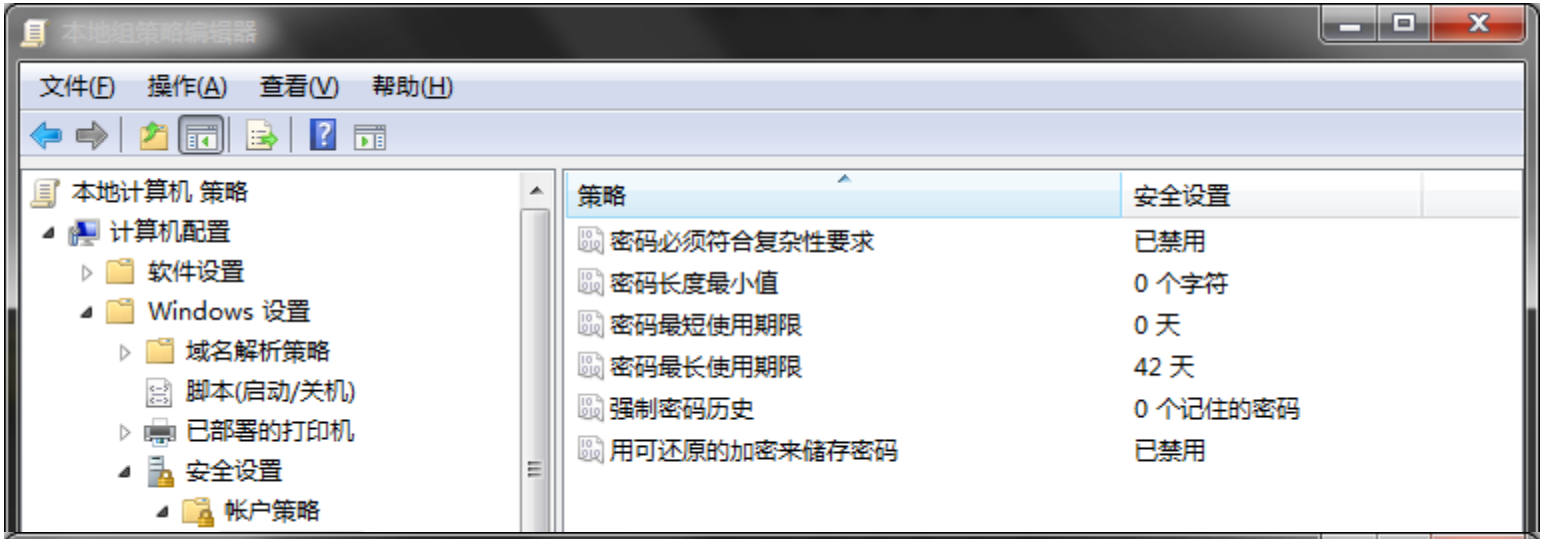
- TCP 135
- 远程（本地）管理
- 远程口令破解
- ……
- ……

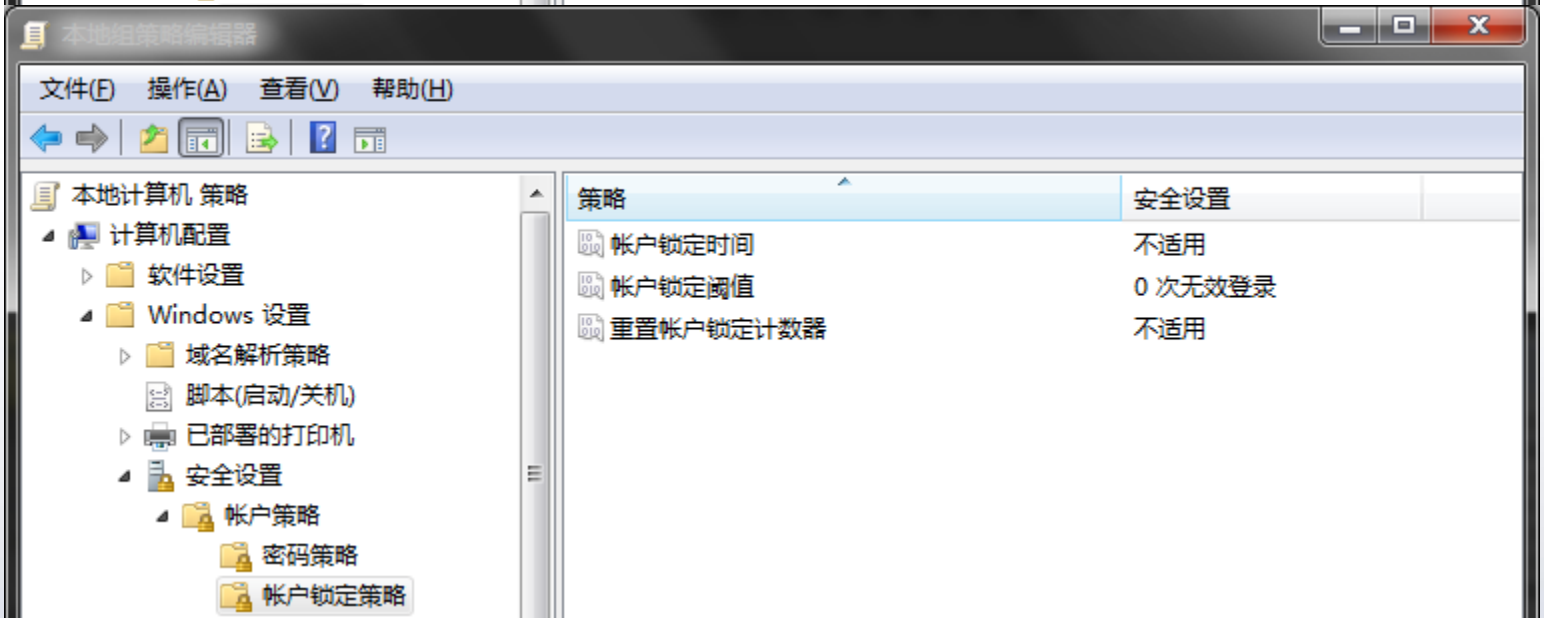
Windows Hack / 安全策略

GPEdit.msc

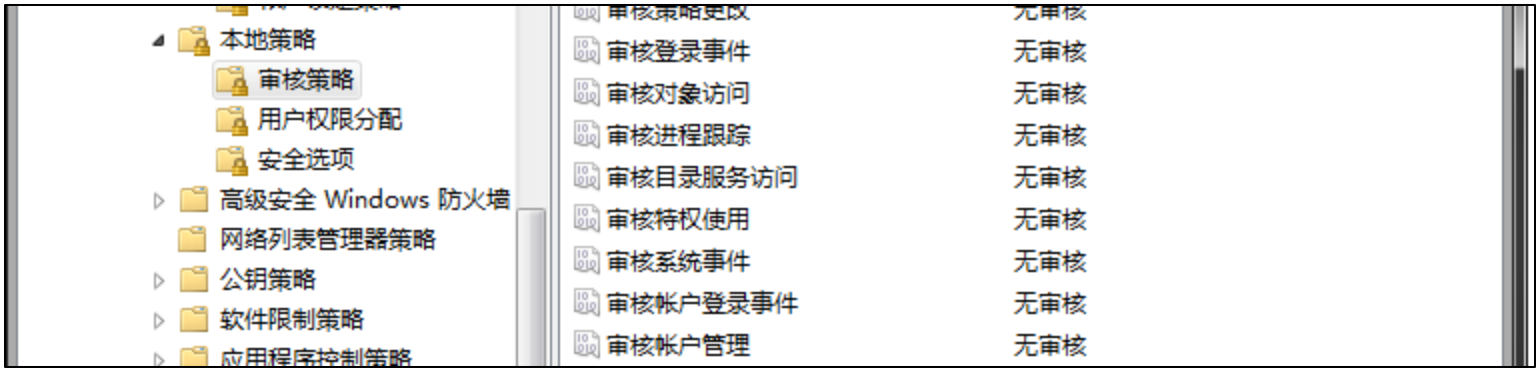
- 账户密码策略
- 账户锁定策略
- 安全审核策略
- 用户权限分配
- 其他安全策略

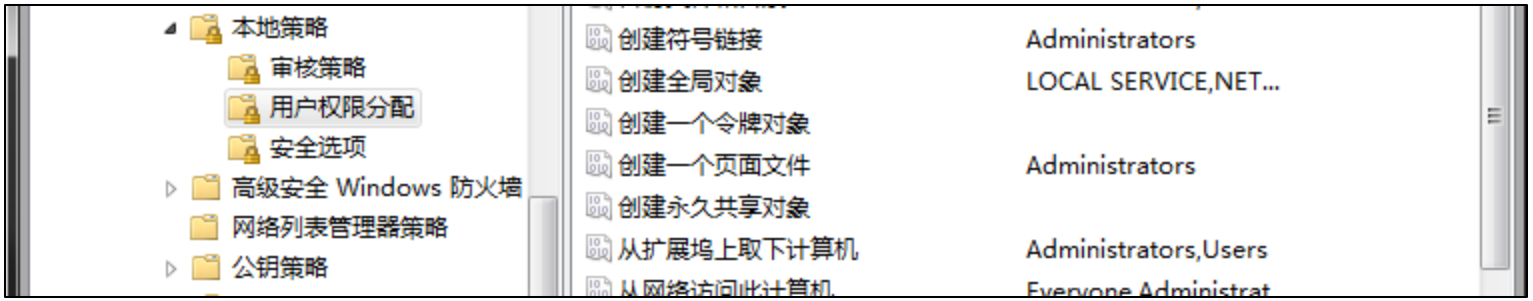
Windows Hack / 安全策略

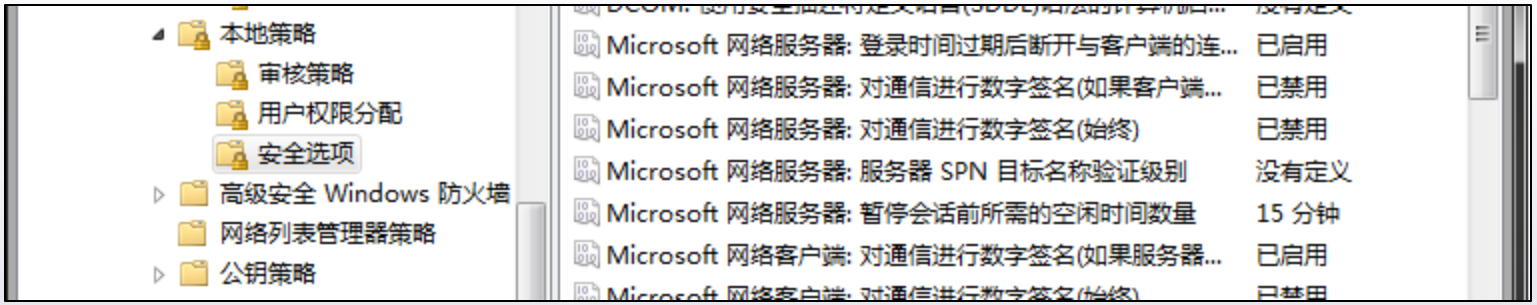




Windows Hack / 安全策略







Windows Hack / 系统日志

EventVwr.exe

- 应用日志
- 安全日志
- 系统日志

Windows Hack ／系统日志

应用日志：第三方应用状态跟踪

应用程序　事件数: 24,985

级别	日期和时间	来源
信息	2015/5/25 22:23:57	MySQL
信息	2015/5/25 22:23:57	MySQL
信息	2015/5/25 22:23:57	MySQL

事件 100，MySQL

常规　详细信息

Server hostname (bind-address): '*'; port: 3306

For more information, see Help and Support Center at http

应用程序　事件数: 24,985

级别	日期和时间	来源
信息	2014/11/3 16:36:43	Desktop Window Manager
信息	2014/11/3 16:34:04	Windows Error Reporting
错误	2014/11/3 16:34:02	Application Error
信息	2014/11/3 16:29:40	Office Software Protection Platform Service
信息	2014/11/3 16:24:40	Office Software Protection Platform Service

事件 1000，Application Error

常规　详细信息

错误应用程序名称: chrome.exe，版本: 36.0.1985.143，时间戳: 0x53e2e515

错误模块名称: chrome.dll，版本: 36.0.1985.143，时间戳: 0x53e2e1c7

异常代码: 0xc0000005

错误偏移量: 0x00f21ffe

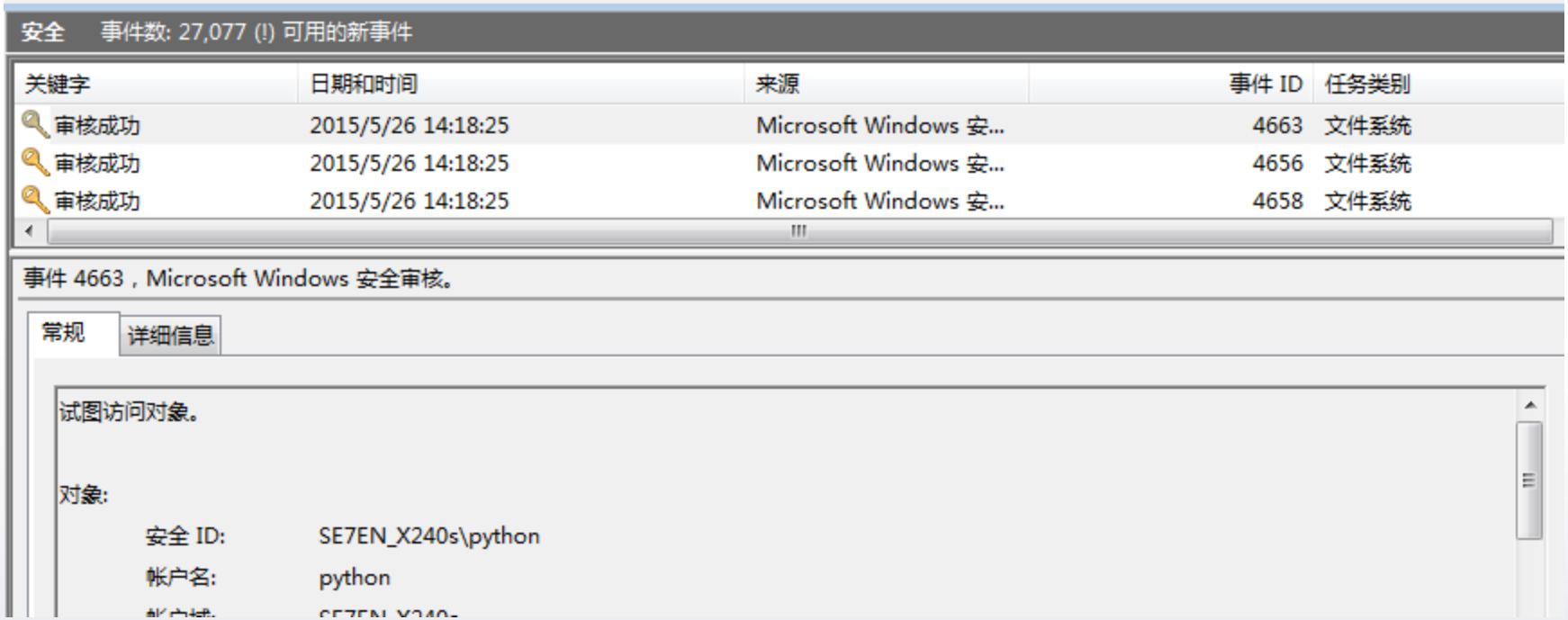
错误进程 ID: 0x790

错误应用程序启动时间: 0x01cff71545b72373

错误应用程序路径: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Windows Hack / 系统日志

安全日志：审核策略跟踪



Windows Hack / 系统日志

安全日志：登录行为审核

安全　事件数: 27,099

关键字	日期和时间	来源	事件 ID	任务类别
审核成功	2015/5/26 14:23:46	Microsoft Windows 安...	4634	注销
审核成功	2015/5/26 14:23:46	Microsoft Windows 安...	4672	特殊登录
审核成功	2015/5/26 14:23:46	Microsoft Windows 安...	4624	登录

事件 4634，Microsoft Windows 安全审核。

常规　详细信息

主题:

安全 ID:　SE7EN_X240s\python

帐户名:　python

帐户域:　SE7EN_X240s

登录 ID:　0x56f280c

登录类型:　7

2 ：交互式登录
3 ：网络登录
7 ：用户解锁

在登录会话被破坏时生成此事件。可以使用登录 ID 值将它和一个登录事件准确关联起来。在同一台计算机上重新启动的区间中，登录 ID 是唯一的。

Windows Hack / 安全工具

Windows 后门检查：常规 —— Autoruns

Autoruns [SE7EN_X240s\python] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter:

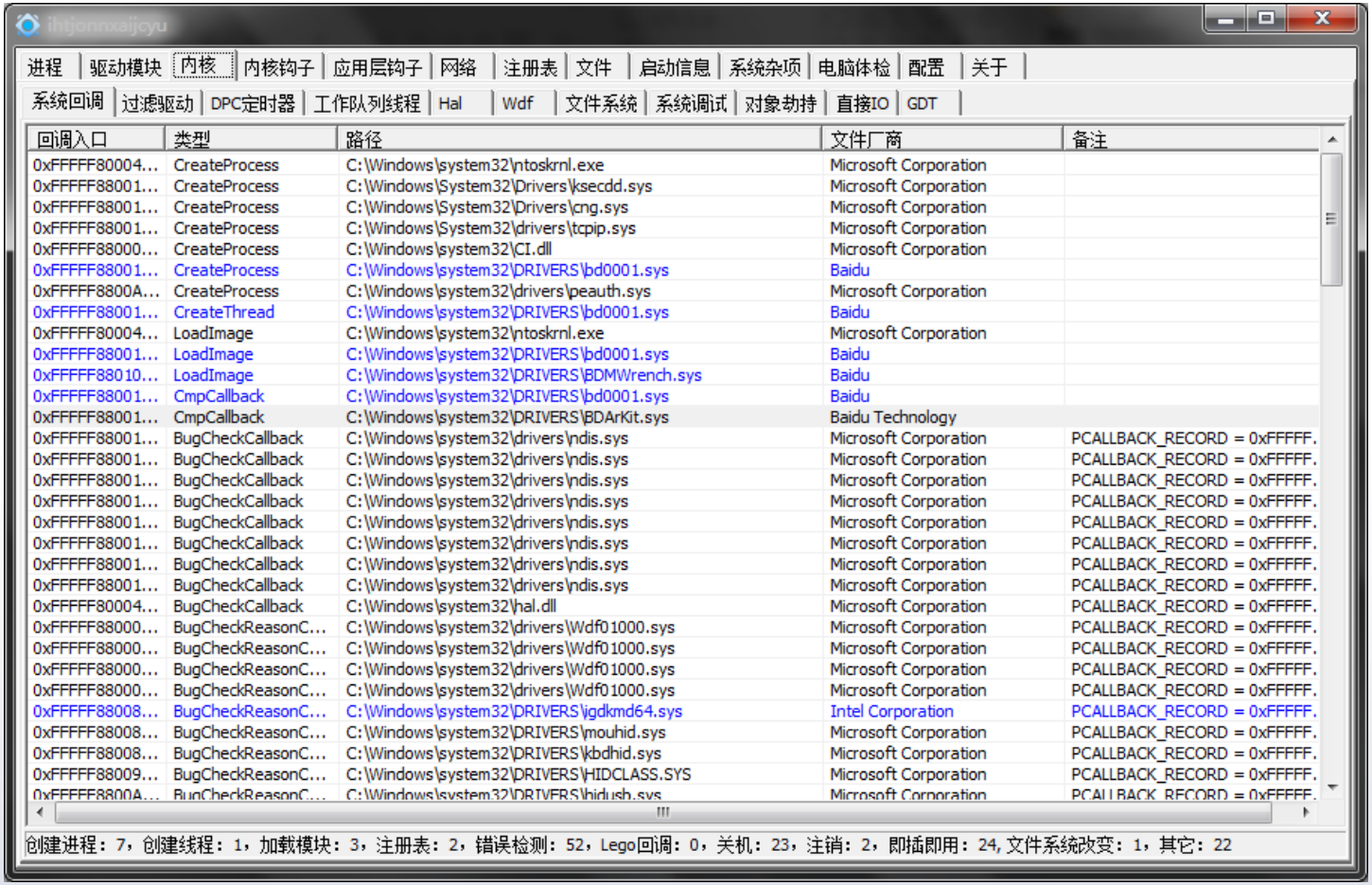
Winsock Providers | Print Monitors | LSA Providers | Network Providers

Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute | In

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2015/3/26 10:36
AdobeAAMUp...	Adobe Updater Startup Utility	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\oobe\pdapp\uwa\updaterstartuputility.exe	2012/3/25 6:49
baidusdTray	百度杀毒托盘程序	百度在线网络技术（北京...	c:\program files (x86)\baidu\baidusd\3.0.0.4605\baidusdtray.exe	2015/2/27 17:31
Hoekey	System-wide hotkey utility	bCheck	d:\tools\hoekey116\hoekey.exe	2006/5/6 23:30
ISCT Tray	ISCT SysTray	Intel Corporation	c:\program files\intel\intel(r) smart connect technology agent\isctsystray8.exe	2014/4/4 5:55
Railendar	Rainlendar2		c:\program files (x86)\rainlendar2\rainlendar2.exe	2013/3/11 1:58
SynTPEnh	Synaptics TouchPad 64-bit ...	Synaptics Incorporated	c:\program files\synaptics\syntp\syntpenh.exe	2014/4/8 1:50
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2015/3/26 10:39
AdobeCS6Ser...	Adobe CS6 Service Manager	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\cs6servicemanager\cs6servicemanager.exe	2012/3/9 23:25
baidusdTray	百度杀毒托盘程序	百度在线网络技术（北京...	c:\program files (x86)\baidu\baidusd\3.0.0.4605\baidusdtray.exe	2015/2/27 17:31
IMSS	PIcon startup utility	Intel Corporation	c:\program files (x86)\intel\intel(r) management engine components\imss\piconstartup.exe	2013/6/27 6:40
InterPass3000...	certreg MFC Application	ICBC OEM From Feitian Te...	c:\program files (x86)\icbcebanktools\feitian-interpass3000\certd_nps3000_icbc.exe	2014/8/29 9:20
iTunesHelper	iTunesHelper	Apple Inc.	c:\program files (x86)\itunes\ituneshelper.exe	2014/10/15 18:56
MiWiFi			c:\program files (x86)\xiaomi\miwifi\miwifimonitor.exe	2014/8/18 16:02

Windows Hack / 安全工具

Windows 后门检查：Hook —— PC Hunter



回调入口	类型	路径	文件厂商	备注
0xFFFFF80004...	CreateProcess	C:\Windows\system32\ntoskrnl.exe	Microsoft Corporation	
0xFFFFF88001...	CreateProcess	C:\Windows\System32\Drivers\ksecdd.sys	Microsoft Corporation	
0xFFFFF88001...	CreateProcess	C:\Windows\System32\Drivers\cng.sys	Microsoft Corporation	
0xFFFFF88001...	CreateProcess	C:\Windows\System32\drivers\tcpip.sys	Microsoft Corporation	
0xFFFFF88000...	CreateProcess	C:\Windows\system32\CI.dll	Microsoft Corporation	
0xFFFFF88001...	CreateProcess	C:\Windows\system32\DRIVERS\bd0001.sys	Baidu	
0xFFFFF8800A...	CreateProcess	C:\Windows\system32\drivers\peauth.sys	Microsoft Corporation	
0xFFFFF88001...	CreateThread	C:\Windows\system32\DRIVERS\bd0001.sys	Baidu	
0xFFFFF80004...	LoadImage	C:\Windows\system32\ntoskrnl.exe	Microsoft Corporation	
0xFFFFF88001...	LoadImage	C:\Windows\system32\DRIVERS\bd0001.sys	Baidu	
0xFFFFF88010...	LoadImage	C:\Windows\system32\DRIVERS\BDMWrench.sys	Baidu	
0xFFFFF88001...	CmpCallback	C:\Windows\system32\DRIVERS\bd0001.sys	Baidu	
0xFFFFF88001...	CmpCallback	C:\Windows\system32\DRIVERS\BDArKit.sys	Baidu Technology	
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88001...	BugCheckCallback	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF80004...	BugCheckCallback	C:\Windows\system32\hal.dll	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88000...	BugCheckReasonC...	C:\Windows\system32\drivers\Wdf01000.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88000...	BugCheckReasonC...	C:\Windows\system32\drivers\Wdf01000.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88000...	BugCheckReasonC...	C:\Windows\system32\drivers\Wdf01000.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88000...	BugCheckReasonC...	C:\Windows\system32\drivers\Wdf01000.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88008...	BugCheckReasonC...	C:\Windows\system32\DRIVERS\igdkmd64.sys	Intel Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88008...	BugCheckReasonC...	C:\Windows\system32\DRIVERS\mouhid.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88008...	BugCheckReasonC...	C:\Windows\system32\DRIVERS\kbdhid.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF88009...	BugCheckReasonC...	C:\Windows\system32\DRIVERS\HIDCLASS.SYS	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.
0xFFFFF8800A...	BugCheckReasonC...	C:\Windows\system32\DRIVERS\hidusb.sys	Microsoft Corporation	PCALLBACK_RECORD = 0xFFFFF.

Windows Hack / 安全工具

Windows 调试工具集 —— Sysinternals

http://live.sysinternals.com/

Linux Hack

用户

passwd & shadow

文件系统

系统日志

后门检查

安全工具

Linux Hack / 用户

UID User Indentifer

UID 相对 SID 更加简单、直接

Linux Hack / 用户

UID User Indentifer

UID = 0 ，便是 root

```
root@Sec:~# grep test /etc/passwd
test:x:1001:1001::/home/test:
root@Sec:~# id test
uid=1001(test) gid=1001(test) groups=1001(test)
root@Sec:~# vim /etc/passwd
root@Sec:~# grep test /etc/passwd
test:x:0:1001::/home/test:
root@Sec:~# id test
uid=0(root) gid=1001(test) groups=0(root)
```

Linux Hack / passwd & shadow

/etc/passwd

nobody:x:99:99:Nobody:/:/sbin/nologin

用户名:密码:UID:GID:全名:主目录:shell

/etc/shadow

root:1ldYmgH8A$UWj6aj4a3Gn4KsrxWo0:13661:0:99999:7:::

Salt（4096种）

Linux Hack / passwd & shadow

```
root@Sec:~# ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root       1212  5 26  23:20 /etc/passwd
-rw-r----- 1 root shadow  773   5 26  23:20 /etc/shadow
```

文件的 inode

每个文件中

包含信息

- 文件所有者的UID/GID
- 类型，大小，位置等
- 创建时间，访问时间，修改时间等
- 权限信息（Permission Bits）

Linux Hack / 文件系统

文件的 inode

```
root@Sec:~# df -i
Filesystem                Inodes   IUsed   Ifree     IUse%  Mounted on
/dev/mapper/Sec-root 1228800  65834  1162966   6%     /
none                      126302    2       126300    1%     /sys/fs/cgroup
udev                      123510   488      123022    1%     /dev
tmpfs                     126302   543      125759    1%     /run
none                      126302    4       126298    1%     /run/lock
none                      126302    1       126301    1%     /run/shm
none                      126302    2       126300    1%     /run/user
/dev/sda1                  62248   298       61950    1%     /boot
```

Permission Bits

```
root@Sec:~# ls -l /etc/passwd
-rw-r--r-- 1 root root      1212  5 26  23:20 /etc/passwd
```

-rw-r--r--

文件类型 | 所有者权限 | 用户组权限 | 其他用户权限

Permission Bits

文件类型

- 普通文件
d 目录
b block
c character
l symbolic link
p pipe
s socket

权限标识

r 读
w 写
x 执行
s setuid, setgid
t 粘住位

Linux Hack / 文件系统

Permission Bits —— 危险的SetUID

```
root@Sec:~# ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 47032  2 17  2014 /usr/bin/passwd
```

Linux Hack / 文件系统

Permission Bits —— 哪些文件设置了SetUID

root@Sec:~# find /usr /bin -perm -4000

/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/mtr
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/sbin/pppd
/usr/sbin/uuidd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/bin/mount
/bin/su
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ping

umask

[root@RHEL5 home]# **umask**
0022

[root@RHEL5 home]# **touch file1**
[root@RHEL5 home]# **ls -l file1**
-rw-r--r-- 1 root root 0 Jul 26 07:17 file1
(644)

[root@RHEL5 home]# **umask 0066**
[root@RHEL5 home]# **touch file2**
[root@RHEL5 home]# **ls -l file2**
-rw------- 1 root root 0 Jul 26 07:18 file2
(600)

[root@RHEL5 home]# **umask 0**
[root@RHEL5 home]# **umask**
0000
[root@RHEL5 home]# **touch file3**
[root@RHEL5 home]# **ls -l file3**
-rw-rw-rw- 1 root root 0 Jul 26 07:25 file3 (666)

Linux Hack / 文件系统

权限最特殊的目录 —— /tmp

```
root@Sec:~# find / -perm -0777 -type d
/var/crash
/tmp
/run/shm
/run/lock
```

所有 Linux/UNIX 中都会存在的 **777** 目录

Linux Hack / 系统日志

w	当前的登录
last	最近的登录
lastlog	所有用户最近的登录
dmesg	启动信息
history	最近N条命令历史（N = $HISTSIZE）
/var/log/auth.log (secure)	安全认证模块产生的日志
/var/log/apache2 (httpd)	Apache 日志
/var/log/mysql	MySQL 日志

Linux Hack / 系统日志

口令破解 —— /var/log/auth.log (secure)

```
May 27 00:13:07 Sec sshd[2051]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.7.11  user=root
May 27 00:13:07 Sec sshd[2049]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.7.11  user=root
May 27 00:13:07 Sec sshd[2050]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.7.11  user=root
May 27 00:13:07 Sec sshd[2048]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.7.11  user=root
May 27 00:13:10 Sec sshd[2051]: Failed password for root from 192.168.7.11 port 51586 ssh2
May 27 00:13:10 Sec sshd[2049]: Failed password for root from 192.168.7.11 port 51584 ssh2
May 27 00:13:10 Sec sshd[2050]: Failed password for root from 192.168.7.11 port 51585 ssh2
```

Linux Hack / 系统日志

异常登录 —— lastlog

```
root@SecEdu:~# lastlog
Username         Port     From             Latest
root                                      **Never logged in**
daemon                                    **Never logged in**
bin              pts/0    192.168.1.109    Apr 3 21:00:01 +0800 2015
……................
……................
mysql                                     **Never logged in**
messagebus                                **Never logged in**
landscape                                 **Never logged in**
python           pts/0    192.168.7.11     May 27 00:11:05 +0800 2015
sshd                                      **Never logged in**
```

Linux Hack / 系统日志

history 命令 加上时间标签

export HISTTIMEFORMAT="%F %T "

```
root@SecEdu:~# history
    1  2015-05-27 00:07:27 ifconfig eth0 up
    2  2015-05-27 00:07:27 ifconfig eth0 192.168.7.77 netmask 255.255.255.0
    3  2015-05-27 00:07:27 ping 192.168.7.11
    4  2015-05-27 00:07:27 ifconfig
    5  2015-05-27 00:07:27 tasksel
    6  2015-05-27 00:07:27 cat /etc/apt/sources.list
    7  2015-05-27 00:07:27 cat /etc/apt/sources.list | grep -i rom
    8  2015-05-27 00:07:27 vim
    9  2015-05-27 00:07:27 cp /usr/share/vim/vimrc ./.vimrc
   10  2015-05-27 00:07:27 vim .vimrc
   11  2015-05-27 00:07:27 cp .vimrc /home/python/
   12  2015-05-27 00:07:27 vim /etc/apt/sources.list
```

Linux Hack ／系统日志

日志采集最佳流程

- w
- last
- history
- lastlog
- 其他

- 内存信息
- 网络信息
- 结果影响最小
- 固化信息（硬盘、非动态信息）

Linux Hack / 后门检查

```
root@SecEdu:~# chkrootkit
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
Checking `ifconfig'...                                      not infected
Checking `inetd'...                                         not infected
Checking `inetdconf'...                                     not found
Checking `identd'...                                        not found
```

Chkrootkit

```
root@SecEdu:~# rkhunter -c
[ Rootkit Hunter version 1.4.0 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                              [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                       [ None found ]
    Checking for preloaded libraries                        [ None found ]
    Checking LD_LIBRARY_PATH variable                       [ Not found ]

  Performing file properties checks
    Checking for prerequisites                              [ OK ]
    /usr/sbin/adduser                                       [ OK ]
    /usr/sbin/chroot                                        [ OK ]
    /usr/sbin/cron                                          [ OK ]
    /usr/sbin/groupadd                                      [ OK ]
    /usr/sbin/groupdel                                      [ OK ]
    /usr/sbin/groupmod                                      [ OK ]
    /usr/sbin/grpck                                         [ OK ]
    /usr/sbin/nologin                                       [ OK ]
    /usr/sbin/pwck                                          [ OK ]
    /usr/sbin/rsyslogd                                      [ OK ]
    /usr/sbin/tcpd                                          [ OK ]
```

Rootkit Hunter

Linux Hack / 安全工具

- AFICK / integrit
- John the Ripper
- Snort / TCPDump
- TCP Wrappers

More : http://sectools.org/

THANKS