原 Linux系统入侵痕迹分 证

2017年08月28日 15:25:58 阅读数：1527

获取基本信息

向服务器运维人员询问，系统的基 ，安装的发行版本，建立和使用的账户，
所在网络拓扑的位置、网络配置情 其所承载的服务。

系统信息

```
[root@localhost ~]# uname -a
- 省略......
[root@localhost ~]# lsb_version -a
- 省略......
[root@localhost ~]# head -n 1 /etc/issue
- 省略......
```

用户及组

```
[root@localhost ~]# cut -d: -f1 /etc/passwd
- 省略......
[root@localhost ~]# cut -d: -f1 /etc/group
- 省略......
```

防火墙及路由

```
[root@localhost ~]# iptables -L
- 省略......
[root@localhost ~]# route -n
- 省略......
```

获取网络信息

网络接口

```
[root@localhost ~]# ifconfig -a
```

开放端口

```
[root@localhost ~]# netstat -tanp
[root@localhost ~]# ss -tanp
```

系统运行状态

计划任务

系统cron任务

```
检查 /etc/crontab 有无存在异常项
```

用户cron任务

```
1 检查各用户cron任务
2 每个用户都有专用的cron任务文件 /var/spool/cron/USERNAME
```


进程和服务

ps

```
1 使用 ps 命令查看当前运行的进程
```

- PS常用组合
  - ps aux
    - a 与终端相关的进程
    - u 以用户为中心组织进程状态显示
    - x 与终端无光的进程
  - ps -ef
    - e 显示所有进程
    - f 显示完整格式程序信息
  - ps -eFH
    - e 显示所有进程
    - F 显示完整格式的进程信息
    - H 以进程层级格式显示进程相关信息

top、htop

```
1 使用 top 或 htop 命令用来显示系统中正在运行的进程的实时状态CPU 利用情
2 况、内存消耗情况，以及每个进程情况
```

启动服务

```
1 使用 chkconfig 或 systemctl 命令列出所有启动的系统服务 程序
```

日志分析

登录日志

二进制日志文件 [登录]

```
1 1. 最近一次注册日志
2 [ /var/log/lastlog ] # 最近一次用户登录的时间记录
```

```
1 2. 用户登录日志
2 [ /var/log/wtmp ]
3 [root@localhost ~]# last
4 - 或
5 [root@localhost ~]# last -f <filename> # 指定输入文件
```

应用日志

1. Apache服务器日志

```
1 /var/log/httpd/access.log # 其中包含Apache服务器的客户系统访问记录
2
3 /var/log/httpd/error.log # 其中包含Apache服务器的所有出错记录
```

2. CUPS打印系统日志

```
/var/log/cups/access_log # 志文件，其中记录了打印机的设置情
况，提交的打印作业，以及打印作 态记录等信息

/var/log/cups/error_log # 日志文件，存储各种错误信息
```

3. Samba 服务器日志

```
> [目录] /var/log/samba
[root@localhost ~]# ls /var samba
> log.smbd # 其中包含Samba服 动以及SMB/CIFS文件与打印共享方面的信息
> log.nmbd # 其中包含基于IP NETBIOS网络通信方面的信息
> log.sysname # 用于记录特定 统的服务请求信息，文件名中的sysname是客户系统的主机名，如 log.winxp
```

4. 其他日志

```
/var/log/xferlog # 用于记录FTP服务器的文件传输日志信息
/var/log/mysqld.log # 用于记 QL数据库服务器的日志信息
/var/log/yum.log # 用于记录 n安装、删除或更新软件的日志信息
```

系统日志

1. 系统内核环形缓冲区

```
/var/log/dmesg 日志文件，重现系统引导过程中控制台的输出信息。如果在引
导过程中出现问题，系统内核引导信息有助于诊断问题，分析产生问题的原因
```

> [root@localhost ~]# dmesg | less

2. 系统消息日志

```
/var/log/messages 是系统信息的集中存储位置，除了专门的日志文件之外，
其中记录了大部分系统进程、使用程序甚至应用程序输出的日志信息。
```

3. 安全审计日志

```
/var/log/audit/audit.log 用于记录系统安全审计信息，尤其是SELinux安全审计信息
```

3. 安全认证日志

```
/var/log/secure 用于记录系统安全认证信息，包含验证和授权方面信息，尤
其是sshd会将所有信息记录[其中包括失败登录]在这里信息

/var/log/auth.log 同上
```


文章标签： linux 取证 日志

个人分类： Linux

相关热词： linux系统g linux系统卡 linux系统题 linux系统r linux系统双

上一篇 Apache2.2.x 安装与配置详解

下一篇 CentOS7下的LAMP搭建

区块链开发学习线图（高薪）

区块链开发平均薪资是多少？快速学习区块[illegible]，掌握以太坊开发和智能合约应用。

UNIX/Linux系统取证之信息采集[illegible] - CSDN博客 7-16

在UNIX/Linux系统取证中,及时收集硬盘的[illegible]非重要,《Unix/Linux网络日志分析与流量监控》一书中,将详细讨论各种常见系统进程系...

使用Linux 工具进行计算机取证 - [illegible]博客 7-9

使用Linux 工具进行计算机取证　本文通过[illegible]inux 系统工具(Ftkimage、xmount、Volatility、dd、netcat)来介绍使用计算机取证的方...

Linux入侵取证：从一次应急事件[illegible] 1622

转载地址：http://www.freebuf.com/article[illegible]em/50728.html 0×00 背景 最近接手了一起应急事件，事件的起因是这样，某IP地址...

【实战】Linux取证 - CSDN博客 1-15

来源:山警网络安全实验室指导教师:张璇学[illegible]轩 马珺 王润正 赵一屹一、关于Linux raid部分　...

使用Linux 工具进行计算机取证 - CSDN博客 7-26

本文通过介绍 Linux 系统工具(Ftkimage、xmount、Volatility、dd、netcat)来介绍使用计算机取证的方法和步骤。 ...

六款优秀的Linux数字取证工具 1152

之前许多文章中谈论了开源软件的优点。开源和闭源软件之间的争论通常集中在自由，可靠性，互操作性、开放标准、支持和哲学理...

内存取证——文件 362

文件 notepad里的秘密（二）0x00文接上文，前一篇关于内存取证读取进程。这篇总结一下，内存取证读取文件。0x01step1:常规操...

Linux入侵取证:从一次应急事件讲起 - CSDN博客 6-5

不良信息举报 举报内容: Linux入侵取证:从一次应急事件讲起 举报原因: 色情 政治 抄袭 广告 招聘 骂人 其他 原文地址: 原因补充: 最多只...

在线linux 系统初步取证 - CSDN博客 7-12

在线unix/linux 系统初步取证下面我们来做个实验取证对像是192.168.1.101,收集数据的机器是192.168.1.97 在192.168.1.101上运行 [ro...

一次Linux系统被攻击的分析过程 1762

一、 一次Linux被入侵后的分析 下面通过一个案例介绍下当一个服务器被rootkit入侵后的处理思路和处理过程，rootkit 攻击是Linux系...

Linux取证之事后取证 - CSDN博客 7-20

事后取证:从Linux系统中搜索并提取恶意软件以及相关线索 1.从Linux系统中发现和提取恶意软件 前提: 熟悉Linux工作原理 ext2和ext3文...

Linux 环境下取证 - CSDN博客 7-17

linux环境下取证 易失性数据 特点: Linux自带命令可被恶意代码修改不可信 Unix系统存在一个脚本程序用于记录系统命令的运行及输出...

深度解析CentOS通过日志反查入侵 4418

昨天晚上群里有一个朋友的服务器发现有入侵的痕迹后来处理解决但是由于对方把日志都清理了无疑给排查工作增加了许多难度。刚...

在线linux 系统初步取证 533

在线unix/linux 系统初步取证 下面我们来做个实验 取证对像是192.168.1.101，收集数据的机器是192.168.1.97 在192.168.1.101上运...

linux取证之内存取证 - CSDN博客

7-20

linux取证之内存取证2018年07月19日 17:4 读数:3 内存取证 内存取证工具:可以列出当前已经打开的文件,正在活动的网络连接,运...

Linux入侵检测基础

2870

个人认为是一篇很不错的Linux应急基础的 近遇到了很多服务器被入侵的例子，为了方便日后入侵检测以及排查取证，我查询...

使用 Linux 工具进行计算机取证

3034

使用 Linux 工具进行计算机取证 本文通 inux 系统工具（Ftkimage、xmount、Volatility、dd、netcat）来介绍使用计算机取...

最好的入侵linux教程基本知识

769

原贴：http://www.vipcn.com/InfoView/Ar 2535.html最好的入侵linux教程一：基本知识 1：常见UNIX版本： SC...

入侵取证调查

4024

0x00 前言 在我们日常运维中，难免有几个 者主机被入侵，这时就出现应急响应需求。那么我们应该怎样着手分析呢？本文将...

黑客常用 Linux 入侵常用命令

1463

原文地址：http://blog.csdn.net/jHstGeWWubw/article/details/78941387写个php一句话后门上去：[jobcruit@wa64-054 rankup...

Linux下简单的入侵检测

2053

总的来说，要判断主机是否正在或者已经遭受了攻击，需要以下几个步骤。 1、终结非授权用户 2、找出并关闭非授权进程 3、分析...

优化linux系统并防止入侵操作（修改内核参数）

123

vim /etc/sysctl.conf 来改内核参数。 优化内核参数 net.ipv4.tcp_fin_timeout = 2 net.ipv4.tcp_tw_reuse = 1 net.i...

UNIX/Linux系统取证之信息采集案例

5859

在UNIX/Linux系统取证中，及时收集硬盘的信息至关重要，《Unix/Linux网络日志分析与流量监控》一书中，将详细讨论各种常见系...

【实战】Linux取证

225

来源：山警网络安全实验室指导教师：张璇学生：李雨轩 马珺 王润正 赵一屹一、关于Linux raid部分 先了解一下raid技术吧，独立...

Web服务器日志取证分析方法

DOCX

2017年12月25日 582KB 下载

【黑客非法侵入案件的电子取证分析】

221

转自：警察技术杂志作者：赖世锋 王江海摘 要：从电子数据取证的角度出发，说明在黑客非法侵入案件中电子证据应注意提取的几...

【实战-Linux】--搭建CA认证中心实现https取证

4528

环境 CA认证中心服务端：xuegod63.cn IP：192.168.1.63 客户端：xuegod64.cn IP：192.168.1.64 CA认证中心简述 ...

个人资料

2GameZero 关注

原创	粉丝	喜欢	评论
25	5	2	0

等级： 博客 2 访问： 1万+
积分： 347 排名： 24万+