十一、日志系统

Linux黑客基础-69-日志系统的管理

日志文件存储关于操作系统和应用程序运行 时发生的事件的信息，包括任何错误和安全警报。

作为黑客，日志文件可以跟踪目标的活动和身份

日志服务

syslogd程序通常包括 rsyslog 和 syslog-ng

日志服务器 监听在UDP/514端口

locate rsyslog----查看日志文件的配置文件

与rsyslog相关的文件

/etc/rsyslog.conf　　配置文件

/etc/init.d/rsyslog　rsyslog的服务脚本

/usr/sbin/rsyslogd　rsyslog的服务程序

systemctl status rsyslog　查看服务状态

日志规则的作用

rsyslog 规则决定记录哪种类型的信息，记录哪些程序的消息，以及将日志存储在何处。

facility 关键字引用正在记录其消息的程序，例如邮件、内核或打印系统

priority 关键字决定为该程序 记录哪种类型的消息。在最右边的

action 关键字引用将发送日志的位置

格式： facility.priority action

日志消息的类型

优先级告诉系统要记录哪种消息。

代码从最低优先级列出，从调试开始到最高优先级，以严重结束。

- debug---调试（最低）
- info
- notice
- warning
- warn
- error
- err
- crit
- alert
- emerg
- panic（最高）

warning、warn、error、err、emerg、panic，这些都已被弃用，不应该使用。

日志消息级别

0 Emergency: system is unusable

1 Alert: action must be taken immediately

2 Critical: critical conditions

3 Error: error conditions

4 Warning: warning conditions

5 Notice: normal but significant condition

6 Informational: informational messages

7 Debug: debug-level messages

如果优先级为*，则记录所有优先级的消息。

指定优先级时，将记录该优先级及更高优先级的消息。

日志文件通常被发送到/var/log 目录 ， 其文件 名描述为生成它们的工具

action部分

指定的文件

@IP地址 发送到指定的日志服务器中

tail -f /var/log/auth.log 实时监视日志

Linux黑客基础-70-使用logrotate自动清理日志

rotate---循环

日志文件会占用空间，所以如果不定期删除它们，它们最终会填满整个硬盘驱动器。另一方面，如果 太频繁地删除日志文件，那么在将来的某个时间点就没有日志供研究了。

logrotate 是通过将日志文件移动到其他位置来定期归档日志文件的过程，从而为您留下一个新的日志 文件。然后，在指定的一段时间之后，归档的位置将被清理。

logrotate的配置文件

/etc/logrotate.conf

Linux黑客基础–71–日志的清理

从攻击者的角度，对日志的清理可以不让系统留下入侵的痕迹，保存隐身

（1）删除活动的任何日志

shred：可以删除文件并多次擦写覆盖它，这使得恢复变得更加困难

shred将删除文件并多次覆盖它，默认情况下，shred将覆盖四次

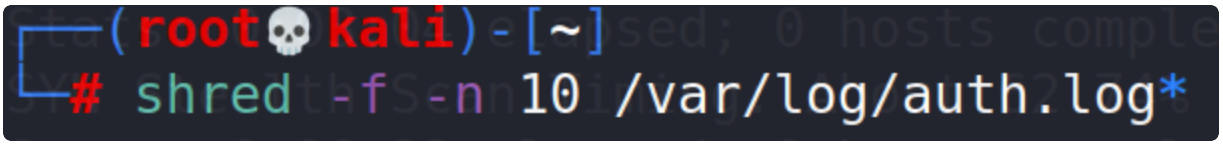
常用选项：

–f, ––force　　必要时修改权限以使目标可写

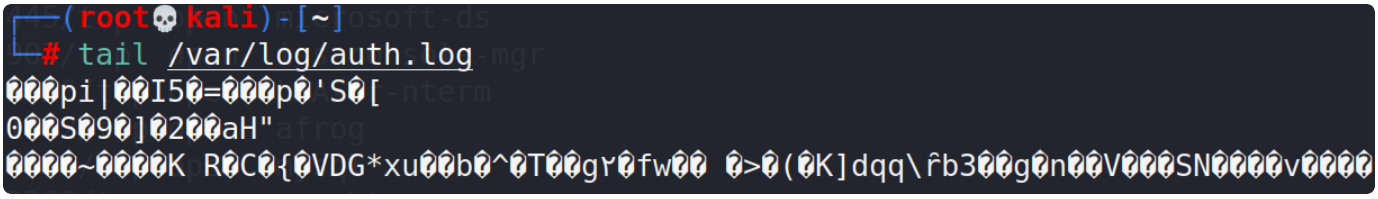
–n, ––iterations=N　覆盖N 次，而非使用默认的3 次

清除和认证相关的目录

shred –f –n 10 /var/log/auth.log*



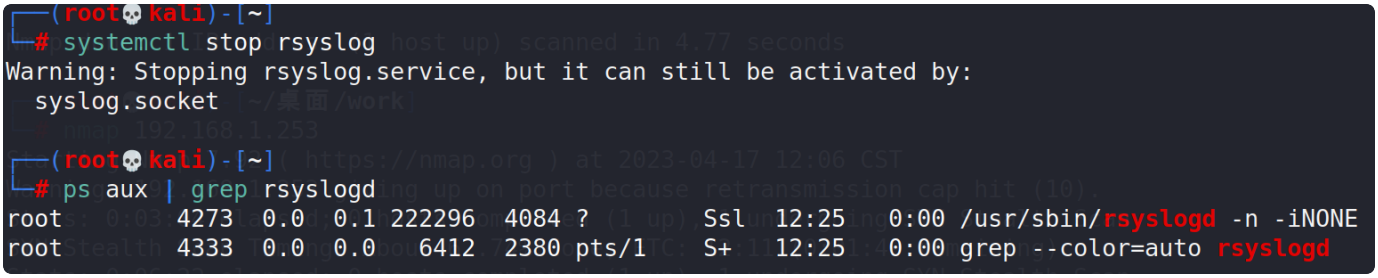
当我们再次查看的时候发现她已经是乱码了



（2）禁用日志记录–––需要root

当黑客控制了一个系统，他们可以立即禁用日志，以防止系 统跟踪他们的活动。当然，这需要 root 特权。

systemctl stop rsyslog 禁用日志服务



可以看到并没有真正的关闭日志服务，我们就需要强制杀死进程