**应急响应**

**实验报告**

姓名：

日期：

1. **实验内容**

web日志地址/opt/tomcat9/logs/

系统日志地址：/var/log/

遇到任何提示权限不够的，直接在命令前面加sudo

账户密码为w\_w

1.2022-06-26日安全保障人员检测到网站主机与其他主机存在大量流量交互行为。请借助日志对事件进行分析研判，说明网站主机的失陷原因，服务器中存在那些异常文件，攻击者的IP是什么？阐述相应分析过程、研判结果、提供截图并以文字说明

2.请分析2022-06-26日的服务器遭受的暴力破解安全事件是否为误报，若为误报请提供误报的可能原因、非误报的情况下说明是否利用成功，以及攻击者的后续操作，并阐述分析过程，研判结果，提供截图并以文字说明。（截图说明）

3.查询任意一个网站的信息，需包含网站注册者，网站注册人邮箱，域名服务商，网站使用IP地址，IP定位等

例如：

网站：https://www.leadsec.com.cn/

网站注册者：北京网御星云信息技术有限公司

网站注册人邮箱：lilj3@leadsec.com.cn

域名服务商：阿里云计算有限公司（万网）

网站使用IP：112.90.43.190

IP定位：中国 广东省 揭阳市

1. **实验总结**

（在实验中遇到的问题及解决方法、收获是什么）