**应急响应**

**实验报告**

姓名： 蔡欣彤

日期： 2023.7.10

1. **实验内容**

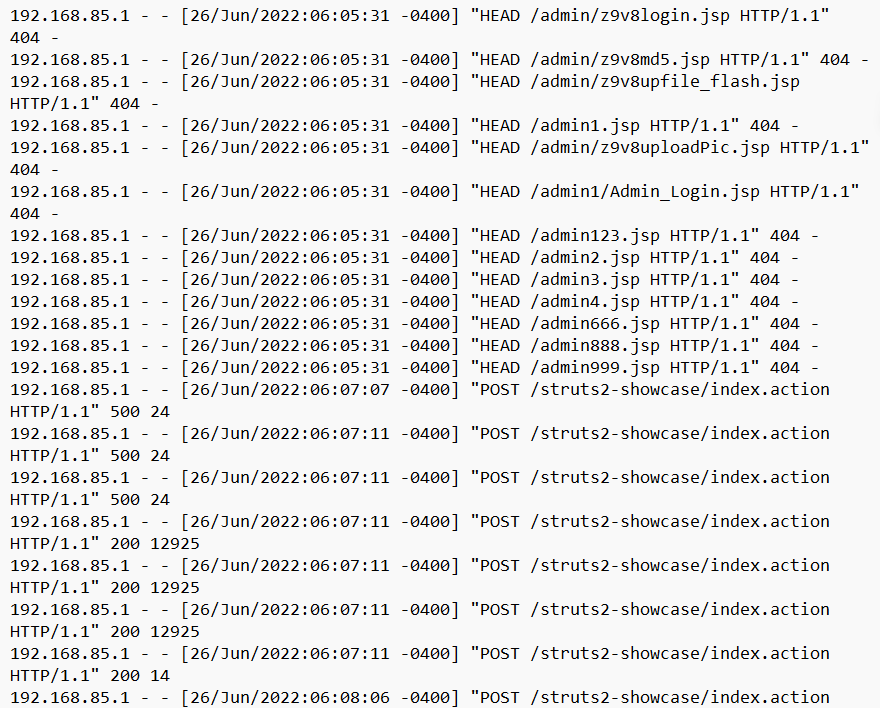
web日志地址/opt/tomcat9/logs/

系统日志地址：/var/log/

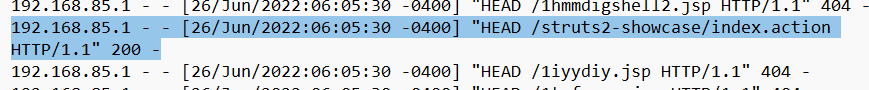
遇到任何提示权限不够的，直接在命令前面加sudo

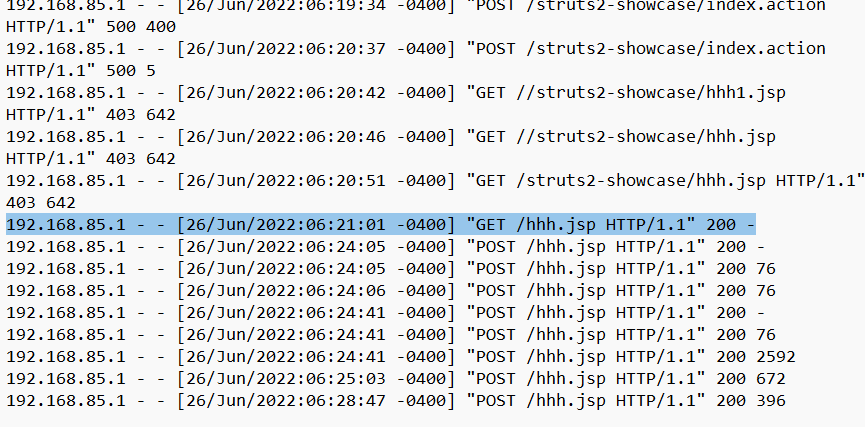
账户密码为w\_w

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



根据上图，我们可以看到攻击者往/struts2-showcase/index.action目录上传了东西，返回了500几次，后返回200。对该目录进行ctrl+F，在前面找到了网站对这个目录的请求回应了200的状态码。





上图可用看到攻击者请求目录下的hhh.jsp，网站回复了403，然而请求根目录下的hhh.jsp，网站回复了200。

说明攻击者对网络主机进行了漏洞扫描，扫描目录，并对回应了200的目录上传了东西，在网站的根目录下的hhh.jsp.

综上

网站主机的失陷原因：漏洞扫描时，该/struts2-showcase/index.action目录回应了状态码20022

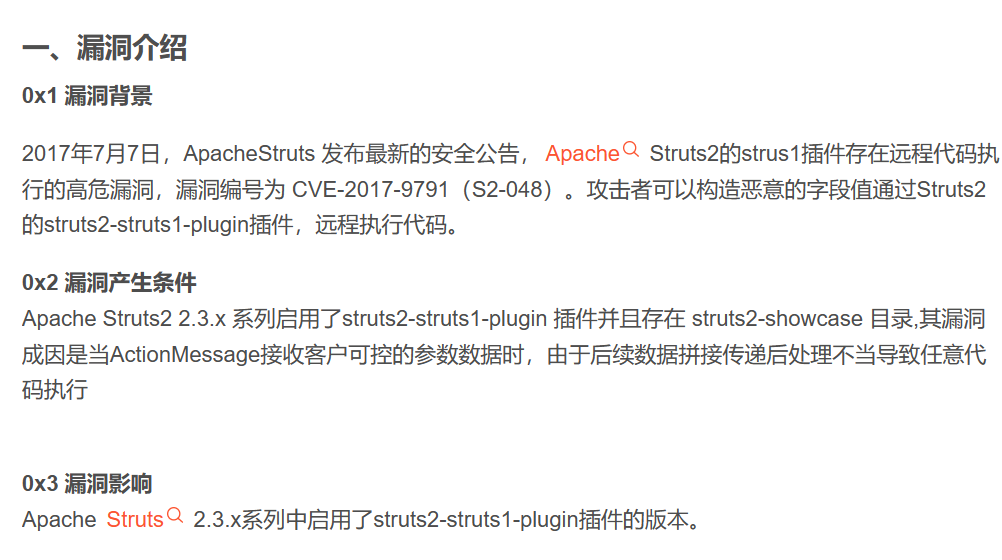
服务器中存在那些异常文件：根目录下的hhh.jsp

攻击者的IP：192.168.85.1

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）

应该是利用成功的。

题1的分析我们得知，攻击者通过/struts2-showcase/index.action目录漏洞，往网站根目录上传了hhh.jsp文件，在互联网上查找该目录，发现网上已有该漏洞的一些介绍。



攻击者的后续操作：没看懂，附上链接

https://blog.csdn.net/qq\_45590334/article/details/121691108

本人理解：发现漏洞后，往网站上传一些已有的木马或者暗门之类的，再利用这些木马/暗门进行进一步的攻击。

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.kanjux.com/

网站注册者：NameSilo, LLC

网站注册人邮箱：[abuse@namesilo.com](mailto:abuse@namesilo.com)

域名服务商：public-dns-a.dnspai.com

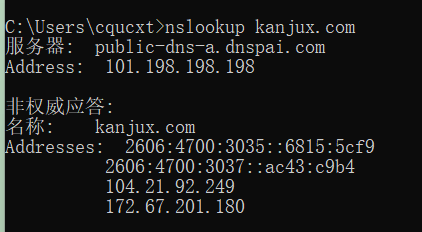
Address: 101.198.198.198

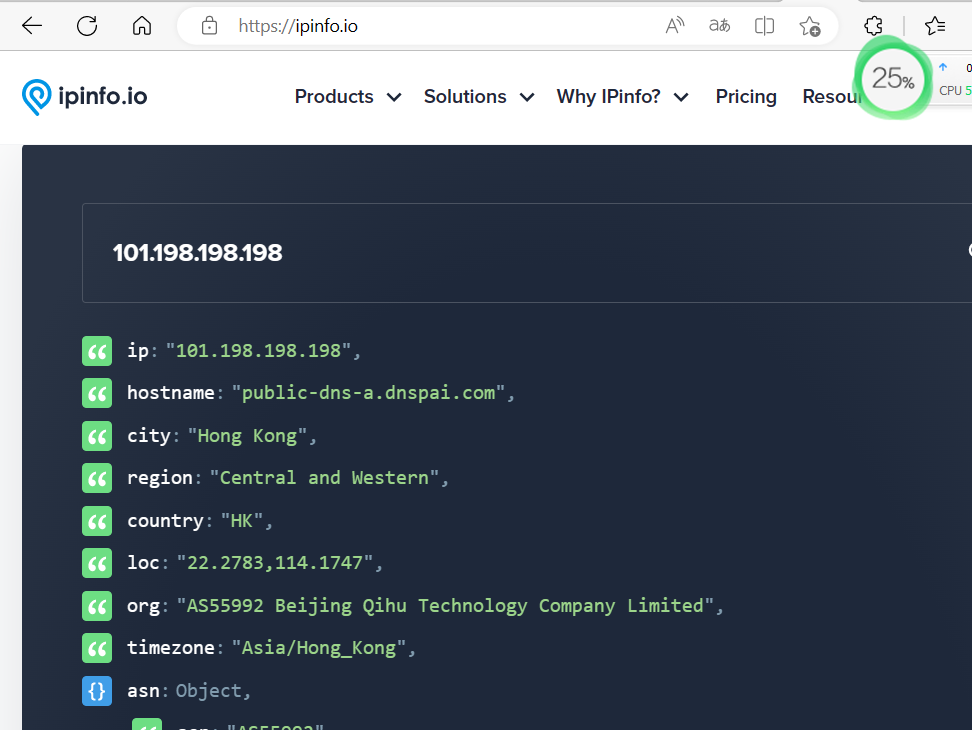
IP定位：Asia/Hong\_Kong 中国

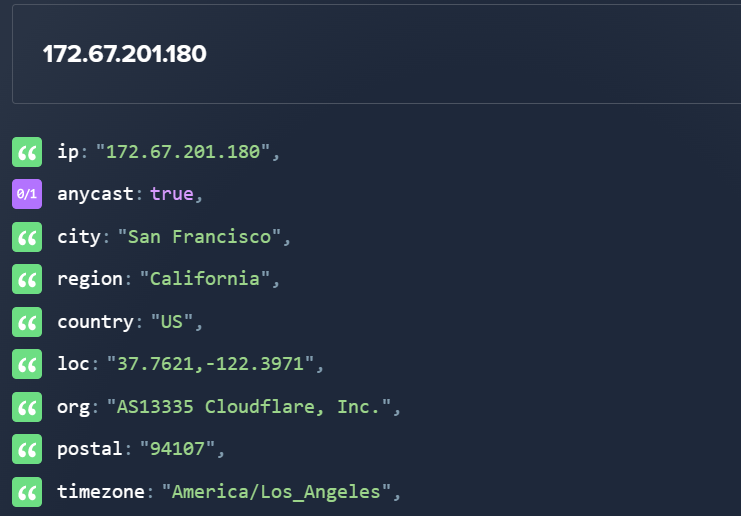
网站使用IP：172.67.201.180

IP定位：America/Los\_Angeles









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）

更了解了日志对于安全的重要性，也清楚了一点关于应急响应的流程和工具。