应急响应

实验报告

姓名：蔡欣彤

日期：2023.7.10

一、 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

```
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin/z9v8login.jsp HTTP/1.1"
404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin/z9v8md5.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin/z9v8upfile_flash.jsp
HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin1.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin/z9v8uploadPic.jsp HTTP/1.1"
404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin1/Admin_Login.jsp HTTP/1.1"
404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin123.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin2.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin3.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin4.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin666.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin888.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:31 -0400] "HEAD /admin999.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:07:07 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 500 24
192.168.85.1 - - [26/Jun/2022:06:07:11 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 500 24
192.168.85.1 - - [26/Jun/2022:06:07:11 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 500 24
192.168.85.1 - - [26/Jun/2022:06:07:11 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 200 12925
192.168.85.1 - - [26/Jun/2022:06:07:11 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 200 12925
192.168.85.1 - - [26/Jun/2022:06:07:11 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 200 12925
192.168.85.1 - - [26/Jun/2022:06:07:11 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 200 14
192.168.85.1 - - [26/Jun/2022:06:08:06 -0400] "POST /struts2-showcase/index.action
```

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。

```
192.168.85.1 - - [26/Jun/2022:06:05:30 -0400] "HEAD /1hmmd1gshell2.jsp HTTP/1.1" 404 -
192.168.85.1 - - [26/Jun/2022:06:05:30 -0400] "HEAD /struts2-showcase/index.action
HTTP/1.1" 200 -
192.168.85.1 - - [26/Jun/2022:06:05:30 -0400] "HEAD /1iyydiy.jsp HTTP/1.1" 404 -
```

```
192.168.85.1 - - [26/Jun/2022:06:19:34 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 500 400
192.168.85.1 - - [26/Jun/2022:06:20:37 -0400] "POST /struts2-showcase/index.action
HTTP/1.1" 500 5
192.168.85.1 - - [26/Jun/2022:06:20:42 -0400] "GET //struts2-showcase/hhh1.jsp
HTTP/1.1" 403 642
192.168.85.1 - - [26/Jun/2022:06:20:46 -0400] "GET //struts2-showcase/hhh.jsp
HTTP/1.1" 403 642
192.168.85.1 - - [26/Jun/2022:06:20:51 -0400] "GET /struts2-showcase/hhh.jsp HTTP/1.1"
403 642
192.168.85.1 - - [26/Jun/2022:06:21:01 -0400] "GET /hhh.jsp HTTP/1.1" 200 -
192.168.85.1 - - [26/Jun/2022:06:24:05 -0400] "POST /hhh.jsp HTTP/1.1" 200 -
192.168.85.1 - - [26/Jun/2022:06:24:05 -0400] "POST /hhh.jsp HTTP/1.1" 200 76
192.168.85.1 - - [26/Jun/2022:06:24:06 -0400] "POST /hhh.jsp HTTP/1.1" 200 76
192.168.85.1 - - [26/Jun/2022:06:24:41 -0400] "POST /hhh.jsp HTTP/1.1" 200 -
192.168.85.1 - - [26/Jun/2022:06:24:41 -0400] "POST /hhh.jsp HTTP/1.1" 200 76
192.168.85.1 - - [26/Jun/2022:06:24:41 -0400] "POST /hhh.jsp HTTP/1.1" 200 2592
192.168.85.1 - - [26/Jun/2022:06:25:03 -0400] "POST /hhh.jsp HTTP/1.1" 200 672
192.168.85.1 - - [26/Jun/2022:06:28:47 -0400] "POST /hhh.jsp HTTP/1.1" 200 396
```

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。

一、漏洞介绍

0x1 漏洞背景

2017年7月7日，ApacheStruts 发布最新的安全公告， Apache Struts2的strus1插件存在远程代码执行的高危漏洞，漏洞编号为 CVE-2017-9791（S2-048）。攻击者可以构造恶意的字段值通过Struts2的struts2-struts1-plugin插件，远程执行代码。

0x2 漏洞产生条件

Apache Struts2 2.3.x 系列启用了struts2-struts1-plugin 插件并且存在 struts2-showcase 目录,其漏洞成因是当ActionMessage接收客户可控的参数数据时，由于后续数据拼接传递后处理不当导致任意代码执行

0x3 漏洞影响

Apache Struts 2.3.x系列中启用了struts2-struts1-plugin插件的版本。

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

域名服务商：public-dns-a.dnspai.com

Address: 101.198.198.198

IP 定位：Asia/Hong_Kong 中国

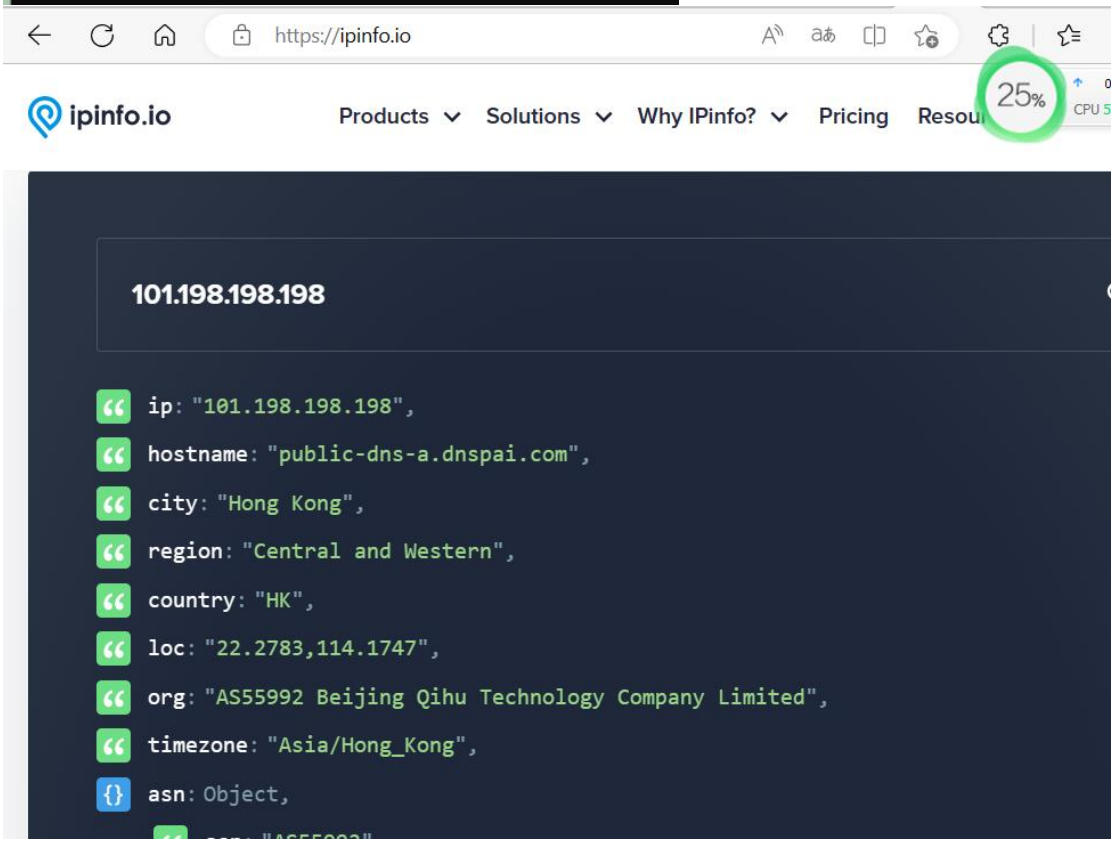
网站使用 IP：172.67.201.180

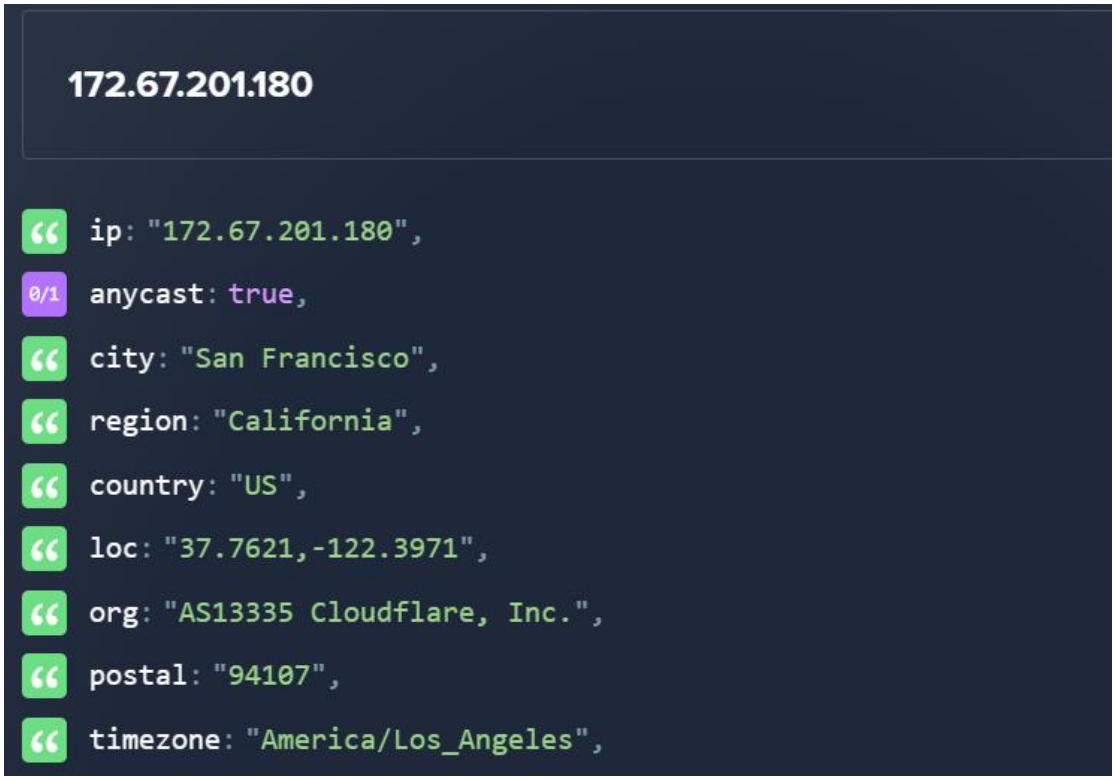
IP 定位：America/Los_Angeles

```
root@kali:~# whois kanjux.com
   Domain Name: KANJUX.COM
   Registry Domain ID: 2657037049_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namesilo.com
   Registrar URL: http://www.namesilo.com
   Updated Date: 2022-11-22T01:15:30Z
   Creation Date: 2021-11-23T21:15:11Z
   Registry Expiry Date: 2023-11-23T21:15:11Z
   Registrar: NameSilo, LLC
   Registrar IANA ID: 1479
   Registrar Abuse Contact Email: abuse@namesilo.com
   Registrar Abuse Contact Phone: +1.4805240066
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
   Name Server: CARTMAN.NS.CLOUDFLARE.COM
   Name Server: KRISTINA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-07-10T08:09:52Z <<<
```

```
C:\Users\cqucxt>nslookup kanjux.com
服务器:  public-dns-a.dnspai.com
Address:  101.198.198.198

非权威应答:
名称:    kanjux.com
Addresses:  2606:4700:3035::6815:5cf9
          2606:4700:3037::ac43:c9b4
          104.21.92.249
          172.67.201.180
```





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

二、 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。