

TRAINING KIT – HOST2

**Hardening web
application servers**



Security Audit Intrusion Test

Trust implies control,
Rate your vulnerability !

TLP: WHITE

EXCELLIUM

Your first call when it comes to IT and Security!



Agenda

- Labs objective
- Tomcat and web application installation
- Security issues analysis
- Tomcat hardening
- Q&R



Introduction



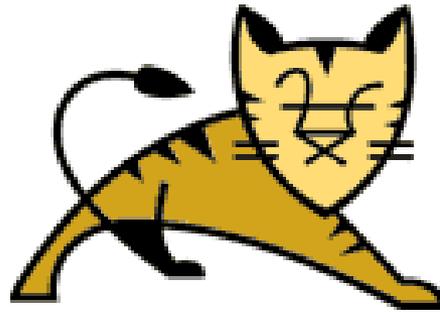
Introduction

- The labs objective is to discover the impacts of a “default” installation of Tomcat web container and, further, how to harden the installation at different levels in order to reduce the attack surface.
- The target operating system used will be Windows 2012 R2 because, on Linux environment (ex: Ubuntu / Debian), the package provides a basic hardening level that is not applied into Windows installer of Tomcat.

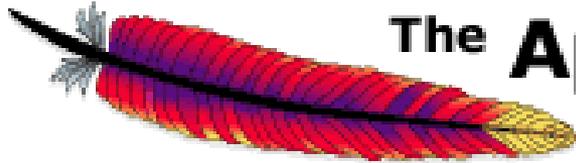


Introduction

- Tomcat Windows installer version will also be used because, often, Tomcat is provided, as module, of a commercial package and the global installer of the commercial package install Tomcat using default settings.



Apache
Tomcat



The **Apache Software Foundation**

<http://www.apache.org/>



Tomcat installation



Tomcat installation

Required files are on your working VM:

- **Apache Tomcat 8.0.28 for Windows**
 - `C:\Workspace\Courses\trainingkit_host2\apache-tomcat-8.0.28.exe`
- **JDK 8 64 bits for Windows**
 - `C:\Workspace\Courses\trainingkit_host2\jdk-8u91-windows-x64.exe`
- **Vulnerable application**
 - `C:\Workspace\Courses\trainingkit_host2\TestVulnApp.war`



Tomcat installation

- Java JDK installation steps:

The screenshot shows a Windows file explorer window in the 'Downloads' folder. Two files are visible: 'apache-tomcat-8.0.28.exe' and 'jdk-8u66-windows-x64.exe'. The 'jdk-8u66-windows-x64.exe' file is selected, and its context menu is open, with the 'Run' option highlighted. In the foreground, two installation windows are displayed. The first window, titled 'Java SE Development Kit 8 Update 66 (64-bit) - Complete', shows a successful installation message: 'Java SE Development Kit 8 Update 66 (64-bit) Successfully Installed'. It includes a 'Next Steps' button and a 'Close' button. The second window, titled '(64-bit) - Custom Setup', shows a 'Feature Description' section with the text: 'Java SE Development Kit 8 Update 66 (64-bit), including the JavaFX SDK, a private JRE, and the Java Mission Control tools suite. This will require 180MB on your hard drive.' It features a 'Change...' button and 'Next >' and 'Cancel' buttons at the bottom.



Tomcat installation

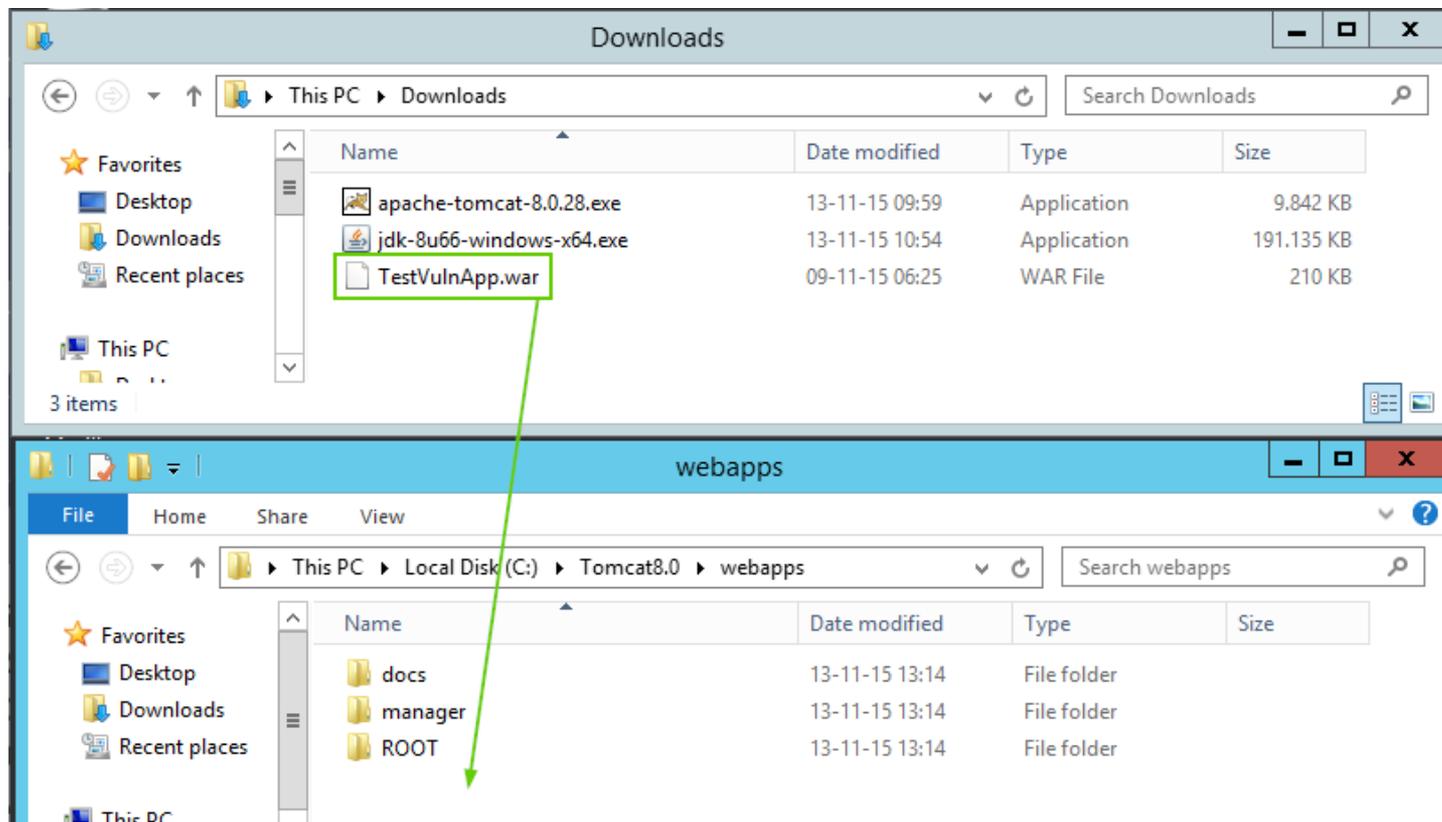
- Tomcat installation steps:

The screenshot shows a Windows desktop environment. At the top, a file explorer window displays the 'Downloads' folder. Below it, the 'Apache Tomcat Setup' window is open. In the foreground, a web browser window is active, showing the Apache Tomcat 8.0.28 installation success page. The browser's address bar is highlighted with a green box and contains 'localhost:8080'. The success page features a green banner with the text 'If you're seeing this, you've successfully installed Tomcat. Congratulations!' and a cartoon cat logo. Below the banner, there are links for 'Recommended Reading' and three buttons: 'Server Status', 'Manager App', and 'Host Manager'. At the bottom of the browser window, the 'Apache Tomcat 8' title bar is visible, and the 'Finish' button in the taskbar is highlighted with a green box.



Tomcat installation

- Vulnerable application installation (copy WAR file and wait 5 secs):





Tomcat installation

- Open application access to final users....

The screenshot shows the Tomcat Manager web interface at localhost:8080. A video overlay of a man with long hair and a beard is centered on the screen, with the subtitle "Oh dear, we are in trouble" at the bottom. The interface includes a navigation menu, a "Server Status" section, and a table of applications. The table lists three applications: /TestVulnApp, /docs, and /manager. The /manager application is highlighted with a green border. The interface also shows a "Message" field, a "Manager" section, and a "List Applications" link. The bottom of the screenshot shows a status bar with "3 requests" and a logo for EXCELLIUM.

Path	Version	Start	Stop	Reload	Undeploy
/TestVulnApp	None specified	Start	Stop	Reload	Undeploy
/docs	None specified	Start	Stop	Reload	Undeploy
/manager	None specified	Start	Stop	Reload	Undeploy



Security issues analysis



Sec. Issues analysis

- **Cause 1:** Application source code level.

```
@WebServlet("/loader")
public class Loader extends HttpServlet {

    * (non-Javadoc)
    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
        try {
            String path = req.getParameter("path");
            if (path == null || "".equals(path.trim())) {
                path = "/Luxemburg.png";
            }
            InputStream is = this.getClass().getResourceAsStream(path);
            resp.setContentType("image/png");
            if (is == null) {
                resp.setContentType("text/plain");
                is = new FileInputStream(path);
            }
            IOUtils.copy(is, resp.getOutputStream());
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```



Sec. Issues analysis

- **Cause 2:** Windows service credentials configuration level.

The screenshot shows the Windows Services console with the 'Services (Local)' window open. The 'Apache Tomcat 8.0 Tomcat8' service is selected and highlighted in blue. The 'Log On As' column for this service is highlighted with a green box, showing 'Local System'. Other services listed include App Readiness, Application Experience, Application Identity, Application Information, Application Layer Gateway, and Application Management.

Name	Description	Status	Startup Type	Log On As
Apache Tomcat 8.0 Tomcat8	Apache To...	Running	Manual	Local System
App Readiness	Gets apps re...		Manual	Local System
Application Experience	Processes a...		Manual (Trig...	Local System
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local System
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...	Running	Manual	Local System



Sec. Issues analysis

- **Cause 3:** Tomcat credentials storage protection level.

```
C:\Tomcat8.0\conf\tomcat-users.xml -
File Edit Selection Find View Goto Tools Project Preferences Help
tomcat-users.xml x
1 <?xml version='1.0' encoding='cp1252'?>
2 <!--
3 Licensed to the Apache Software Foundation (ASF) under one or more
4 contributor license agreements. See the NOTICE file distributed with
5 this work for additional information regarding copyright ownership.
6 The ASF licenses this file to You under the Apache License, Version 2.0
7 (the "License"); you may not use this file except in compliance with
8 the License. You may obtain a copy of the License at
9
10 http://www.apache.org/licenses/LICENSE-2.0
11
12 Unless required by applicable law or agreed to in writing, software
13 distributed under the License is distributed on an "AS IS" BASIS,
14 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15 See the License for the specific language governing permissions and
16 limitations under the License.
17 -->
18 <tomcat-users xmlns="http://tomcat.apache.org/xml"
19 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
20 xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
21 version="1.0">
22 <user username="tomcat" password="tomcat" roles="manager-gui" />
23 <!--
```



Sec. Issues analysis

- **Cause 4:** Network access segregation level for access to TC admin app.

The screenshot displays a Windows File Explorer window titled "META-INF" showing the directory path: This PC > Local Disk (C:) > Tomcat8.0 > webapps > manager > META-INF. A table of files is shown:

Name	Date modified	Type	Size
context.xml	07-10-15 20:26	XML Document	2 KB

An inset window titled "C:\Tomcat8.0\webapps\manager\META-INF\context.xml • - Sublime Text (UNREGISTERED)" shows the XML content of context.xml:

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <Context antiResourceLocking="false" privileged="true" >
3   <!--
4     Remove the comment markers from around the Valve below to limit access to
5     the manager application to clients connecting from localhost
6   -->
7   <!--
8   <Valve className="org.apache.catalina.valves.RemoteAddrValve"
9     allow="127.\d+.\d+.\d+:::1|0:0:0:0:0:0:0:1" />
10  -->
11 </Context>
12
```

The code editor shows the XML content with line numbers 1 through 12. A green box highlights the comment and the RemoteAddrValve configuration on lines 4 through 10.



Sec. Issues analysis

- **Cause 5:** Access right level for TC owner user on « **webapps** » TC folder.

Permission Entry for webapps

Principal: CREATOR OWNER [Select a principal](#)

Type:

Applies to:

Advanced permissions: [Show basic permissions](#)

- Full control
- Traverse folder / execute file
- List folder / read data
- Read attributes
- Read extended attributes
- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Delete
- Read permissions
- Change permissions
- Take ownership

Only apply these permissions to objects and/or containers within this container



Sec. Issues analysis

- **Cause 6:** TC JVM Security Manager level.

elp

C:\Tomcat8.0\logs\catalina.2015-11-14.log - Sublime Text (UNREGISTERED)

Tools Project Preferences Help

```
[main] org.apache.catalina.startup.VersionLoggerListener.log Server version:      Apache Tomcat/8.0.28
[main] org.apache.catalina.startup.VersionLoggerListener.log Server built:         Oct 7 2015 18:25:21 UTC
[main] org.apache.catalina.startup.VersionLoggerListener.log Server number:      8.0.28.0
[main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:            Windows Server 2012 R2
[main] org.apache.catalina.startup.VersionLoggerListener.log OS Version:        6.3
[main] org.apache.catalina.startup.VersionLoggerListener.log Architecture:      amd64
[main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:          C:\jdk1.8.0_66\jre
[main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:        1.8.0_66-b18
[main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:         Oracle Corporation
[main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:     C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:     C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.home=C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.base=C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.endorsed.dirs=C:\Tomcat8.0\endorsed
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.io.tmpdir=C:\Tomcat8.0\temp
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.config.file=C:\Tomcat8.0\conf\logging.properties
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: exit
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xms128m
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xmx256m
[main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent The APR based Apache Tomcat Native library which allows optimal performance in product
```



Sec. Issues analysis

- **Cause 7:** TC Documentation and ROOT applications are still online.

PC ▶ Local Disk (C:) ▶ Tomcat8.0 ▶ webapps ▶

Name	Date modified
docs	13-11-15
manager	13-11-15
ROOT	13-11-15
TestVulnApp	13-11-15
TestVulnApp.war	09-11-15



Hardening



Hardening

- Based on the security issues analysis, we will apply hardening operations on every security issues, one by one, in order to close as much exploitability path as possible...



Hardening

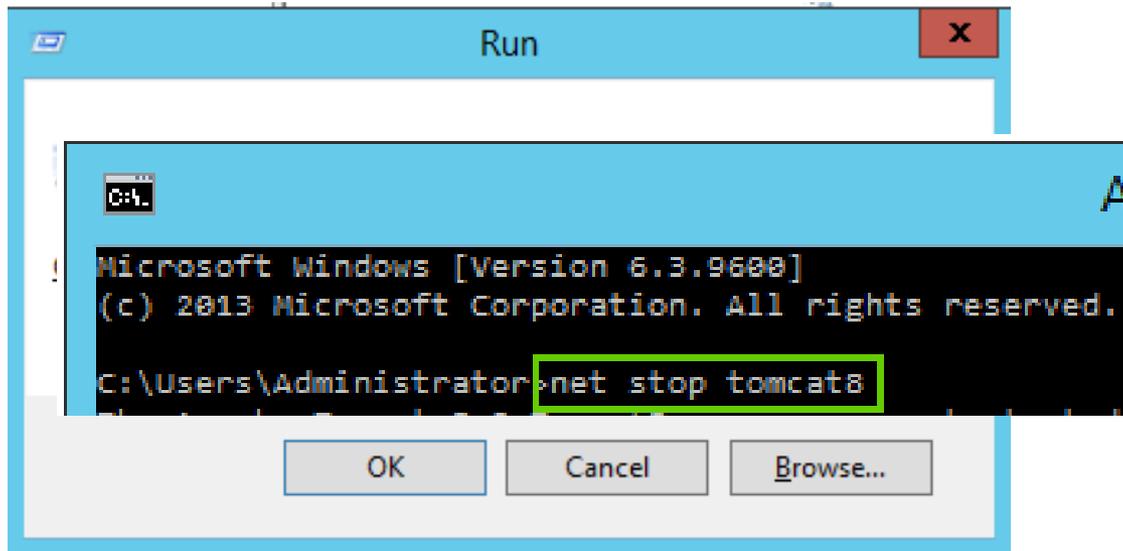
As reminder, this is the working areas (**C** = **Cause**):

- **C1:** Application source code level.
- **C2:** Windows service credentials configuration level.
- **C3:** Tomcat credentials storage protection level.
- **C4:** Network access segregation level for access to TC admin app.
- **C5:** Access right level for TC owner user on « **webapps** » TC folder.
- **C6:** TC JVM Security Manager level.
- **C7:** TC Documentation and ROOT applications are still online.



Hardening

!!! Before to start any hardening step, stop Tomcat Windows service !!!





Hardening – C1

→C1: Application source code level.

- We assume here that we cannot act on application code because it's a Open Source commercial product and the vendor will provide us a security patch in 6 month !





Hardening – C2

→**C2**: Windows service credentials configuration level.

Objective:

Create a dedicated user for Tomcat in order to avoid that Tomcat application alter Operating System or access to OS sensitive files.



Hardening – C2

→ **C2:** Windows service credentials configuration level.

Soluce:

Step 1: Open OS

The screenshot shows the 'tomcat Properties' dialog box with the 'Remote control' tab selected. The 'Enable remote control' checkbox is highlighted with a green box. The 'Require user's permission' checkbox is checked. The 'Level of control' section shows 'Interact with the session' selected. The 'Name' list on the left includes 'Adminis...', 'Guest', and 'tomcat...'. The 'user.' label is visible on the right side of the dialog box.



Hardening – C2

→ C2: Windows service credentials configuration level.

Solve

Step

access

The screenshot shows the 'Tomcat8.0 Properties' dialog box with the 'Security' tab selected. The 'Object name' is 'C:\Tomcat8.0'. The 'Group or user names' list includes 'CREATOR OWNER', 'SYSTEM', and 'Administrators (WIN-VU6JG9R0AMQ\Administrators)'. The 'Permissions for CREATOR OWNER' table is as follows:

	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

The 'Advanced' button is highlighted with a green box. The 'Apply' button at the bottom right is also highlighted with a green box.

ict
ser.



Hardening – C2

→ **C2**: Windows service credentials configuration level.

Soluce:

Step 3: Configure Tomcat Windows service to use the Tomcat dedicated user.

The screenshot shows the Windows Services console with the 'Apache Tomcat 8.0 Tomcat8 Properties' dialog box open. The 'Log On As' tab is selected, and the user '.\tomcat' is highlighted in the 'Log On As' column. The 'Confirm password' field is visible at the bottom.

Name	Description	Status	Startup Type	Log On As
Apache Tomcat 8.0 Tomcat8	Apache Tomcat 8.0.28 Serv...		Manual	.\tomcat
App Readiness	Gets apps ready for use the ...		Manual	Local System



Hardening – C2

→ **C2**: Windows service credentials configuration level.

Soluce:

Step 4: Start

Challenge

```

tomcat8-stderr.2015-11-18.log
85
86
87
88
89
90
91 at java.io.FileInp
92 at java.io.FileInp
93 at java.io.FileInp
94 at eu.excellium.Lo
95 at javax.servlet.h

```

Hardening
access for



Completed

access restriction.

```

deployment
o-8080"
-8009"]
[nied)

```

now limited
ugh Tomcat...

ost Manager



Hardening – C3

→ **C3:** Tomcat credentials storage protection level.

Objective:

Protect credentials stored in Tomcat user XML file.

Hints:

https://tomcat.apache.org/tomcat-8.0-doc/realm-howto.html#Digested_Passwords

<http://davidghedini.blogspot.lu/2010/07/tomcat-manager-password.html>

<https://tomcat.apache.org/tomcat-8.0-doc/config/credentialhandler.html>



Hardening – C3

→ **C3:** Tomcat credentials storage protection level.

Soluce:

Step 1: Generate a SHA512 hash of the user password using Tomcat digest script and replace the plain-text password with this hash into the «tomcat-users.xml file». Hash must be salted, use iterations count > 10000 and use a key length of 512 bits.

```
C:\Tomcat8.0\bin>set
C:\Tomcat8.0\bin>dig
tomcat:cde1eafb73378ad2de1002939f77d1b63
C:\Tomcat8.0\bin>
```

```
tomcat-users.xml  server.xml
1 <?xml version='1.0' encoding='cp1252'?>
2 <tomcat-users xmlns="http://tomcat.apache.org/xml"
3   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4   xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
5   version="1.0">
6 <user username="tomcat" password="cde1eafb7337885ce4bc05fb8a04ab459b7acf608ee9b2f9563"
7 </tomcat-users>
```



Hardening – C3

```
tomcat-users.xml  ×  server.xml  ×
1  <?xml version='1.0' encoding='utf-8'?>
2  <Server port="8005" shutdown="SHUTDOWN">
3    <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
4    <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
5    <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
6    <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
7    <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
8  <GlobalNamingResources>
9    <Resource name="UserDatabase" auth="Container"
10      type="org.apache.catalina.UserDatabase"
11      description="User database that can be updated and saved"
12      factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
13      pathname="conf/tomcat-users.xml" />
14  </GlobalNamingResources>
15  <Service name="Catalina">
16  <Connector port="8080" protocol="HTTP/1.1"
17    connectionTimeout="20000"
18    redirectPort="8443" />
19  <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
20  <Engine name="Catalina" defaultHost="localhost">
21  <Realm className="org.apache.catalina.realm.LockOutRealm">
22    <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase">
23      <CredentialHandler className="org.apache.catalina.realm.MessageDigestCredentialHandler" algorithm="sha-512"/>
24    </Realm>
25  </Realm>
26  <Host name="localhost" appBase="webapps"
27    unpackWARs="true" autoDeploy="true">
28  <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
29    prefix="localhost_access_log" suffix=".txt"
30    pattern="%h %l %u %t &quot;%r&quot; %s %b" />
31  </Host>
32  </Engine>
33  </Service>
34  </Server>
```



Hardening – C3

→ **C3**: Tomcat credentials storage protection level.

Soluce:

Challenge

Completed

Application Hardening completed. Brute force attack is not possible.

The application must use password.

```
<?xml version='1.0' encoding='UTF-8'>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.StandardThreadPerConnectorAdapter" />
  <Listener className="org.apache.catalina.core.StandardHostManager" />
  <Listener className="org.apache.catalina.core.StandardContext" />
  <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000" redirectPort="8443" />
  <Connector port="8009" protocol="AJP/1.3" />
  <Engine name="Catalina" />
  <Realm className="org.apache.catalina.realm.DigestRealm" />
  <Realm className="org.apache.catalina.realm.DigestRealm"
    digestAlgorithm="SHA-512" />
  <CredentialHandler className="org.apache.catalina.realm.DigestRealmMessageDigestCredentialHandler" algorithm="sha-512"/>
</Server>
```

5819c97

List Applications HTML Manager Help Manager Help



Hardening – C4

→**C4**: Network access segregation level for access to TC admin app.

Objective:

Restrict access to Tomcat admin application only from localhost or 127.0.0.1.



Hardening – C4

→ **C4**: Network access segregation level for access to TC admin app.

Soluce:

Step 1: Edit the «context.xml» file of the Tomcat manager application to enable the restriction valve in order to restrict access from specified domain/ip.

```
C:\Tomcat8.0\webapps\manager\META-INF\context.xml -
File Edit Selection Find View Goto Tools Project Preferences Help
context.xml
1 <?xml version="1.0" encoding="UTF-8"?>
2 <Context antiResourceLocking="false" privileged="true" >
3   <Valve className="org.apache.catalina.valves.RemoteAddrValve"
4     allow="127.0.0.1|::1|0:0:0:0:0:0:0:1" />
5 </Context>
```

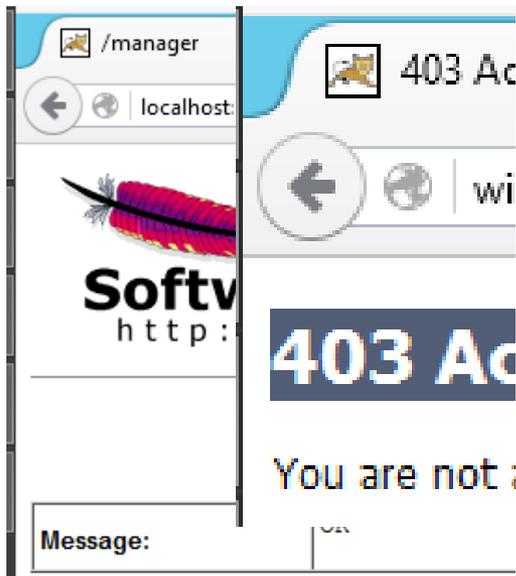


Hardening – C4

→ **C4**: Network access segregation level for access to TC admin app.

Soluce:

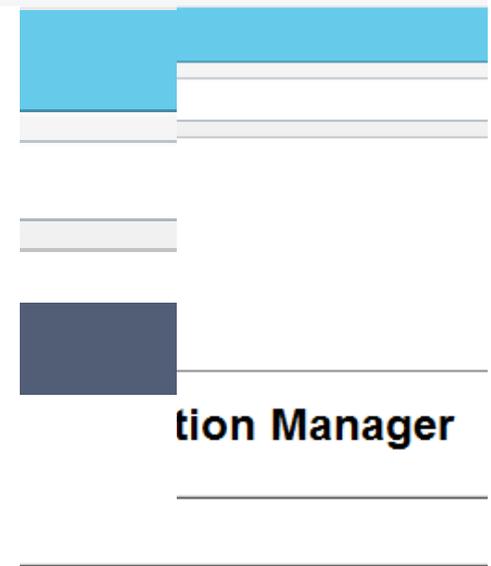
Step 2: Start the Tomcat Windows service and verify the network restriction.



Challenge



Completed





Hardening – C5

→**C5**: Access right level for TC owner user on « **webapps** » TC folder.

Objective:

Update access right in order to avoid that Tomcat dedicated user write into «webapps» application in order to avoid that an application create a webshell through a jsp or a compiled servlet.



Hardening – C5

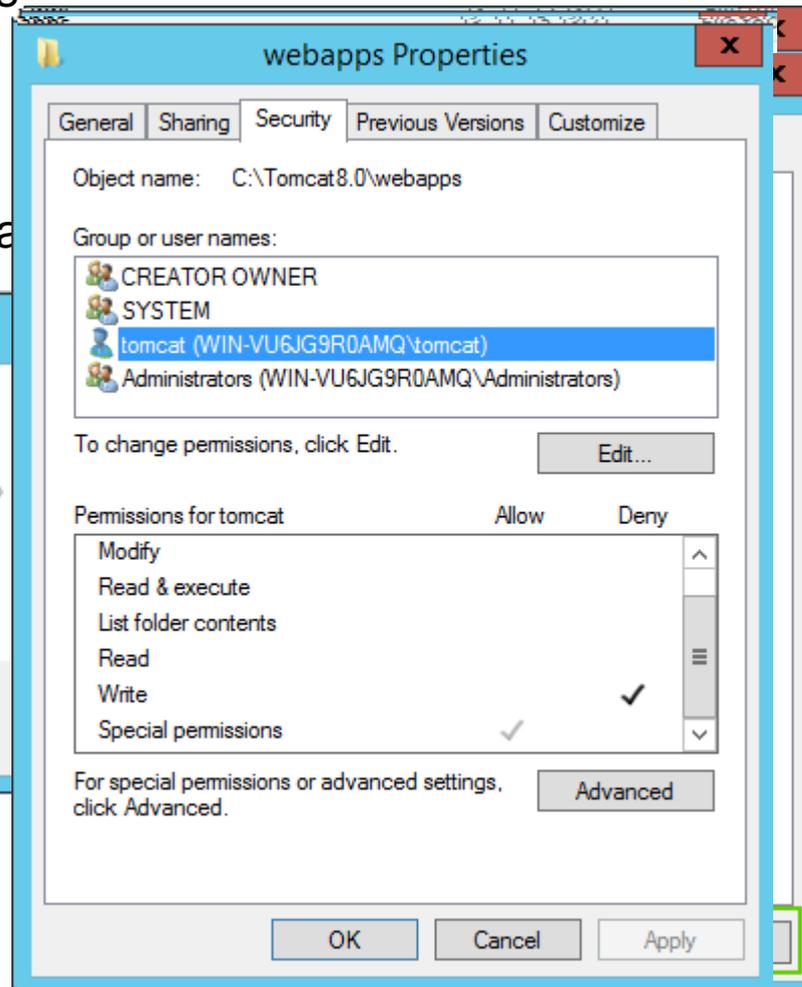
→ **C5**: Access right level for TC owner user on « **webapps** » TC folder.

Objective:

Step 1: Update a

user on <

s to Tomcat dedicated



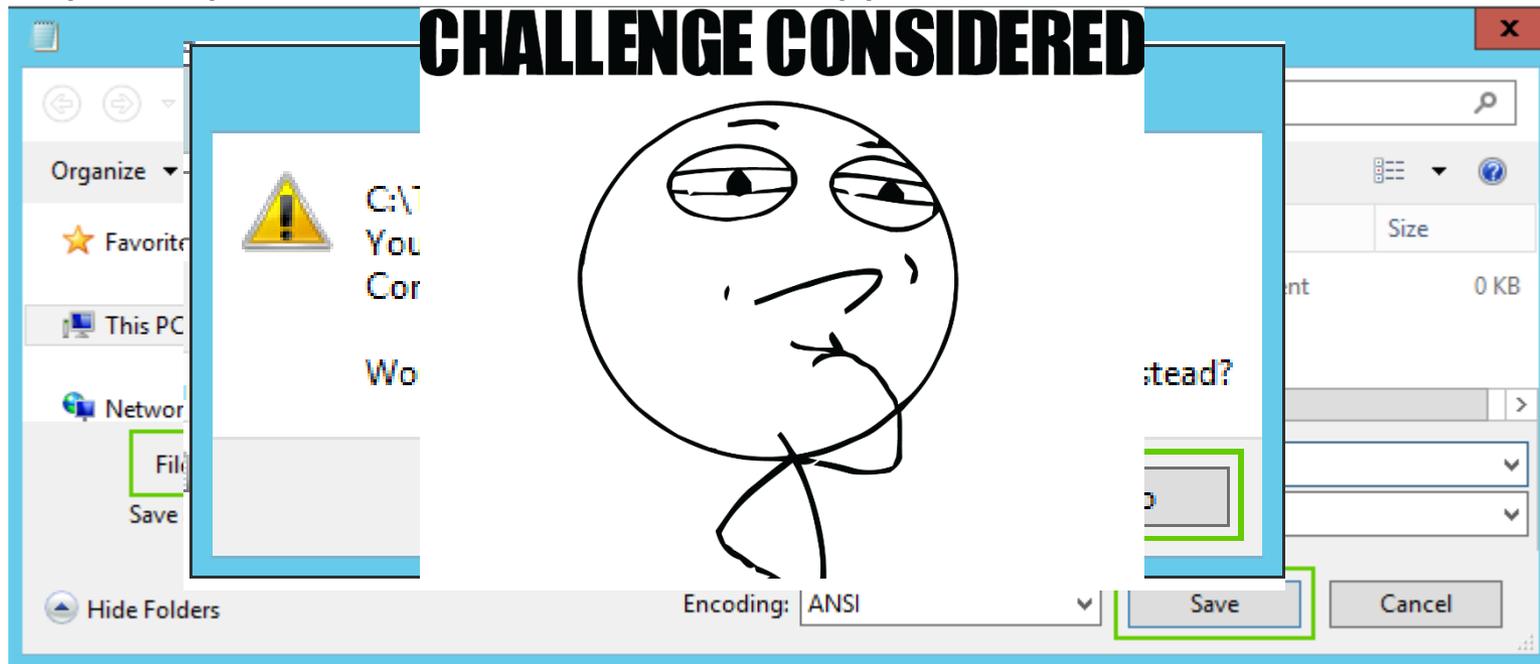


Hardening – C5

→ **C5**: Access right level for TC owner user on « **webapps** » TC folder.

Objective:

Step 1: Try to write a file into the «webapps» folder as Tomcat dedicated user.





Hardening – C5

Undo this hardening...

ing...

webapps Properties

General | Sharing | Security | Previous Versions | Customize

Advanced Security Settings for webapps

Name: C:\Tomcat8.0\webapps
Owner: tomcat (WIN-VU6JG9R0AMQ\tomcat) [Change](#)

Permissions | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	tomcat (WIN-VU6JG9R0AMQ\...	Write	None	This folder, subfolders and files
Allow	SYSTEM	Full control	C:\Tomcat8.0\	This folder, subfolders and files
Allow	Administrators (WIN-VU6JG9...	Full control	C:\Tomcat8.0\	This folder, subfolders and files
Allow	tomcat (WIN-VU6JG9R0AMQ\...	Full control	C:\Tomcat8.0\	This folder only
Allow	CREATOR OWNER	Full control	C:\Tomcat8.0\	Subfolders and files only

Add | Remove | Edit

Disable inheritance

Replace all child object permission entries with inheritable permission entries from this object

OK | Cancel | Apply



Hardening – C6

→ **C6:** TC JVM Security Manager level.

Objective:

Enable Java Security Manager to restrict action that can be performed by the application deployed on TC server.

Hints:

<https://docs.oracle.com/javase/7/docs/technotes/guides/security/PolicyFiles.html>

<https://docs.oracle.com/javase/7/docs/technotes/guides/security/permissions.html>

<https://tomcat.apache.org/tomcat-7.0-doc/security-manager-howto.html>

http://tomcat.apache.org/tomcat-8.0-doc/config/host.html#Standard_Implementation



Hardening – C6

C:\Tomcat8.0\conf\server.xml

Edit Selection Find View Goto Tools Project Preferences Help

```
server.xml x
1 <?xml version='1.0' encoding='utf-8'?>
2 <Server port="8005" shutdown="SHUTDOWN">
3   <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
4   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
5   <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
6   <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
7   <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
8   <GlobalNamingResources>
9     <Resource name="UserDatabase" auth="Container"
10       type="org.apache.catalina.UserDatabase"
11       description="User database that can be updated and saved"
12       factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
13       pathname="conf/tomcat-users.xml" />
14   </GlobalNamingResources>
15   <Service name="Catalina">
16     <Connector port="8080" protocol="HTTP/1.1"
17       connectionTimeout="20000"
18       redirectPort="8443" />
19     <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
20     <Engine name="Catalina" defaultHost="localhost">
21       <Realm className="org.apache.catalina.realm.LockOutRealm">
22         <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase">
23           <CredentialHandler className="org.apache.catalina.realm.MessageDigestCredentialHandler" algo
24         </Realm>
25       </Realm>
26     <Host name="localhost" appBase="webapps"
27       unpackWARs="true" autoDeploy="true" deployXML="true">
28       <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
29         prefix="localhost_access_log" suffix=".txt"
30         pattern="%h %l %u %t &quot;%r&quot; %s %b" />
31     </Host>
```



Hardening – C6

→ **C6:** TC JVM Security Manager level.

Soluce:

Step 2: Start the Tomcat Windows service and verify the access possibility of the application.

Challenge



Completed

```
http://localh  
java.security.AccessControlExcept  
at java.security.AccessContro  
at java.security.AccessContro  
at java.lang.SecurityManager.  
at java.lang.SecurityManager.  
at java.io.FileInputStream.<i  
at java.io.FileInputStream.<i  
at eu.excellium.Loader.doGet(  
at javax.servlet.http.HttpSe
```

```
...  
t8.0\conf\server.xml" "read")  
)
```

Message: OK



Hardening – C7

→**C7**: TC Documentation and ROOT applications are still online..

Objective:

Undeploy theses applications.



Hardening – C7

→**C7**: TC Documentation and ROOT applications are still online..

Soluce:

Step 1: Remove theses applications from folders « webapps ».

```
C:\Tomcat8.0\work\Catalina\localhost>rmdir /S /Q docs  
C:\Tomcat8.0\work\Catalina\localhost>rmdir /S /Q ROOT
```



Hardening – C7

→ **C7**: TC Documentation and ROOT applications are still online..

Soluce:

localhost:8080/manager/html

Tomcat Web Application Manager

Message: OK

Challenge



Completed

Applications		
Path	Version	
/TestVulnApp	None specit	
/manager	None specit	

Running	Sessions	Comm
true	0	Start Exp
true	1	Start Exp

952 ms
329 ms



Questions