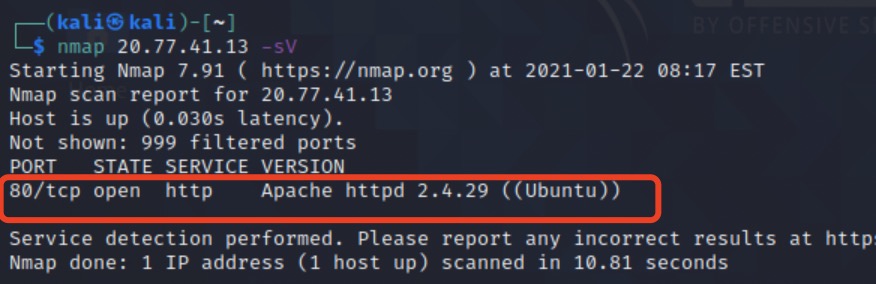
# Penetration Testing

**10655496 Huanjie Guo**

**Target IP：20.77.41.13**

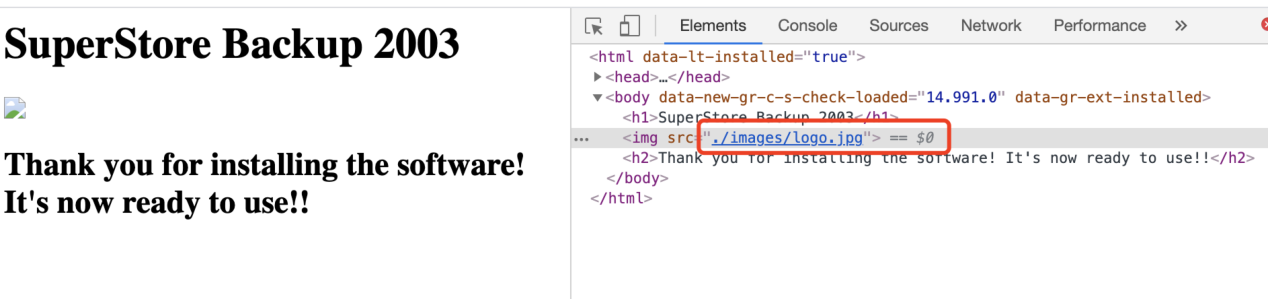
**Manual scanning**

I use nmap 20.77.41.13 -sV to scan what software is running on the port of the server.

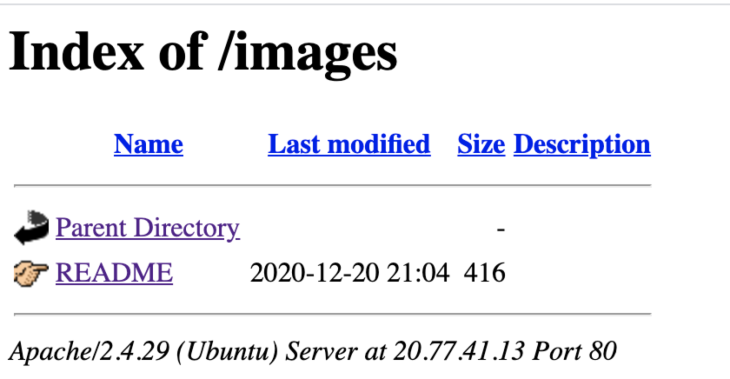


I found that port 80 is open, and the HTTP service is running on this port. The version of HTTP is Apache httpd 2.4.29.

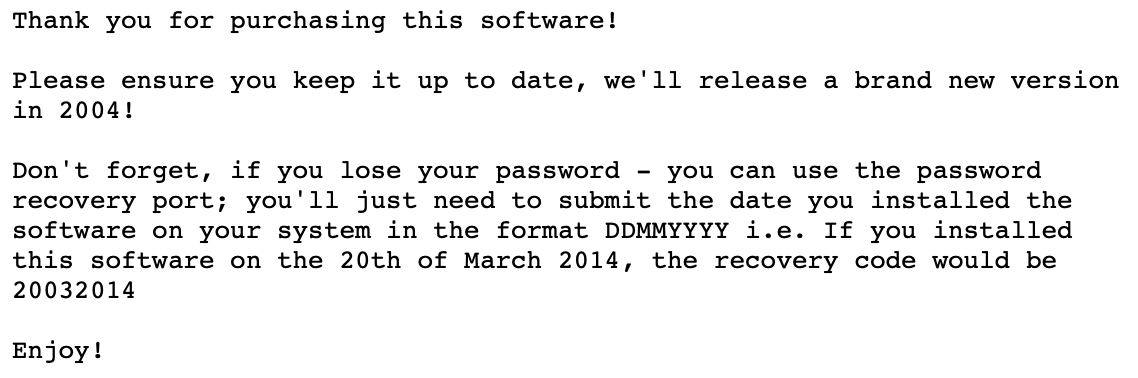
I input the IP address in chrome, then it shows the HTML page of the website. I inspect the image on the page and get the path of the image.



I input "20.77.41.13/images" and find a readme File.

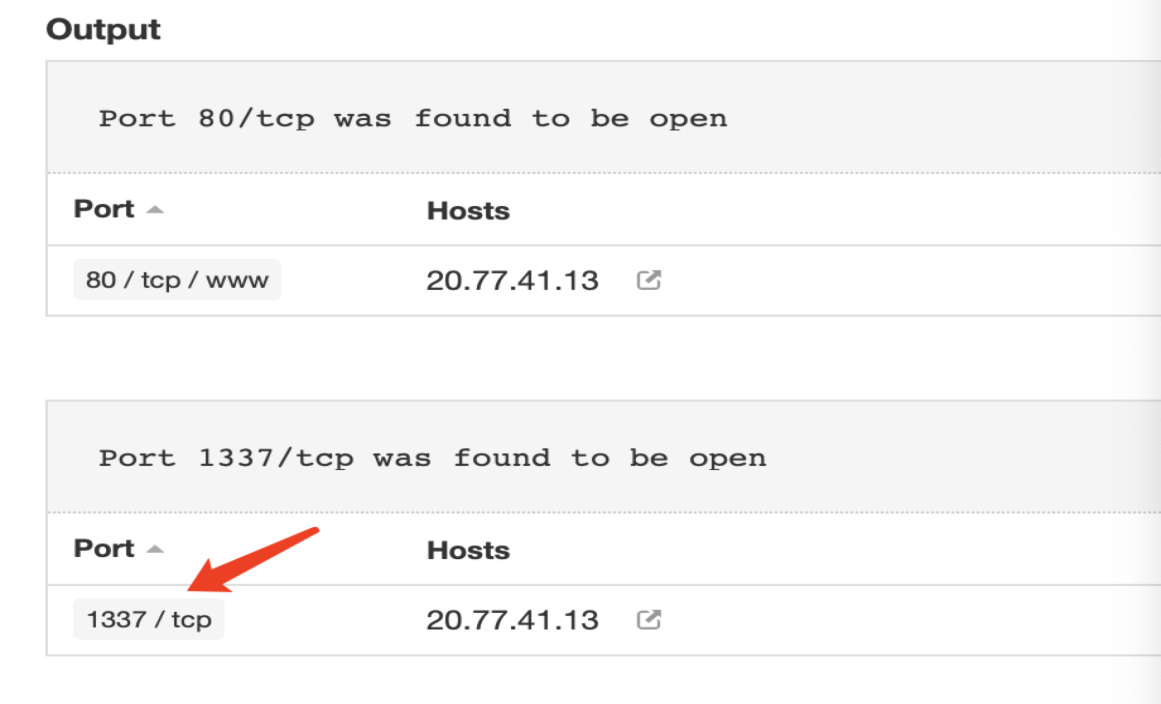


Open it, and I get the information.

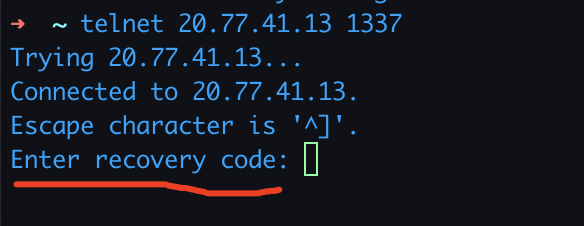


**Auto Scanning**

I used Nessus to do an auto-scan and found that there is a port of 1337 open, but I cannot found it when I used nmap.



Then I used telnet, input "telnet 20.77.41.13 1337" to check if I can connect to it, and it returned the message as follow:



I found that this port is a recovery port, and the detail of the code is mentioned in the README file. Now, I need to guess the code of it.

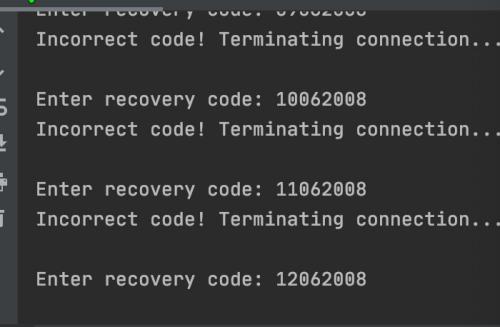
**Write a brute force script**

I used Java to write a script which try to input the year from 2000 to 2020, the day from 01 to 30, and the month from 01 to 12.

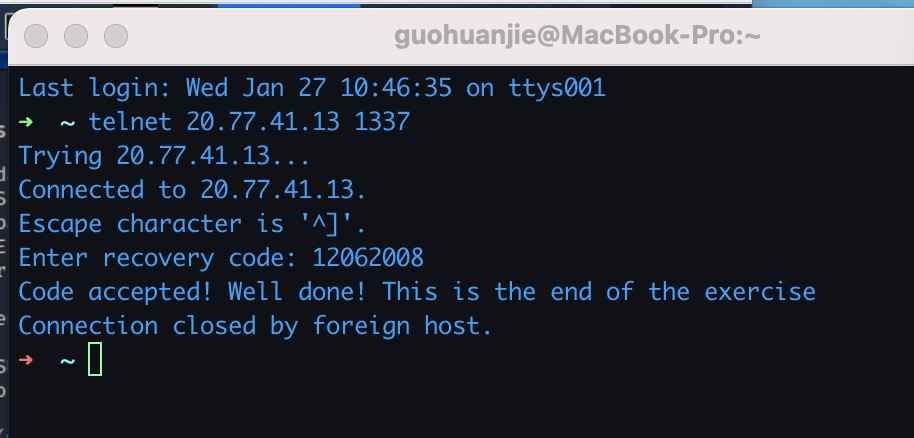
The code has been uploaded to my github:

<https://github.com/HuanjieGuo/Algorithm/blob/master/src/telnet/Penetrate.java>

I run it, and when the program tried to use 12062008, it found the password.



I open the terminate, use '12062008' as the code, and it returns as followed.



**Vulnerability and Recommendation**

**Browsable Web Directories**

|  |  |
| --- | --- |
| Rating | Medium |
| Description | Directories on the web server that are browsable.  http://20.77.41.13/images/ |
| Impact | Leak important information |
| Remediation | Make sure that browsable directories do not leak important information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do. |

**Weak Credentials**

|  |  |
| --- | --- |
| Rating | Critical |
| Description | The password of the recovery port is the date. It is only about 3650 possibilities in the past ten years and can be broken within minutes. |
| Impact | Using a common enumeration and brute-forcing techniques, it is possible to  retrieve the password. |
| Remediation | Ensure that the recovery port is protected with complex passwords or passphrases. Avoid the use of common or business-related words, which could be found or easily constructed with the help of a dictionary and personal information. |