

Penetration Testing

10655496 Huanjie Guo

Target IP: 20.77.41.13

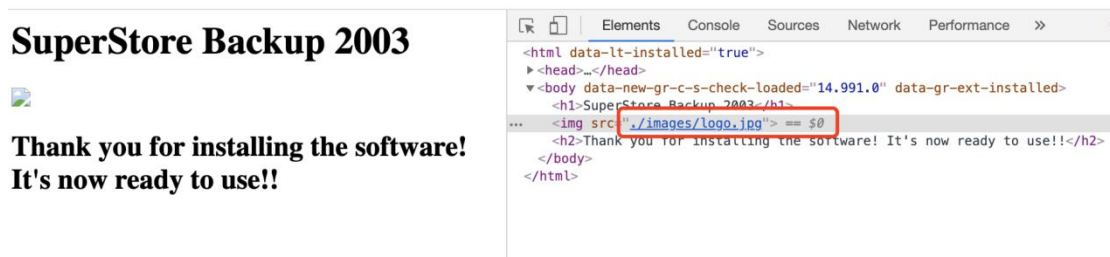
Manual scanning

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

```
(kali㉿kali)-[~]  
└─$ nmap 20.77.41.13 -sV  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-22 08:17 EST  
Nmap scan report for 20.77.41.13  
Host is up (0.030s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))  
  
Service detection performed. Please report any incorrect results at http://nmap.org  
Nmap done: 1 IP address (1 host up) scanned in 10.81 seconds
```



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.

Index of /images

Name	Last modified	Size	Description
 Parent Directory		-	
 README	2020-12-20 21:04	416	

Apache/2.4.29 (Ubuntu) Server at 20.77.41.13 Port 80

Open it, and I get the information.

Thank you for purchasing this software!



Please ensure you keep it up to date, we'll release a brand new version in 2004!

Don't forget, if you lose your password - you can use the password recovery port; you'll just need to submit the date you installed the software on your system in the format DDMMYYYY i.e. If you installed this software on the 20th of March 2014, the recovery code would be 20032014

Enjoy!

Auto Scanning

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

Output	
Port 80/tcp was found to be open	
Port ^	Hosts
80 / tcp / www	20.77.41.13 
Port 1337/tcp was found to be open	
Port ^	Hosts
1337 / tcp	20.77.41.13 

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:

```
→ ~ telnet 20.77.41.13 1337
Trying 20.77.41.13...
Connected to 20.77.41.13.
Escape character is '^]'.
Enter recovery code: 
```

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/Penetrates.java>

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

```
Enter recovery code: 07062008
Incorrect code! Terminating connection...

Enter recovery code: 10062008
Incorrect code! Terminating connection...

Enter recovery code: 11062008
Incorrect code! Terminating connection...

Enter recovery code: 12062008
```

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

```
guohuanjie@MacBook-Pro:~
Last login: Wed Jan 27 10:46:35 on ttys001
→ ~ telnet 20.77.41.13 1337
Trying 20.77.41.13...
Connected to 20.77.41.13.
Escape character is '^]'.
Enter recovery code: 12062008
Code accepted! Well done! This is the end of the exercise
Connection closed by foreign host.
→ ~ 
```

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.