TryHackMe penetration test report, BruteIt room

General Info and Goals

The purpose of the test is to find vulnerabilities that allow you to gain access to the machine on the given IP address, try to get the content of the root.txt flag and possibly obtain the highest privileges in the tested environment by finding and using vulnerabilities that enable it. Based on the results of the report, corrective actions are suggested.

Tools used

- nmap
- gobuster
- hydra
- john
- GTFOBins

Process

a) The first step of the test was to get information about the machine and find a possible input vector. For this purpose, the nmap program was used together with switches enabling obtaining the software version and scanning only ports on the given IP address.

b) The next step after finding a working service on port 80(http) was an attempt to find a useful path using the bruteforce method, using the gobuster program, using the most popular subpage names (URL) contained in the “common.txt” dictionary list

c) Having a potential username for the admin panel on port 80 in the /admin path, it is possible to bruteforce a login attempt. In this case, the hydra program was used, which uses a dictionary list with the most popular used passwords called "Rockyou.txt"

d) Possessing the RSA key, an attempt was made to obtain the user's password from the key using the JohnTheRipper program

e) Login to the machine via the SSH port using the previously obtained data. Then check the capabilities of the obtained user on the machine. The user we are on does not have the highest privileges, however, he can use programs that give him higher privileges. The sudo -l command was used for this purpose

f) Using the CAT program with higher permissions, we get access to files and folders that can only be read with the highest permissions. In this case, we accessed files containing useful information for obtaining other user logins such as etc/passwd and etc/shadow, then decrypting the user logins and passwords in these files.

Results

a) Information about open ports and visible names of software and services. Port 22 and 80.

b) The path was found: “http:///admin” serving as the admin panel. After inspecting the site, a comment left by the developer was found with the content stating that the login may be "admin".

c) A successful attempt to log in to the admin panel found earlier login "admin" with the bruteforce password "xavier". Then, after logging in, a private RSA key was found on the website that allows logging in via the SSH port and extracting the password from it. We can also find out that the RSA key was prepared for a user named “john”.

d) The result of the action is to receive a password from the RSA key with the content "rockinroll"

e) Received information that the user "john" can use the CAT program with the highest privileges.

f) The login details of the top user "root" and full access to the tested machine and files were obtained. The ability to read and download the flag that was the target of this pentest.

5. Summary and suggested corrective actions

a) hiding the names of the services used and changing the number or hiding the SSH port to 22.

b) changing the path of the subpage with login on the admin panel to a less popular and obvious one, and removing the comment with the login in the page code.

c) the suggested action is to temporarily disable the possibility of logging in after several failed login attempts and possible security or additional encryption of the RSA key if it is required to be left on the website.

d) no suggested solutions

e) Disabling users from using programs with higher privileges.

f) Securing access to the /etc directory. And disabling the ability to read and edit similarly sensitive files and folders by the CAT program and similarly capable text editors such as NANO or VIM.