TryHackMe penetration test report, Agent T room

General Info and Goals

The purpose of the test is to find vulnerabilities that allow access to the machine on the given IP address, and to obtain the highest permissions in the tested environment by finding and using vulnerabilities that enable. Based on the results of the report, corrective actions are suggested.

Tools used

- nmap
- python3
- vulnerability: https://www.exploit-db.com/exploits/49933
- netcat

Process

a) The first step was to scan the ports on the machine with the given IP using the nmap program.

b) Checking the service on port 80 by the browser.

c) Exploitation of the found vulnerability with the number EDB-ID: 49933 The use of a vulnerability executable by a script created in Python3.

Results

a) Found http service on port 80, but without information about services and software.

b) Found admin panel without providing login details together with information about services and software version.

c) Full access with the highest privileges with the ability to execute commands and a stable reverse shell.

Summary and suggested corrective actions

a) No suggested action, hidden service name.

b) Securing the admin panel with the possibility of logging in along with temporary disabling of login access after, for example, 3 failed attempts, protecting against bruteforce attacks.

c) Changing or updating the service on port 80 to a less vulnerable one.