TryHackMe penetration test report, Source room

Description and Purpose

The purpose of the test is to find vulnerabilities that allow you to gain 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 it. Based on the results of the report, corrective actions are suggested.

Tools used

- nmap
- metasploit

Process

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

b) After receiving information about open ports, the built-in script of the nmap program was used to detect vulnerabilities on exposed services.

c) Checking the vulnerability found using the metasploit program.

Results

a) Found open ports 22 and 10000 along with the names of the offering services. The ability to enter the admin login panel after entering the address http://:10000.

b) A vulnerability found on the offered MiniServ 1.890 service on port 10000 with the number: CVE-2019-15107.

c) Vulnerability exploited and possible operation on a machine with the highest privileges after obtaining a stable shell using Python.

Summary and suggested corrective actions

a) Changing the number of SSH port 22 or hiding or disabling it. Disabling the ability to send information about services on the machine.

b) Updating or changing the service on port 10000 to a less vulnerable one. Suggested action in this direction as soon as possible, due to the high threat rating [9.8 out of 10].