Beep

The first step of Pentesting is Reconnissance but in this case we already know about the network IP hence we go forward with the next step which is Enumeration.

Used **Nmap** tool to enumerate and scan for open ports and services on the machine.

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

There is a long list of open ports on the machine yet we will target on those which can easily be exploited which leads to port 80 which is a unsecured HTTP protocol and can be a high probability of getting attacked.

Used **Gobuster** tool to scan for available sub directories on the target website. Lets run it against a simple common.txt file which contains common sub-directories.

A computer screen capture

Description automatically generated with medium confidence

With the above results, enumerated more on the website directories to find any exploitable vectors.

The robots.txt file doesn’t give much information though.

Graphical user interface, text, application

Description automatically generated

As looked more into vulnerabilities on the hosted website which is FreePBX. It seems to be vulnerable to LFI vulnerability.

Graphical user interface, text, application

Description automatically generated

The presence of vtigercrm subdirectory helps to understand that this can be used to exploit the LFI vulnerability.

Text

Description automatically generated

There you go! Using the LFI vulnerability we are able to access the page which contains lots of sensitive information which includes Admin credentials of the PBX webserver.

Text

Description automatically generated

Same creds will let us into the Admin portal of the website.

Graphical user interface, text, application

Description automatically generated

The same credentials also lets you get access to the SSH service on root privileges.

Logged in to SSH service with root credentials and got the flag.

Text

Description automatically generated

Graphical user interface, text

Description automatically generated