Bashed

As an initial step, ran **Nmap** tool to scan the machine for open ports and services.

Text

Description automatically generated

Since there is only one port open – 80, started enumerating more on the same by running **Gobuster** tool and list out all the sub directories on the machine.

A screenshot of a computer

Description automatically generated with medium confidence

There are quite a few of them being resulted after the scan. And started exploring each one of them.

This is the main page of the website having details about the product and the application it is running.

Graphical user interface, text, application

Description automatically generated

While enumerating more, found a dev site which has the original code of the application being exposed.

Graphical user interface, text, application, email

Description automatically generated

As tried accessing the same resulted out functionality of the application.

Text

Description automatically generated

Since it gives us the interactive shell but not much to do on the same. Use the python reverse shell script to create a shell onto your local machine.



Text

Description automatically generated

Stabilize the shell using the command - **python3 -c 'import pty; pty.spawn("/bin/bash")'**

Text

Description automatically generated

Once stabilized, enumerate more on the machine and found that the user scriptmanager has access to run anything with root privileges on the machine.

Text

Description automatically generated

Use the command and sudo privilege to change the user as scriptmanager to access a specific directory named – **scripts**.

Once change the user and listed out the contents of the Scripts folder, we could see that the **test.py** script is running and creating another txt file named -**test.txt** which has root privileges.

Text

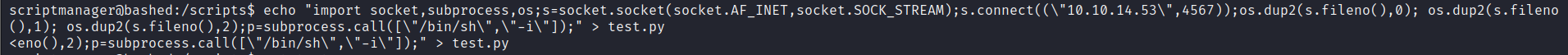
Description automatically generated

Also noticed that the python file is being executed every minute like a cron job.

Graphical user interface

Description automatically generated with medium confidence

Since the **test.py** has full access to scriptmanager, hence edit the python file in order to create another shell with root access.



Open up a listener with the same port and wait for the cronjob to be run and get the root shell.

Text

Description automatically generated

Finally we get the root shell and owned the machine with the root.txt.

Shape, arrow

Description automatically generated