Nibbles

As the initial step, used **Nmap** tool to run a scan for open ports and services on the machine.

Text

Description automatically generated

With port 80 open, Opened the same on the browser.

Graphical user interface, text, application

Description automatically generated

Immediately checked on the source code of the webpage which revealed another directory of the web server which has more content.

Graphical user interface, text, application, chat or text message

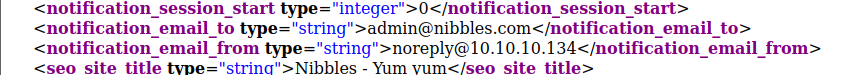
Description automatically generated

Next enumerated more on the web sub-directories on the designated webpage which exposed more sub-directories.

Text

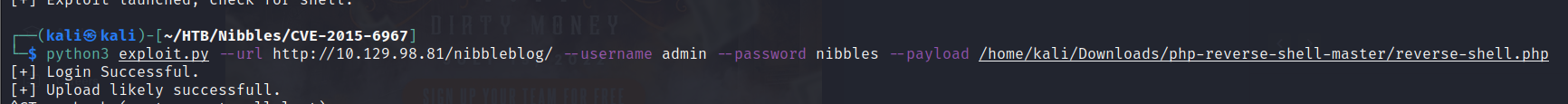
Description automatically generated

As enumerated more on the webpage, the email address of the administrator has been revealed.



As researched more on google for open vulnerabilities on Nibble-blog, found an interesting Shell upload vulnerability and followed the URL - <https://github.com/dix0nym/CVE-2015-6967>

Followed the steps in the URL to get a shell onto our local machine.



Graphical user interface, text

Description automatically generated

The current shell has the user – **Nibbler**  privileges. When tried to check the Sudo privileges on the machine, it seems that the user Nibbler can run **monitor.sh** script with root privileges. Hence this can be exploited further to get root privileges.

Text

Description automatically generated

Changed the **Monitor.sh**  script to a one-liner sudo privileges.

Text

Description automatically generated

Finally we get the root access to the machine and found the root flag.

Graphical user interface

Description automatically generated