Expose

1. Nmap scan reveal 1337(http), ftp, ssh, dns and mqtt
2. gobuster revealed myphpadmin(mysql page), admin_101 and admin page. It seems like admin_101 page is the valid one since it has predeclared username.
3. Password crack did not amount to anything so try sql injection using sqlmap `sqlmap -r req.txt --dump` after generating the post form via burpsuite on admin_101 page
4. Using sqlmap we found the password of hacker@root.thm which is VeryDifficultPassword!!#@#@!#!@#1231
5. The sqlmap also dumped a few interesting directory and their login password, mainly `/file1010111/index.php` which has password easytohack and another directory `/upload-cv00101011/index.php` which says only accessible to username with z.
6. Navigating to `/file1010111/index.php`, we provide the password but it's a dead end. However, it is vulnerable to remote file inclusion by doing `http://10.10.81.199:1337/file1010111/index.php?file?=/etc/passwd` and we found username zeamkish
7. navigating to /upload-cv00101011/index.php, we found a upload form that only accepts png file. To bypass this, we fire up burpsuite and modify our reverse shell from rev.phpD.png. We then upload and intercept with burpsuite, set the D bit to terminating byte essentially changing the file name to rev.php and forward which is successful. Inspecting the source we found the upload dir is `/upload_thm_1001`
8. Navigate to `http://10.10.81.199:1337/upload-cv00101011/upload_thm_1001` we see our reverse shell script and execute it by clicking on it. We gain a reverse shell.
9. We cannot view the usr flag but we do get a ssh login. Login in via ssh we managed to view usr flag.
10. To get root flag, we run `find / -perm -u=s -type f 2>/dev/null` to find suid permission. We see that nano has suid id permission and that means we can just nano /root/flag.txt to read the flag.