webpack (.96)	
Operating System	Linux
Points	20
Similar Machine (User)	TryHackMe's Ignite
Similar Machine (Root)	HackThebox's Jarvis

Exploit in Getting User

1. Run un gobuster on port 80 and you will get /index.php/fuel
2. Login as admin:admin
3. FuelCMS is vulnerable to https://www.exploit-db.com/exploits/47138
4. Modify the URL and directories
5. For the reverse shell make sure you use port 80 to bypass the iptables
6. User shell!

Privilege Escalation to Root

1. Run Linux Enumeration script
2. You will see it has systemctl
3. /var/www/html/assets/images/ is writable
4. Follow this - https://medium.com/@klockw3rk/privilege-escalation-leveraging-misconfigured-systemctl-permissions-bc62b0b28d49
5. Root shell!

Recent Update for Priv.Esc.:

1. Locate Webmin's writable miniserv.users with Linux Enumeration script
2. Use openssl passwd -1 "yourpassword"
3. Overwrite the "x" in the miniserv.users with the hash generated
4. Run sudo systemctl restart webmin
5. Browse port 10000 and login with root/yourpassword
6. Execute nc in the System>Running Process
7. Root shell!