ISEC3002 Penetration Testing and Defence Workshop 9

Using running web applications and services to get a shell to escalate the privilege

Please upload your solution with screenshots to ***Class Works and Tutorials Submission*** folder under Assessments on Blackboard. You need to include commands and screenshots in your answers.

The purpose of this workshop is to learn how to exploit a vulnerability in running services and web applications to gain root access to a system. You might need to check the tutorials provided in the reference section.

Exercise 1- VulnHub → RIPPER: 1

Follow the steps in the link below to learn how to get a shell and do privilege escalation using running web applications. You will be exploiting all the services running in RIPPER: 1.
https://resources.infosecinstitute.com/topic/ripper-1-vulnhub-ctf-walkthrough/

Exercise 2- CyberRange → Vulnerable Machines

Exploit the running services and web application vulnerabilities of the following machines to gain root access to the system.

- Tel-Aldruhn → 192.168.2.9
- Pelagiad → 192.168.2.7

Reference

https://www.vulnhub.com/entry/ripper-1,706/

https://resources.infosecinstitute.com/topic/ripper-1-vulnhub-ctf-walkthrough/

https://www.cvedetails.com/vulnerability-list/vendor_id-358/Webmin.html

https://www.exploit-db.com/exploits/50809