

ISEC3002 Penetration Testing and Defence

Workshop 10

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 → GEMINI INC: 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 running services.

- <https://www.hackingarticles.in/hack-the-gemini-inc-ctf-challenge/>
- <https://scriptkidd1e.wordpress.com/geminiinc-v1-vm-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.

- Balmora → 192.168.2.10
- DagonFel → 192.168.2.24

Reference

<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>
<https://www.hackingarticles.in/comprehensive-guide-on-dirb-tool/>
<https://learnhacking.io/a-complete-guide-to-web-enumeration-with-dirb/>
<https://www.hackingarticles.in/escalate-linux-vulnhub-walkthrough-part-1/>

<https://www.exploit-db.com/docs/49411>

https://www.youtube.com/watch?v=u_Q00e7f4K0

<https://phoenixnap.com/kb/linux-ftp>

<https://pentestmonkey.net/tools/web-shells/php-reverse-shell>