

Ethical Hacking and Penetration Testing, Spring 2024
Assignment 6

1 Description

Privilege Escalation usually involves going from a lower permission account to a higher permission one. More technically, it's the exploitation of a vulnerability, design flaw, or configuration oversight in an operating system or application to gain unauthorized access to resources that are usually restricted from the users.

2 Guidelines

Escalate linux - Intentionally developed Linux vulnerable virtual machine.
The main focus of this machine is to learn Linux Post Exploitation (Privilege Escalation) Techniques.

ESCALATE LINUX

<https://drive.google.com/file/d/1ah38R3639I0RvVM7zte98waaa6jNt1BT/view>

3 Deliverables

You are required to submit a pdf file that include :-

1. Enumeration steps.
2. Vulnerability scanning steps.
3. Exploitation steps.
4. Privilege escalation steps with two ways:
Exploiting SUID (Misconfiguration).
Exploiting crontab.
5. Screenshots of each step and a description at each screenshot.

German International University
Faculty of Informatics and Computer Science
Dr. Marwa Zamzam
Eng. Zyad Mostafa

4 Submission

- You should submit your PDF at the following link:
<https://forms.office.com/r/kBHH5ueHvD>
- The filename should be of form <ID_Name>.
For example: 1001234_Adam_Smith.zip
- Online submission is due on Monday, April 22, by 23:59 pm.