**Title: Exploit SUDO Security Policy Bypass Vulnerability in LINUX**

**Learning Objectives:** The learning objective of this exercise is to understand the SUDO Security Policy Bypass Vulnerability in Linux, and learn how to exploit sudoedit bypass to achieve unauthorized privilege escalation. Participants will gain hands-on experience in identifying affected systems, exploiting the vulnerability, recognizing indicators of compromise (IOCs), and implementing effective detection, mitigation, and prevention techniques to secure Linux environments against this vulnerability.

**Description:** The SUDO Security Policy Bypass Vulnerability allows unauthorized users to gain elevated privileges by exploiting a flaw in specific versions of sudo. This vulnerability can be used to execute commands with root-level access, bypassing security restrictions. Understanding and exploiting this vulnerability will help you learn crucial techniques for assessing and securing Linux systems against privilege escalation attacks.

**Instructions to Follow Before Executing the Exercise:**

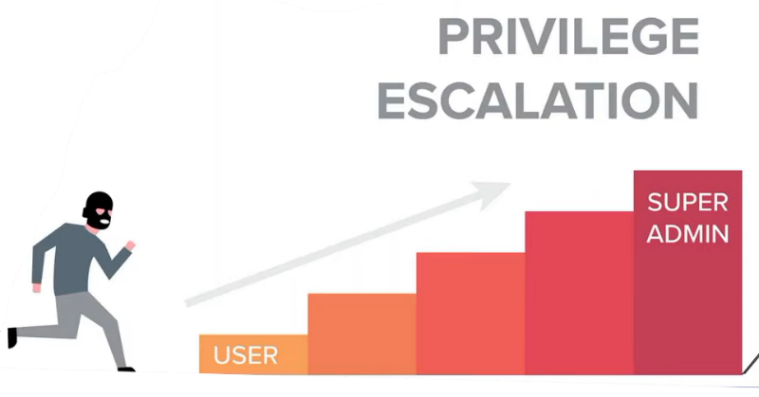
1. **Setup a Secure Testing Environment:**

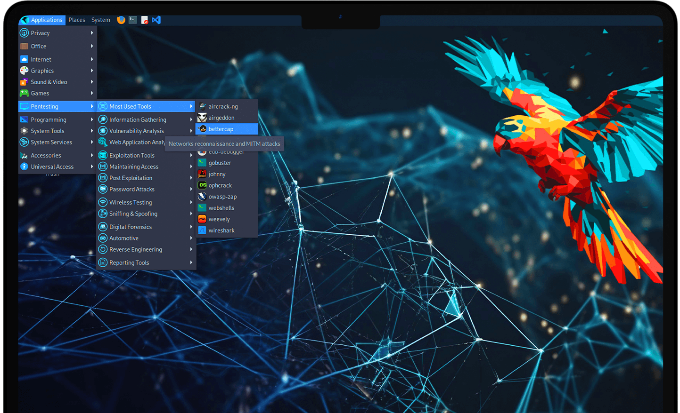
* Use a virtual machine or isolated environment to conduct the exercise, preventing any accidental damage to the systems.
* Ensure the environment is backed up to revert to a previous state if needed.

1. **Verify System Requirements:** Confirm that the Linux distribution and version you are using are within the range affected by the vulnerability (Sudo versions 1.8.0 to 1.9.12p1).
2. **Install Necessary Tools:** Ensure essential tools like vim (or alternative text editors) and the sudo package are installed.
3. **Create a Limited Privilege User:** Establish a user account with restricted permissions to simulate an attack scenario, granting sudoedit access to at least one file.
4. **Review Safety Precautions:** Understand the potential impact of the exploit and take necessary precautions to avoid disrupting services unintentionally.
5. **Plan for Post-Exercise Cleanup:** Be prepared to restore any changes made to the system during the exercise, particularly any modifications to sensitive files like `/etc/passwd`.

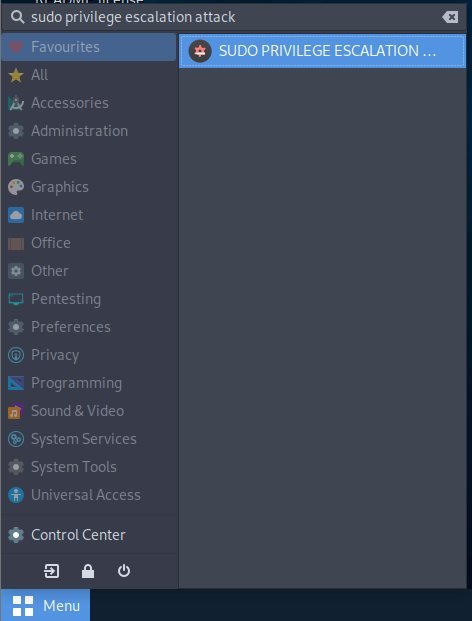
Following these instructions will help ensure that the exercise is conducted safely and effectively, minimizing risks and maximizing learning experience.

**About the Exercise lab infrastructure:**

For this exercise, you need one virtual machine running any Linux distribution (such as parrot OS, Kali Linux or Ubuntu) with a sudo version falling within the range of 1.8.0 to 1.9.12p1.



Launch Attack by clicking on “SUDO BYPASS ATTACK” button.

Go to the **Application tab>Education > SUDO PRIVILEGE ESCALATION ATTACK**.

For detailed instructions, refer to the step-by-step guide provided in the "Exploit SUDO Security Policy Bypass Vulnerability in LINUX" lab manual.