Basic Privilege Escalation

On Linux systems, services may be running as a non-root user. For e.g., by default, Apache and Nginx run as the user www-data. Therefore, even if a web application or the service itself is compromised, the attacker will only get access as the www-data user which has limited privileges. To gain full control of a system, it is important to escalate privileges from a user with low privileges to the root user (vertical escalation).
It might not be always possible to escalate from the current user to the root user. In such cases, other users on the machine must be compromised (horizontal escalation), and then used to try to attain root privileges.

The objective of this section is to teach the student the various techniques of privilege escalation in the Linux environment.

What will you learn?

- Leveraging misconfigured Cron jobs for escalating privileges.
- Leveraging SUID binaries for escalating privileges.
- Performing Shared Library injection and escalate privileges.
- Breaking out of restricted environments such as rbash and chroot.
- Exploiting vulnerable services to escalate privileges.

References:

1. Privilege Escalation (https://en.wikipedia.org/wiki/Privilege_escalation)

Labs:

Basics:

- Exploiting Setuid Programs
  - Objective: Leverage setuid binaries on the system and escalate privileges to the root user.
- Cron Jobs Gone Wild!
  - Objective: Leverage the popular wildcards gone wild misconfiguration in cron job and escalate privileges to the root user.
- Permissions Matter!
  - Objective: Leverage misconfigured file permission on /etc/shadow and escalate privileges to the root user.
- Editing Gone Wrong
  - Objective: Abuse Sudo privilege and escalate privileges to the root user.
- The Golden Logs
  - Objective: Read the logs, identify the misconfiguration, and leverage it to escalate privileges to the root user.
- Shared Server
  - Objective: Leverage credentials reuse attack and escalate privileges to root user.
- Load Order Matters
  - Objective: Perform shared library injection based on LD_PRELOAD and escalate privileges to root user.
- Restricted Shell
  - Objective: Breakout of restricted bash by leveraging shell support provided by interactive tools.
- Chroot Jail I
  - Objective: Breakout of chroot by using build tools such as GCC.
- Fallen Guardian
  - Objective: Exploit the vulnerable rootkit detector and escalate privileges to the root user.

More labs for this topic are available under the Privilege Escalation section on AttackDefense.