Linux Privilege Escalation

Objective

Linux powers the Internet today, making it a favorite target for attackers. Linux security mechanisms are fairly comprehensive when it comes to coverage, but are also equally complex to get right unless you are an expert. As Linux offers multi-user tenancy, the common perception is that it is impossibly hard to escalate privileges to root.

The focus of this bootcamp is to familiarize you with beginner-to-advanced privilege escalation techniques on Linux. You will learn how to identify and leverage misconfigurations to perform horizontal/vertical escalation. The bootcamp will cover techniques starting from traditional privilege escalation methodologies to advanced concepts such as Linux capabilities.

Completing the bootcamp and passing the certification exam will prepare you for performing privilege escalation effectively on Linux-based machines.

Prerequisites

- A basic knowledge of computers and networking
- Familiarity with any Linux OS such as Ubuntu

Course Content

Module I: Basic Privilege Escalation Techniques Part I

- Linux Concepts
    - Linux Users and Groups
    - Linux File Permissions
    - Interactive programs
        - Text Editor
        - Terminal based Browsers
    - Popular Linux Utilities
    - Cron Job
        - Crontab File formats
        - User vs System crontab.

    - Shared Libraries
        - Understanding the Load Order
        - Creating a shared library
- Misconfigured SUID
- Misconfigured SUDO
- Misconfigured File Permissions

Module II: Basic Privilege Escalation Techniques Part II

- Leveraging Cron Jobs
    - Unix Wildcards gone wild
    - World writable scripts
    - World readable cron error messages
    - Symlinks and PATH-based misconfigurations.
- Vulnerable Application and Services
- Web to Root
- App to Root
- Shared Library Injection

Module III: Breaking out of Restricted Environments

- Restricted Shells
- Chroot Jail
- Docker Environment
    - Privileged Containers
    - Mounted Docker Socket
    - Shared Network Namespace
    - Additional Capabilities
    - Leveraging Management Tools
- Best Practices

Module IV: Linux Capabilities

- Introduction to Linux Capabilities
    - History
    - Process and file capabilities
    - Linux Capabilities Sets
    - Identifying capabilities provided to binaries and running process
    - Managing capabilities
- Abusing Linux Capabilities

- CAP_DAC_READ_SEARCH
- CAP_SYS_MODULE
- CAP_SYS_ADMIN
- CAP_SYS_PTRACE