GETTING STARTED
Linux Privilege Escalation

This section covers some of the advanced Linux features such as Linux Capability, Apparmor and seccomp.

Linux Capabilities

With the advent of Linux capabilities, the privileges associated with a superuser were divided into distinct units, known as capabilities. To perform a privileged task, it was now possible to provide only the required capability instead of creating a *suid* binary or providing *sudo* privileges. Linux capabilities significantly decreased the attack surface. However, binaries and utilities with certain capabilities can still pose a threat. In this section, first, we will go through the basics of Linux capabilities, then we will take a look at how to leverage capabilities to attain root privileges.

AppArmor

AppArmor is a Mandatory Access Control (MAC) system that allows a system administrator to confine programs to a limited set of resources and capabilities. It binds access control attributes to programs rather than to users. In this section, first, we will take a look at how to create an AppArmor profile to confine services and restrict utilities for performing certain operations, then we will take a look at how a misconfiguration could be leveraged to escalate privileges.

Seccomp

Seccomp or Secure Computing mode is a feature of the Linux kernel which can act as a syscall filter and not a sandbox. It is used to restrict the system calls that can be made from a process. In this section, we will take a look at how to use seccomp to strengthen the security of a system.

What will you learn?

- Understanding advanced features such as Linux Capability, AppArmor and seccomp
- Leveraging Linux capability and escalating privileges to root
- Leveraging AppArmor profile and escalating privileges to root
- Restricting operations on docker containers by creating AppArmor and seccomp profiles

References:

1. Linux Capabilities (https://man7.org/linux/man-pages/man7/capabilities.7.html)
2. Seccomp (https://man7.org/linux/man-pages/man2/seccomp.2.html)
3. Seccomp Filtering (https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt)
4. AppArmor (https://wiki.ubuntu.com/AppArmor)

Labs:

Linux Capabilities:

- Linux Capabilities I
  - Objective: Learn about Linux Capabilities using an example of the ping command.
- Linux Capabilities II
  - Objective: Learn about Linux Capabilities using an example of tcpdump command.
- Linux Capabilities III
  - Objective: Learn about inherited and ambient Linux Capabilities sets using an example of a semi-privileged environment.
- Linux Capabilities IV
  - Objective: Learn how to cap the capabilities of a service.
- The Basics: CAP_DAC_READ_SEARCH
  - Objective: Abuse the CAP_DAC_READ_SEARCH capability on tar utility and get the password hash of the root user.
- The Basics: CAP_SYS_MODULE
  - Objective: Abuse the CAP_SYS_MODULE capability on kmod utility and escalate privileges to root user.

- The Basics: CAP_NET_RAW
  - Objective: Abuse the CAP_NET_RAW capability on tcpdump utility and sniff traffic from the interface.
- The Basics: CAP_DAC_OVERRIDE
  - Objective: Abuse the CAP_DAC_OVERRIDE capability on vim utility and escalate privileges to root user.
- The Basics: CAP_SYS_ADMIN
  - Objective: Abuse the CAP_SYS_ADMIN capability on python interpreter and escalate privileges to root user.
- The Basics: CAP_SYS_PTRACE
  - Objective: Abuse the CAP_SYS_PTRACE capability on python interpreter, perform process injection, and escalate privileges to root user.

AppArmor:

- AppArmor Profile
  - Objective: Create an AppArmor profile for a copy of the cat utility and restrict (and audit) it while it tries to read passwd file.
- AppArmor Profile II
  - Objective: Create an AppArmor profile for a copy of the cat utility. Use Easyprof to generate the default template and then modify the profile so the binary can only read passwd file.
- Confining Services with AppArmor
  - Objective: Create AppArmor profiles to confine the PHP webshell in such a way that the remote user can only execute "id" and "date" command. Also, restrict directory listing to the webroot directory.
- Confining Services with AppArmor II
  - Objective: Create AppArmor profiles to confine the FTP service in such a way that the "student" user is able to login, however, no user can get a shell using the backdoor.
- Confining Containers with AppArmor
  - Objective: Learn how to use AppArmor profiles with Docker for confining the containers.
- Privilege Escalation I (AppArmor)
  - Objective: Leverage the misconfiguration, Elevate access, and retrieve the flag.
- Confining Containers with AppArmor II
  - Objective: Learn how to apply AppArmor profiles from a user-friendly format using the bane tool.

Seccomp:

- Introduction to seccomp
  - Objective: Learn how to use seccomp profiles with Docker for blocking syscalls!
- Docker seccomp Profile
  - Objective: Learn how to use seccomp profiles with Docker by editing the default docker seccomp profile file. Enforce restrictions such as blocking commands and preventing processes from listening on a socket.