Linux Privilege Escalation Notes Cheat Sheet

**Helpful Commands**

**Hostname(hostname):**

Will return the hostname of the target machine.

**uname -a:**

Will print system information about the kernel used by the system.

**/etc/issue**:

Looking at this file usually gives us some information about the operating system.

**/proc/version:**

Gives information on the kernel version and additional data such as whether a compiler is installed.

**ps:**

Shows running processes.

**env:**

Shows environmental variables.

**Sudo -l:**

Shows all commands current user can run as root.

**Id:**

The id command will provide a general overview of the user’s privilege level and group memberships.

**/etc/passwd:**

Reading the /etc/passwd file can be an easy way to discover users on the system.

**history:**

Looking at earlier commands with the history command can give us some idea about the target system and, albeit rarely, have stored information such as passwords or usernames.

**find Command**

Searching the target system for important information and potential privilege escalation vectors can be fruitful. The built-in “find” command is useful and worth keeping in your arsenal.

Below are some useful examples for the “find” command.

**Find files:**

* find . -name flag1.txt: find the file named “flag1.txt” in the current directory
* find /home -name flag1.txt: find the file names “flag1.txt” in the /home directory
* find / -type d -name config: find the directory named config under “/”
* find / -type f -perm 0777: find files with the 777 permissions (files readable, writable, and executable by all users)
* find / -perm a=x: find executable files
* find /home -user frank: find all files for user “frank” under “/home”
* find / -mtime 10: find files that were modified in the last 10 days
* find / -atime 10: find files that were accessed in the last 10 day
* find / -cmin -60: find files changed within the last hour (60 minutes)
* find / -amin -60: find files accesses within the last hour (60 minutes)
* find / -size 50M: find files with a 50 MB size

This command can also be used with (+) and (-) signs to specify a file that is larger or smaller than the given size.