Linux Privilege Escalation

Enumeration:

MAKE SURE TO MANUALLY TEST EVERYTHING. IF IT SAYS YOU CANNOT WRITE TO SOMETHING, STILL TRY. YOU MIGHT BE MISINTERPRETING SOME RESULTS.

GitHub - C0nd4/OSCP-Priv-Esc: Mind maps / flow charts to help with privilege escalation on the OSCP.
first thing- check all the folders that are in root and default. in fact jsut go thru the entire directory on each machine

PSSpy or process spy lets you check for process being which beats checking crontab. can read all input by everyone without need for root
System Enumeration:- cat /proc/version
- uname -a
- lscpu
- cat /etc/issue
- ps aux
- hostname

User Enumeration:- whoami
- id
- sudo -l
- cat /etc/passwd
- cat /etc/shadow
- cat /etc/group
- history

Network Enumeration:- ifconfig
- ip a
- route
- arp -a
- ip neigh
- netstat -ano

Password Hunting:- grep --color=auto -rnw '/' -ie "PASSWORD=" --color=always 2> /dev/null
- locate password | more
- find / -name id_rsa 2> /dev/null \

Automatic tooling- LinPeas, LinEnum, LinuxExploitSuggester, Linuxprivchecker, always run all of them once you are done with manual enumeration, running all confirms possible escalation paths.

Kernel Exploits

https://github.com/lucyoa/kernel-exploits

Dirty Cow Kernel Eploit-
Classic Exploit- just run the script as needed.

Or run linux exploit suggester.
Works for any linux version before 2018, search dirtycow ninja

Passwords and File Permissions

Recover passwords using search methods, use a cheat sheet to find the search methods

If can edit a service file, edit and use systctl to restart it

SUDO

Use GTFObins to figure this out

SUID

Allows user to execute a file as a root user

cmd- find / -perm -u=s -type f 2>/dev/null

Shared object injection- use xtrace to track a suid file as it runs. This will tell you if it accesses any file on the system, if it does, and that file is missing, then that file can be overwritten with our own code and used for rce.

Libraries are mostly in C, so this rce would certainly be in C too.

nginxed-root.sh escalation ability- nginx log file can be replaced with a symlink to rce.

Replace log file and restart the server.

Enivronmental variables- if the path variable is set, and if a service is using it to execute a file stored in $PATH/ , then we can put a file with the same name in an earlier $PATH variable so that that gets run over the actual service. You can also add a PATH to the env variable in order to run a file stored in /tmp/

if the file acesses the full path use a function method tecnique to overwrrite the function of the path

Capabilities

cmd**-** getcap -r / 2>/dev/null

winpeas can detect this

via Cron

cmd**-** cat /etc/crontab

if something is running every few minutes, is a very likely candidate for exploitation.

if a file is being run using cron, then the file can be edited to run our own malicious code

wildcards- if a command is being run with the wildcard symbol (*), then we can write a file that is included in the wildcard criteria and can be used for CE.

NFS Root Squashing

Can be detected by WinPeas

folders on remote machines can be mounted on the local machine and be edited as root

Docker

gtfobins command for docker