Service Exploits

Graphical user interface, text, application

Description automatically generated

Using a misconfigured root access to mysql to escalate privileges.

Misconfigured File Permissions

First, This is how file permissions work and they can be viewed witth the “ls -als” command.

Graphical user interface, text, application

Description automatically generated with medium confidence

Misconfigured file permissions of the following files can allow a user to change the password and gain root access. The shadow and passwd files if readable or writeable can be viewed or overwritten to change or crack passwords.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Sudo Shell Escape Sequences

By going to the GTFO bins, it is possible to use sudo to escalate to a root shell

Graphical user interface, text, application

Description automatically generated

Sudo Environment Variables

Graphical user interface, text, application

Description automatically generated

Cronjobs – File Permissions

Graphical user interface, text, application, Teams

Description automatically generated

Cronjobs – PATH Environment Variable

Graphical user interface, text, application, Teams

Description automatically generated

Cronjobs – Wildcards

Graphical user interface, text, application

Description automatically generated

SUID / SGID Executables – Known Exploits

Graphical user interface, text, application, email

Description automatically generated

SUID /SGID Executables – Shared Object Injection

Graphical user interface, text, application

Description automatically generated

SUID / SGID Executables – Environment Variables

Graphical user interface, text, application, email

Description automatically generated

SUID / SGID Executables - Abusing Shell Features (#1)

Graphical user interface, text, application, email, Teams

Description automatically generated

SUID / SGID Executables - Abusing Shell Features (#2)

Graphical user interface, text, application

Description automatically generated

Password & Keys – History Files

Graphical user interface, text, application, email

Description automatically generated

Passwords & Keys - Config Files

Graphical user interface, text, application, email

Description automatically generated

Passwords & Keys - SSH Keys

Graphical user interface, text, application, email

Description automatically generated

NFS

The mount command should have the ip address of the target machine

Graphical user interface, text, application, email

Description automatically generated

Dirty c0w Privilege Escalation

Graphical user interface, application, Teams

Description automatically generated