

Pwning 1

Escalamiento de Privilegios

CC5325 - Taller de Hacking Competitivo

Pwning

— — —

pwn

verb [T] • informal

UK  /pəʊn/ US  /paʊn/



to defeat or take control of someone or something, usually in an internet video game:

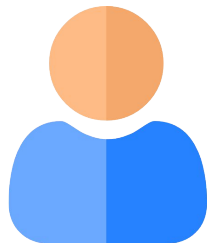
- *You were just pwned!*

<https://dictionary.cambridge.org/dictionary/english/pwn>

- **En CTF:** Tomar control de una máquina ajena a partir del aprovechamiento de vulnerabilidades en ella o los programas que corre.

Usuarios y Grupos en Linux

- Usuario
 - Identificado por un UID (/etc/passwd)
 - Pertenece a uno o más **grupos**.
 - Puede poseer **archivos y carpetas**.
 - Autoasignado a grupo con mismo nombre.



íconos de Freepik
en <https://flaticon.com>



- Grupo
 - Identificado por un GID (/etc/group)
 - Usuarios pertenecen a él
 - Puede poseer **archivos y carpetas**.

Permisos en Linux



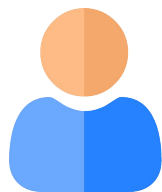
Archivos y carpetas tienen:

- **Owner**
- **Group**



Permisos en Archivos y Carpetas

Se pueden establecer permisos distintos para



Owner



Group



Other

Los permisos existentes para cada grupo son:

- **R:** Leer archivo o entrar a carpeta
- **W:** Editar archivo o crear nuevos archivos en carpeta
- **X:** Ejecutar archivo o listar archivos dentro de carpeta

Permisos Adicionales

- **SETUID:**



En archivos: El usuario con permisos de ejecución que corra este programa lo hará con los permisos del **owner** del archivo.

- **SETGID:**



En Archivos: El usuario con permisos de ejecución que corra este programa lo hará con los permisos del **grupo** del archivo.




- **Sticky:**



En Carpetas: Los archivos dentro del directorio solo pueden ser eliminados y editados por el owner del directorio o del archivo.

Permisos como

íconos de Freepik
en <https://flaticon.com>

! extra			user			group			other			
SU	SG	ST	R	W	X	R	W	X	R	W	X	
 0	0	1	1	1	1	0	0	0	0	0	0	1700
 0	0	0	1	0	0	1	0	0	1	0	0	0444
 1	0	0	1	1	1	1	0	1	1	0	1	7755

Permisos totales para owner + Sticky Bit

Cualquiera puede leer el archivo, pero no escribir o ejecutar

Cualquiera puede leer y ejecutar el archivo. Al ejecutarlo se ejecuta como su **owner**

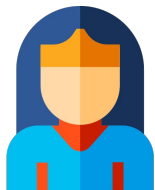
Cambiar permisos, owners y groups:

- **chown** (superusuario)
- **chgrp** (superusuario)
- **chmod** (owner o group)

Editar grupos de un usuario:

- **gpasswd** (superusuario)

Superusuario (root) y Sudoers



- root

- UID=0
- Permisos completos en todo el sistema por defecto
- Puede leer o escribir cualquier archivo.
- Puede cambiar **owners** y **groups**
- Puede cambiar **permisos** de cualquier archivo

- sudoers

- pertenecen al grupo **sudo** o **wheel** (depende la distro)
- pueden ejecutar comandos como superusuario con **sudo <cmd>**
- Permisos se definen en **/etc/sudoers**

Run



Run as Administrator

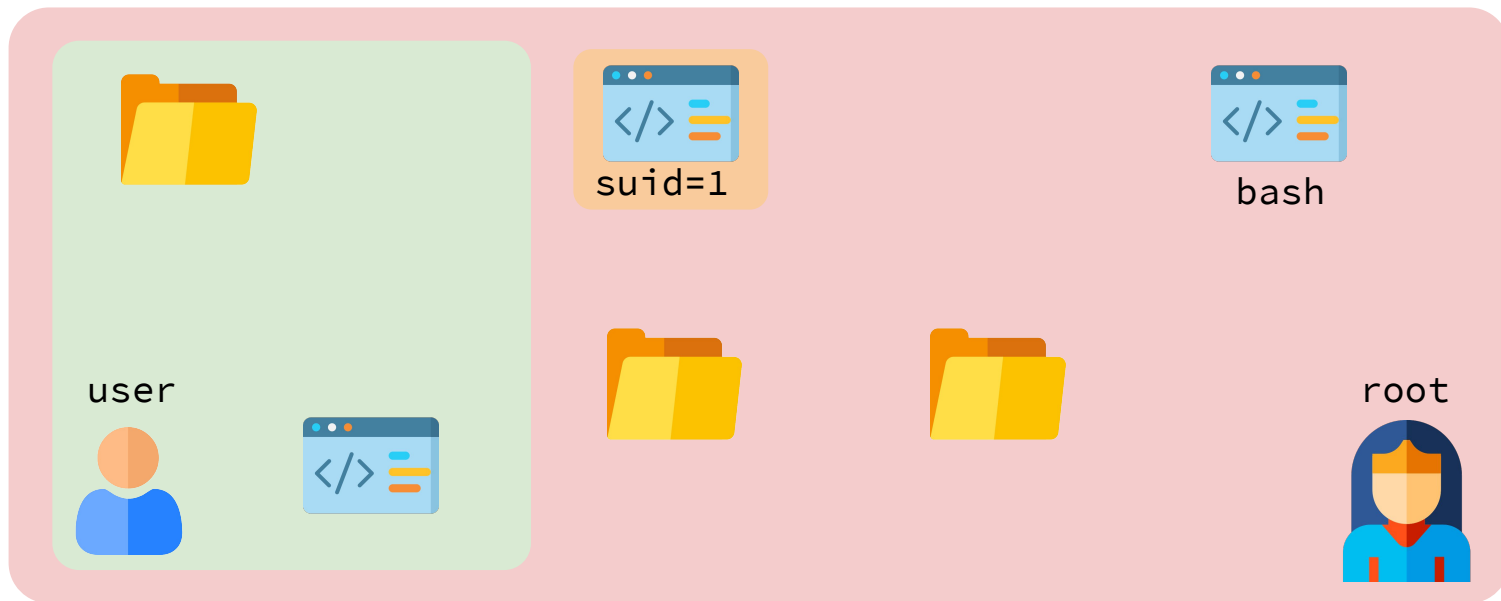


Archivos y carpetas ocultas

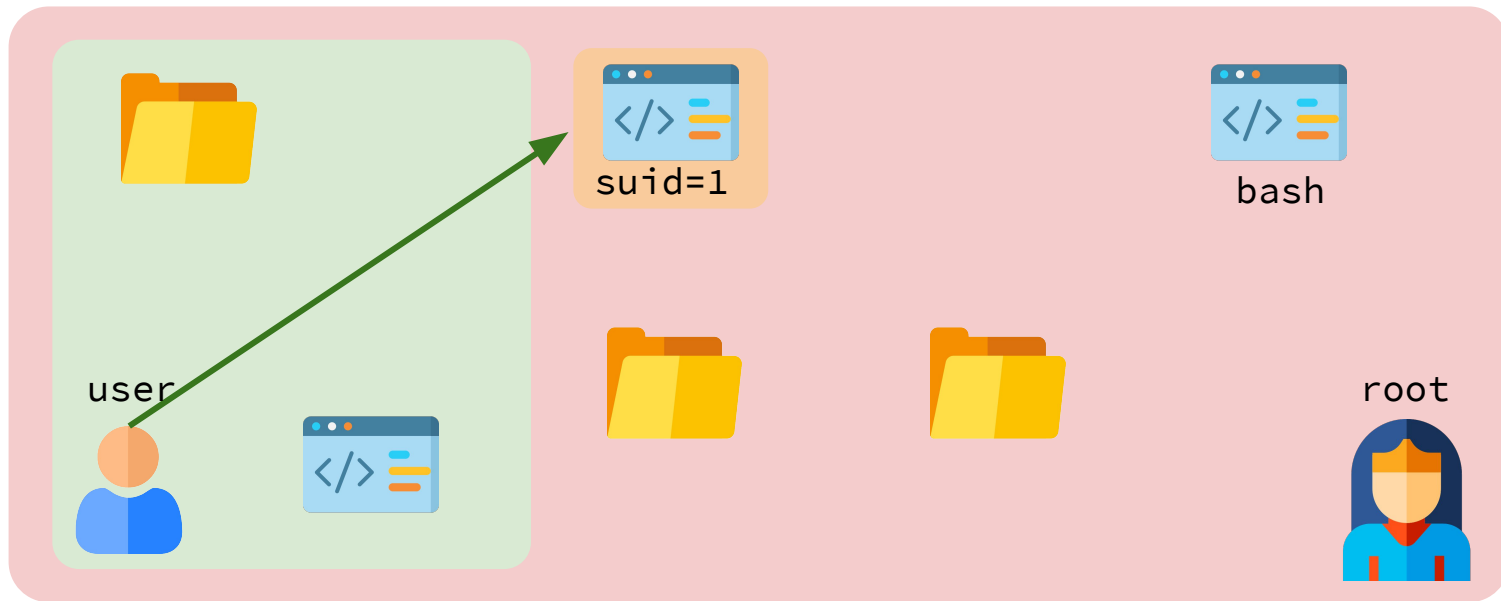
- Su nombre parte con punto (.)
- Al hacer **ls** no se ven
- Al hacer **ls -a** sí se ven
- ¿Es más seguro?
 - No, solo no se ven por defecto.



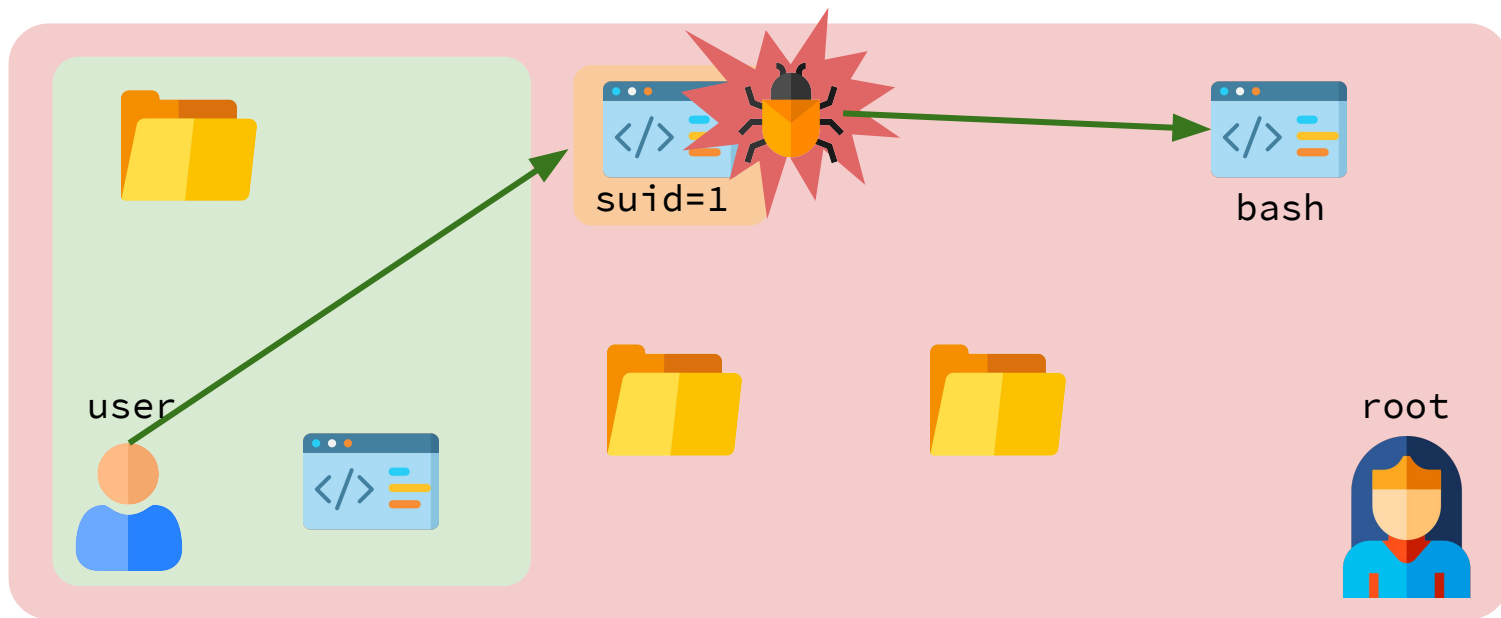
Escalamiento de privilegios



Escalamiento de privilegios



Escalamiento de privilegios

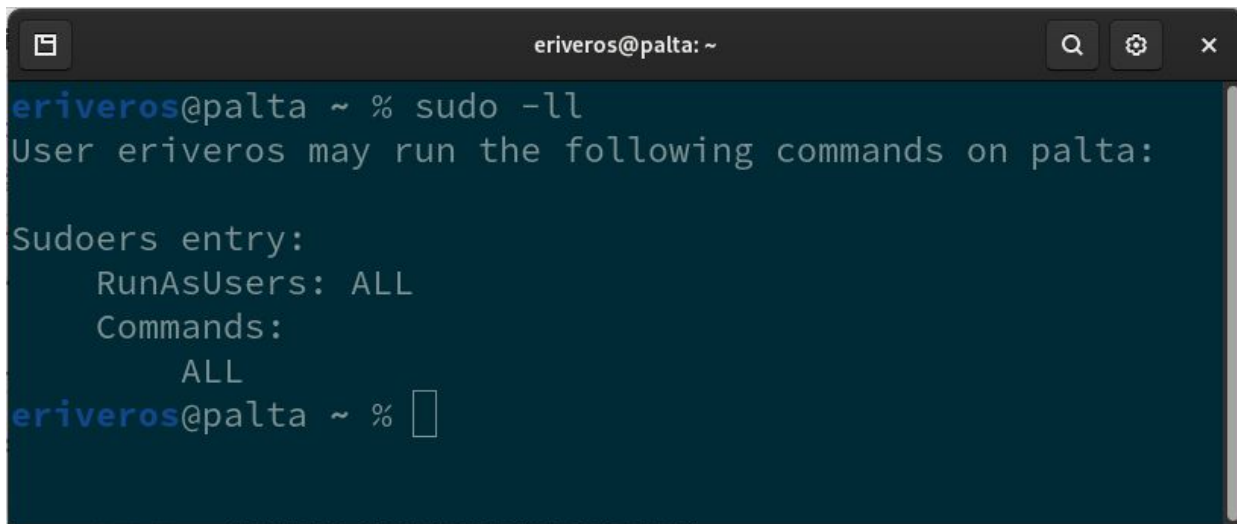


Algunas Convenciones en CTF con EP

- En general buscas obtener acceso a **root** o a un usuario con permisos elevados.
- A veces lo anterior no es necesario, y basta con leer un archivo restringido a **root** u otro usuario con permisos elevados.
- Se parte buscando en **/root/** (o **/home/<usuario_con_privilegios>**)
- Cada competidor trabaja en una carpeta temporal
- Archivo **.bash_history** deshabilitado para evitar filtración entre equipos jugando simultáneamente
- Si hay que bajar archivos, se suele trabajar en carpetas temporales (**mktemp -d**).

Algunas estrategias genéricas

1. Revisar Privilegios por defecto del usuario inicial



```
eriveros@palta: ~ % sudo -ll
User eriveros may run the following commands on palta:

Sudoers entry:
    RunAsUsers: ALL
    Commands:
        ALL
eriveros@palta ~ %
```

Algunas estrategias genéricas

2. Revisar owners, groups y permisos (incluyendo setuid/setgid) de carpetas y archivos sensibles

- Buscar recursivamente por permiso, owner o group
 - `find / -perm -4000`
 - `find / -user root`
 - `find / -group root`
- Revisar `/etc/shadow`
 - Si es legible, puedes intentar crackear la contraseña con **john the ripper**

Algunas estrategias genéricas

3. Revisar procesos corriendo de forma periódica

- Programas corriendo actualmente:
 - `ps aux`
 - `top`
- Programas agendados para correr de forma periódica
 - `cat /etc/cron.d/*`

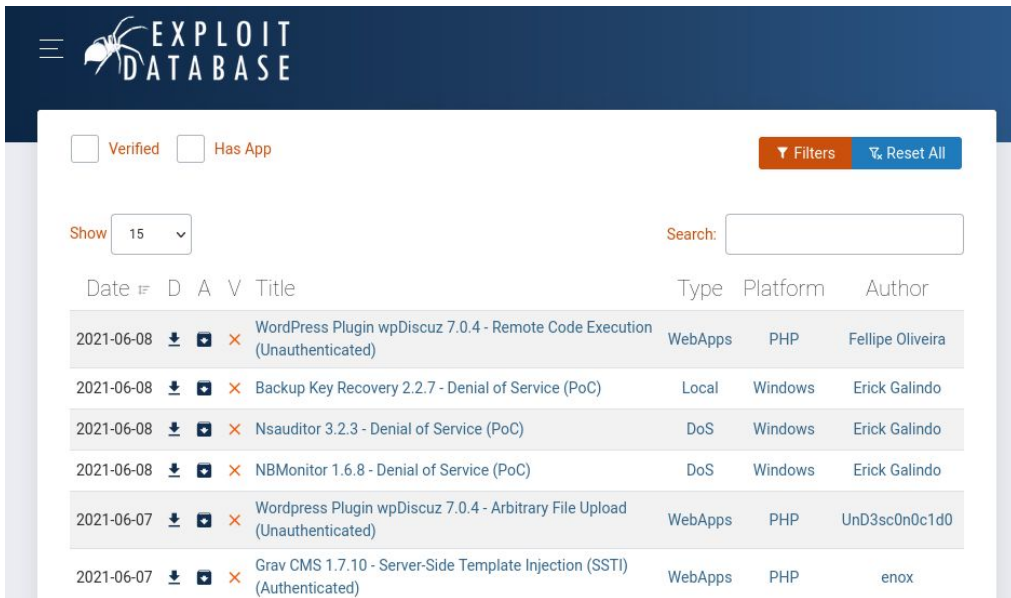
Algunas estrategias genéricas

4. Revisar archivos con contraseñas

- Similar al caso de forense:
 - buscar en /etc/
 - buscar en / palabra "password" o similar.

Algunas estrategias genéricas

5. Revisar exploits específicos para OS o servicios



The screenshot shows the Exploit Database interface. At the top left is the logo with a spider icon and the text "EXPLOIT DATABASE". Below the logo are filter checkboxes for "Verified" and "Has App", and buttons for "Filters" and "Reset All". A "Show" dropdown is set to "15". A search bar is present. The main content is a table of exploits with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2021-06-08				WordPress Plugin wpDiscuz 7.0.4 - Remote Code Execution (Unauthenticated)	WebApps	PHP	Fellipe Oliveira
2021-06-08				Backup Key Recovery 2.2.7 - Denial of Service (PoC)	Local	Windows	Erick Galindo
2021-06-08				Nsauditor 3.2.3 - Denial of Service (PoC)	DoS	Windows	Erick Galindo
2021-06-08				NBMonitor 1.6.8 - Denial of Service (PoC)	DoS	Windows	Erick Galindo
2021-06-07				Wordpress Plugin wpDiscuz 7.0.4 - Arbitrary File Upload (Unauthenticated)	WebApps	PHP	UnD3sc0n0c1d0
2021-06-07				Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) (Authenticated)	WebApps	PHP	enox

- <https://exploit-db.com>
- Buscar por software + versión un CVE.

Bypasses con programas conocidos

— — —

- Programa inofensivo con permisos suid a veces puede ejecutar un proceso arbitrario (como /bin/sh)
 - **awk**
 - **find**
 - **vim**
 - **less**
 - **more**

GTFOBins 4,757

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate [functions](#) of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).



[Shell](#) [Command](#) [Reverse shell](#) [Non-interactive reverse shell](#) [Bind shell](#) [Non-interactive bind shell](#)
[File upload](#) [File download](#) [File write](#) [File read](#) [Library load](#) [SUID](#) [Sudo](#) [Capabilities](#) [Limited SUID](#)

Search among 266 binaries: <binary> +<function> ...

Binary

[apt-get](#)
[apt](#)
[ar](#)
[aria2c](#)
[arp](#)
[ash](#)
[at](#)
[atobm](#)
[awk](#)

Functions

[Shell](#) [Sudo](#)
[Shell](#) [Sudo](#)
[File read](#) [SUID](#) [Sudo](#)
[Command](#) [Sudo](#) [Limited SUID](#)
[File read](#) [SUID](#) [Sudo](#)
[Shell](#) [File write](#) [SUID](#) [Sudo](#)
[Shell](#) [Command](#) [Sudo](#)
[File read](#) [SUID](#) [Sudo](#)
[Shell](#) [Non-interactive reverse shell](#) [Non-interactive bind shell](#) [File write](#) [File read](#) [SUID](#)

Scripts de Enumeración Automática

Scripts que automatizan la detección de exploits o bypasses:

- [Linux Exploit Suggester](#)
- [LinEnum](#)
- [Unix-Privesc-Check](#)
- [LinPrivchecker.py](#)
- [Más material de Privilege Escalation](#) en CTFs