

DEEPSEC ACADEMY

DeepSec Linux Hacking Course



DEEPSEC **ACADEMY**

Instructor

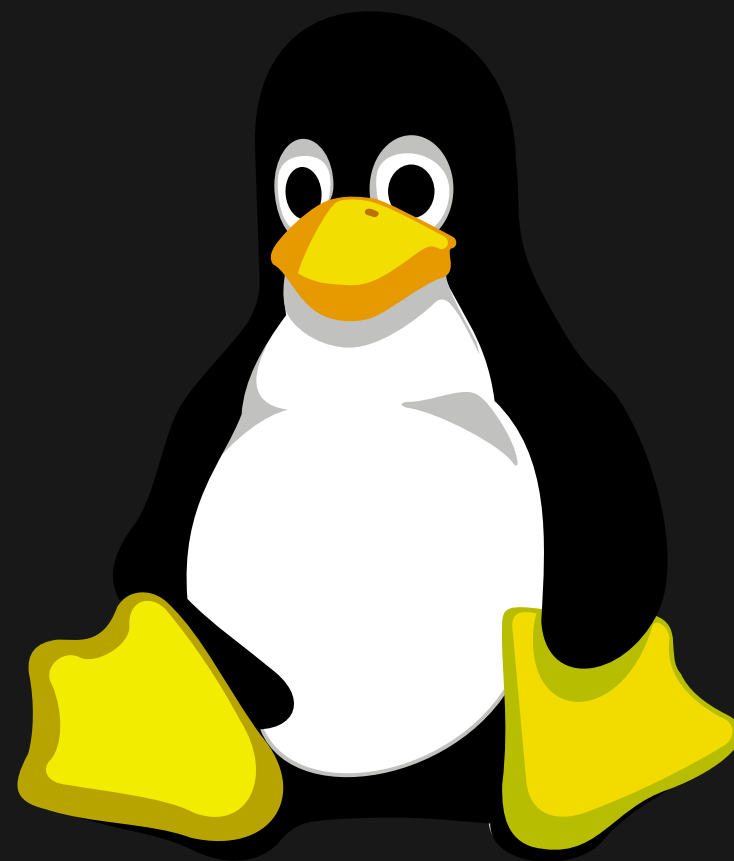


Diego Condori

Objetivos del curso

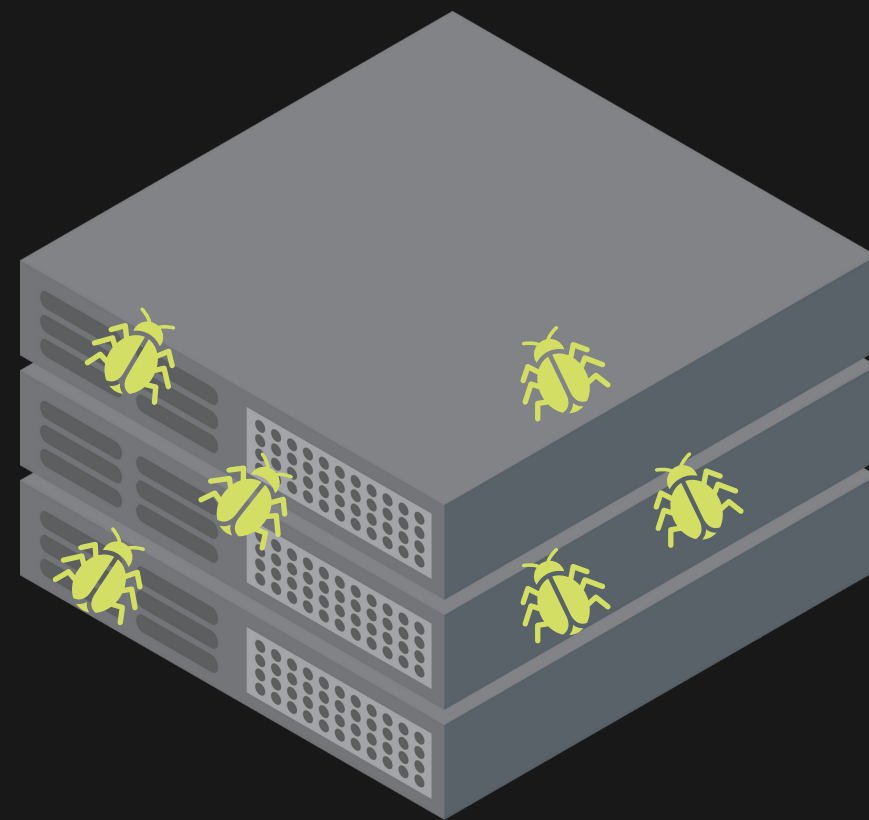
DEEPSEC ACADEMY

Manejo de Sistemas Linux



DEEPSEC **ACADEMY**

Dominio De Programacion Tecnicas de Pentesting



Reglamento



Puntualidad

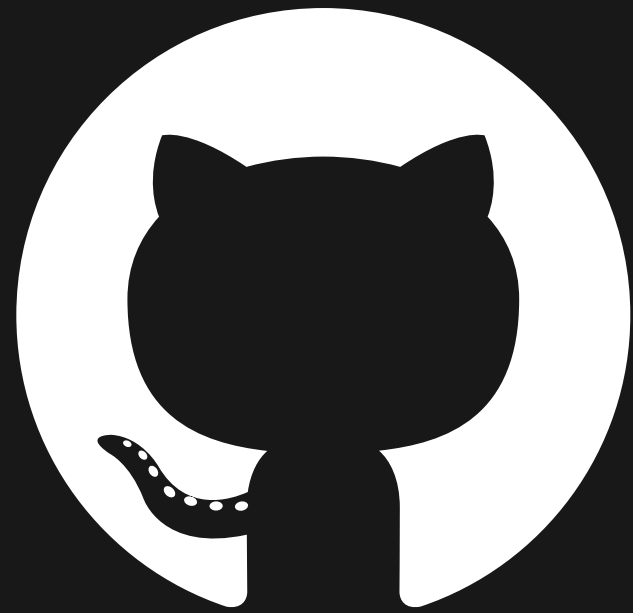


**Microfono
Apagado**



Respeto

Material de Trabajo



Git-Hub

Todos los scripts los
almacenaremos en un
repositorio



Material de Trabajo

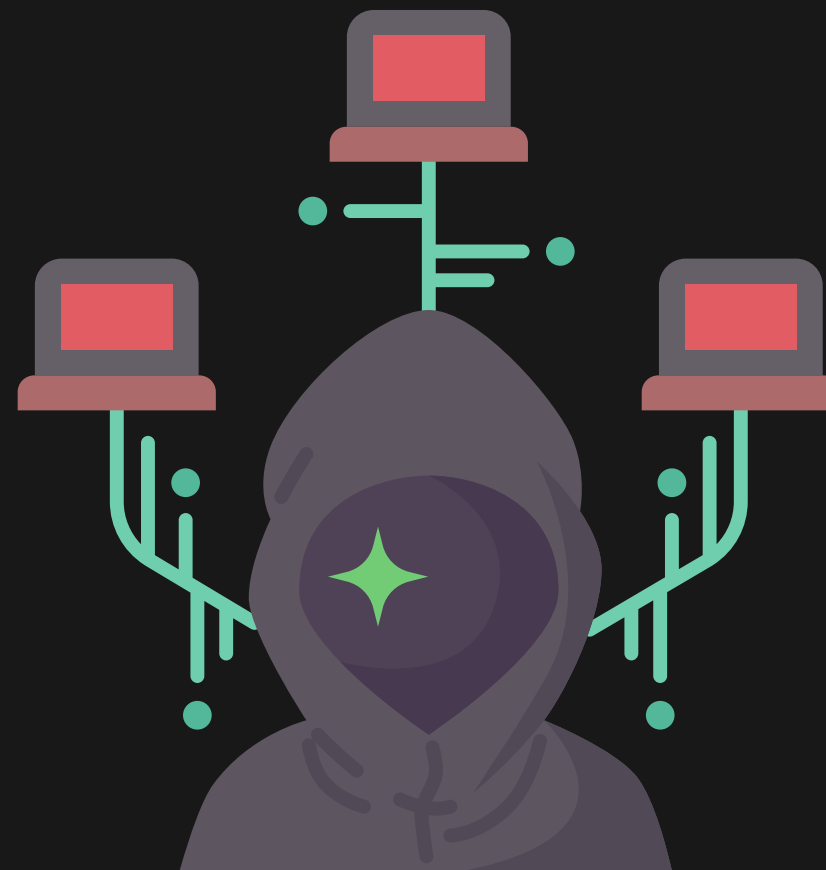


Telegram

Las clases se subiran al
grupo de telegram

¿Porque Linux Para el Pentesting?

- La instalacion de herramientas es mucho mas sencilla y rapida.
- Las herramientas disponibles para Linux es inmensa.
- Automatizacion de procesos mucho mas sencilla gracias a la programacion en SHELL



Ramas de la Seguridad Informatica

- Seguridad de Hardware: Proteccion de dispositivos, redes, apps y programas de amenazas exteriores.
- Seguridad de Software: Salvaguardia de los sistemas ante ataques maliciosos.
- Seguridad de Red: Proteccion de los datos en la red.



FASES DEL PENTESTING

Fases de un proyecto de Pentesting



¿Que es Unix?

Características de Unix

- Originalmente desarrollado por AT&T, Bell Labs del cual derivan los demas sistemas operativos
- La certificación no es gratuita y los desarrolladores que desean incluir el nombre Unix en su sistema operativo deberán pagar una comisión.



¿Que es Unix y Linux?

Linux se basa en Unix pero solamente en espíritu y funcionalidad, no en su código. Como sistema operativo, Linux nació de la unión de dos proyectos basados en Unix, The GNU Project, iniciado por Richard Stallman en 1983, y el Kernel de Linux, escrito por Linus Torvalds en 1991. El objetivo del proyecto GNU fue construir un sistema operativo similar a Unix pero sin su código, para que así pudiese ser distribuido libremente. Como el Kernel Linux estaba incompleto, GNU Project aceptó el desafío y lo desarrolló al completo, surgiendo el sistema operativo GNU/Linux.



¿Que es Linux?

Características de Linux

- Cuando nos referimos al término Linux de manera estricta, solo nos estamos refiriendo al núcleo (kernel)
- Como la mayoría de las aplicaciones las desarrolla GNU Project, el nombre completo del sistema operativo es GNU/Linux.



Diferencias Unix vs Linux

- Linux es gratuito y libre.
- El sistema Unix original no lo es, aunque algunas de sus distribuciones lo son.
- Linux es un clon del sistema Unix original, aunque no contiene su código.
- Linux es solo el núcleo (kernel) del sistema, mientras que Unix es un sistema operativo completo.
- Linux fue desarrollado para ser ejecutado en PCs, mientras que Unix fue desarrollo principalmente para grandes estaciones de trabajo y servidores. Actualmente, Linux admite más plataformas que Unix.
- Linux soporta más tipos de sistemas de archivos que Unix.

Linux Basics (ls)

```
~/tmp ls
spooof.py
```

```
~/tmp ls -a
.  ..  spoof.py
```

```
diegojoel301@diegojoel301:~/tmp$ ls -l
```

```
total 4
```

Enlaces

-rw-rw-r--	1	diegojoel301	diegojoel301	1610	dic 28 16:00	spooof.py
------------	---	--------------	--------------	------	--------------	-----------

Owner Group All

Group

Owner

Size

Date

File

Linux Basics (ls)

Parametro	Descripcion
-a	Muestra ficheros ocultos (que empiezan por .)
-l	Muestra el formato largo, añadiendo al nombre datos sobre permisos, ultimo acceso y propietarios
-R	ls accede a todos los directorios por debajo del actual listando su contenido
-t	Muestra los ficheros en orden cronologico
-r	Invierte el orden en el que aparece el listado

Linux Basics (cd)

cd

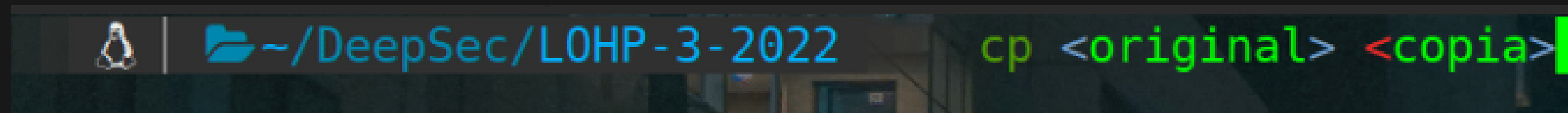
Este comando se utiliza para navegar por la estructura de directorios. Existen dos formas de llegar a un directorio cualquiera a traves de este comando: utilizando rutas absolutas desde el directorio raiz (/) y utilizando rutas absolutas, desde el directorio actual



Linux Basics (cp)

cp

Nos permite, entre muchas otras cosas, copiar archivos, aunque no directorios(a menos que se haga uso del parametro -r). Para utilizarlo de manera basica:

A screenshot of a Linux terminal window. The title bar shows a Tux penguin icon and the path ~/DeepSec/LOHP-3-2022. The terminal prompt is a blue folder icon followed by the path. The command 'cp <original> <copia>' is entered in green text, with a green cursor at the end.

```
~/DeepSec/LOHP-3-2022$ cp <original> <copia>
```

Linux Basics (mv)

mv

Nos permite mover o renombrar archivos. El uso es similar al cp.

A screenshot of a Linux terminal window. The title bar at the top reads "Terminal". The terminal shows a prompt character followed by the directory path "~/DeepSec/LOHP-3-2022". To the right of the path, the command "mv" is shown in green, followed by two arguments in angle brackets: "<original>" in green and "<copia>" in red. The terminal background is dark with a faint grid pattern.

```
Terminal  
~ | ~/DeepSec/LOHP-3-2022 mv <original> <copia>
```

Linux Basics (rm/rmdir)

rm y rmdir

Como los anteriores comandos, rm nos permite borrar ficheros y carpetas con el parametro -r. De forma similar, rmdir nos permite borrar directorios, aunque previamente tienen que estar vacios.

```
> rm <nombre_fichero>  
> rmdir <nombre_directorio>  
> rm -r <nombre_directorio>
```

Linux Basics (whoami)

whoami

Permite conocer que usuario se esta utilizando en un momento dado, ya que diferentes usuarios pueden tener diferentes permisos de acceso. Su mayor utilidad proviene de la frecuencia con que el administrador cambia de usuario, a veces en funcion de la tarea, generando cierta confusion sobre que usuario esta realizando determinada accion (por ejemplo: guardar un fichero).

```
> whoami  
parrot
```

Linux Basics (id)

id

Facilita datos sobre el usuario que se esta utilizando y los grupos de usuarios a los que pertenece

```
> id  
uid=1000(parrot) gid=1001(parrot) grupos=  
,120(bluetooth),131(lpadmin),137(sca
```

Linux Basics (id)

uname

Permite conocer datos generales sobre el sistema en el que se esta. Sin parametros muestra el tipo de kernel. Con el parametro -a muestra la version del kernel, el nombre del equipo y diversos datos sobre el kernel y el procesador.

```
> uname -a  
Linux diegomachine 5.16.0-12parrot1-amd64 #1 SMP PREEMPT Debian 5.16.12-2parrot1 (2022-03-11) x86_64 GNU/Linux
```


DEEPSEC ACADEMY

¡Muchas gracias!