

# ROOTKITS

The background is a solid red color with various white and orange line-art icons. On the left, there are vertical circuit lines with circular nodes. In the center, there is a large, faint shield with an eye in the middle. To the right of the shield is a computer monitor. Below the monitor, there is a magnifying glass focusing on a small bug icon. To the right of the magnifying glass are two server rack units. There are also some faint plus signs and a cloud icon in the upper part of the background.

Rodrigo Francisco

Beatriz Sánchez

# Temas:

1- ¿Qué es un Rootkit?

2 - Uso de un rootkit

4- Clasificación de los rootkits

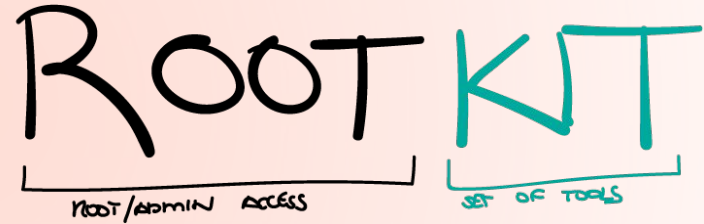
Modo usuario (Anillo 3 de seguridad)

Modo kernel (Anillo 0 de seguridad)

5. Funcionamiento de un rootkit

5- Detección de un rootkit

6. Eliminación de un rootkit



ROOTKIT

ROOT/ADMIN ACCESS

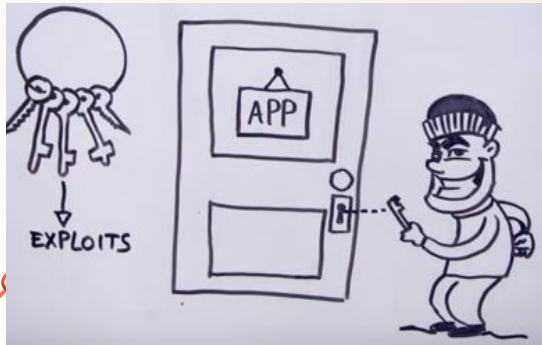
SET OF TOOLS

# Malware

También llamado “software de actividades ilegales es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya” , además se refiere a todo aquel software cuyo objetivo está en corromper la estructura del sistema operativo , así como recolectar información personal de usuarios de manera ilegítima, hasta el empleo de recursos de forma remota



# Exploit



Programas que son creados para explotar específicamente una vulnerabilidad, lo cual no es más que tratar de aprovechar un error en el diseño o programación de un sistema o aplicación. Cuando logra sacar provecho de un error, quien utiliza el *exploit* busca obtener, por ejemplo, privilegios de administrador sobre el sistema operativo y de esta forma poder controlarlo.

# Un rootkit **no es** un malware



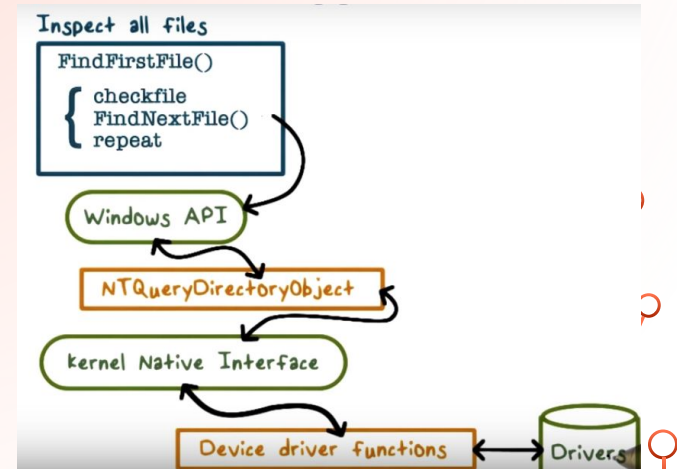
El enfoque de muchos rootkits recientes ha sido cooperar con malware con el fin de ocultar la funcionalidad de control y comando remoto del malware. El malware requiere acceso remoto a las estaciones de trabajo infectadas, y los rootkits proporcionan el sigilo para permitir que el malware se ejecute sin ser detectado, es esto el cómo se relaciona un rootkit con el malware.





# ¿Qué es un rootkit?

Un **rootkit** es un programa o un conjunto de programas que adquieren y mantienen acceso privilegiado al sistema operativo mientras que activamente están ocultando su presencia. Hoy en día los rootkits se asocian con malwares (para cualquier sistema operativo) que encubren su existencia y sus acciones de los usuarios y de otros procesos el sistema.



# Un rootkit puede ...

- **Ejecutarse.** Un rootkit desea poder ejecutarse sin restricciones en un equipo de destino.  
Los rootkits aprovechan las vulnerabilidades de estos mecanismos o utilizan los ataques de ingeniería social para instalarse, de modo que no tengan restricciones sobre lo que pueden hacer.
- **Esconderse.** El rootkit debe permanecer invisible a otras aplicaciones para evitar ser desinstalado por software de seguridad.
- **Actuar.** Un autor de rootkit desea obtener algo de la computadora comprometida, como robar contraseñas o ancho de banda de la red, o instalar otro software malicioso.

# ¿En dónde trabajan los rootkits?

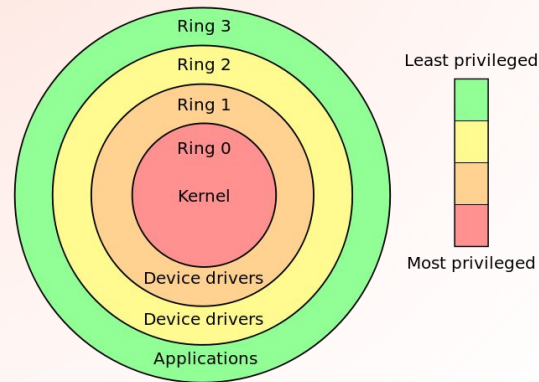
En general un sistema operativo cuenta con dos áreas de memoria bien diferenciada: el espacio de usuario y el espacio de kernel. En una arquitectura típica, estos espacios se ubican en "anillos de seguridad" con nivel de privilegios distintos.

Espacio de usuario

Anillo 3: Espacio de usuario,  
privilegios mínimos. Ejecución  
de aplicaciones

Espacio de kernel

Anillo 0: Espacio Kernel.  
Acceso Total a los recursos





# Rootkits en espacio de usuario

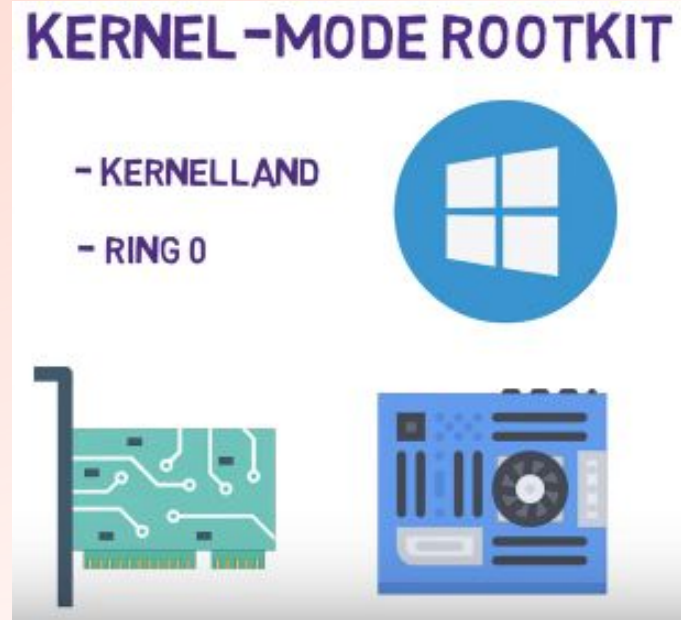
Conjunto de colección de programas y código capaz de no ser detectado y que reside en un espacio de aplicación no perteneciente al kernel, permitiendo la presencia constante en un ordenador o sistema de información



# Rootkits en espacio de kernel

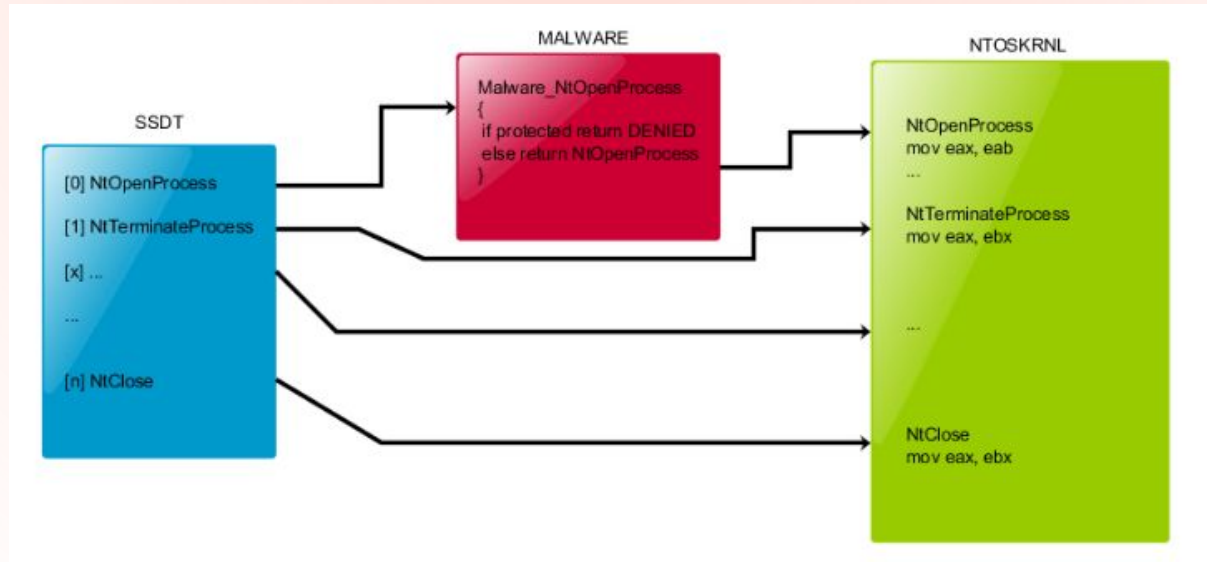
Los rootkits de modo kernel son simplemente binarios maliciosos que se ejecutan en el nivel de privilegio más alto disponible en la CPU que es implementado por el sistema operativo (es decir, Ring 0).

La mayoría de los rootkits del modo kernel tienen algunos atributos definitorios que tienden a dificultar su captura y eliminación.



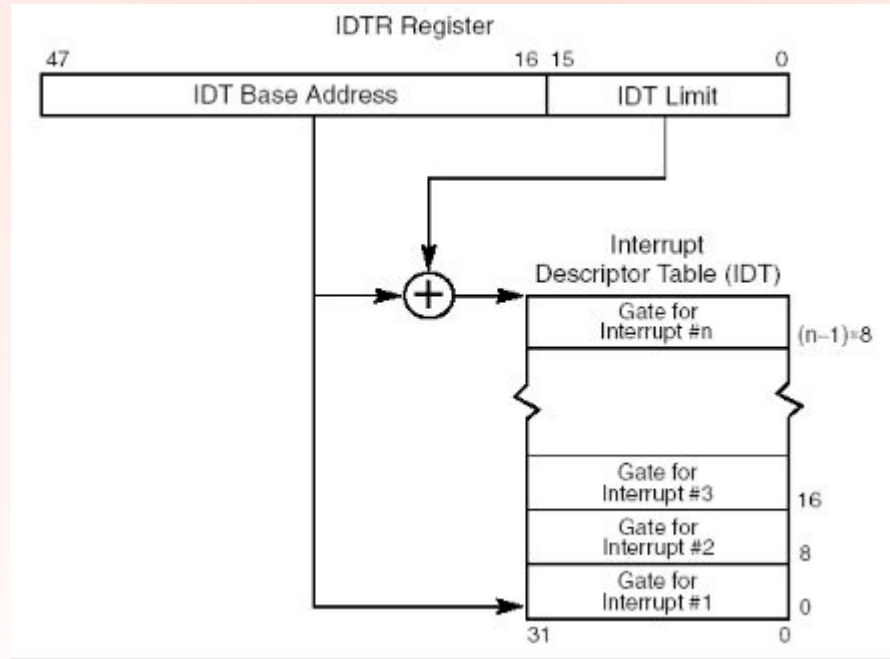
# Técnicas específicas que utilizan los rootkits EN MODO KERNEL

## SSDT HOOKING (Enganche a Tabla de despacho de servicio del sistema)



# Técnicas específicas que utilizan los rootkits EN MODO KERNEL

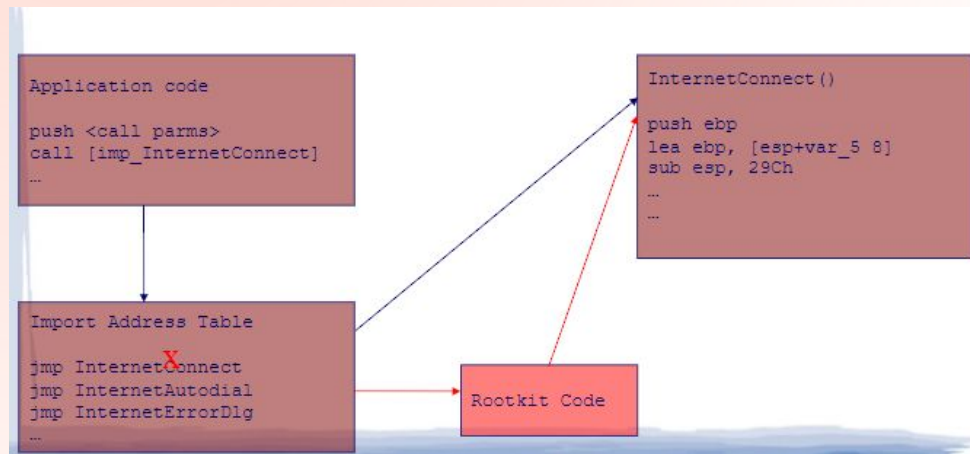
## IDT HOOKING (Enganche a Tabla de envío de interrupciones)



# Técnicas específicas que utilizan los rootkits EN MODO KERNEL Y MODO USUARIO

## IAT HOOKING (Enganche a Tabla de direcciones importantes)

El enganche no solo ocurre en el modo kernel. El enganche en modo usuario se produce con frecuencia y es muy fácil de implementar. Uno de los ganchos de usuario más prominentes es el gancho IAT.

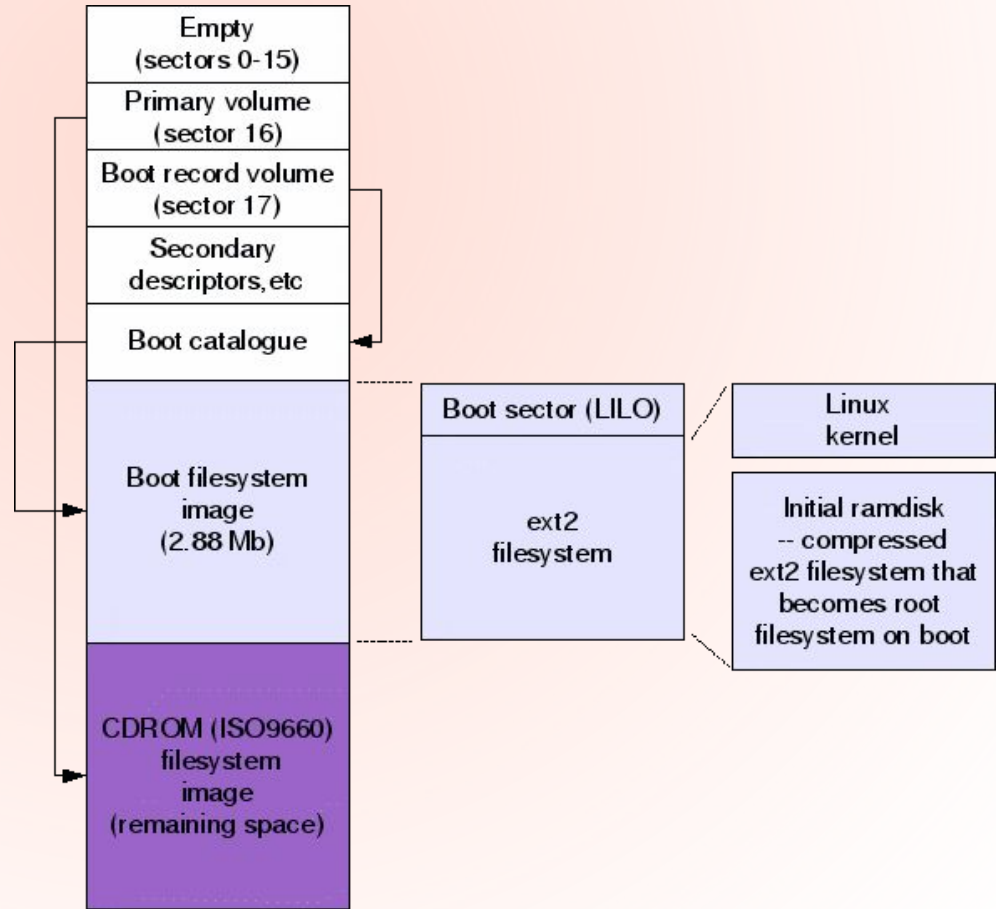




# Bootkits

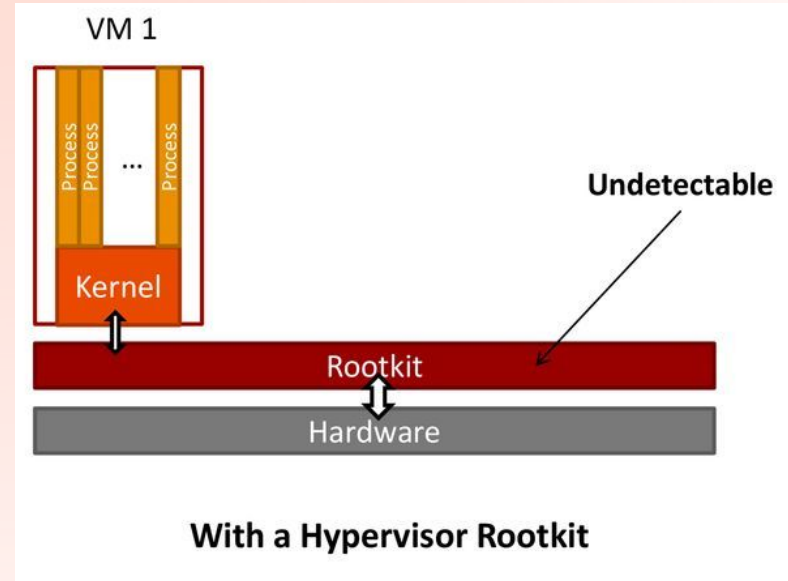
Buscan afectar al Master Boot Record, un pequeño programa que se ejecuta cuando una computadora arranca.

Este tipo de rootkits puede persistir pese al reemplazo del sistema operativo de la computadora e inclusive después del reemplazo del disco duro.

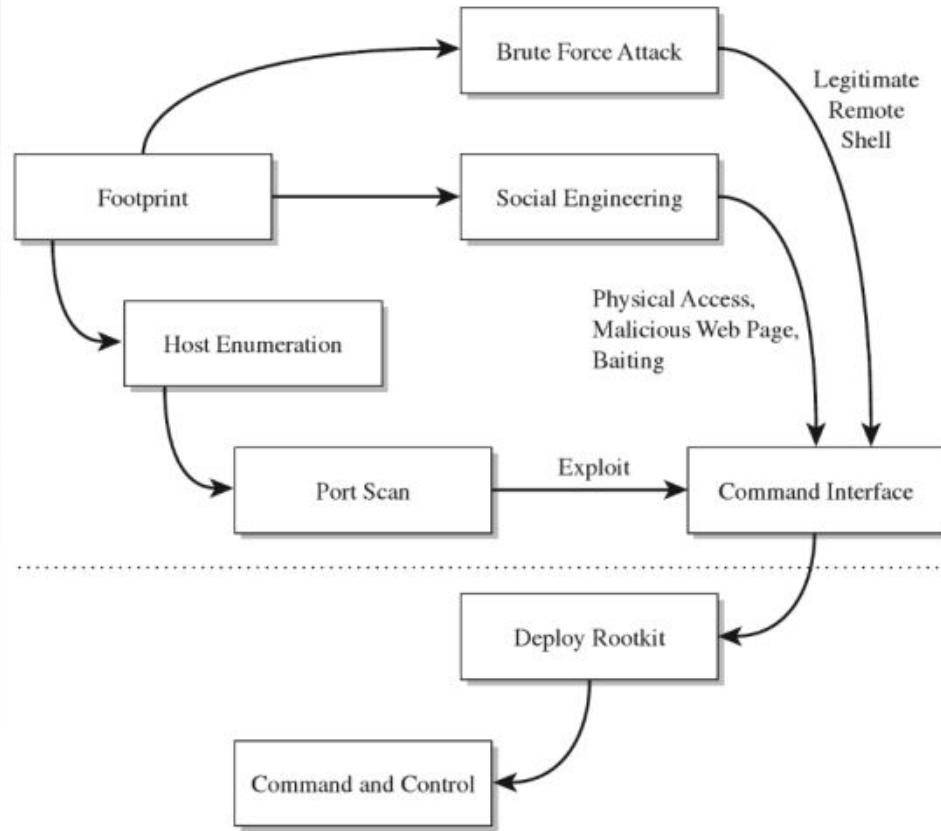


# Virtual Kits

El rootkit virtual contiene una funcionalidad para detectar y, opcionalmente, escapar del entorno virtual (si está implementado dentro de una de las máquinas virtuales invitadas), así como también secuestrar completamente el sistema operativo nativo (host) instalando un hipervisor malicioso debajo.



# El ciclo de ataque

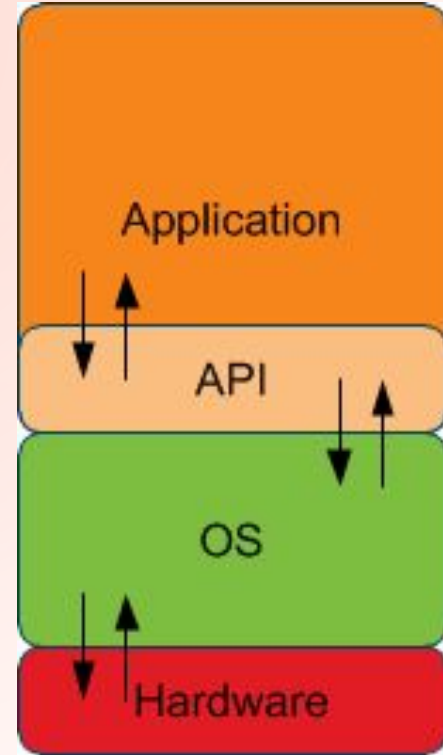


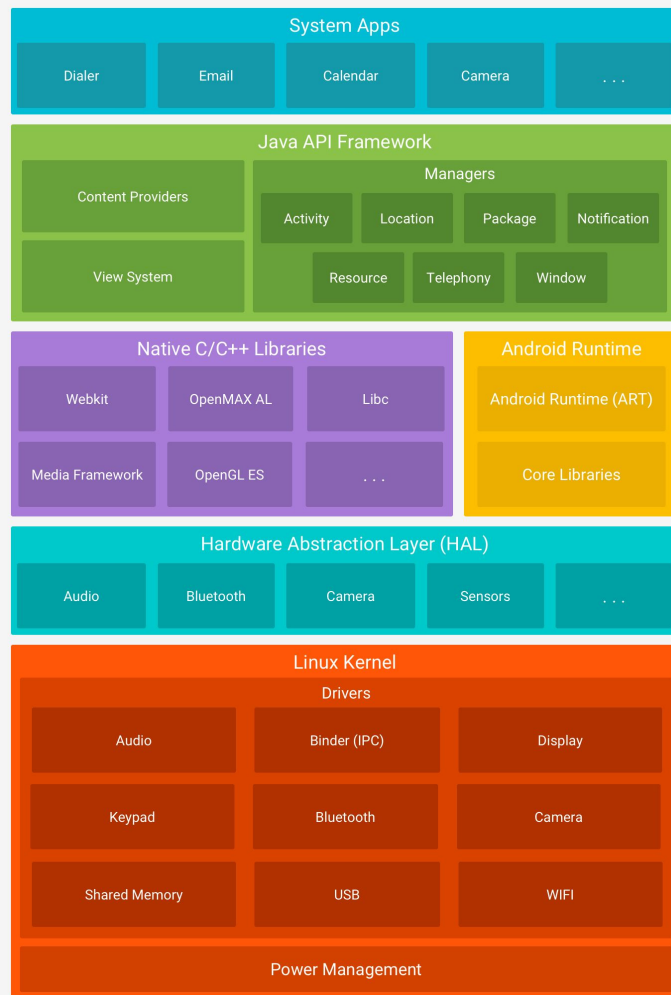
Antes de que un atacante pueda instalar un rootkit tiene que tener acceso al sistema a vulnerar para lo cual existen varias maneras.

Luego de ingresar al sistema debe buscar escalar sus privilegios de usuario y finalmente dejar una vía para accesos posteriores.

# La API del sistema

Generalmente los sistemas operativos proporcionan una interfaz de programación de aplicaciones (API por sus siglas en inglés) que permite a los programas del usuario hacer llamadas al sistema.

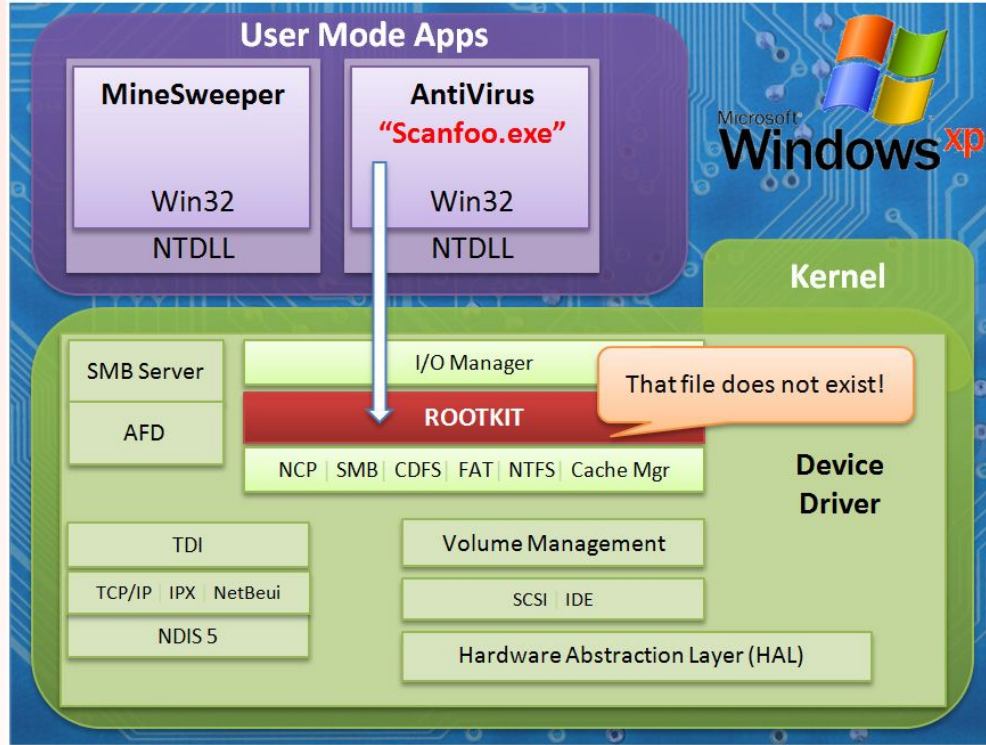




En la imagen observamos la arquitectura de la plataforma android.



# Funcionamiento de un rootkit



# Funcionamiento de un rootkit

En modo usuario y en modo kernel el rootkit funciona implementando un mecanismo llamado “hooking”. Los rootkits secuestran la API del sistema operativo y están atentos a cualquier pregunta que una aplicación le pueda hacer que pueda ser incriminatoria.

# Funcionamiento de un rootkit

```
rho@maxwell:~/datafiles/MyProjects/projects-compilation/linux_rt$ ls
mi_ls.c  mi_ls.so
rho@maxwell:~/datafiles/MyProjects/projects-compilation/linux_rt$ cat mi_ls.c
#include <stdio.h>
#include <stdlib.h>

int strlen(const char *c){
    puts("No ha ficheros en este directorio \n");
    exit(1);
}
rho@maxwell:~/datafiles/MyProjects/projects-compilation/linux_rt$ export LD_PRE
LOAD=$PWD/mi_ls.so
rho@maxwell:~/datafiles/MyProjects/projects-compilation/linux_rt$ ls
No ha ficheros en este directorio

rho@maxwell:~/datafiles/MyProjects/projects-compilation/linux_rt$
```

# Detección de un rootkit

Una vez que el instalador de rootkit ha podido hacer su trabajo, las cosas se complican y los métodos de detección son más complejos, sin embargo, los métodos existen y se aplican dependiendo al tipo de enganche (hooking) con el que trabajó el rootkit.

Algunos de los hooking que pueden ser detectados son:

- ENGANCHES SSDT ( **tabla de descriptor de servicio del sistema**)
- ENGANCHES IDT
- ENGANCHES DE CONEXIÓN EN LÍNEA
- ENGANCHES IAT
- ENGANCHES DKOM (**manipulación directa de objetos del kernel**)

# Eliminación de un rootkit

La eliminación de rootkits puede ser difícil, especialmente para los rootkits que se han incorporado a los kernels del sistema operativo, al firmware o en los sectores de arranque de dispositivos de almacenamiento. Si bien algunos programas anti rootkit pueden detectar y eliminar algunos rootkits, este tipo de malware puede ser difícil de eliminar por completo.



# FUENTES DE CONSULTA

Fuentes de consulta:

Sean Bodmer, Aaron LeMasters, Michael A. Davis, Christopher C. Elisan. (2016). Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition. New York: McGraw-Hill Education

Reveren Bill Blunden. (2009). The Rootkit Arsenal: Escape and Evasion. Burlington: Jones&Barlett learning

Kernel mood rootkits de <https://www.adlice.com/kernelmode-rootkits-part-1-ssdt-hooks/>

La amenaza de los Rootkits de <http://www.bvs.hn/cu-2007/ponencias/SEG/seg021.pdf>

Rootkit de <https://en.wikipedia.org/wiki/Rootkit>