

# SKD: Rootkit per a sistemes operatius UNIX

Albert Sellarès Torra

<whats@wekk.net>

Facultat d'Informàtica de Barcelona

12 de Gener de 2010

- 1 Definició
- 2 Motivació
- 3 Objectiu
- 4 El rootkit
  - Funcionalitats
  - Arquitectura client servidor
  - Heartbeat
  - Keylogger
- 5 Evolució
- 6 Conclusions

# Definició de “rootkit”

# Definició de “rootkit”

Eina o conjunt d'eines...

...que té com a finalitat ocultar-se i permetre que un tercer administri la màquina on està instal·lat.

# Definició de “rootkit”

## Principals característiques:

- S'amaga i oculta el seu funcionament.

## Antivirus

Considerats com a virus per els antivirus.

# Definició de “rootkit”

## Principals característiques:

- S'amaga i oculta el seu funcionament.
- Permet l'accés al seu propietari.

## Antivirus

Considerats com a virus per els antivirus.

# Definició de “rootkit”

## Principals característiques:

- S'amaga i oculta el seu funcionament.
- Permet l'accés al seu propietari.
- Permet administrar la màquina.

## Antivirus

Considerats com a virus per els antivirus.

# Definició de “rootkit”

## Principals característiques:

- S'amaga i oculta el seu funcionament.
- Permet l'accés al seu propietari.
- Permet administrar la màquina.
- Perdura instal·lat el màxim de temps possible.

## Antivirus

Considerats com a virus per els antivirus.



# Definició de “rootkit”

## Principals característiques:

- S'amaga i oculta el seu funcionament.
- Permet l'accés al seu propietari.
- Permet administrar la màquina.
- Perdura instal·lat el màxim de temps possible.
- Facilita l'obtenció d'informació sensible.

## Antivirus

Considerats com a virus per els antivirus.

# Motivació

# Motivació

Motius per complicar-me la vida:

- Passió per la seguretat informàtica.

# Motivació

## Motius per complicar-me la vida:

- Passió per la seguretat informàtica.
- Devoció per el programari lliure i GNU/Linux.

# Motivació

## Motius per complicar-me la vida:

- Passió per la seguretat informàtica.
- Devoció per el programari lliure i GNU/Linux.
- Utilitat que necessitava.

# Motivació

## Motius per complicar-me la vida:

- Passió per la seguretat informàtica.
- Devoció per el programari lliure i GNU/Linux.
- Utilitat que necessitava.
- Per aprendre.

# Motivació

## Motius per complicar-me la vida:

- Passió per la seguretat informàtica.
- Devoció per el programari lliure i GNU/Linux.
- Utilitat que necessitava.
- Per aprendre.
- Per investigar.

# Motivació

## Motius per complicar-me la vida:

- Passió per la seguretat informàtica.
- Devoció per el programari lliure i GNU/Linux.
- Utilitat que necessitava.
- Per aprendre.
- Per investigar.
- Per diversió.



# Objectiu del projecte

# Objectiu del projecte

## Objectiu principal

Crear un rootkit multiarquitectura per a sistemes basats en UNIX que exploti al màxim les característiques comentades anteriorment.

# El rootkit

# El rootkit

## El nostre rootkit:

- **Funcionalitats.**
- Arquitectura.
- Heartbeat.
- keylogger.

# El rootkit

## Implementació

- Executable sense dependències i autocontingut.
- Multiplataforma i compatible amb les variants de UNIX.

## Comunicació

- Autenticació per contrasenya.
- Comunicació xifrada.
- Connexió directa.
- Connexió inversa.
- Protocol raw.

# El rootkit

## Funcionalitats bàsiques

- Tasques programades.
- Heartbeat.
- Ocultació.
- Detecció del rootkit.
- Supervivència del rootkit.
- Obtenció d'una shell i un TTY.
- Transferència de Fitxers.
- Mode comanda / Mode servei.

# El rootkit

## Funcionalitats avançades

- Proxy SOCKS.
- Independència de la shell.
- Tècniques per evitar firewalls i filtres.
- Keylogger.

# El rootkit

## El nostre rootkit:

- Funcionalitats.
- **Arquitectura.**
- Heartbeat.
- keylogger.



# El rootkit

INTERNET

Servidor

rootkit

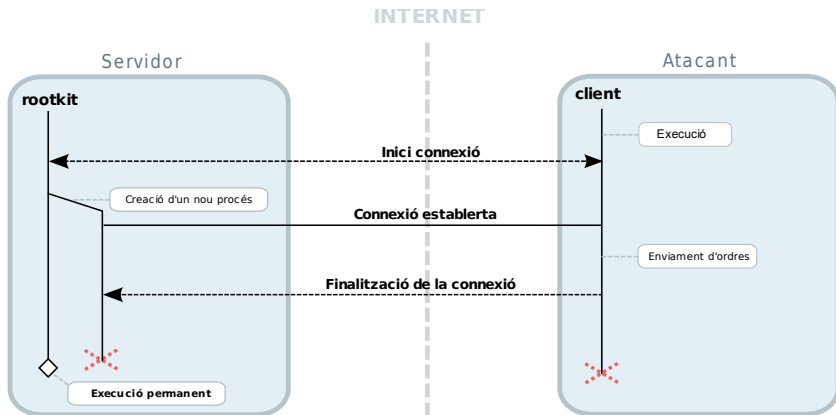


Atacant

client



# El rootkit



# El rootkit

## El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- **Heartbeat.**
- keylogger.

# El rootkit

- Exemple de funcionament amb gràfics/esquemes i tal...
- Comentar les característiques

# El rootkit

## El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- Heartbeat.
- **keylogger.**

# El rootkit

## Objectiu

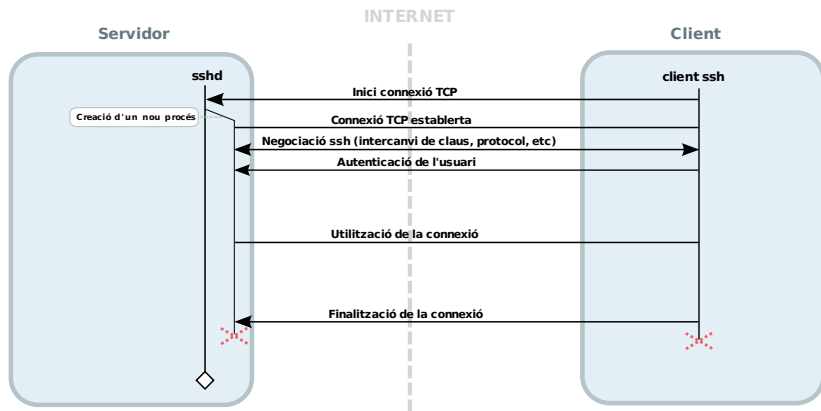
Aconseguir els passwords dels diferents usuaris del sistema

## Característiques

- Funcionament en entorn d'usuari.
- Poder capturar desde múltiples serveis.

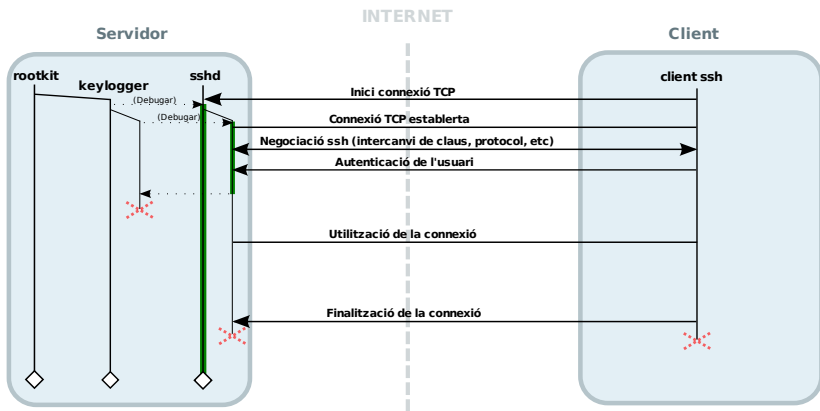
Keylogger: Exemple de funcionament

# El rootkit



Keylogger: Exemple de funcionament

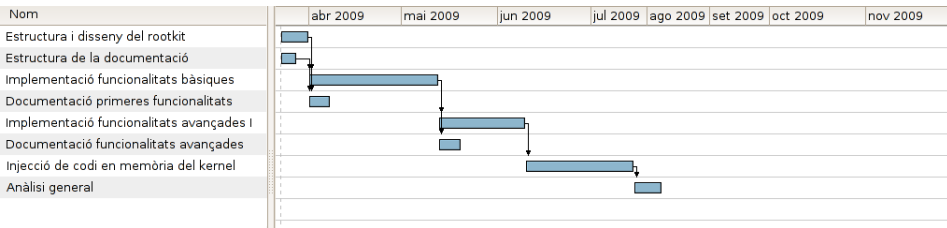
# El rootkit





# Evolució

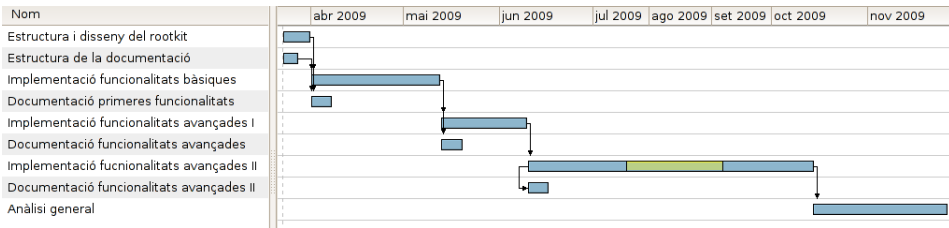
# Planificació inicial



## Característiques

- No deixar la documentació pel final.
- Agrupació per funcionalitats.
- Estructura i disseny només inclou el core.
- Anàlisi general per conciliar-ho tot i afinar el producte.

# Planificació final



## Característiques

- Funcionalitat de injecció no implementada.
- Funcionalitats avançades — a canvi.
- Període d'exàmens i vacances no tingut en compte.
- Anàlisi general i conciliació ha portat molta més feina.

# Conclusions

## Funcionalitats inicials

Injecció de codi en memòria de kernel reemplaçada per motius aliens.

## Objectius i motivació

Complets amb escreix.

## Part teòrica i pràctica

Les dues parts tenen molt de pes.

- Investigació i recerca.
- Prova de concepte i desenvolupament en el rootkit.

## Projecte amb una certa dificultat

Sempre és més difícil nadar contra corrent.

# Conclusions

En definitiva...

...es pot dir que m'he complicat una mica la vida però ha valgut la pena. :)

# Preguntes?