

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
 - Arquitectura
 - Funcionalitats
 - Funcionalitat en detall: 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.
- 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 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 investigar.
- 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 investigar.
- Per aprendre.
- 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:

- **Arquitectura.**
- Funcionalitats.
- Keylogger.

El rootkit

INTERNET

Servidor

rootkit

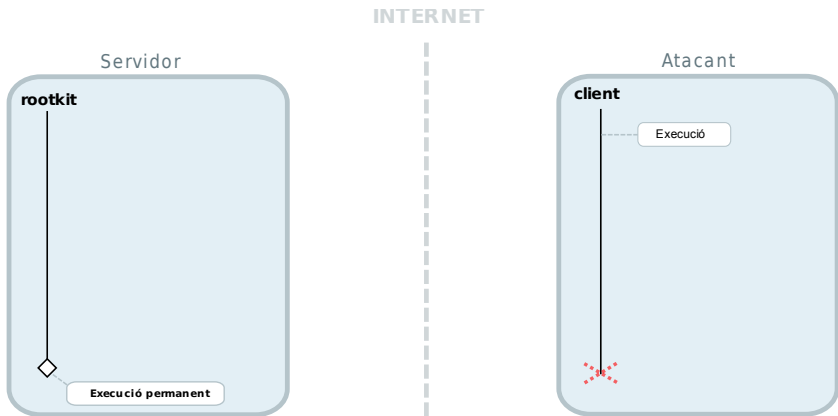


Atacant

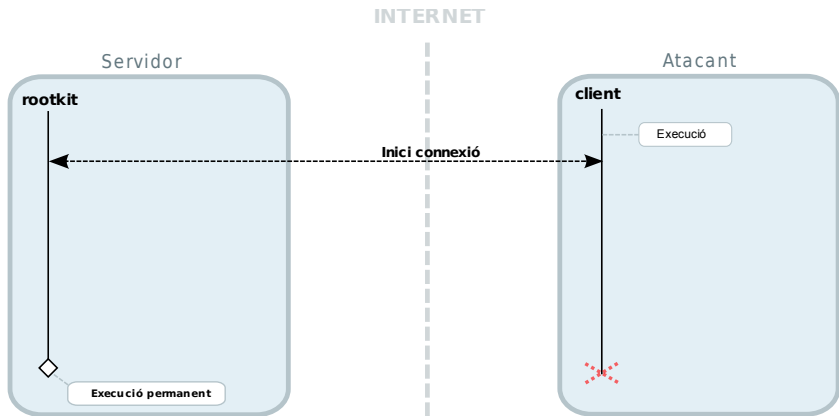
client



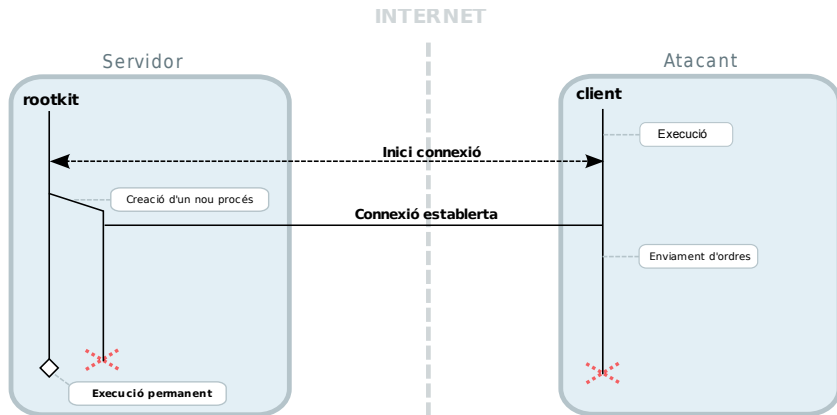
El rootkit



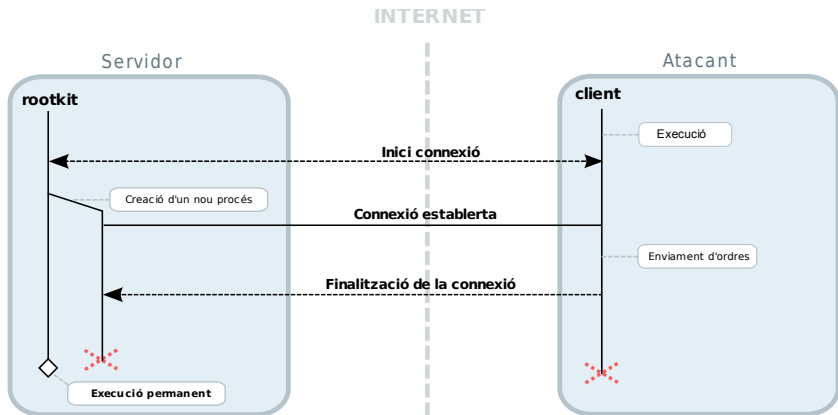
El rootkit



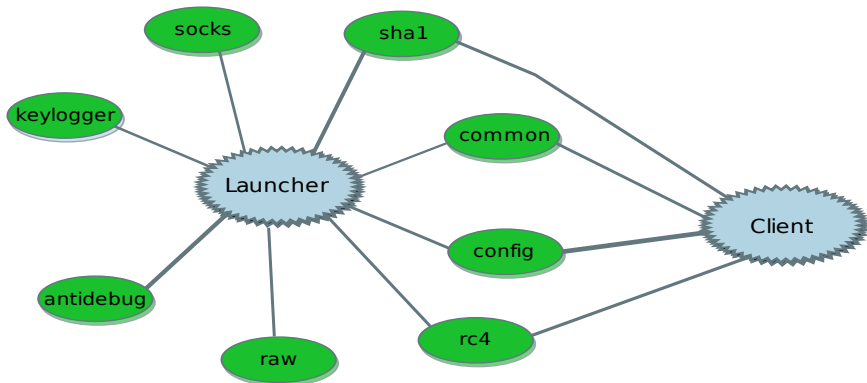
El rootkit



El rootkit



El rootkit



El rootkit

El nostre rootkit:

- Arquitectura.
- **Funcionalitats.**
- Keylogger.

El rootkit

Implementació

- Executable sense dependències i autocontingut.

El rootkit

Implementació

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

El rootkit

Implementació

- Executable sense dependències i autocontingut.
- Multiarquitectura i compatible amb les variants de UNIX.
- Protegit contra enginyeria inversa i depuració.

El rootkit

Implementació

- Executable sense dependències i autocontingut.
- Multiarquitectura i compatible amb les variants de UNIX.
- Protegit contra enginyeria inversa i depuració.

Comunicació

- Autenticació per contrasenya.

El rootkit

Implementació

- Executable sense dependències i autocontingut.
- Multiarquitectura i compatible amb les variants de UNIX.
- Protegit contra enginyeria inversa i depuració.

Comunicació

- Autenticació per contrasenya.
- Comunicació xifrada.

El rootkit

Implementació

- Executable sense dependències i autocontingut.
- Multiarquitectura i compatible amb les variants de UNIX.
- Protegit contra enginyeria inversa i depuració.

Comunicació

- Autenticació per contrasenya.
- Comunicació xifrada.
- Protocol TCP: Connexió directa / Connexió inversa.

El rootkit

Implementació

- Executable sense dependències i autocontingut.
- Multiarquitectura i compatible amb les variants de UNIX.
- Protegit contra enginyeria inversa i depuració.

Comunicació

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

El rootkit

Funcionalitats bàsiques

- Ocultació.

El rootkit

Funcionalitats bàsiques

- Ocultació.
- Tasques programades.

El rootkit

Funcionalitats bàsiques

- Ocultació.
- Tasques programades.
- Heartbeat.

El rootkit

Funcionalitats bàsiques

- Ocultació.
- Tasques programades.
- Heartbeat.
- Detecció del rootkit.

El rootkit

Funcionalitats bàsiques

- Ocultació.
- Tasques programades.
- Heartbeat.
- Detecció del rootkit.
- Supervivència del rootkit.

El rootkit

Funcionalitats bàsiques

- Ocultació.
- Tasques programades.
- Heartbeat.
- Detecció del rootkit.
- Supervivència del rootkit.
- Obtenció d'una shell i un TTY.

El rootkit

Funcionalitats bàsiques

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

El rootkit

Funcionalitats bàsiques

- Ocultació.
- Tasques programades.
- Heartbeat.
- 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.

El rootkit

Funcionalitats avançades

- Proxy SOCKS.
- Independència de la shell.

El rootkit

Funcionalitats avançades

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

El rootkit

Funcionalitats avançades

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

El rootkit

El nostre rootkit:

- Arquitectura.
- Funcionalitats.
- **Keylogger.**

El rootkit

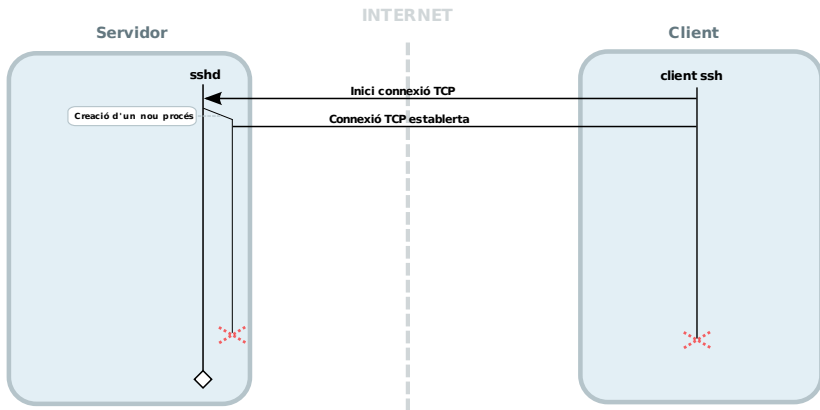
Objectiu

Aconseguir els passwords dels diferents usuaris del sistema

Característiques

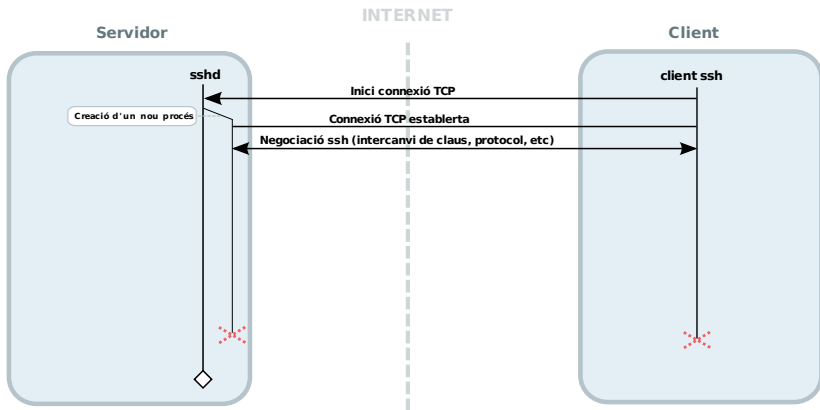
- Funcionament en entorn d'usuari.
- Poder capturar desde multiples serveis.

El rootkit



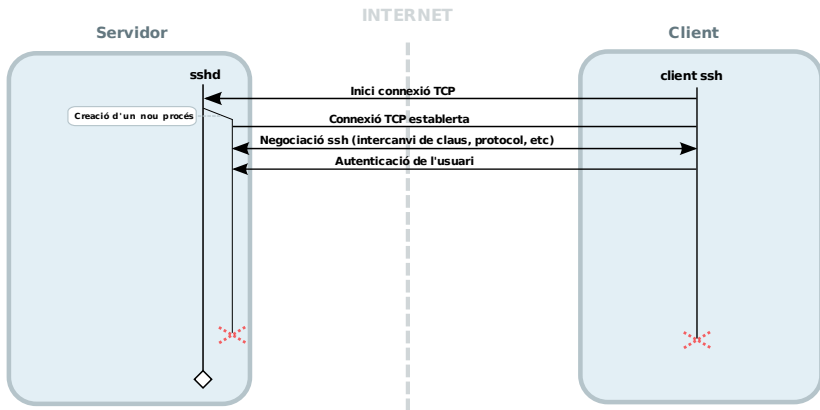
Keylogger: Exemple de funcionament

El rootkit



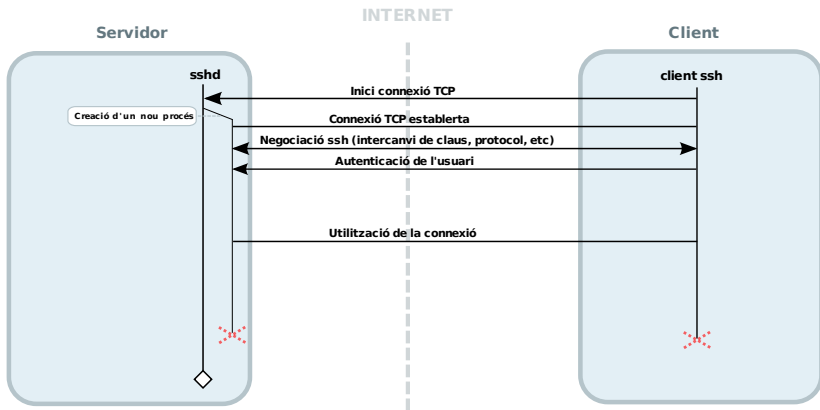
Keylogger: Exemple de funcionament

El rootkit

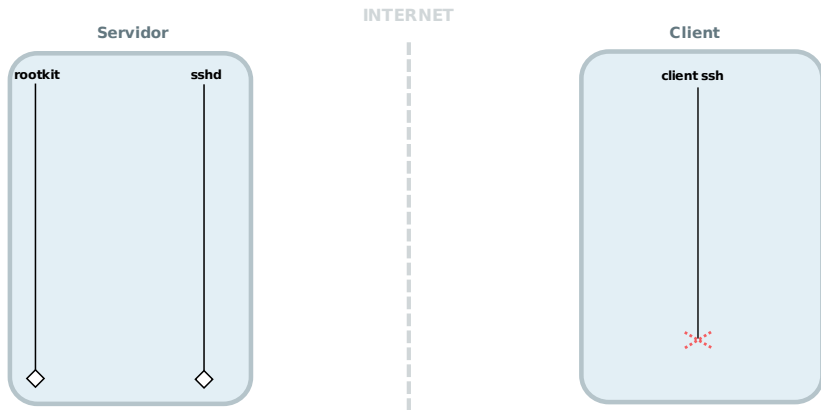


Keylogger: Exemple de funcionament

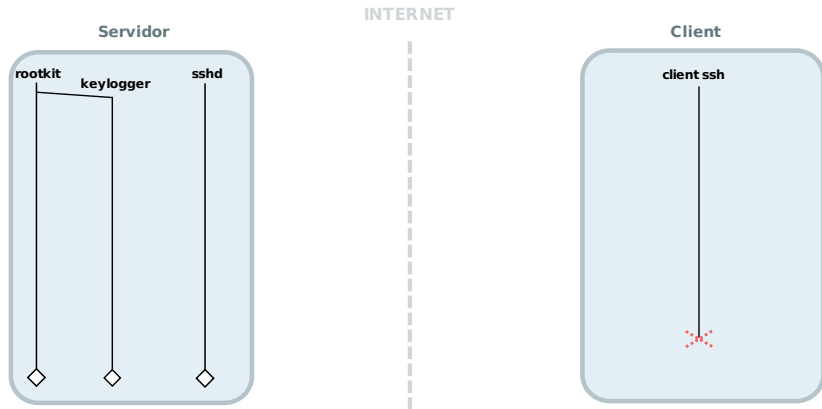
El rootkit



El rootkit



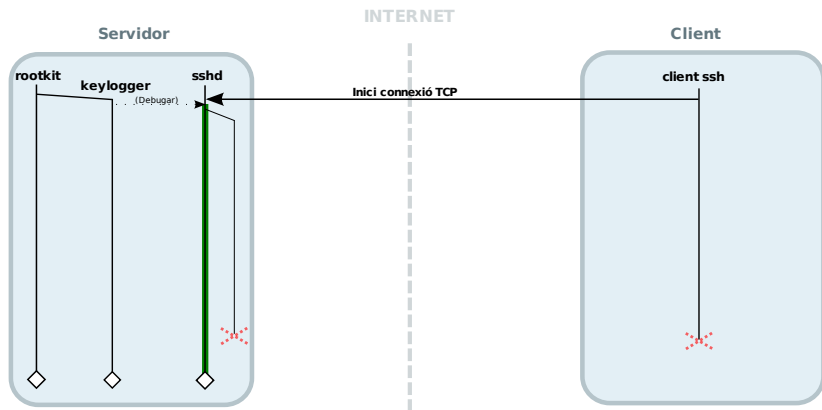
El rootkit



INTERNET

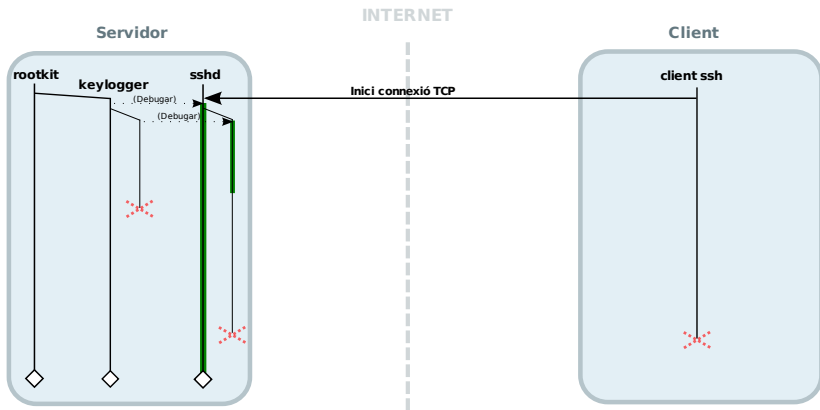


El rootkit



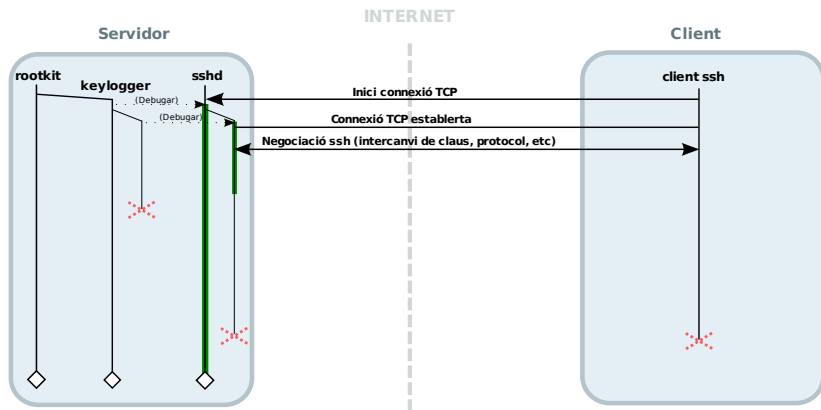
Keylogger: Exemple de funcionament

El rootkit

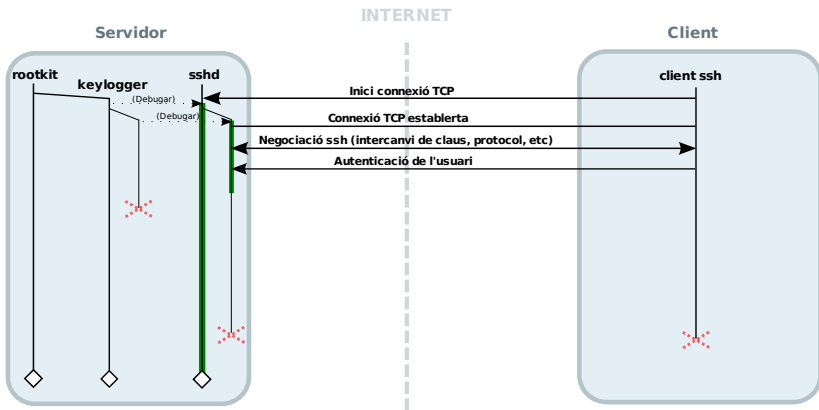


Keylogger: Exemple de funcionament

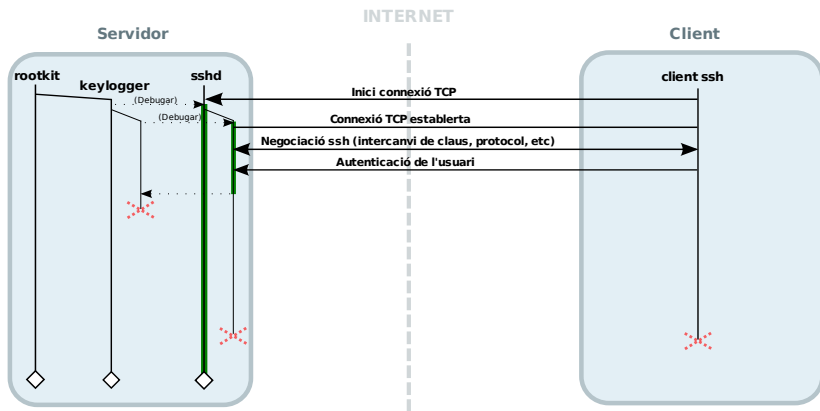
El rootkit



El rootkit

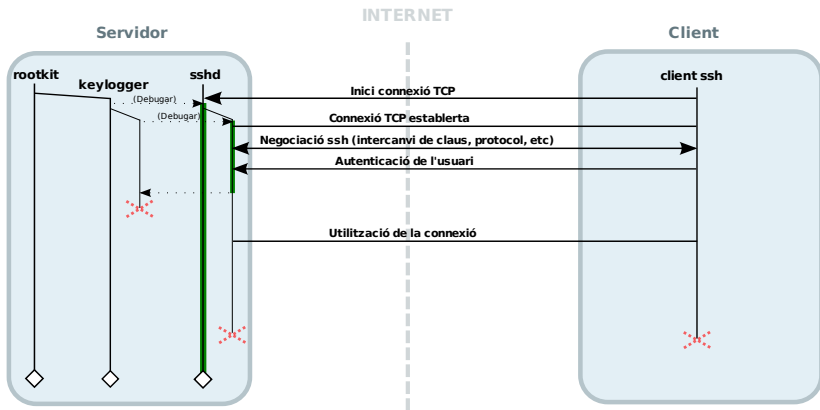


El rootkit



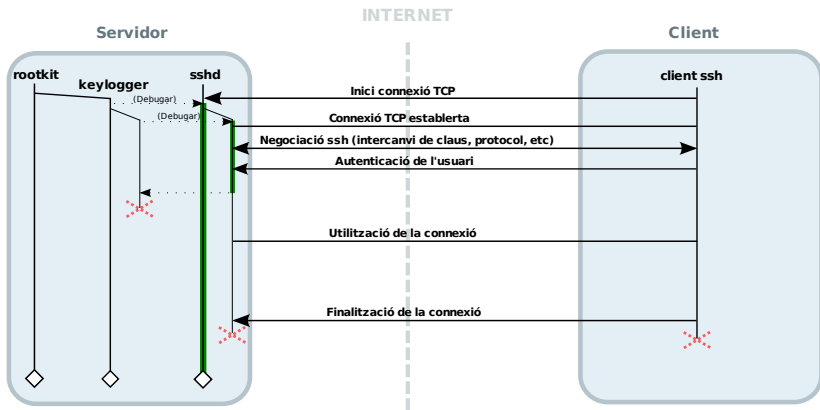
Keylogger: Exemple de funcionament

El rootkit



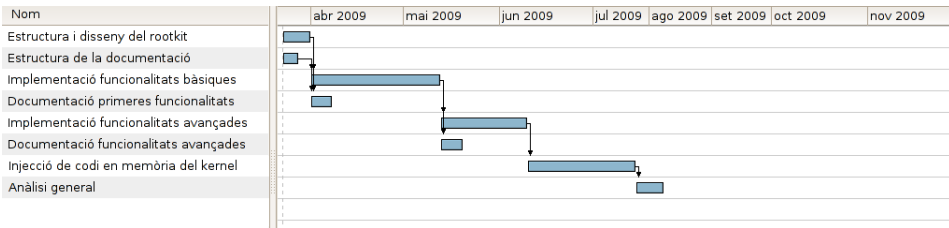
Keylogger: Exemple de funcionament

El rootkit



Evolució

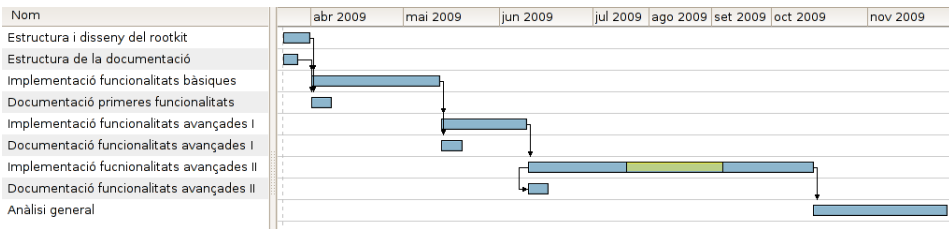
Planificació inicial



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.
- Més funcionalitats avançades a canvi.
- Període d'exàmens i vacances no tingut en compte.
- Anàlisi general i conciliació ha portat molta més feina.

Conclusions

Conclusions

Motivació i objectius

- Motivació completa.
- Objectius complerts.
- L'única funcionalitat no completa per motius aliens ha estat reemplaçada per altres funcionalitats.

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?