SKD: Rootkit per a sistemes operatius UNIX

Albert Sellarès Torra
<whats@wekk.net>

Facultat d'Informàtica de Barcelona

12 de Gener de 2010

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.

Objectiu del projecte

Objectiu del projecte

Objectiu principal

Crear un rootkit multiarquitectura i multiplataforma (*NIX) que exploti al màxim les característiques comentades anteriorment.

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.

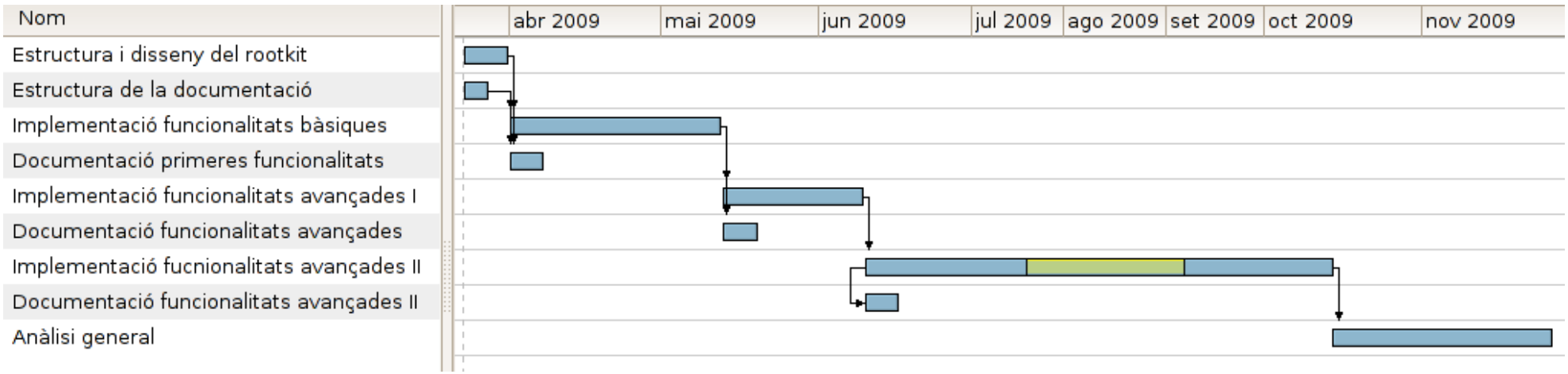
Motivació

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.

Planificació

Planificació



El rootkit

El rootkit

El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- keylogger.
- Comunicació raw.
- Proteccions de l'executable.

El rootkit

Implementació

- Executable ELF estàtic.
- Multiplataforma i multiarquitectura.

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.
- Proteccions de l'executable.
- Keylogger.

El rootkit

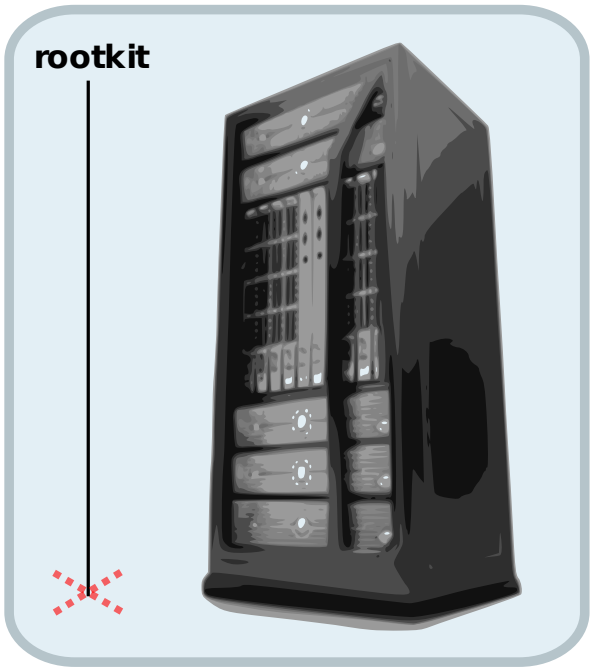
El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- keylogger.
- Comunicació raw.
- Proteccions de l'executable.

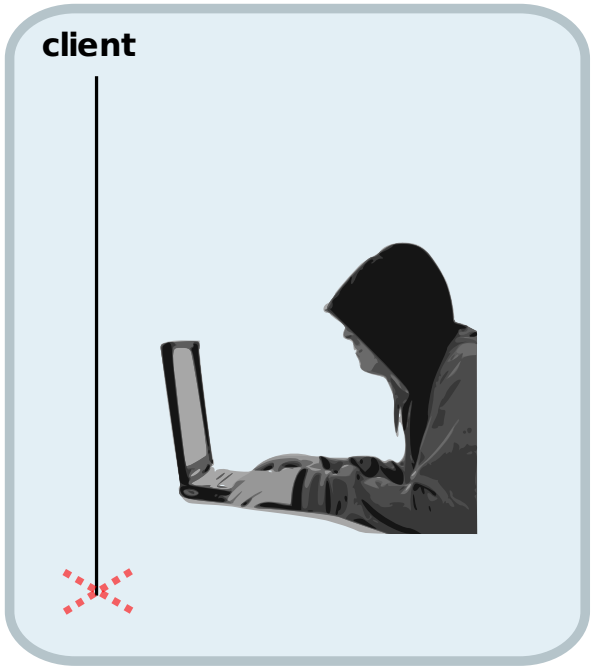
El rootkit

INTERNET

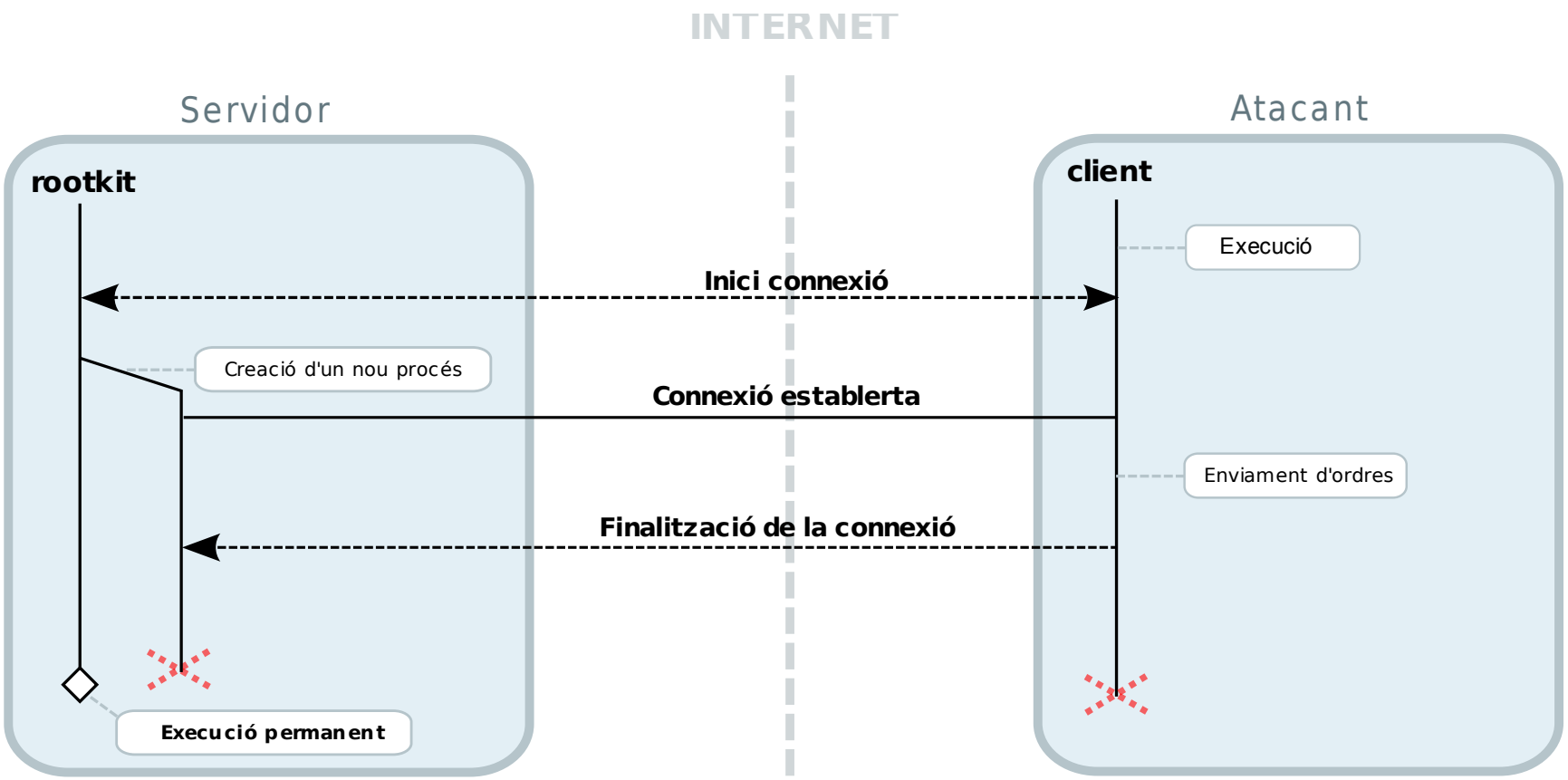
Servidor



Atacant



El rootkit


INTERNET
Servidor
Atacant
rootkit
client
Execució
Inici connexió
Creació d'un nou procés
Connexió establerta
Enviament d'ordres
Finalització de la connexió
Execució permanent

El rootkit

El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- keylogger.
- Comunicació raw.
- Proteccions de l'executable.

El rootkit

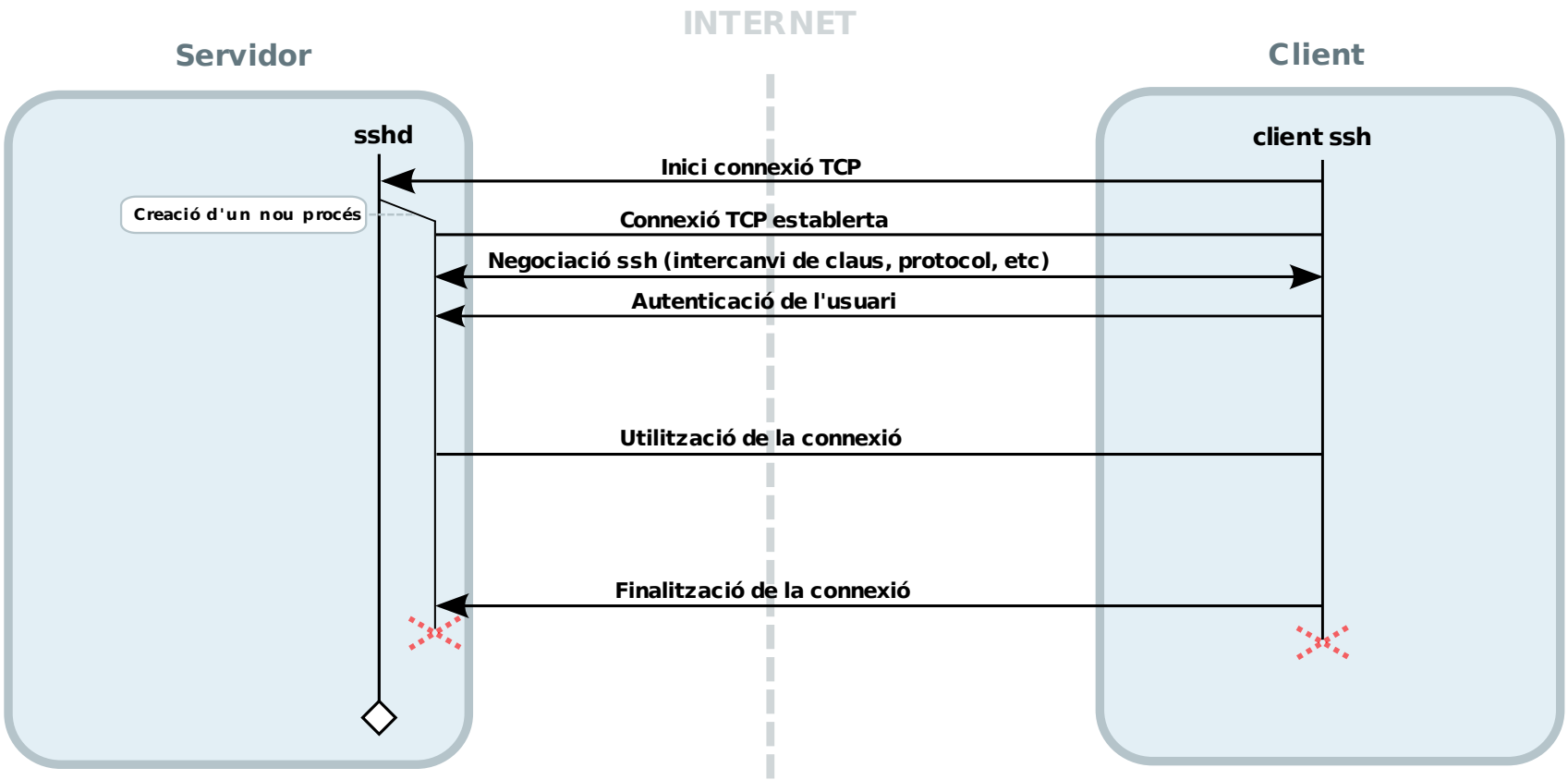
Objectiu

Aconseguir els passwords dels diferents usuaris del sistema

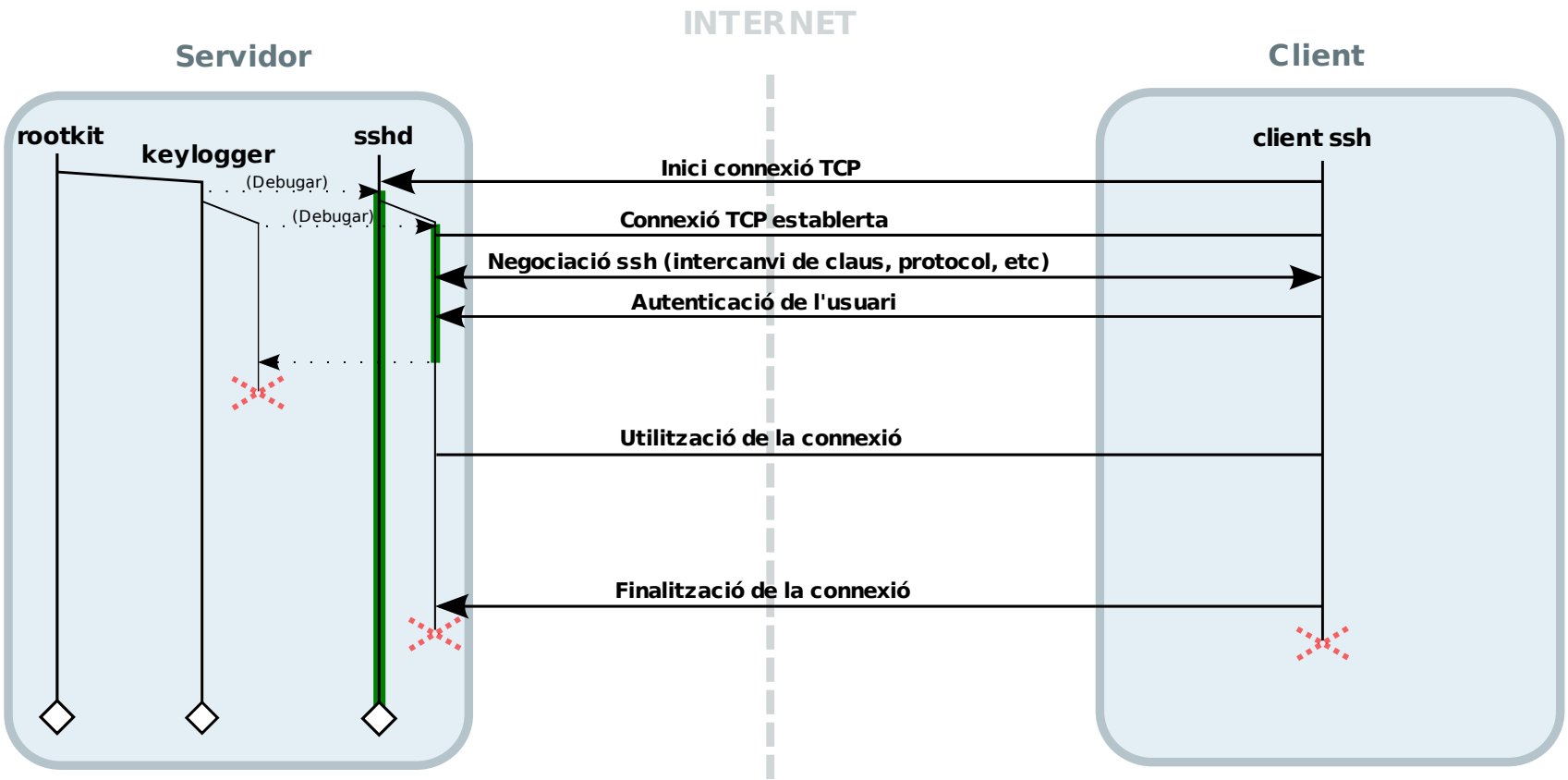
Característiques

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

El rootkit


INTERNET
Servidor
Client
sshd
client ssh
Inici connexió TCP
Creació d'un nou procés
Connexió TCP establerta
Negociació ssh (intercanvi de claus, protocol, etc)
Autenticació de l'usuari
Utilització de la connexió
Finalització de la connexió

El rootkit


INTERNET
Servidor
Client
rootkit
keylogger
sshd
client ssh
(Debugar)
(Debugar)
Inici connexió TCP
Connexió TCP establerta
Negociació ssh (intercanvi de claus, protocol, etc)
Autenticació de l'usuari
Utilització de la connexió
Finalització de la connexió

El rootkit

El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- keylogger.
- Comunicació raw.
- Proteccions de l'executable.

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

El rootkit

El nostre rootkit:

- Funcionalitats.
- Arquitectura.
- keylogger.
- Comunicació raw.
- Proteccions de l'executable.

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

Conclusions

Objectius i motivació

Complerts 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 dificil nadar contra corrent.

Conclusions

En definitiva...

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

Preguntes?