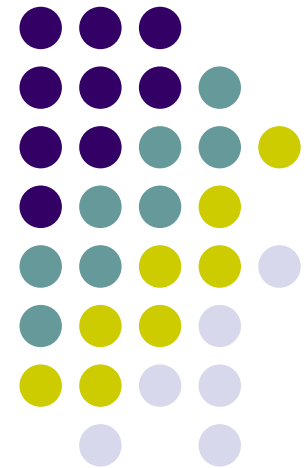


Hackers

Un estil de vida propi





Index

- 1.- Introducció al moviment hacker
- 2.- Tipus de hackers
- 3.- Coneixements necessaris per ser un bon hacker
- 4.- Com realitzar un atac?
- 5.- Algunes tècniques bàsiques de hackers



Hackers (I)

- Què és un hacker?
- Etimologia de la paraula hacker
 - La nova filosofia hacker: “La ética del hacker”
- Documents claus de la cultura hacker:
 - JARGON (Actualment en la versio 4.4.1)
 - <http://catb.org/~esr/jargon/>
 - <http://www.gamerjargon.com/>
 - Manifesto hacker (The mentor, 1986)
 - CAT: http://www.linuxsilo.net/docs/manifiesto-hacker_ca.html
 - CAS: http://www.linuxsilo.net/docs/manifiesto-hacker_es.html
 - ENG: http://www.linuxsilo.net/docs/manifiesto-hacker_en.html



Hackers (II)

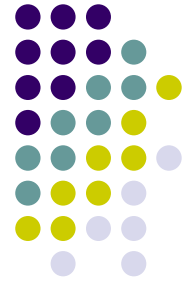
- Característiques dels bons hackers:
 - Autodidactes
 - Necessiten satisfer la seva curiositat i el seu afany de superació
 - Capacitat d'estudi
 - Pacència... El hacking real es un 'art'
 - Estar sempre al dia
 - Fanàtics de la informatica 'en general'



Hackers (III)

- Motivacions dels hackers:
 - Personals
 - Autosuperació
 - Competicions
 - Econòmiques
 - Beneficis directes / indirectes
 - Polítiques:
 - Patriotisme
 - Cyberwars

Hackers (IV)



- Tipus de hackers:
 - Hackers vs. Crackers (White Hat vs. Black Hat)
 - Old school hackers vs. Script kiddies
 - Altres: CypherPunks, Phreakers, Virus Writers, ...
- Que no hem de ser? Lamers ;-)



Hackers Famosos (I)

- **Robert Morris** (*rtm*)
 - Creador del primer cuc que va saturar la xarxa en 1988
 - Primer en ser empresonat per un delicte digital



Hackers Famosos (II)



- **Kevin Mitnick** (*condor*)
 - Es va fer famós al ser el primer hacker que apareixia en un cartell de 'Top Wanted' del FBI
 - Va relitzar intrusions a grans multinacionals americanes.





Hackers Famosos (III)

- **Vladimir Levin**

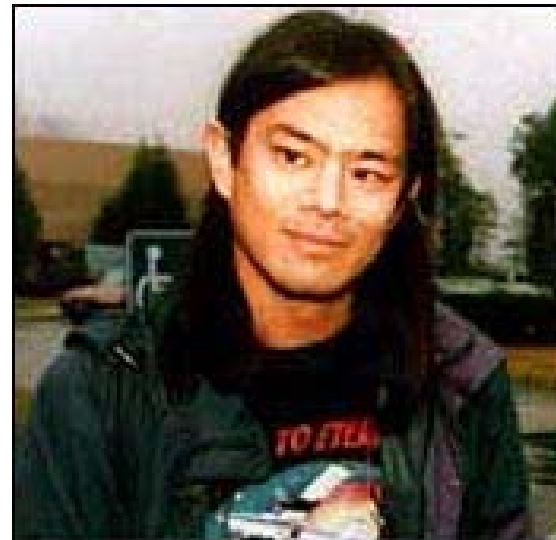
- Va robar 10 milions de \$ de Citybank des del seu ordinador a St. Petesburg, i capturat uns mesos després a Londres.
- Des de llavors Citybank te una de les xarxes mes segures del món....





Hackers Famosos (IV)

- **Tsutomu Shimomura**
 - Famos per ser el que va poder capturar a Kevin Mitnick a partir d'un atac realitzat contra una de les seves màquines.
 - Tot el procés de captura es pot llegir en el llibre '*TAKEDOWN*', escrit per ell mateix.

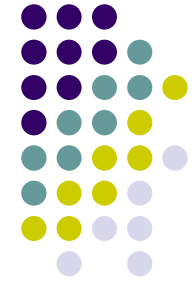




Hackers Famosos (V)

- Altres:
 - **Richard Stallman**: Creador del FSF
 - **Dennis Ritchie i Ken Thompson**: Creadors del Unix i del llenguatge C
 - **Steve Wozniak**: Un dels co-creadors d'apple
- Mes informació del 'HALL OF FAME'
- <http://tlc.discovery.com/convergence/hackers/hackers.html>

Coneixements: Introducció



- Que cal saber per ser un bon hacker = Que hem de saber per prevenir-nos d'ells
- Moltes disciplines que s'ensenyen al llarg de la carrera universitària... que cal completar pel nostre compte ;-)



Coneixements: Xarxes

- Que permeten?
 - Moure'ns per la xarxa
 - Entendre el funcionament del trafic
 - Localitzar els recursos
- Que cal saber?
 - Arquitectura de xarxes, protocols, coneixer la infraestructura, hardware, ...
- On ho trobem?
 - Llibres de xarxes, tutorials per internet, RFCs, manuals dispositius ...



Coneixements: Sist. Oper.

- Que permeten?
 - Navegar per dintre el sistema
 - Reconfigurar els parametres
 - Crear i executar programes
- Que cal saber?
 - Comandes bàsiques, llenguatge scripting, funcionament del kernel, privilegis, gestio dels recursos, ...
- On ho trobem?
 - Manuals dels sistemes, tutorials,



Coneixements: Serveis

- Que permeten?
 - Descobrir com funcionen les portes d'un servidor
- Que cal saber?
 - Quins son els protocols, ports, etc.. utilitzats
 - Com funcionen els servidors i quins recursos utilitzen
- On ho trobem?
 - RFCs, etc..
 - Codis i manuals de les diferents aplicacions



Coneixements: Programació

- Que permeten?
 - Crear o manipular eines d'atac
- Que cal saber?
 - Llenguatges programació
 - Llenguatges scripting
 - Debuggejar codi
- On ho trobem?
 - Manuals, tutorials, llibres, etc...



Coneixements: Seguretat

- Que permeten?
 - Saltar-nos les proteccions i no ser detectats
 - Desxifrar codis, passwords, etc..
- Que cal saber?
 - Tecniques utilitzades per prevenir i protegir atacs
 - Criptografia
- On ho trobem?
 - Manuals dels components, tutorials, ...

Coneixements: Conclusions



- Consells per aprendre al màxim:
 - Tenir una idea global de cadascun dels temes i tenir a mà eines de consulta ràpida per a dubtes concrets (Google!!).
 - Practicar tots els conceptes teòrics explicats durant el curs en la mesura de les possibilitats.
 - Estar al dia al respecte de novetats que apareguin en qualsevol dels camps citats (subscripcions a llistes, magazines, forums, webs ...).



Com realitzar un atac? (I)

- 1. Recollir informació de la maquina
 - En el cas de tenir 1 objectius concret, centrar-nos en ports, servidors, SO, ...
 - En el cas de no tenir un objectius, escanejar la xarxa
- 2. Cerca de vulnerabilitats
 - Bases de dades d'internet
 - Desenvolupament de noves vulnerabilitats

Com realitzar un atac? (II)



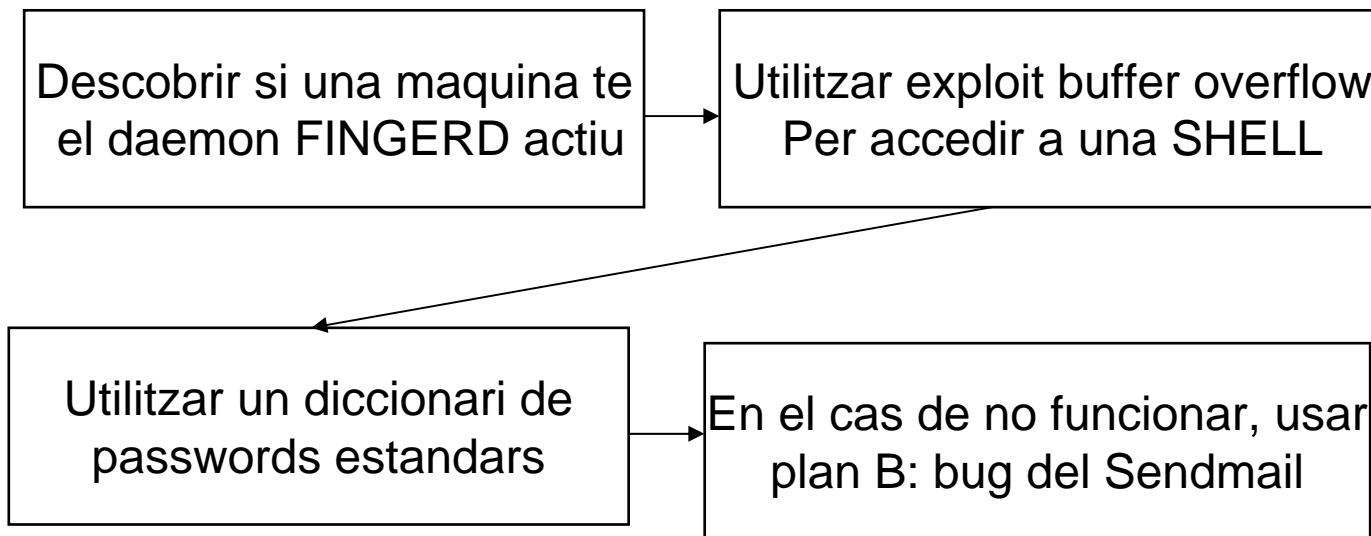
- 3. Utilitzar l'exploit per accedir al sistema
 - Aconseguir compte de superusuari, si fa falta amb altres exploits
 - Realitzar les accions que ens convingui
 - Esborrar el rastre de tot el que hem intentat fer
 - Deixar algun mecanisme ocult per a poder-nos connectar posteriorment (*Backdoor*) o capturar més informació (*sniffer*)

Com realitzar un atac?

Exemple



- The Morris Worm, 1988



- Després d'aquest problema es va crear el CERT (Computer Emergency Response Team)
- Més informació i codi del Worm
<http://www.snowplow.org/tom/worm/>



Eines i tècniques varies (I)

- Buffer overflow exploits
 - L'error mes utilitzat per aconseguir accesos no
 - Basat en una mala gestio de la memoria
- Packet Sniffing
 - Capturar informacio de la xarxa sense ser detectat per extreure el que ens interressi
- Snooping / Data downloading
 - Similar al sniffing, pero descarregant la informació directament a la nostra computadora.



Eines i tècniques varies (II)

- Spoofing
 - Sistema per ocultar la identitat d'alguna cosa (Es pot realitzar d'adreces, ports, ...) per evitar ser detectats i que ens puguin relacionar amb l'atac.
- Jamming /Flooding
 - Inundar el servidor/servei amb mes informacio de la que sigui capaç de processar.
 - Normalment provoca el que es coneix per DoS (Denial Of Service).
- Enginyeria Social
 - La tecnica mes simple i efectiva