Hacking Ético

salvando el mundo con ceros y unos

#HACKINGETSIIT16
@GDGgranada
@Terceranexus6

Índice

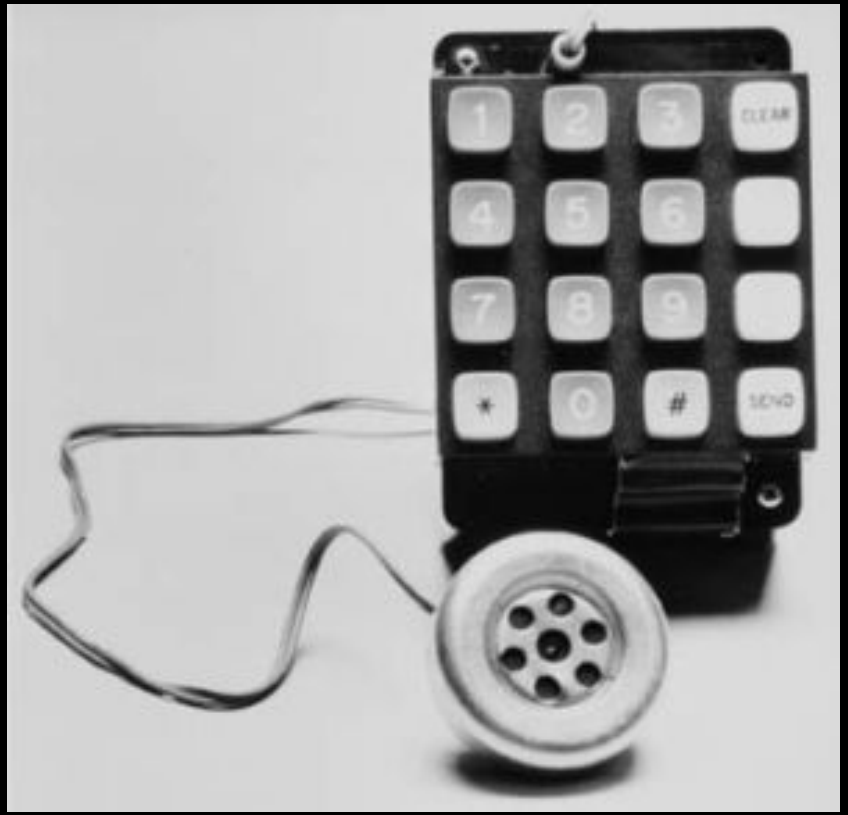
Un poco de historia

¿Hacker, Cracker o Phreaker?

Hacker
Todo individuo que se dedica a programar de forma entusiasta.
En seguridad, distinguimos White Hat, Black Hat y Grey Hat.

Cracker
Es parecido a hacker pero se dedican exclusivamente a romper sistemas ajenos por diversión o fines lucrativos

Phreakers
Expertos en los teléfonos que sabían aprovechar los errores de seguridad.

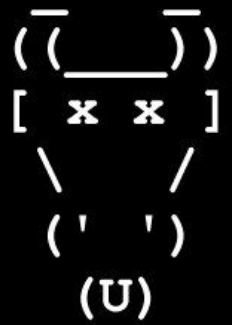


> Un poco de historia

Las guerras hacker

MoD vs LoD
Master of Deception, buscar y destruir
Legion of Doom, entrar y divulgar

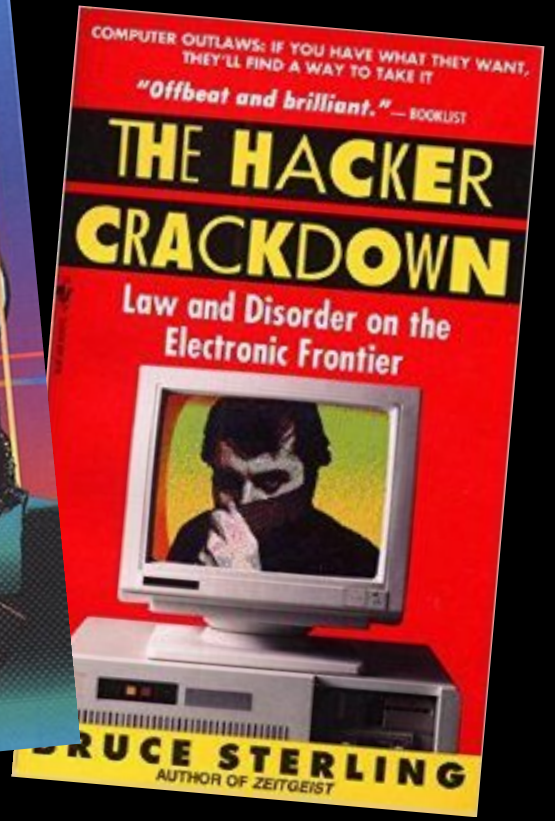
The hacker crackdown
La caza de brujas de los 80 y 90



En la actualidad
Cicada, Cult of the dead cow, Anonymous
DEFCON

> Un poco de historia

La subcultura



> Black hat

Sinónimo de **cracker**, se dedican a entrar ilegalmente en sistemas, para reventarlos, espiarlos, vender información sobre este, etc.

Este acto está penado por la ley tanto de forma nacional como internacional, más tarde veremos algunos ejemplos de estas leyes.

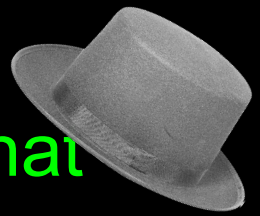
> White hat

Experto en seguridad informática, especializado en técnicas de intrusión, pero tiene todos los permisos necesarios para hacerlo, y tiene como objetivo descubrir los errores de seguridad que le permitirían a un black hat acceder.

“Hacker ético”

Certificados de la NSA

> Grey hat



A veces actúa ilegalmente pero sus intenciones en todo momento son buenas. Término acuñado por L0pht. Pueden actuar como los white hat, o informar a comunidades en internet.

Movimientos en internet, contra pedofilia, terrorismo y otros crímenes de internet.

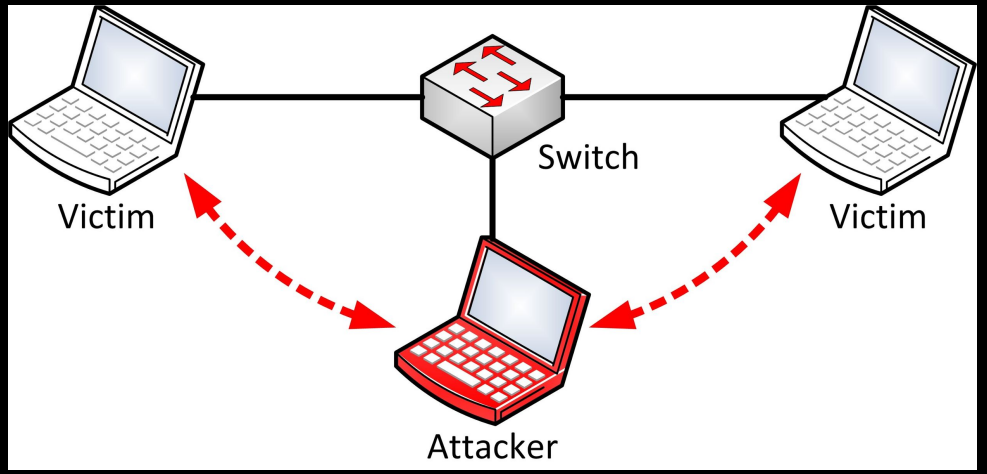
> Técnicas más usadas

- ★ Arp Spoofing y Sniffing
- ★ Web Spoofing
- ★ Exploits
- ★ Ingeniería social

> Arp Spoofing y sniffing

Aprovechamos que arp (en la capa de enlace de datos) pueden ser Broadcast (tráfico de difusión) para impersonar al receptor, de modo que cualquier información dirigida al ip de la víctima se dirigirá al atacante.

- MIDM
- DOS
- Blind/Non blind



> Web spoofing

Similar a Phising.

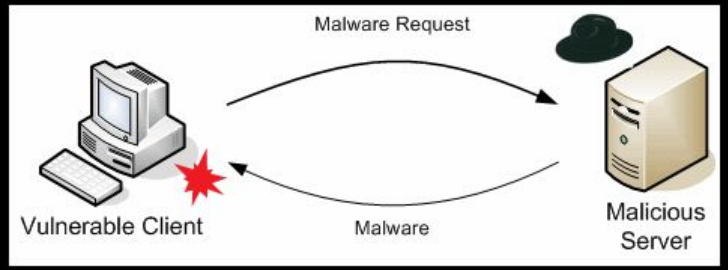
Suplantar el login de una página web para atrapar las credenciales de una víctima. Hay varias técnicas para hacer a alguien caer.

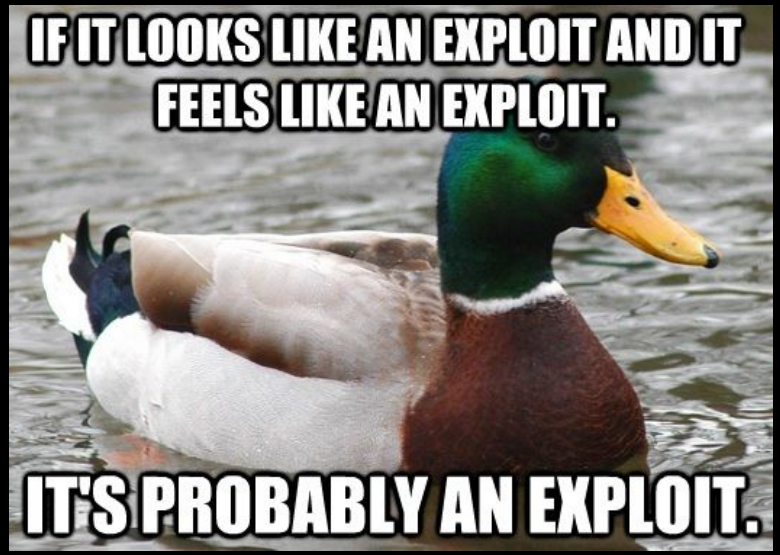
Difícil de detectar, sólo por la ip.

> Exploits

Un exploit es un programa que aprovecha vulnerabilidades en el sistema de seguridad para conseguir un comportamiento no deseado del mismo.

- **Remoto**
- **Local**
- **ClientSide**





> Ingeniería social

Los peores exploits de un sistema de seguridad son los usuarios.

Por mucho que un sistema esté bien protegido a nivel de código si el usuario no sabe cuidarse, será inútil.

Contraseñas poco seguras, estafas y en general, cualquier tipo de debilidad.

> Leyes contra hacking

Nacional

http://www.gitsinformatica.com/legislacion.html

http://www.gitsinformatica.com/legislacion.html

- Los ataques contra la dignidad de una persona (injuria), incluyendo cibernética van de 1 a 4 años de cárcel.
- Protección de datos y propiedad intelectual
- El mero acceso no autorizado no está penado en España
- Las direcciones IP se consideran datos de carácter personal, así como la dirección o el DNI, y disfrutan de la misma protección ante la ley

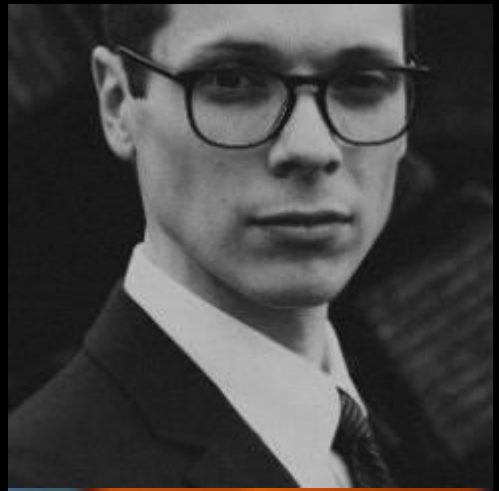
> Leyes contra hacking

USA

- Los servicios españoles conocen la intrusión de la NSA
- Si USA se siente amenazada por tu intrusión, estés donde estés, está penado, “*Computer fraud and abuse act*”
- hasta 10 años de cárcel y una fianza de 10.000$
- Dependen del estado, en algunos la intrusión sin daños no es delito y otra con daños a partir de cierta cantidad de dinero.

> Ejemplos famosos

Johnatan James (c0mrade): hackeo a la NSA con quince años, fue enviado a prisión, y posteriormente fue culpado por algo que, presuntamente no hizo, y se suicidó por ello.



Kevin Mitnick: hackeó el sistema de seguridad nacional de los EEUU, cumplió pena en prisión durante 5 años y ahora es consultor de seguridad.

> Ejemplos famosos

Kevin Poulsen (Dark Dante): se hizo a sí mismo ganador de un concurso de la radio y además, hackeó al FBI. 56000 $ y 50 meses de prisión.

Gary McKinnon (Solo): hackeó casi cien ordenadores de las fuerzas armadas de USA. Decía estar interesado en descubrir “la verdad sobre los OVNIS” cuando lo hizo. Fue condenado a cadena perpetua.

> Ejemplos famosos

Edward Snowden: ex-agente de la CIA que expuso sin tener acceso a ellos datos confidenciales de la NSA sobre investigaciones, escuchas y demás (wikileaks). El revuelo social y mediático reabrió la preocupación sobre la privacidad de las personas. Huyó a Rusia donde se mantiene en una localización desconocida.
https://en.wikipedia.org/wiki/Edward_Snowden

¡Muchas gracias!

¿Preguntas?