Seguridad informática

José Antonio Martínez Torres
http://www.antoniomtz.org

Grupo de Usuarios de GNU/Linux de la Laguna
GULAG

5 de febrero de 2009

Frase celebre...

"Ser lo que soy, no es nada sin la seguridad" ... William Shakespeare(1594)

Seguridad Informática

- Consiste en asegurar que los recursos del sistema de información sean utilizados de la manera que se decidió y que el acceso a la información allí contenida sólo sea posible a las personas que se encuentren acreditadas.
- la seguridad puede entenderse como aquellas reglas destinadas a **prevenir**, **proteger** y **resguardar** lo que es considerado como susceptible de robo, pérdida o daño.

Seguridad Física

- La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención.
- La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.
- Tipos de desastres:
  - Incendios, inundaciones, terremotos, instalación eléctrica

Seguridad lógica

- Nuestro sistema no sólo puede verse afectado de manera física, si no también contra la información almacenada.
- El activo más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren.
- Algunas técnicas de seguridad lógica:
  - Control de accesso, autentificación, encriptación, firewalls, antivirus (en caso de usar windows).

Definición de Hacker

- Persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras.
- Un verdadero Hacker es curioso y paciente.
- Un verdadero Hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad.
- Un verdadero Hacker crea, no destruye.
- Un hacker es un también llamado Geek.

Definición de Cracker

- Un cracker, en realidad es un hacker cuyas intenciones van más allá de la investigación.
- Es una persona que tiene fines maliciosos.
- Demuestran sus habilidades de forma equivocada ó simplemente hacen daño sólo por diversión.

Definición de Phreakers

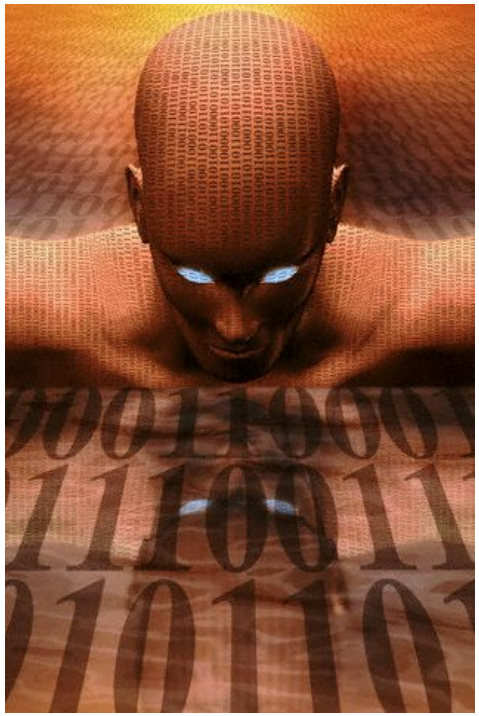
- Personas con un amplio (aveces mayor que los mismo empleados de las compañias telefónicas) conocimiento en telefonía.
- El phreaking es el antecesor de hacking ya que es mucho más antiguo. Comenzó en la década de los 60's cuando Mark Bernay descubrió como aprovechar un error de seguridad de la compañia Bell, el cual le permitió realizar llamadas gratuitas.
- De ahí han existido muchos phreakers famosos como Joe Engressia, kevin Mitnick y John Draper mejor conocido como Capitán Crush.

Ingeniería social

- Es el arte de manipular a las personas, con el fin de obtener información que revele todo lo necesario para penetrar la seguridad de algún sistema.
- Esta técnica es una de las más usadas a la hora de averiguar nombres de usuario y contraseñas.

Scanning

- Método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo.
- Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están **escuchando** por las respuestas recibidas o no recibidas.



Smurf o broadcast storm

- Es un ataque bastante simple, pero a su vez devastador.
- Consiste en recolectar una seria de direcciones Broadcast ó proxys las cuales realizaran peticiones PING a la máquina victima.

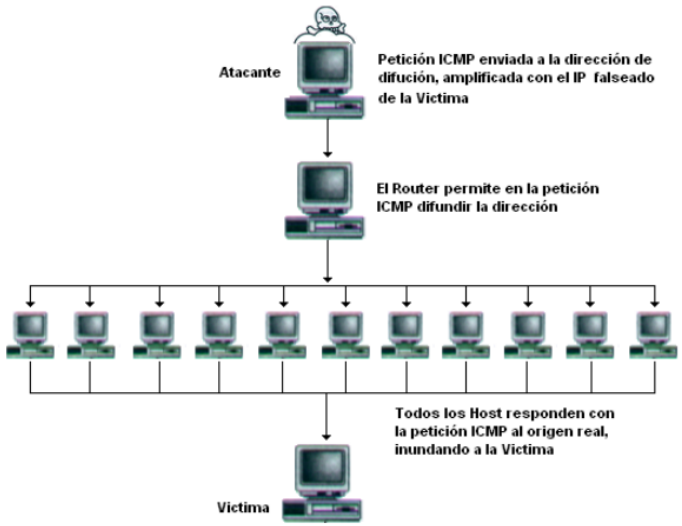
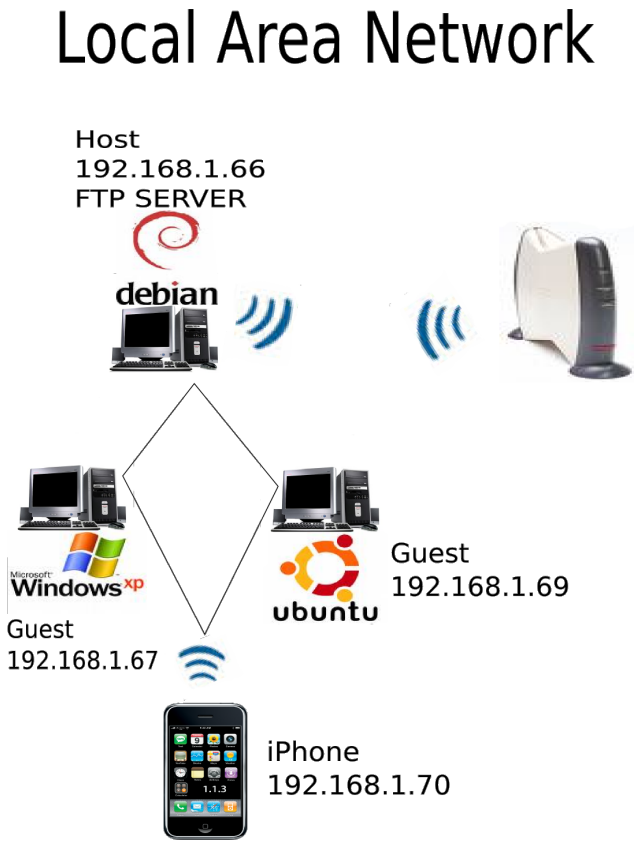


Gráfico 7.4 – Ataque Smurf

Sniffing

- Técnica para capturar tráfico (paquetes) en una red.
- Puedes capturar passwords, emails, conversaciónes de msn y cualquier otra información ya sea de caracter público ó privado.



Otras amenazas

- Spoofing
  - IP spoofing
  - DNS spoofing
  - Web spoofing
- Backdoors ó troyanos.
- Exploits.
- Denial of Service (DoS Attack)
- E-mail bombing
- Phishing.
- SQL injection.
- etc...

Medidas preventivas

- Mantener las máquinas actualizadas y seguras físicamente.
- Mantener personal especializado en cuestiones de seguridad.
- los administradores de red, los cuales deben configurar adecuadamente sus routers.
- Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados.
- Utilizar protocolos seguros como https, ssh.
- Encriptación de mails mediante GPG.
- Migrar a otros sistemas operativos como GNU/Linux, Solaris, BSD.

Preguntas??

Dudas, comentarios, preguntas??