La gestión de la seguridad informática

Víctor Cuchillac

Contenido

1. La gestión de la seguridad información.
2. Hacking ético
3. Hacking

La gestión de la seguridad informática

Consideraciones

- **¿Por dónde empezamos?**
  1. Existe mucho material
  2. No hay una plataforma educativa formal.
  3. Los cambios tecnológicos.
- Estudiaremos este tema desde el punto de vista del ***Hacking Ético***.
- **No nos concentraremos mucho en …**
- Detalles de cómo explotar algunas vulnerabilidades. Las vulnerabilidades son superadas rápidamente. Círculo vicioso.

Breve historia

- En los años 70, las organizaciones empiezan a informatizar sus procesos.
- En los siguientes años, se incremento la fluidez de las comunicaciones interpersonales, inter-sucursales exponiendo datos a terceros.
- En los 80 empezaron a salir a la prensa los primeros casos de intrusión.

Breve historia

- La gran mayoría de casos no salía a la luz para salvaguardar el prestigio de las organizaciones.
- Se hizo necesaria la protección de estos ataques.
- Se inició la carrera por la consecución de servicios profesionales que imitara esos ataques.

Breve historia

- También se capacitó al personal en las mismas técnicas usadas por el intruso.
- Así se evaluarían las mismas condiciones de seguridad. Seguridad preventiva.
- Algunos especialistas y hackers se unieron y empezaron a estudiar y practicar metodologías de intrusión.
- Sus servicios se ofrecían como Ethical Hacking.

Breve historia

- Entre los servicios brindados: vulnerability scanning y penetration test (network security assessment).
- Para los 90 se inició con fuerza el movimiento e-commerce, se iniciaba la integración de pequeñas y medianas empresas a la red.
- Luego, se sumó el público en general.

Breve historia

- Aparecía malware más sofisticado.
- No había conciencia sobre administración segura de servidores.

- **Nota: MALWARE**
- Código malicioso (programas). Se trata de gusanos o worms, spyware, troyanos, virus o scripts malintencionados. Amenazas detectadas por antivirus

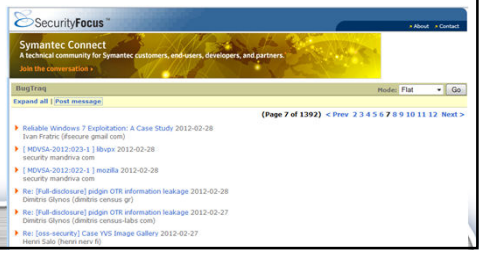
Breve historia

Eran tiempos ende ausencia de plataforma educativa. Se empezaba a llevar en algún postgrado en USA.

En el ámbito informal nació Bugtraq: Una lista de posteo donde se trata temas de seguridad

Breve historia

- Eran tiempos ende ausencia de plataforma educativa. Se empezaba a llevar en algún postgrado en USA.
- En el ámbito informal nació Bugtraq: Una lista de posteo donde se trata temas de seguridad



Breve historia

1982 John Shoch (uno de los creadores de ethernet), junto a un colega, escribieron el primer reporte sobre un gusano (worm), tomando ese nombre de una novela de ciencia ficción de 1975 en la que, bajo el nombre Tapeworms, describían a programas autómatas que viajaban por las redes transportando información.

1983 Ese año se estrenó la famosa película War Games, en la que el actor Matthew Broderick interpretaba a un chico que ingresaba en una base militar a través de su computadora y casi desata una guerra nuclear.

1984 Se crearon la publicación 2600, el CCC chaos computer club, Legion of doom y la división de fraude con tarjetas y computadoras del Servicio Secreto.

1988 Robert Tappan Morris soltó un gusano en Arpanet (como se llamaba Internet antes) y de ese modo infectó miles de servidores Unix. Fue enjuiciado y conde nado a cumplir 400 horas de trabajo social.

1992 Kevin Mitnick, luego de estar prófugo y ser atrapado por el FBI, fue sentenciado por robo de software e intrusiones en organizaciones.

1994 Vladimir Levin robó, desde San Petersburgo, a través de los sistemas de Citi bank, más de 10 millones de dólares por medio de transferencias a sus cuentas. En los dos años siguientes, desde otros bancos de los Estados Unidos, 300 mi llones de dólares se movilizaban electrónicamente de modo fraudulento.

Daños

- ***Tipificación de los daños por el hackeo nocivo***
- **Alteración:** modificación a conciencia datos / registros
- **Borrado:** Destruyendo información, sobre escritura.
- **Dar conocer información a terceros:** Irrumpiendo las normas de confidencialidad.
- **Sustracción:** Robando o guardando datos en almacenamientos externos.

HACKING ÉTICO

- **¿Por qué *ético*?**
- Para emular la metodología de un intruso informático y no serlo, tiene que haber ética de por medio.
- Premisa del policía y del ladrón
  - ¿Quién será un buen policía?
  - ¿Quién será un buen ladrón?

HACKING ÉTICO

Desde los inicios del hacking, siempre se ha mantenido una extraña dicotomia entre lo legal, lo ético y lo moral, siendo estas características, lo que resaltar para esclarecer la diferencia entre cada una de las amenazas existentes en la RED.

¿De dónde deriva la palabra hacker?

Deriva del Inglés HacK, que se usaba como forma familiar para describir como los técnicos telefónicos arreglaban las cajas defectuosas.

HACKING ÉTICO

- Los Hackers inventaron a los **Crackers** para diferenciar a aquel que analizaba y modificaba en una computadora con aquel que creaba un virus dañino o copiaba un software. Así, frente a una computadora ajena un Hacker y un Cracker no son la misma cosa.
- Por otro lado en algunas ocasiones un Hacker es muy útil porque siempre detecta un agujero en cualquier programa nuevo... El Cracker aprovecharía este error para entrar en el programa y copiarlo.

HACKING ÉTICO

- **Hacker**
- Un Hacker es una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

HACKING ÉTICO

- **Cracker**:
- Persona que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño.
- Persona que diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican.
- Persona que practica el cracking, acción de modificar el código fuente a un programa

HACKING ÉTICO

- ***Códigos de conducta*** del hacker ético

1. Hacer su trabajo de la mejor manera posible.
2. Dar el mejor reporte.
3. Acordar un precio justo.
4. Respetar el secreto.
5. No hablar mal ni inculpar a un administrador o equipo de programadores.
6. No aceptar sobornos.
7. No manipular o alterar resultados o análisis.
8. Delegar tareas específicas en alguien más capacitado.
9. No prometer algo imposible de cumplir.
10. Ser responsable en su rol y función.
11. Manejar los recursos de modo eficiente.

HACKING ÉTICO

❖ ***El proceso*** del hacker ético

1. La organización desea saber si sus sistemas son realmente seguros.
2. Selecciona y contrata un servicio profesional de ethical hacking.
3. Lo autoriza a realizar el trabajo mediante diversas pautas.
4. Planifican estratégicamente cómo se realizará y el alcance que tendrá.

HACKING ÉTICO

❖ ***El proceso*** del hacker ético (Continúa)

5. El profesional, luego de llevar a cabo los análisis preliminares, realiza su tarea imitando al atacante real, pero sin comprometer dato alguno.
6. Luego, analiza los resultados del security assessment.
7. Confecciona un reporte detallado para que la organización lo evalúe.
8. Soluciona lo vulnerable o mitiga lo potencial para dejar el sistema más seguro.
9. Se reafirma la defensa del sistema en general.
10. Se adoptan políticas de control y seguimiento (normativa).

HACKING ÉTICO

Motivaciones de los atacantes

Money
Ideology
Compromise
Ego

Consideraciones económicas
- Robo de información para posterior venta.
- Pago de rescates por información robada.

Diversión

Reconocimiento social

Ideología
- Ataques con contenido político

Un ejemplo de ataque motivado por la diversión

Un ejemplo de ataque motivado por una protesta.

Hacking

Fases de un ataque

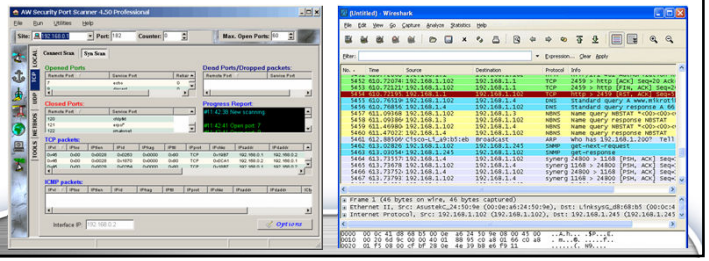
1. Descubrimiento y exploración del sistema.
2. Búsqueda de vulnerabilidades del sistema.
3. Explotación de las vulnerabilidades detectadas
4. Corrupción del sistema: modificación de programas, instalación de puertas traseras o troyanos, etc.
5. Eliminación de las pruebas. Eliminación de logs. Algunos atacantes llegan a arreglar la vulnerabilidad para que no pueda ser utilizada.

Hacking

❖El triángulo de la intrusión

Herramientas de hacking

1. **Scanner de puertos:** Detección de servicios instalados.
2. **Sniffers**: Dispositivos que capturan los paquetes de datos en tránsito



Herramientas de hacking

3. **Exploits**: Herramientas que buscan y explotan vulnerabilidades conocidas. Los ejemplos más comunes de los exploits de seguridad son de inyección SQL y XSS
4. **Backdoors kits** (herramientas de puerta traseras): Programas que permiten abrir y explotar puertas traseras.
5. **Rootkits**: Programas utilizados para ocultar puertas traseras en los propios ficheros ejecutables y servicios del sistema

Herramientas de hacking

6. **Autorooters**: Herramientas que pueden automatizar totalmente un ataque, realizando toda la secuencia de actividades para localizar un sistema, escanear sus posibles vulnerabilidades, explotarla y obtener el acceso al sistema.
7. **Password crakers**: Aplicaciones que permiten averiguar las contraseñas.
8. **Spoofing**: Herramienta que facilitan la ocultación y suplantación de direcciones IP. Dificultan la identificación del atacante.

Muchas Gracias

Favor leer la información