Hacking Ético

Jesús Torres Quesada

Conceptos

- Hacker
- Cracker
- Hacker ético

Elementos de seguridad

- Confidencialidad
- Autenticidad
- Integridad
- Disponibilidad

Qué puede hacer un hacker

- Reconocimiento
  - Pasivo o activo
  -
- Rastreo (escaneo)

- Acceso
  - Niveles de sistema operativo/aplicación
  - Redes
  - Denegacion de servicio

- Mantener el acceso

- Borrado de huellas

Reconocimiento

RECONOCIMIENTO

- Previo a cualquier ataque
- Información sobre el objetivo
- Reconocimiento pasivo:
  - Google hacking
  - Ingenieria social
  - Monitorización de redes de datos
- Reconocimiento Activo: Probar la red para detectar
  - Host accesibles
  - Puertos abiertos
  - Localización de routers
  - Detalles de OS y servicios

ESCANEO

Escaneo

- Es una fase de pre-ataque
- Se escanea la red, con la información de la fase previa
- Detección de vulnerabilidades y puntos de entrada
- Puede incluir scanners de puertos, network mapping, sweeping, vulnerability scanners, etc.

Obtener acceso

Obtener acceso

- Se refiere al ataque propiamente dicho

- Haciendo uso por ejemplo de un exploit o bug
  - stack-based buffer overflows
  - DoS
  - session hijacking
  - password filtering

- EL hacker puede obtener acceso a nivel de S.O. o de red

Mantener acceso

Mantener acceso

- Mantenimiento del acceso, reteniendo los privilegios obtenidos

- A veces se blinda el sistema contra otros posibles hackers, protegiendo sus puertas traseras, rootkits y troyanos

Borrado de huellas

Borrado de huellas

- Se intenta no ser descubierto

- Hay técnicas más intrusivas y más delatoras que otras

Tipos de hacker

- Black hats, tambien llamados crackers
- White Hats
- Gray Hats

Que puede hacer un hacker ético

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.” Sun Tzu, Art of War.

Intenta responder a las siguientes preguntas

- ¿Qué puede saber un intruso de su objetivo? Fases 1 y 2
- ¿Qué puede hacer un intruso con esa información? Fases 3 y 4
- ¿Se podría detectar un intento de ataque? Fases 5 y 6

Habilidades de un hacker ético

- Experto de algún campo de la informática
- Amplios conocimientos de diversas plataformas (windows, Unix, Linux)
- Conocimientos de redes
- Conocimientos de hardware y software

Qué debe hacer un hacker ético

- Preparación: Se debe tener un contrato firmado.

- Gestión: Preparación de un informe donde se detallen las pruebas y posibles vulnerabilidades detectadas

- Conclusión: Comunicación a la empresa del informe y de las posibles soluciones

Modos de hacking ético

- Redes remotas: simulación de un ataque desde internet
- Redes locales: simulación de un ataque desde adentro
- Ingeniería social: probar la confianza de los empleados
- Seguridad física: accesos físicos

Tipos de tests de seguridad

- Black box
- White box
- Gray box o test interno

Cual es el resultado del trabajo de un hacker ético

- Ethical Hacking Report
- Detalles de los resultados de las actividades y pruebas de hacking realizadas. Comparación con lo acordado previamente en el contrato
- Se detallarán las vulnerabilidades y se sugiere cómo evitar que hagan uso de ellas
- Debe ser confidencial

Hackers famosos

- Paul Baran, considerado el primer hacker de la historia.
- Kevin Mitnick, el gobierno de USA lo acusó de haber sustraído información del FBI y arrestado, ahora tiene una empresa de seguridad.
- Mark Abene lideró en New York el grupo de hacker llamado Masters of Deception.
- John Draper, Captain Crunch, introdujo el concepto de Phreaker.
- Dennis Ritchie y Ken Thompson (creador de C y creadores de Unix)

Hackers famosos

- Steve Jobs y Steve Wozniak (Apple)
- Linus Torvalds (Linux)
- Richard Stallman (Emacs, GNU y FSF)
- Bill Gates (Microsoft)

Algunas herramientas

- Nmap: ports scanner
- Nessus: vulnerability scanner
- Nikto: vulnerability scanner
- Kismet: wireless networks sniffing
- Metasploit: vulnerability scanner
- Nagios: Traffic Monitoring Tool
- Tripwire: Rootkit Detector
- John the Ripper: Password Cracker