

Accesos no autorizados

Mayo 2015

Introducción

- Existen varios pasos para completar este proceso
- Las fases ejecutadas incluyen:
 - **Ruptura/Descifrado de contraseñas**
 - Escalamiento de privilegios
 - Ejecución de aplicaciones
 - Ocultamiento de archivos
 - Cubrimiento de rastros
 - Pruebas de penetración

Romper contraseñas

Cracking Passwords

- Se utilizan técnicas para recuperar contraseñas
- La mayoría de estas técnicas aprovechan la debilidad de las contraseñas
 - Muchas personas optan por usar contraseñas fáciles de recordar: **nombres de mascotas, nombres de pila, años de nacimiento, etc.**

Complejidad en las contraseñas

- Contraseñas con letras, caracteres especiales y números: **kam@3**
- Contraseñas con números: **123456**
- Contraseñas con caracteres especiales: **@#\$\$!**
- Contraseñas con letras y números: **ad123**
- Contraseñas con letras: **perro**
- Contraseñas con letras y caracteres especiales: **asd#%**
- Contraseñas con caracteres especiales y números: **334~%#@~**

Técnicas

- Ataque mediante diccionario
 - Un diccionario es cargado para intentar acceder con un usuario y contraseña
- Ataque por fuerza bruta
 - Combina caracteres hasta que la contraseña es descifrada
- Ataque híbrido
 - Depende de un diccionario, utiliza palabras de un diccionario y las combina con números y símbolos: system32, admin1
- Ataque sílaba
 - Es utilizado cuando las contraseñas no necesariamente son palabras existentes, se pueden combinar palabras del diccionario
- Ataque basado en reglas
 - Se tiene información sobre la contraseña: longitud, uso de números o letras. Combina fuerza bruta, diccionario y sílaba

Tipos de ataques

- Pasivos en línea
 - Monitorear
 - Recolectar datos
 - Solo se observa:
 - Sniffing
 - Man-in-the-middle
 - Replay

Tipos de ataques

- Activo offline/fuera de línea
 - Contraseñas y usuarios almacenados localmente en bd/archivos del sistema
 - Se aprovechan vulnerabilidades de los algoritmos de cifrado
- Ataques no electrónicos
 - No requiere conocimientos técnicos
 - Ingeniería Social
 - Analizar basura, etc.

Tipos de ataques

- Activo en línea
 - Trojans/Spyware, keylogger
 - Inyección de tablas hash
 - Phishing