DAVID FELIPE GUSTIN RIVAS

1 Juego

Es una técnica de ciberseguridad en la que un atacante intenta adivinar una contraseña, una clave de cifrado o cualquier otra forma de autenticación, probando sistemáticamente todas las combinaciones posibles hasta encontrar la correcta. Este método de prueba y error, exhaustivo pero potencialmente lento dependiendo de la complejidad de la contraseña, se utiliza para descifrar credenciales y acceder a sistemas protegidos por autenticación. El atacante identifica un sistema o cuenta objetivo y emplea herramientas de software automatizadas que generan y prueban combinaciones de caracteres, incluyendo diccionarios de contraseñas comunes, listas de palabras y caracteres especiales, y generadores de combinaciones aleatorias. El proceso consiste en probar combinaciones una por una, pudiendo durar desde segundos hasta semanas, hasta encontrar la correcta. La probabilidad de éxito aumenta con contraseñas débiles o cortas, mientras que las contraseñas largas y complejas, que combinan letras mayúsculas y minúsculas, números y símbolos, son mucho más difíciles de descifrar. Para prevenir estos ataques, se recomienda utilizar contraseñas fuertes y únicas, habilitar la autenticación de dos factores (2FA), configurar el bloqueo de cuentas tras intentos fallidos, limitar los intentos de inicio de sesión y utilizar captchas para evitar ataques automatizados.

17/17

David Felipe Gustin Rivas

2 Juego

Es una técnica de ciberseguridad utilizada para descifrar contraseñas, claves de cifrado o acceder a sistemas protegidos por autenticación, mediante la prueba sistemática de palabras y frases comunes que se encuentran en diccionarios y listas predefinidas. Este tipo de ataque de fuerza bruta se enfoca en probar contraseñas que son palabras o frases comunes, en lugar de probar todas las combinaciones posibles de caracteres, basándose en la suposición de que muchos usuarios eligen contraseñas débiles y predecibles, como palabras del diccionario, nombres propios, fechas de nacimiento o combinaciones sencillas. Aunque es más rápido que un ataque de fuerza bruta pura, su efectividad depende de la calidad y el tamaño del diccionario utilizado, así como de la debilidad de las contraseñas objetivo, y se puede automatizar utilizando herramientas de software especializadas. El atacante identifica un sistema o cuenta protegida por una contraseña que desea descifrar y utiliza un diccionario o una lista de palabras y frases comunes, que pueden incluir palabras del diccionario en diferentes idiomas, nombres propios, fechas, combinaciones de números y letras, y contraseñas utilizadas con frecuencia. Las herramientas de software prueban automáticamente las palabras del diccionario contra el sistema o la cuenta objetivo, incluyendo funciones para generar variaciones de las palabras del diccionario. El proceso consiste en probar las palabras del diccionario, una por una, hasta encontrar la contraseña correcta, pudiendo durar desde segundos hasta horas. Si la contraseña objetivo se encuentra en el diccionario o es una variación de una palabra del diccionario, el atacante tendrá éxito, mientras que las contraseñas fuertes y aleatorias son mucho más difíciles de descifrar. Existen variaciones y mejoras de los ataques de diccionario, como el ataque de diccionario híbrido, que combina un ataque de diccionario con un ataque de fuerza bruta, y el ataque de diccionario basado en reglas, que utiliza reglas para generar variaciones de las palabras del diccionario. Para prevenir estos ataques, se recomienda utilizar contraseñas fuertes y aleatorias, habilitar la autenticación de dos factores (2FA), configurar el bloqueo de cuentas tras intentos fallidos, limitar los intentos de inicio de sesión y monitorear la actividad sospechosa.

24/24

David Felipe Gustin Rivas

3 juego

Es una técnica de ciberseguridad que explota la información obtenida de la implementación física de un sistema, en lugar de atacar directamente las vulnerabilidades del software o del algoritmo. Este tipo de ataque se basa en la observación y el análisis de las emisiones o efectos secundarios de un sistema informático, como el consumo de energía, el tiempo de ejecución, las emisiones electromagnéticas o el sonido, y se utiliza para obtener información confidencial, como claves de cifrado o datos encriptados, sin necesidad de descifrar el algoritmo de cifrado en sí. Es un ataque no invasivo que no requiere modificar el software o el hardware del sistema objetivo, y su efectividad depende de la precisión de las mediciones y del análisis de los datos obtenidos, siendo especialmente eficaz contra sistemas criptográficos y dispositivos embebidos. El atacante identifica un sistema o dispositivo que emite información de canal lateral durante su funcionamiento, y utiliza herramientas especializadas para medir y registrar las emisiones o efectos secundarios del sistema objetivo, como osciloscopios, analizadores de espectro, micrófonos o cámaras térmicas. Luego, analiza los datos recopilados para identificar patrones y correlaciones que puedan revelar información confidencial, utilizando técnicas de análisis estadístico y procesamiento de señales para extraer la información deseada. Finalmente, utiliza la información obtenida para descifrar contraseñas, claves de cifrado o acceder a datos protegidos. Los tipos comunes de ataques de canal lateral incluyen ataques de tiempo, que analizan el tiempo que tarda un sistema en realizar ciertas operaciones; ataques de consumo de energía, que miden las variaciones en el consumo de energía; ataques electromagnéticos, que analizan las emisiones electromagnéticas; y ataques acústicos, que graban y analizan los sonidos emitidos por un dispositivo. Para prevenir estos ataques, se recomienda implementar contramedidas criptográficas, diseñar hardware seguro y monitorear y detectar anomalías. Es importante destacar que los ataques de canal lateral son complejos y requieren conocimientos especializados, pero su potencial para comprometer la seguridad de los sistemas los convierte en una amenaza importante en el panorama de la ciberseguridad.

DAVID FELIPE GUSTIN RIVAS

4 juego

Es una técnica de ciberseguridad que manipula a las personas para que revelen información confidencial, realicen acciones perjudiciales o den acceso a sistemas protegidos, aprovechándose de la psicología humana y la confianza en lugar de explotar vulnerabilidades técnicas. Este conjunto de técnicas manipula psicológicamente a las personas para obtener información confidencial, acceso a sistemas o la realización de acciones específicas, basándose en la explotación de la confianza, la curiosidad, el miedo o la urgencia de las víctimas. Es un ataque no técnico, centrado en la manipulación humana, cuya efectividad depende de la habilidad del atacante para engañar a la víctima, siendo difícil de detectar y prevenir debido a su aprovechamiento de las emociones y la psicología humana. El atacante recopila información sobre la víctima u organización objetivo y utiliza técnicas de manipulación psicológica como phishing, pretexting, baiting, quid pro quo y tailgating para engañarla. Luego, utiliza la información obtenida o el acceso logrado para realizar acciones perjudiciales como robo de datos, instalación de malware o fraude financiero. Los tipos comunes de ataques de ingeniería social incluyen phishing, vishing, smishing e ingeniería social inversa. Para prevenir estos ataques, se recomienda la capacitación y concientización de los usuarios, la implementación de políticas de seguridad, la autenticación de dos factores (2FA), la verificación de identidad y el fomento de una cultura de seguridad en la organización.