Diccionario de contraseñas y ataques de fuerza bruta

Contenido

1. Introducción a los ataques de diccionario de contraseñas y fuerza bruta
2. Identificación de contraseñas débiles
3. Herramientas y técnicas de ataque
4. Mitigación de ataques de diccionario de contraseñas y fuerza bruta

Fuerza bruta: nociones básicas

1. Los atacantes utilizan programas automatizados o scripts para probar todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.
2. Normalmente, se comienza con secuencias numéricas, luego combinaciones alfanuméricas y finalmente caracteres especiales.
3. Este tipo de ataque es intensivo en recursos y puede llevar tiempo, especialmente con contraseñas largas y complejas.
4. Los atacantes pueden utilizar técnicas como la generación de contraseñas basadas en patrones comunes o en información personal para aumentar las posibilidades de éxito.

Diccionarios: nociones básicas

1. Los atacantes utilizan listas predefinidas de palabras comunes o frases conocidas como diccionarios.
2. Prueban estas palabras o combinaciones de palabras en un intento de adivinar la contraseña.
3. Los diccionarios pueden contener palabras comunes, nombres populares, términos relacionados con el usuario objetivo, datos personales u otras palabras que se cree que las personas utilizan con frecuencia como contraseñas.
4. Los atacantes pueden personalizar los diccionarios según el contexto o la información conocida sobre el objetivo para aumentar las posibilidades de éxito.

Fuerza bruta y diccionarios

Diferencias	Descripción
Ataque de Fuerza Bruta	Prueba todas las combinaciones posibles de caracteres para encontrar una contraseña. Es intensivo en recursos y puede llevar tiempo, especialmente con contraseñas largas y complejas.
Ataque de Diccionario	Utiliza una lista predefinida de palabras comunes o frases para adivinar una contraseña. Es más rápido, ya que se basa en la probabilidad de que las personas utilicen contraseñas comunes.

Similitudes
Ambos son métodos utilizados para adivinar contraseñas y comprometer la seguridad de sistemas.
Se basan en la premisa de que las contraseñas pueden ser adivinadas o encontradas mediante técnicas de prueba y error.

Identificación de contraseñas débiles

Característica	Descripción
Longitud corta	La contraseña tiene pocos caracteres, lo que la hace más susceptible a ataques de fuerza bruta.
Uso de información personal	La contraseña contiene información personal como nombres, fechas de nacimiento o números de teléfono.
Palabras del diccionario	La contraseña está formada por palabras comunes que se pueden encontrar en un diccionario.
Patrones predecibles	La contraseña sigue patrones secuenciales o predecibles, como "123456" o "qwerty".
Solo caracteres alfanuméricos	La contraseña no incluye caracteres especiales ni símbolos, limitando su complejidad.
Uso de contraseñas comunes	La contraseña es una de las contraseñas más utilizadas, como "password" o "123456789".
No se actualiza regularmente	La contraseña se mantiene sin cambios durante períodos prolongados, lo que la hace más vulnerable.

Herramientas y técnicas de ataque (BF)

Herramienta	Descripción
THC Hydra	THC Hydra es una herramienta de fuerza bruta muy popular y versátil que admite una amplia gama de protocolos y servicios, como SSH, FTP, HTTP, SMB, entre otros.
Medusa	Medusa también puede utilizarse para ataques de fuerza bruta, donde intenta múltiples combinaciones de contraseñas para autenticarse en un objetivo.
Ncrack	Ncrack es una herramienta de fuerza bruta de código abierto que está diseñada principalmente para realizar ataques de fuerza bruta en servicios de red, como SSH, RDP, entre otros.
Aircrack-ng	Aircrack-ng es una suite de herramientas muy popular utilizada para pruebas de seguridad en redes inalámbricas. Incluye una herramienta de fuerza bruta para descifrar claves WPA/WPA2.
Hydra	Además de su capacidad para realizar ataques de diccionario, Hydra también puede utilizarse para realizar ataques de fuerza bruta probando múltiples combinaciones de contraseñas.

Herramientas y técnicas de ataque (Diccionarios)

Herramienta	Descripción
Hydra	Hydra es una herramienta de fuerza bruta muy conocida y flexible que admite varios protocolos de autenticación, como HTTP, FTP, SSH, entre otros.
Medusa	Medusa es otra herramienta popular de fuerza bruta que puede utilizarse para atacar una amplia gama de protocolos, incluidos FTP, SSH, Telnet, HTTP, entre otros.
John the Ripper	John the Ripper es una herramienta de cracking de contraseñas que admite múltiples modos de ataque, incluido el ataque de diccionario. Es ampliamente utilizado y altamente configurable.
Hashcat	Hashcat es una potente herramienta de recuperación de contraseñas que admite una amplia variedad de algoritmos de hash y modos de ataque, incluido el ataque de diccionario.
Cain and Abel	Cain and Abel es una herramienta de recuperación de contraseñas para Windows que también puede realizar ataques de diccionario y fuerza bruta en redes locales y contraseñas almacenadas.

Practica

Actividad: Desarrolla un ataque de fuerza bruta y un ataque de diccionario usando hydra.

Objetivos:

1. Aprender cómo se desarrolla cada uno de estos ataques
2. Determinar cuál de los dos es más efectivo y bajo qué circunstancias
3. Reflexiona sobre las consecuencias de un ataque de este tipo cuando se efectua sobre un router o una puerta de enlace

Mitigación / Prevención de fuerza bruta

Técnica	Descripción
Uso de contraseñas fuertes	Establecer políticas de contraseñas que requieran una combinación de caracteres alfanuméricos, símbolos y letras mayúsculas y minúsculas.
Bloqueo de cuentas	Implementar mecanismos que bloqueen o restrinjan el acceso a una cuenta después de un número determinado de intentos de inicio de sesión fallidos.
Control de tiempo de respuesta	Configurar un retraso entre intentos de inicio de sesión para ralentizar los ataques de fuerza bruta.

Mitigación / Prevención de diccionario

Técnica	Descripción
Uso de contraseñas fuertes	Establecer políticas de contraseñas que requieran una combinación de caracteres alfanuméricos, símbolos y letras mayúsculas y minúsculas.
Implementación de CAPTCHA	Agregar pruebas CAPTCHA a las páginas de inicio de sesión para verificar que el usuario sea humano y no un programa automatizado que realiza ataques de fuerza bruta.
Monitoreo de actividad	Supervisar los registros de actividad de inicio de sesión y establecer alertas para detectar patrones inusuales, como múltiples intentos de inicio de sesión fallidos desde una misma dirección IP.