**Ingeniería de Seguridad del Software**

**Práctica de Laboratorio No 2:**

**Tema:** Evaluación de herramientas de fuerza bruta en Kali Linux

**Objetivo de Aprendizaje:** Los estudiantes comprenderán el funcionamiento de las herramientas de fuerza bruta incluidas en Kali Linux al configurarlas y ejecutarlas en un entorno controlado utilizando un entorno virtual de red, evaluando su efectividad y limitaciones**.**

**Topología del experimento**

1. Kali Linux.
2. Una máquina objetivo con un sistema operativo como Metasploitable2, o un Servidor SSH o Web server.
3. Documentos con usuarios y contraseñas para los ataques (Diccionarios).
4. Lista de herramientas sugeridas: **John the Ripper, Hydra, Medusa, Burp Suite, o Hashcat**.

**Marco Teórico:**

Un ataque de fuerza bruta está dirigido contra la autenticación en el contexto de seguridad de la información. Vamos a desglosar los conceptos para entenderlo mejor:

**Autenticación vs Identificación**

**Identificación:** Proceso de declarar quién eres.

**Ejemplo**: Proporcionar un nombre de usuario o un identificador único, como un correo electrónico.

Pregunta clave: ¿Quién eres?

**Autenticación**: Proceso de verificar que eres quien dices ser.

**Ejemplo:** Proporcionar una contraseña, token, huella digital, o responder a un desafío basado en un factor de autenticación.

Pregunta clave: ¿Puedes demostrarlo?

**El ataque de fuerza bruta**

Un ataque de fuerza bruta intenta adivinar credenciales de autenticación, como contraseñas o claves. Se realiza probando sistemáticamente combinaciones de contraseñas o valores posibles hasta encontrar la correcta.

**Propósito principal**: Comprometer la autenticación (demostrar que se tienen las credenciales válidas).

No compromete directamente la identificación, porque esta etapa ya suele estar completa (el atacante usualmente conoce o asume un identificador, como un nombre de usuario).

**Desarrollo:**

**Ejecución de los Ataques utilizando John the Ripper**: Crackear un hash de contraseña

**Extraer hashes con unshadow:**

unshadow /etc/passwd /etc/shadow > hashes.txt

**Ejecutar John:**

john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

**Crear el archivo hashes.txt**

El archivo hashes.txt es un archivo que contiene hashes de contraseñas, y es utilizado por herramientas como **John the Ripper** o **Hashcat** para crackear contraseñas. Para construirlo, necesitas extraer los hashes de contraseñas desde un sistema o crearlos manualmente.

**1. Extraer hashes de un sistema Linux**

Si estás trabajando en un entorno controlado con un sistema Linux, los hashes de contraseñas se almacenan en los archivos **/etc/shadow** y **/etc/passwd.** Sigue estos pasos para extraerlos:

**Paso 1: Acceso al sistema**

Asegúrate de tener permisos de superusuario (root) en el sistema donde deseas extraer los hashes.

**Paso 2: Combinar passwd y shadow**

Utiliza el comando unshadow para combinar los archivos /etc/passwd y /etc/shadow en un formato que pueda usar **John the Ripper**.

bash

unshadow /etc/passwd /etc/shadow > hashes.txt

Esto generará un archivo hashes.txt que contiene las credenciales (en formato hash) de las cuentas locales.

**¿Qué es el archivo rockyou.txt?**

El archivo **rockyou.txt** es una lista de contraseñas comúnmente utilizada en pruebas de penetración y auditorías de seguridad. Contiene millones de contraseñas filtradas, ordenadas por popularidad, que provienen de una brecha masiva de datos del sitio de redes sociales RockYou en 2009. Es ampliamente empleado para realizar ataques de fuerza bruta y pruebas de diccionario en herramientas como Hydra, John the Ripper, Medusa, y Hashcat.

**Ubicación del archivo en Kali Linux**

El archivo rockyou.txt está preinstalado en Kali Linux, pero **está comprimido** por defecto para ahorrar espacio en disco. Puedes encontrarlo en la siguiente ruta:

/usr/share/wordlists/rockyou.txt.gz

**Cómo descomprimir el archivo rockyou.txt**

Para usar este archivo, primero necesitas descomprimirlo.

gunzip /usr/share/wordlists/rockyou.txt.gz

**Ahora el archivo estará disponible en:**

/usr/share/wordlists/rockyou.txt

**Documentación**

Cada grupo debe registrar:

* Configuración del entorno.
* Comandos utilizados.
* Resultados obtenidos (éxito/fallo, tiempo, etc.).
* Limitaciones observadas en la herramienta.

**Plenaria de Análisis y Discusión**

Cada grupo presenta sus hallazgos al resto de la clase:

* Comparar la efectividad de las herramientas.
* Identificar estrategias para mitigar ataques de fuerza bruta.

**Conclusiones**

Un ataque de fuerza bruta **se dirige contra la autenticación**, ya que su objetivo es adivinar contraseñas, claves o factores de acceso relacionados con este proceso. Sin embargo, puede complementarse con ataques contra la identificación, como la enumeración de usuarios, para obtener más información sobre posibles objetivos.

La efectividad de los ataques de fuerza bruta depende de varios factores, como la complejidad de las contraseñas, las limitaciones impuestas por el sistema objetivo (por ejemplo, bloqueos tras múltiples intentos fallidos), y la calidad del diccionario utilizado.

En la práctica, los ataques tuvieron mayor éxito contra configuraciones inseguras o contraseñas débiles, resaltando la importancia de implementar contraseñas fuertes y mecanismos de defensa como límites de intentos y autenticación multifactor.

Los resultados demuestran que, aunque efectivos en ciertos escenarios, los ataques de fuerza bruta son altamente dependientes del contexto y consumen tiempo y recursos, especialmente contra sistemas bien configurados.

**Referencias**

* Kali Linux Documentation. (2024). *Tools Listing*. Recuperado de https://www.kali.org/tools/
* Offensive Security. (2024). *Metasploitable 2*. Recuperado de https://sourceforge.net/projects/metasploitable/
* Bishop, M. (2019). *Introduction to Computer Security*. Boston, MA: Addison-Wesley.
* Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography*. Chapman & Hall/CRC.
* W Fuertes, M Macas, Ciberseguridad: Del ciber-crimen a los ataques ciber-físicos, Comité Editorial de la ESPE, Sangolquí, Ecuador. ISBN: 978-9942-765-88-8 1, 190