SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

Lab 3.3

Ataques de contraseñas

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Continuando con los mecanismos de hacking, otra forma de ingresar a un sistema es a través del tradicional inicio de sesión (logon).

Para ello el pentester (hacker) necesita conseguir las credenciales requeridas por el proceso de autenticación de dicho sistema, lo cual se logra usualmente a través de un ataque de claves.

2. TIPOS DE ATAQUES

Fuerza bruta

Basados en diccionarios

Híbridos

Mediante ingeniería social

Usando sniffers

3. ATAQUES DE FUERZA BRUTA

Se prueba "todo el espacio" de combinaciones posibles de claves.

$P = n^x$

P = Permutaciones posibles

n = valores de donde elegir

x = cantidad de valores a elegir

Ejemplo

SUPONGAMOS UNA CLAVE DE 2 CARACTERES NUMÉRICOS. DADO QUE LOS NÚMEROS VAN DEL 0 AL 9 ENTONCES TENEMOS 10 CARACTERES POSIBLES.

$P=N^X$

N=10; X=2 => P=100

ASUMIENDO QUE EL SISTEMA VÍCTIMA NO TIENE NINGÚN MECANISMO DE BLOQUEO DE INTENTOS FALLIDOS.

¿PERO QUÉ TAL QUE LA CLAVE NO ES DE 2 CARACTERES, SINO DE 20 Y LOS CARACTERES POSIBLES SON EL ALFABETO LATINO TRADICIONAL (26 CARACTERES) MÁS CUATRO SÍMBOLOS ESPECIALES * ! - _ Y LA CLAVE ES SENSIBLE A MAYÚSCULAS? EN ESE CASO TENDRÍAMOS QUE:

$P = (26*2 + 4)^{20}$

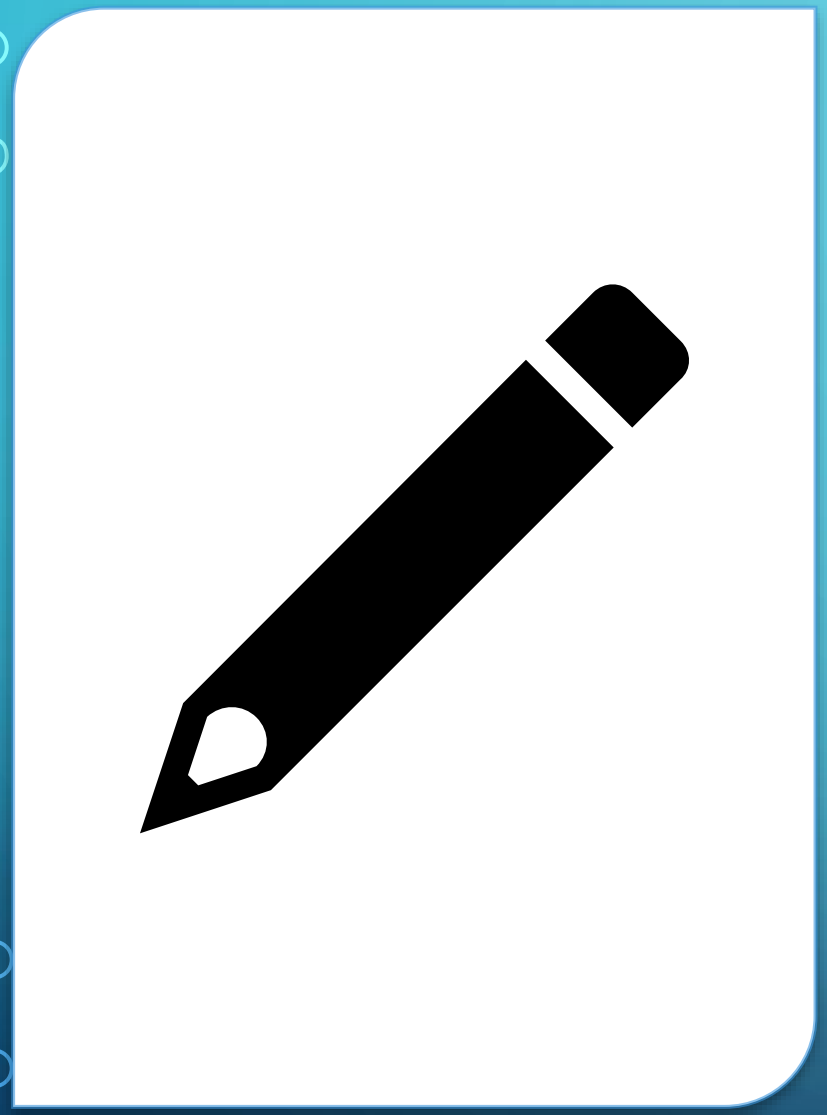
$P = 9.2 * 10^{34}$

4. ATAQUES POR DICCIONARIO

Se recurre a un diccionario de claves previamente armado para ir probando en orden cada una de las claves contenidas en el mismo.

Las personas tendemos a usar como claves palabras que nos resulten familiares, en algunos casos combinadas con números o símbolos.

Ejemplo



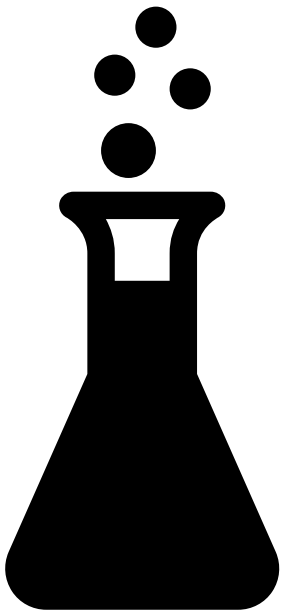
REVISAR EL CONTENIDO DE ALGÚN DICCIONARIO YA COMPILADO COMO POR EJEMPLO ROCKYOU.TXT DE KALI LINUX.

4. ATAQUES HÍBRIDOS

Como su nombre sugiere, en este tipo de ataques se combina una lista de palabras contenida en un diccionario con caracteres adicionales generados automáticamente (fuerza bruta).

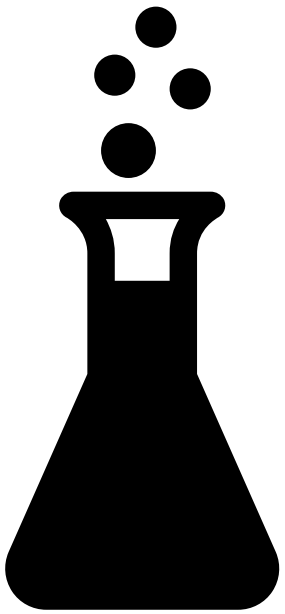
Se crea así un patrón.

Laboratorio



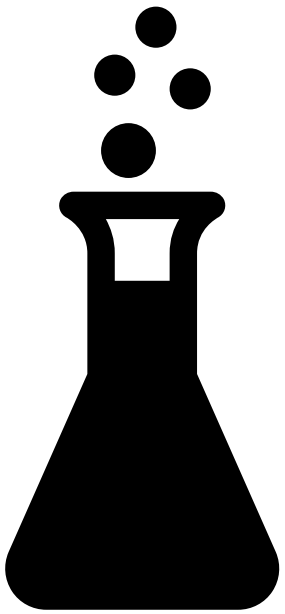
OBTENIENDO CLAVES CON MEDUSA

Laboratorio



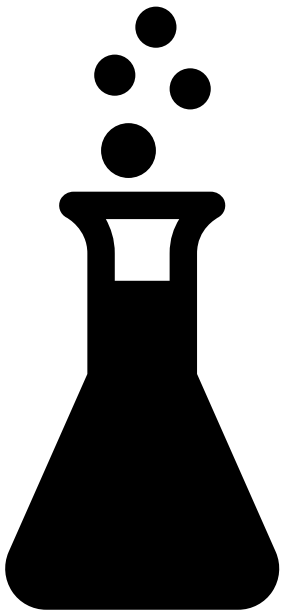
OBTENIENDO CLAVES CON JOHN THE RIPPER

Laboratorio



GENERANDO DICCIONARIOS CON CRUNCH

Laboratorio



OBTENIENDO CLAVES CON HASHCAT