ATAQUES DE FUERZA BRUTA

Un Ataque por Fuerza Bruta se basa en **conseguir un par usuario-contraseña probando gran cantidad de combinaciones hasta conseguir el correcto**

1.

INTRODUCCIÓN

INTRODUCCIÓN

- Ataques de fuerza bruta
- Sistemas de autenticación:
  Usuario y Contraseña
- Herramientas que prueban combinaciones automáticamente

2.

TIPOS DE FUERZA BRUTA

FUERZA BRUTA vs DICCIONARIO

- Efectivo pero costoso
- Combinación de todos los posibles caracteres

aaaaa
aaaab
aaaac
…
zzzzx
zzzzy
zzzzz

- Fichero con posibles contraseñas (*wordlist*)
- Prueba cada palabra

pass
cumpleaños
rex
…
baloncesto
Jose1990
test

PUNTOS A TENER EN CUENTA

- Tipo de servicio
- ¿ ‘Contraseña’ vs ‘Usuario y Contraseña’?
- Obtención de buenos diccionarios

    - Idiomas
    - Servicios, por defecto
    - Contraseñas populares
    - Dificultades
    - …

3.

DICCIONARIOS

CREACIÓN DE DICCIONARIOS

- Crear contraseñas basadas en: números, letras (mayúsculas y/o minúsculas), caracteres especiales o una mezcla.

- Se generarán todas las posibilidades posibles: gran coste

- Ejemplo: *Crunch*

ATAQUE DE DICCIONARIOS

- Gran cantidad de opciones y servicios a los que atacar (*ftp*, *irc*, *mysql*, pop3, *snmp*, ssh, *telnet*…)
- Importante saber puertos y servicios disponibles (Nmap)
- Se comparará el *hash*

4.

HERRAMIENTAS

ALGUNAS HERRAMIENTAS

- ***Medusa*** (http://foofus.net/goons/jmk/medusa/medusa.html)

Software para atacar a nivel de fuerza bruta basándonos en diccionarios de palabras, muy estable, sencillo, rápido y para bastantes servicios.

- ***Ncrack*** (https://nmap.org/ncrack/)

Sintaxis similar a la de Nmap y permite auditorías sobre múltiples hosts. Interfaz flexible permitiendo control total al usuario sobre las operaciones de red. Entre los protocolos soportados encontramos RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, and telnet.

HERRAMIENTAS (***Crunch*** & ***Hydra***)

- Construcción de palabras de longitud mínima y máxima 6 caracteres. (‘*xyz123*’)

  crunch 6 6 xyz123

- Ataque por fuerza bruta a un RDP con el usuario ‘*admin*’ contraseñas en ‘*pass.txt*’ y a la IP/servicio objetivo

  hydra -l admin -P pass.txt 192.168.1.20 rdp