infØrSÉNIA

Taller: Retos CTF de ciberseguridad

La Sénia
Institut d'Educació Secundària
Paiporta

John the Ripper

- Herramienta para recuperación de contraseñas por ataques de fuerza bruta
- Basada en diccionarios
- Uso de convertidores de ficheros

Ejemplo de uso

```
john --wordlist=/usr/share/wordlists/rockyou.txt file.txt
```

Criptografía

- Clave simétrica
- Clave asimétrica (clave pública)
- Cifrado de mensajes

Ejemplo de uso

```
gpg -a --encrypt -o mensaje.txt.asc --recipient Pepito mensaje.txt
```

nmap

- Herramienta para escanear redes
- Múltiples posibilidades: buscar equipos en la red, buscar servicios a la escucha, etc.

Ejemplos de uso

```
nmap -sn 192.168.0.0/24
nmap -sC -sV 192.168.0.135
```

Gobuster

- Herramienta para listar directorios ocultos en servidores web
- Basada en diccionarios
- También puede buscar ficheros

Ejemplo de uso

```
gobuster dir -u URL -w /usr/share/wordlists/dirbuster/directory-list-2.3-big.txt
```

Taller: Retos CTF de ciberseguridad

Codificaciones habituales de passwords en retos CTF

- base32
- base64
- brainfuck

Ejemplo de uso

```
echo “GEZDGNBVGYFA====” |base32 -d
  --> Resultado: 123456
echo “ZXN0ZXJub2NsZWlkb21hc3RvaWRlbw==” |base64 -d
--> Resultado: esternocleidomastoideo
```

Escalado de privilegios

- Consiste en aprovechar vulnerabilidades para, a partir de un usuario corriente, conseguir permisos de root en el sistema.
- Búsquedas en el sistema (`find`)
- Consulta a páginas de Pentesting: ej. GTFOBins