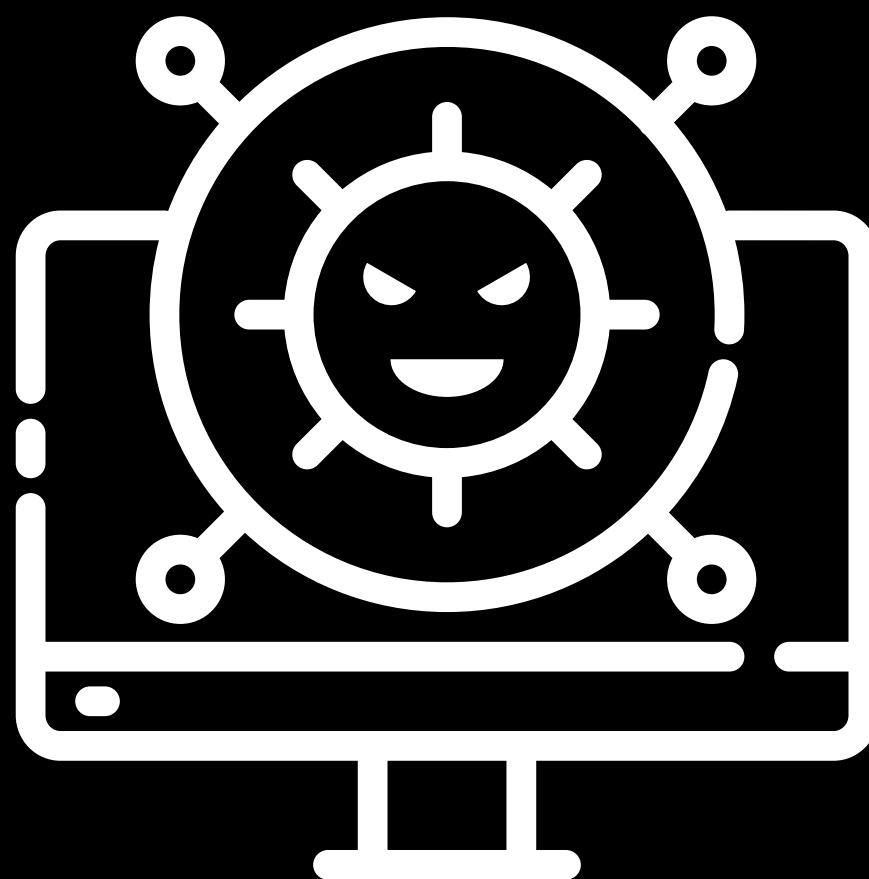
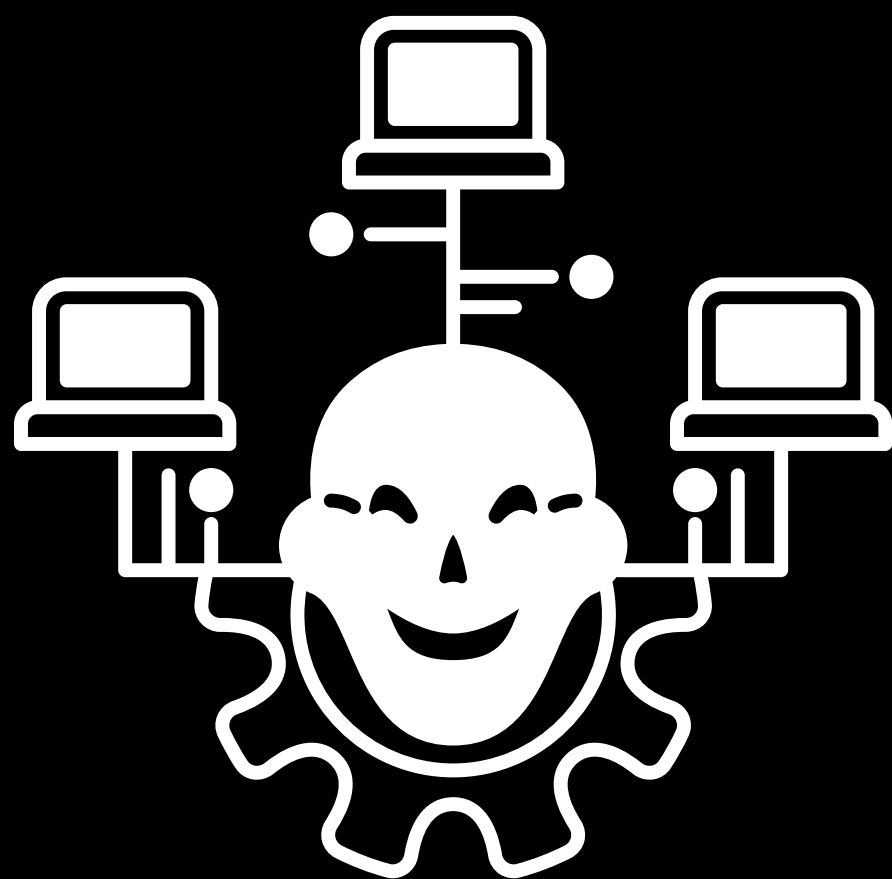


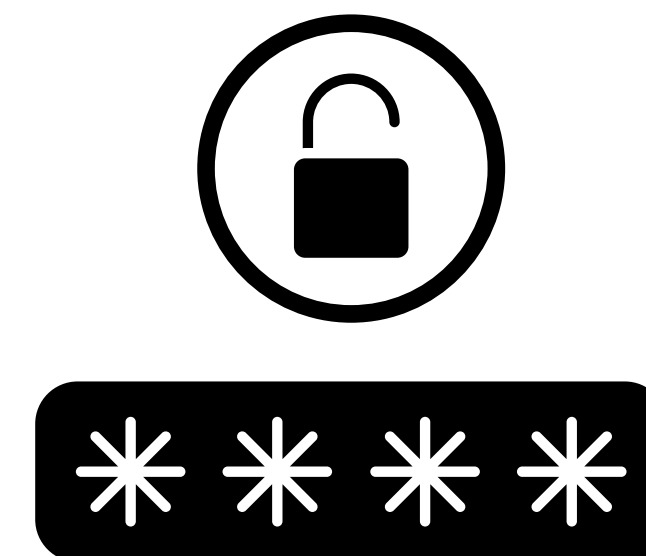
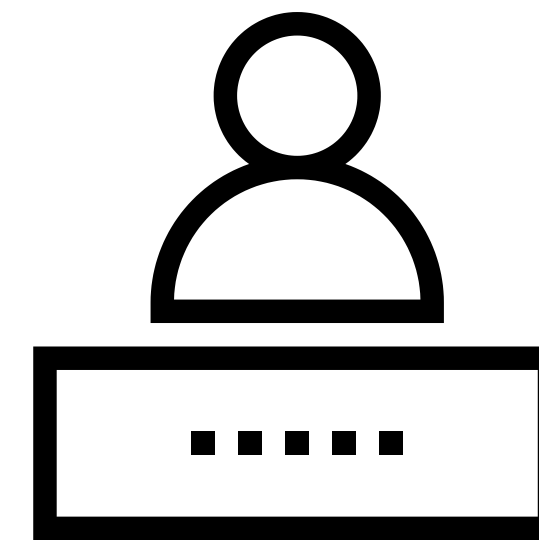
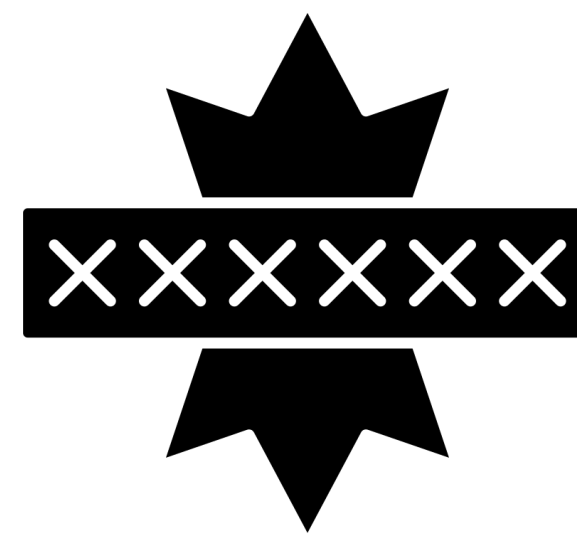
**ATAQUE DE FUERZA BRUTA**

# Motivaciones de los atacantes



# Tipos de ataques de fuerza bruta

- Ataques simples
- Ataques de diccionario
- Ataques híbridos
- Ataques inversos
- Relleno de credenciales



# Herramientas y técnicas

- Software especializado      Optimización por GPU

- John the ripper

- Aircrack-ng

GPU > CPU

x250



```
Aircrack-ng 1.7

[00:00:02] 23828/14344158 keys tested (10723.30 k/s)

Time left: 22 minutes, 15 seconds      0.17%

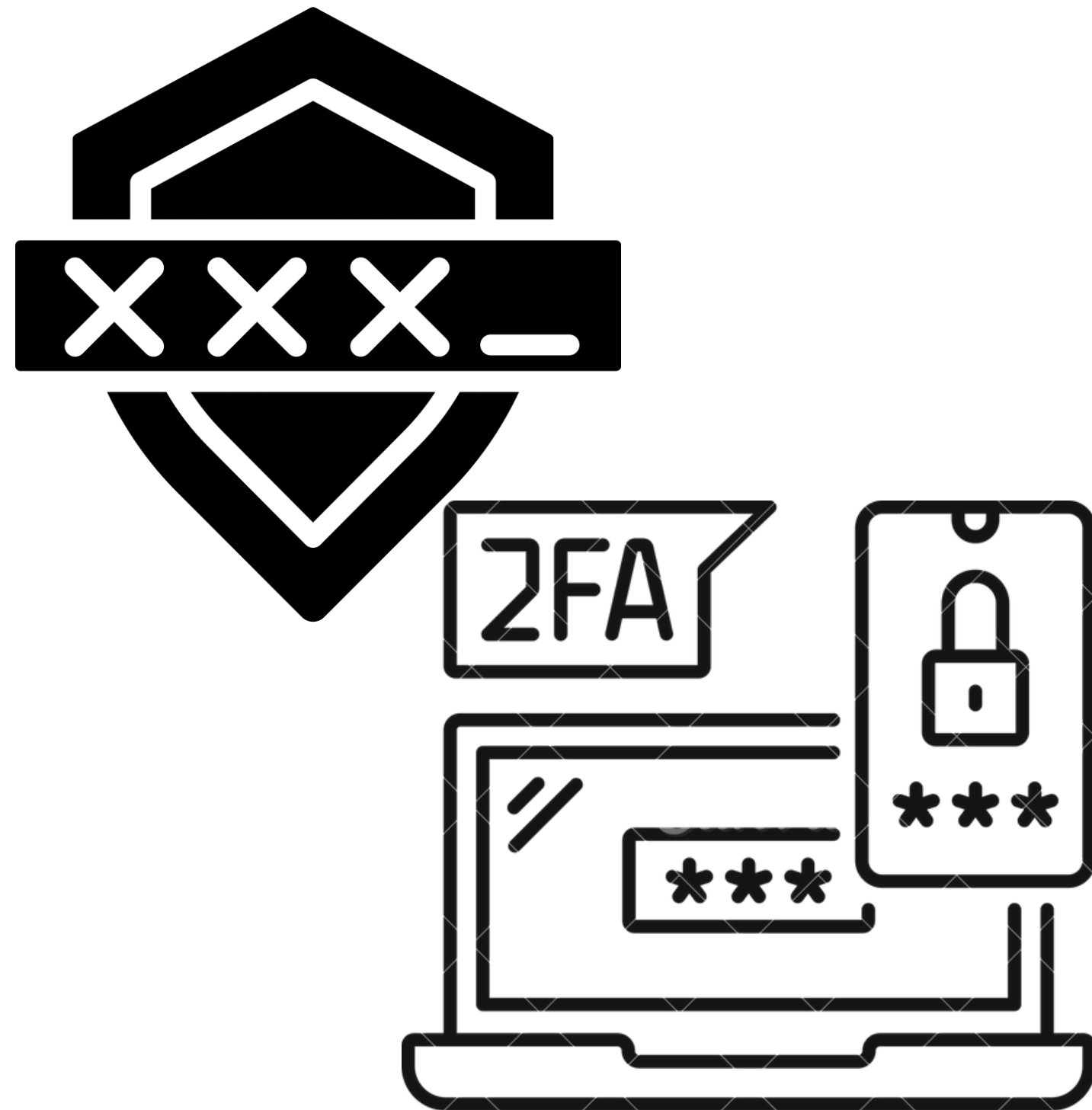
Current passphrase: 002584813

Master Key    : E5 AB B7 E9 76 7E 0D B5 92 80 94 B4 B8 35 D4 42
              : 18 C4 5D F9 6C A3 84 EE BA 20 3C 9A 69 D2 40 05

Transient Key : 49 3C 85 DC F8 46 4C C5 D0 42 6B D6 91 B9 28 0D
              : 2D 97 2A 6A 8E DE 57 A6 9F B0 46 9D E9 28 8B 26
              : 99 43 3A F8 E1 13 FA 39 D9 C3 F2 F3 C6 97 3B A4
              : 16 5A 74 B0 48 E6 95 63 3C 86 6E AD 59 21 91 B4

EAPOL HMAC   : C3 BE 56 63 5D CB EE F1 6B CA E7 D9 EE 19 53 21
```

# Protección y buenas prácticas



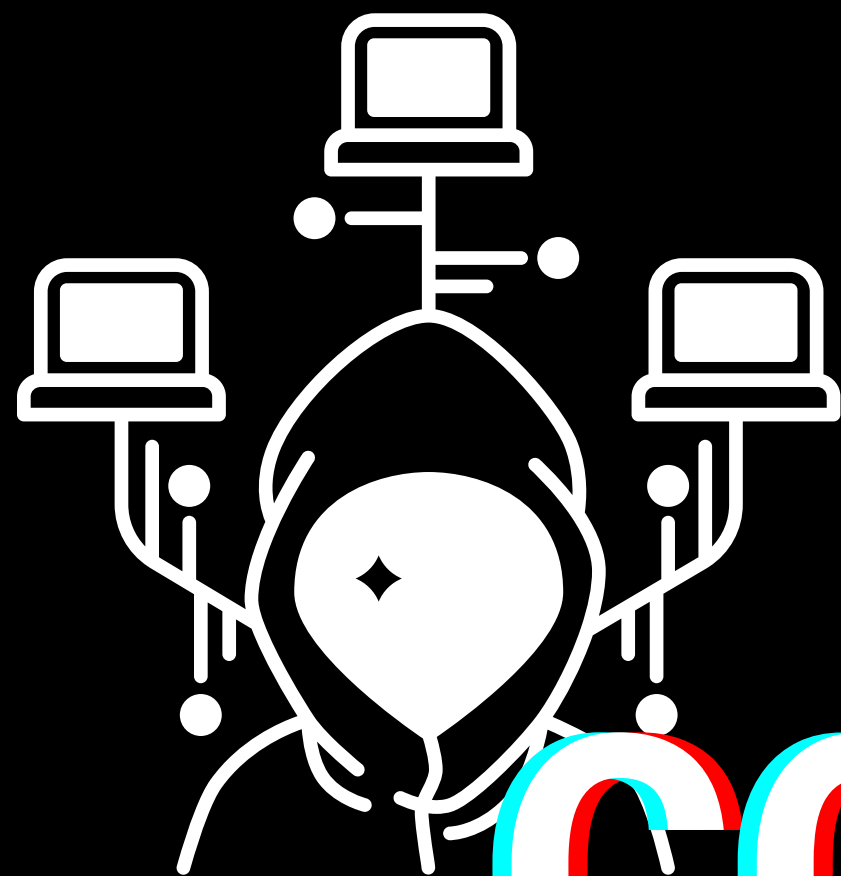
Contraseñas fuertes

No reutilizar credenciales

Eliminar cuentas no usadas

Doble autenticación (2FA)

Actualización constante



# CONCLUSIÓN

