



infobyte

security research team

Federico Kirschbaum  
*Exploiting Physical Security*  
Eko Executive Briefings 2010

# Introduccion

---

## Explotando el Punto mas Debil



# Introduccion

---

## Agenda

- Analisis de la seguridad fisica
- Vectores de acceso
  - Inteligencia Previa
- Control de Acceso
  - Cerraduras
  - Tarjetas de Proximidad
  - Puertas Magneticas
  - Bypass y *Tarjeteo*
- Errores Comunes
- Objetivo Final
- Conclusion



# Introduccion

---

## Analisis de la seguridad fisica

Cual es el grado de dificultad de entrar al edificio?

A una oficina particular?

Y al datacenter?


El personal de seguridad es efectivo?

# Analisis de la seguridad fisica

---

## Vectores de Acceso


Como acceder a un edificio?

- Puntos de Control 
- Patrones de Acceso
- Factor Humano
- Explotacion de confianza

# Vectores de Acceso

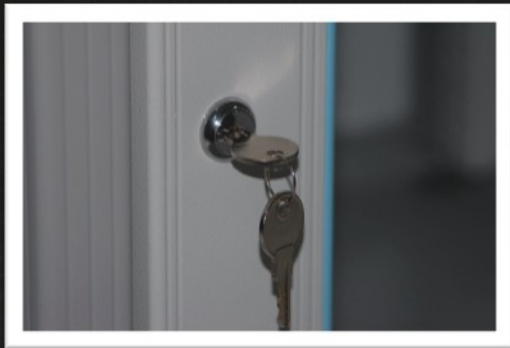
---

## Control de Acceso

- Cerraduras
- Tarjetas de Proximidad
- Puertas Magneticas
- Bypass y *Tarjeteo* 

# Cerraduras

**Elige tu propia aventura:**



# Cerraduras

---

## Waffler



Seguridad: muy baja  
Apertura: 0-1m

# Cerradura

---

## DIMPLE o COMPUTADA



Seguridad: Depende marca y modelo  
En general Baja  
Apertura: Normales 0-1m



# Cerradura

---

## Doble Paleta



Seguridad: Marca / Dificultad

Apertura: Normales 2-5m

# Cerradura

---

## Yale



Seguridad: Depende marca y modelo  
En general Media  
Apertura: Normales 0-3m

# Cerradura

---

## Tubular



Seguridad: baja  
Apertura: 0-1m

# Cerradura

---

## Multipaleta



*“La codificación se establece mediante 5 pernos frontales mecánicos con sistema antiganzua...”*

Seguridad: Media

Apertura: 1-5m

# Control de Acceso

---

## Tarjetas de Proximidad



# Control de Acceso

---

## Tarjetas de Proximidad

125 khz

HID

INDALA

GENERICOS



13,5 MHZ

MIFARE

DESFARE


Protecciones



# Control de Acceso

---

## Errores comunes

- Cables a la vista
- Puertas magneticas
- Cables expuestos 
- Bypass o *Tarjeteo*

# Objetivo

---

## Una vez dentro?

- Puntos de impresion
- Racks
- Puertos ethernet
- Rogue AP + 3g
- Documentacion
- Señuelos (Pendrive- CD)



# Esta todo perdido?

---



infobyte

# Thanks!

---

## Contact

Federico Kirschbaum

[fedek@infobytesec.com](mailto:fedek@infobytesec.com) @fede\_k



<http://www.infobytesec.com>

<http://blog.infobytesec.com>

<http://www.ekoparty.org>