**Hacking de radiofrecuencia**

# **Introducción**

## Requisitos previos

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0df9rserl5cdoaojnrg?&autoplay=true&crosstime=455>

### **Recomendaciones/Notas**

Descargar :

Kali linux

Parrot OS

Herramientas físicas:

Proxmark 3 (ice man collection): <https://hackerwarehouse.com/product/proxmark3-rdv4-kit/>

Proxmark 3 (Modelo chino): <https://www.amazon.es/Digitalkey-Proxmark3-Easy-etiquetas-prueba/dp/B08PC5X42X/ref=sr_1_1?__mk_es_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=proxmark3&qid=1612776824&s=electronics&sr=1-1>

HandHeld RFID Writer: <https://www.amazon.es/HFeng-Handheld-Duplicador-Programador-etiquetas/dp/B07DQR7GW9/ref=sr_1_7?dchild=1&keywords=handheld+rfid+writer&qid=1612776877&sr=8-7>

Multi-Frecuency RFID Copy machine: <https://www.amazon.com/Multi-frequency-Machine-Copier-Reader-Writer/dp/B07Z4JY5HK>

HackRF Portapack: <https://www.amazon.es/PORTAPACK-Software-Definido-Transmisi%C3%B3n-Met%C3%A1lica/dp/B07YYGBLCT>

Dispositivos PMR446: <https://www.amazon.es/Motorola-T42-Rojo-Aparatos-Unidades-16-Canales/dp/B07DYCXZM6>

# **Conceptos básicos y configuración de Proxmark3**

## Proxmark, tarjetas Mifare y tipos de tecnología

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0fvr4serl5cdoaopd5g?&autoplay=true&crosstime=264>

### **Recomendaciones/Notas**

Material de apoyo

Definicion de Mifare : <https://es.wikipedia.org/wiki/Mifare>

Proxmark3 – Definición: <https://www.securityartwork.es/2010/02/03/hacking-rfid-rompiendo-la-seguridad-de-mifare-ii/#:~:text=Aqu%C3%AD%20es%20donde%20juega%20un,la%20que%20se%20basa%20Mifare>.

## Flasheando y Compilando la Proxmark3

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0gm3kserl5cdoaoqvvg?&autoplay=true&crosstime=400>

### **Recomendaciones/Notas**

Material de apoyo

Repositorio proxmark3: <https://github.com/Proxmark/proxmark3>

Guia de compilación de la Proxmark para Parrot: <https://github.com/Chrissy-Morgan/proxmark3/blob/master/Installation_Instructions/Parrot-OS-Proxmark3-RDV4-installation.md>

# **Análisis y auditoria de la tecnología de tarjetas**

## Identificación de la tecnología de una tarjeta

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0gminserl5cdoaor28g?&autoplay=true&crosstime=422>

### **Recomendaciones/Notas**

Recurso

Tipos de tarjeta : <https://a3m.eu/es/tecnologia-de-tarjetas>

## Listando las Keys de los distintos sectores de una tarjeta (Ataque de Fuerza bruta)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0gmt0serl5cdoaor3h0?&autoplay=true&crosstime=353>

### **Recomendaciones/Notas**

Material de apoyo

Cloning a Mifare Classic 1K card: <https://www.gavinjl.me/proxmark-3-cloning-a-mifare-classic-1k/>

## Leyendo los sectores de una tarjeta basado en las Keys descubiertas

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h5nncerl5cdoaoscrg?&autoplay=true&crosstime=219>

### **Recomendaciones/Notas**

Material de apoyo

Cloning a Mifare Classic 1K card: <https://www.gavinjl.me/proxmark-3-cloning-a-mifare-classic-1k/>

## Leyendo los sectores de una tarjeta de empleado con datos reales

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h5u9bjj09frru7anng?&autoplay=true&crosstime=326>

### **Recomendaciones/Notas**

Material de apoyo

Cloning a Mifare Classic 1K card: <https://www.gavinjl.me/proxmark-3-cloning-a-mifare-classic-1k/>

## Incorporando un nuevo diccionario de Keys y descubriendo nuevas claves

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h680rjj09frru7aosg?&autoplay=true&crosstime=441>

### **Recomendaciones/Notas**

Material de apoyo

Cloning a Mifare Classic 1K card: <https://www.gavinjl.me/proxmark-3-cloning-a-mifare-classic-1k/>

Diccionario grande de claves: <https://github.com/ikarus23/MifareClassicTool/blob/master/Mifare%20Classic%20Tool/app/src/main/assets/key-files/extended-std.keys>

## Aplicando ataque Nested para computar el resto de claves que NO son por defecto

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h6d6kerl5cdoaosfkg?&autoplay=true&crosstime=257>

### **Recomendaciones/Notas**

Material de apoyo

RFID Hacking with the Proxmark3: <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/>

## Volcando todo el contenido de una tarjeta a un archivo dumpdata.bin

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h6hgcerl5cdoaosg3g?&autoplay=true&crosstime=118>

### **Recomendaciones/Notas**

Material de apoyo

RFID Hacking with the Proxmark3: <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/>

## Formateo y clonación de datos de una tarjeta para crear una copia exacta

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h6qpjjj09frru7aqpg?&autoplay=true&crosstime=368>

### **Recomendaciones/Notas**

Material de apoyo

RFID Hacking with the Proxmark3: <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/>

## Manipulando el contenido de una tarjeta y volcando el mismo en una nueva tarjeta

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h6vk4erl5cdoaosheg?&autoplay=true&crosstime=334>

### **Recomendaciones/Notas**

Material de apoyo

RFID Hacking with the Proxmark3: <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/>

## Clonando el UID de una tajeta via csetuid

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h7664erl5cdoaosi40?&autoplay=true&crosstime=334>

### **Recomendaciones/Notas**

Material de apoyo

RFID Hacking with the Proxmark3: <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/>

## Modo simulación LF/HF en la Proxmark via 410xim y sim

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0h7dibjj09frru7asq0?&autoplay=true&crosstime=334>

### **Recomendaciones/Notas**

Material de apoyo

RFID Hacking with the Proxmark3: <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/>

## Sistema de control de acceso | Abriendo una cerradura real con una tarjeta clonada

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hae33jj09frru7b5jg?&autoplay=true&crosstime=334>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Sistema de control de Acceso | Clonando tag IDs en llaveros LF desde la Proxmark

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hajjkerl5cdoaossb0?&autoplay=true&crosstime=331>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Compilando y flasheando el modelo mas reciente de Proxmark3

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hashcerl5cdoaosuc0?&autoplay=true&crosstime=331>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark First Use: <https://hackerwarehouse.com/site-news/proxmark-first-use/>

## Arreglando pequeño fallo en el proceso de compilación de la Proxmark3

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hb4pcerl5cdoaosvc0?&autoplay=true&crosstime=186>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Uso de la utilidad fchck para efectuar Fast Checks sobre tarjetas Mifare

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hbdskerl5cdoaot060?&autoplay=true&crosstime=161>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Ataque AutoPwn sobre tarjetas Mifare

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hbj6jjj09frru7baa0?&autoplay=true&crosstime=182>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Ataque StaticNested y listando la memoria de la Proxmark3

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hbov4erl5cdoaot1f0?&autoplay=true&crosstime=234>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Sistema de control de acceso | Uso del modo Standalone para clonar tarjetas

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0hc1fserl5cdoaot2lg?&autoplay=true&crosstime=259>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Uso de HandHeld RFID Writer para copiar y clonar tarjetas

### **Vidéo**

<https://platform.thinkific.com/videoproxy/v1/play/c0hdq5cerl5cdoaot9p0?&autoplay=true&crosstime=259>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

## Uso del Multi-Frequency Card Copier Machine para clonar tarjetas

### **Vidéo**

<https://platform.thinkific.com/videoproxy/v1/play/c0he6ubjj09frru7bl00?&autoplay=true&crosstime=259>

### **Recomendaciones/Notas**

Material de apoyo

Proxmark3 CheatSheet: <https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md>

# **Análisis de frecuencias**

## Introducción al HackRF

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ij194erl5cdoap0760?&autoplay=true&crosstime=103>

### **Recomendaciones/Notas**

Material de apoyo

HackRF wiki: <https://github.com/greatscottgadgets/hackrf>

## Análisis de frecuencias con el hackRF PortalPack

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ijc5jjj09frru7ehb0?&autoplay=true&crosstime=198>

### **Recomendaciones/Notas**

Material de apoyo

HackRF wiki: <https://github.com/greatscottgadgets/hackrf>

## Interceptando las señales emitidas desde un mando

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ijo0bjj09frru7eirg?&autoplay=true&crosstime=161>

### **Recomendaciones/Notas**

Material de apoyo

HackRF wiki: <https://github.com/greatscottgadgets/hackrf>

## Grabación de señales con HackRF

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ijt6serl5cdoap0ai0?&autoplay=true&crosstime=110>

### **Recomendaciones/Notas**

Material de apoyo

HackRF wiki: <https://github.com/greatscottgadgets/hackrf>

## Controlando luces de una silla Gamer desde el hackRF

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ik4o3jj09frru7ek60?&autoplay=true&crosstime=132>

### **Recomendaciones/Notas**

Material de apoyo

HackRF wiki: <https://github.com/greatscottgadgets/hackrf>

## Concepto de Jamming

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ikgj4erl5cdoap0d5g?&autoplay=true&crosstime=262>

### **Recomendaciones/Notas**

Material de apoyo

Jamming desde el HackRF : <https://www.rtl-sdr.com/tag/jamming/>

## Abriendo un coche con el hackRF

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ikpcjjj09frru7em7g?&autoplay=true&crosstime=208>

### **Recomendaciones/Notas**

Material de apoyo

Hacking car Key Fobs with SDR: <https://www.lufsec.com/hacking-car-key-fobs-with-sdr/>

## Interceptando comunicaciones emitidas desde dispositivos PMR446

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0iqr33jj09frru7fg4g?&autoplay=true&crosstime=263>

### **Recomendaciones/Notas**

Material de apoyo

PMR446: <https://www.rtl-sdr.com/tag/pmr446/>

## Escuchando emisiones en una frecuencia dada desde el HackRF y cubicSDR

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ir0qcerl5cdoap17rg?&autoplay=true&crosstime=255>

### **Recomendaciones/Notas**

Material de apoyo

Uso de cubicSDR: <https://youtu.be/fuwW5ZNK_0Y>

## Replicando una comunicación previamente capturada desde el HackRF

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/c0ir5hjjj09frru7fhdg?&autoplay=true&crosstime=117>