

# PROJET K-REV

Kit de Recherche et Exploitation de Vulnérabilités en cybersécurité

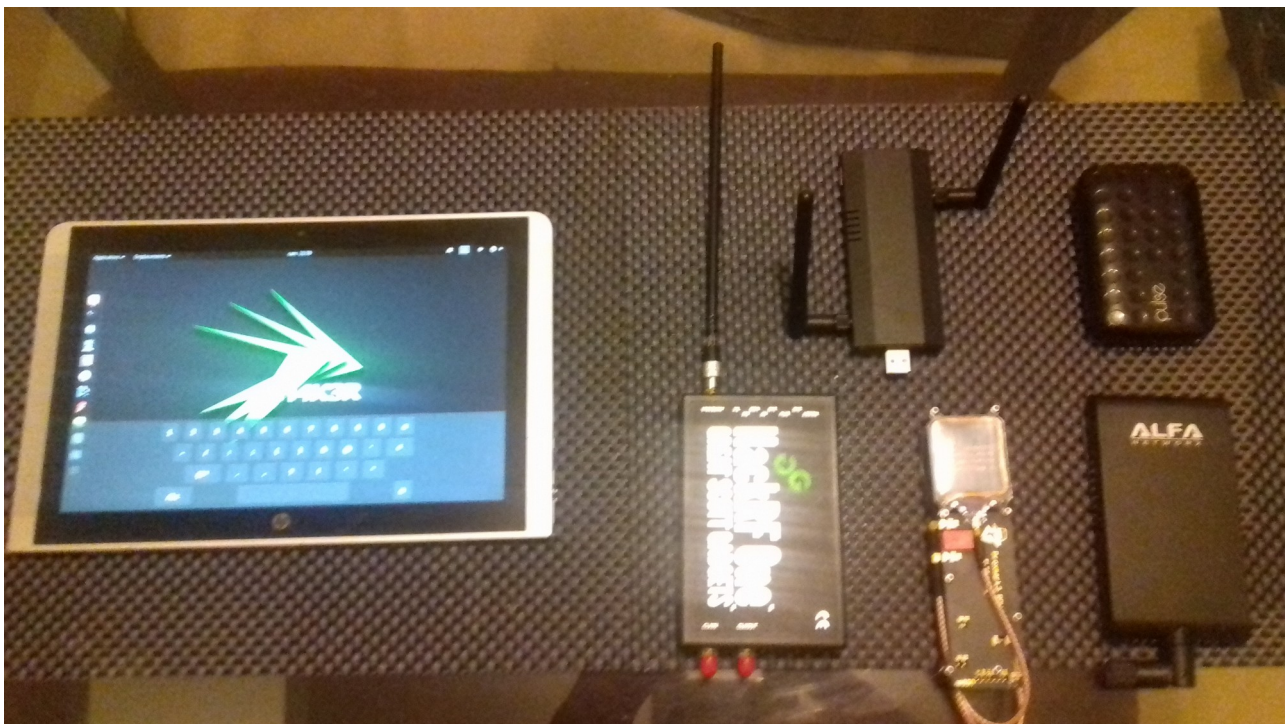
## Qu'est-ce que le projet K-REV ?

Le projet K-REV est un projet créé pour la cybersécurité générale, un système multifonctions, le couteau suisse en matière de pentesting. Son objectif vise à l'amélioration de la détection des vulnérabilités et à leur exploitation afin de mesurer les risques et de trouver des solutions, des corrections et/ou des protections face à des menaces constantes et qui évoluent sans cesse dans le monde de la cybersécurité

Le projet K-REV se concrétise par un outil portable complété par de nombreuses extensions, de matériels et de programmes, permettant une grande flexibilité en matière de recherche et d'exploitation des vulnérabilités en termes de sécurité (WI-FI, GSM, Radiofréquence, RFID, ...).

## Vue d'ensemble

- |                             |   |
|-----------------------------|---|
| - Pc/Tablette HP Kali Linux | (Système Windows remplacé par Kali Linux) |
| - HackRFone                 | (Pentesting RadioFréquence SDR)           |
| - Proxmark v3 rdv2          | (Pentesting RFID)                         |
| - Nano Pineapple            | (Pentesting WIFI)                         |
| - Antenne Apha Awus 15dbi   | (Complément de matériels)                 |
| - Batteries externe Energie | (Complément de matériels)                 |



# Présentation des Modules Extensions

Le projet K-REV est composé de plusieurs modules, connectés et contrôlés, par câble USB ou par communication SSH (Secure Shell, protocole de communication sécurisé) sur le Pc/Tablette HP Kali Linux.

Ces modules sont des extensions capables d'obtenir une grande flexibilité dans la recherche de vulnérabilités et d'exploitation de systèmes de réseaux informatiques sécurisés tels que les réseaux Wi-Fi, les signaux RFID, les fréquences radio, ...

En connectant ces extensions sur le controller (HP Kali Linux tablette), nous avons le choix d'utiliser ces extensions en fonction du domaine que nous souhaitons tester, auditer (Wi-Fi, RFID, GSM, ....).

C'est pour cette raison que plusieurs modules sont équipés de batteries externes, afin de réaliser des tests d'exploitation du ou des défauts de sécurité à distance avec la même approche que pour certains scénarios réels de simulation de compromission de système ou de réseaux informatiques.

## 1) Module Extension externe WIFI Nano Pineapple :



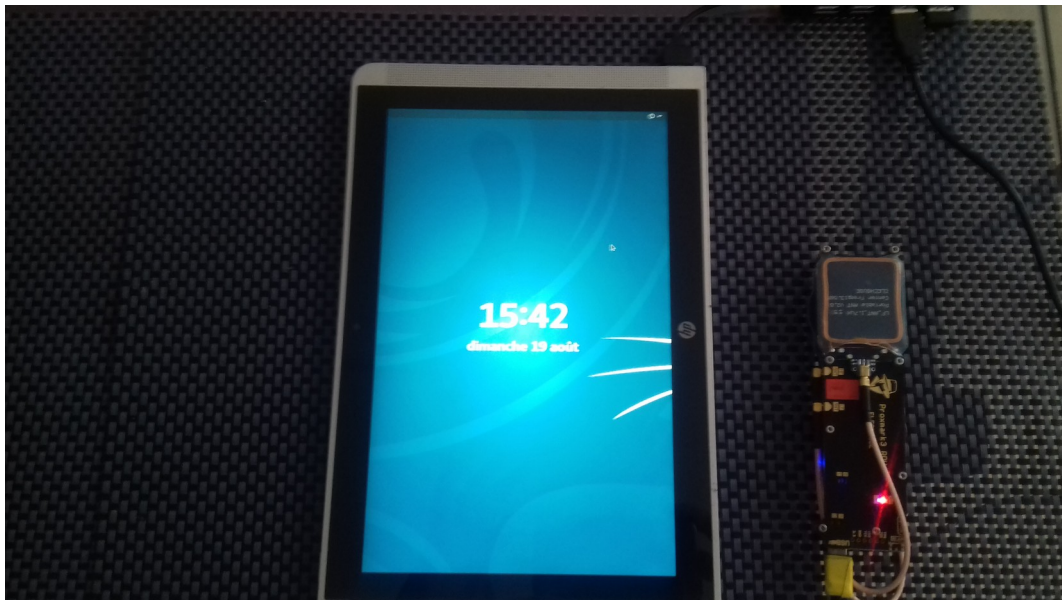
Ceci est la Nano Pineapple connectée sur la tablette controller Kali Linux. Avec un plus petit facteur, plus portable et plus puissant que ses prédécesseurs, un favori pour le pentesting et les spécialistes de sécurité réseau. Conçu pour tirer pleinement parti de la suite PineAP, le WiFi Pineapple fournit au testeur la meilleure expérience d'audit.

Possibilité de fonction sans fil avec une batterie externe avec le protocole de communication SSH (Secure Shell).



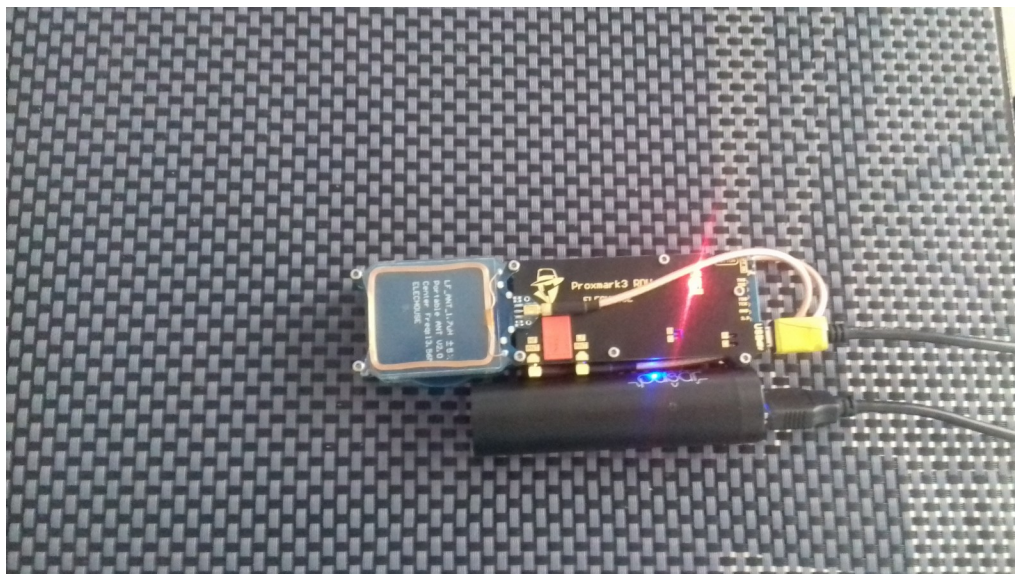


## 2) Module Extension externe RFID :

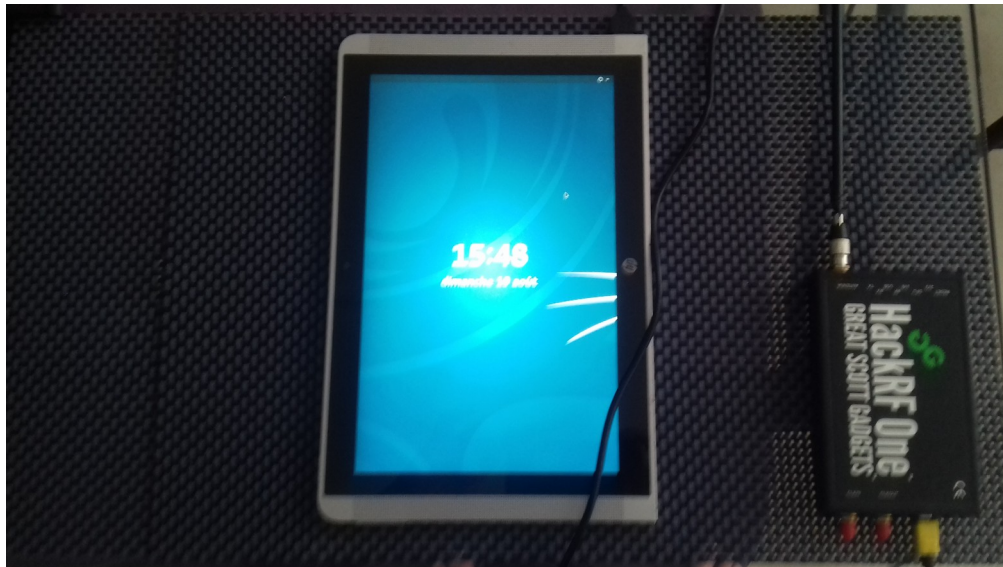


Ceci est le Proxmark3 connecté sur la tablette contrôleur Kali Linux. Le Proxmark3 est l'outil RFID du commerce en matière de détection, de lecture et de clonage de tags RF. Proxmark3 peut fonctionner indépendamment d'un PC alimenté par un tag RFID en option. Des fonctions avancées telles que le chiffrement hors ligne, le reniflage en ligne, le craquage de clé par défaut, le déchargement de données ou la possibilité d'exécuter des simulations. Il est actuellement le "gold standard" en matière de recherche RFID.

Possibilité de fonction sans fil avec une batterie externe et avec le protocole de communication SSH (Secure Shell).



### 3) Module Extension externe SDR :



Ceci est le HackRF One de Great Scott connecté sur la tablette HP controller Kali Linux.

HackRF One de Great Scott Gadgets est un périphérique radio défini par logiciel capable de transmettre ou de recevoir des signaux radio de 1 MHz à 6 GHz. Conçu pour permettre le test et le développement de technologies radio modernes et de nouvelle génération, HackRF One est une plateforme matérielle open source pouvant être utilisée en tant que périphérique USB ou programmée pour un fonctionnement autonome.

- #Fréquence de fonctionnement de 1 MHz à 6 GHz
- #émetteur-récepteur semi-duplex
- #jusqu'à 20 millions d'échantillons par seconde
- #Échantillons en quadrature de 8 bits (I 8 bits et Q 8 bits)
- #compatible avec GNU Radio, SDR #, etc.
- #Gain RX et TX et filtre en bande de base configurables par logiciel
- #port d'antenne contrôlé par logiciel (50 mA à 3,3 V)
- #Connecteur d'antenne femelle SMA
- #SMA entrée d'horloge femelle et sortie pour la synchronisation
- #boutons pratiques pour la programmation
- #en-têtes de broches internes pour l'expansion
- #Hi-Speed USB 2.0
- #Alimenté par USB
- #matériel open source

#### 4) Modules Extensions Externes Secondaires (projets annexes) :

##### ➤ **Projet box Pentesting Portable**



Projet box Pentesting Portable est une box portable (batterie interne) de petite taille (15 x 10 x 10 cm) équipée d'un système d'exploitation Kali Linux, de la carte raspberry pi 3 B+ et d'une carte réseaux internes Alpha Awus ayant pour objectif d'optimiser l'ensemble des performances dans la recherche de failles de sécurité et de leur exploitation, particulièrement sur les réseaux Wi-Fi (contrôle à distance possible, avec SSH).

##### **Exemples d'utilisation :**

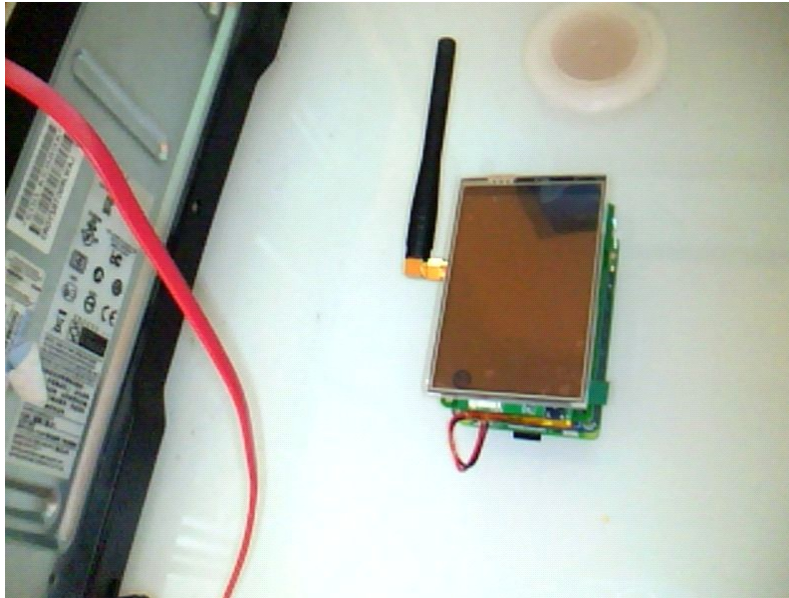
- Scanner des réseaux à distance,
- Capturer les clés Wi-Fi à distance,
- Créer de faux points hotspot Wi-Fi piégés,
- Utiliser un serveur terminal sur le web.

##### **Composants Internes :**

- 1 Raspberry pi 3 model B+
- 1 Carte module batterie interne model B+
- 1 Carte de Réseaux ALPHA Awus 036NH
- 1 Antenne Apha Awus 15 Dbi
- 1 écran 3.5 TFT LCD
- 1 MicroSD carte 64 gb (system KaliLinux ARM)



## ➤ **Projet Pentesting Smartphone / Nano PC Linux**



Ce projet a pour objectif d'utiliser la fonction GSM dans un nano ordinateur avec le système d'exploitation Ubuntu Linux ARM. Grâce à une carte circuit GSM Sim 800, il est possible d'effectuer des appels par exemple à partir de ce nano ordinateur portable smartphone.

### **Composants Internes :**

1 Raspberry pi 3 model B+

1 carte module batterie inteProjet Nano Pc Linux est mini-ordinateur équipé de la carte raspberry pie et un système d'exploitation Linux, et une structure amélioré, ventilé, équipé de dissipateurs de chaleurs : RAM, LAN, Processeurs.

Branchement sur batterie possiblerne B+

1 Carte module GSM modèle SIM 800

1 Ecran 3.5 TFT LCD

1 MicroSD carte 64 gb (système Ubuntu ARM)

Longueur 7 cm / largeur 5 cm / hauteur 5 cm

## ➤ **Projet nano pc Kali Linux**

Nano Pc Kali Linux est un nano ordinateur de poche sur batterie. Il est très petit, dispose d'un écran TFT 3.5 LCD, est équipé de la carte raspberry pi 3 B+ et du system d'exploitation de pentesting Kali Linux.

Le projet Nano PC Kali Linux est destiné à effectuer des audits de sécurité.



### **Composants Internes :**

1 Raspberry pi 3 model B+

1 Carte module batterie interne B+

1 Ecran 3.5 TFT LCD

1 MicroSD carte 64 gb (system Kali Linux ARM)

Longueur 7 cm / largeur 5 cm / hauteur 4 cm

### **➤ Projet Nano pc Linux**



Le projet Nano Pc Linux est un mini-ordinateur équipé de la carte raspberry pie et d'un système d'exploitation Linux avec une structure améliorée, ventilée et équipée de dissipateurs de chaleurs : RAM, LAN, Processeurs.

Branchement sur batterie possible.

#### Composants Internes :

1 Raspberry pi 3 model B+

1 Carte module batterie interne B+

1 Ecran 3.5 TFT LCD

1 MicroSD carte 64 gb (système Raspian Linux ARM)

Longueur 7 cm / largeur 5 cm / hauteur 3 cm