ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

DaVinciCode

Hacker Arsenal: Cahier des charges

1 Introduction

Le projet "Hacker Arsenal" vise à mixer l'Internet Of Things (IOT), l'électronique et la cybersécurité afin de recréer, prototyper et fabriquer des outils électroniques ayant une utilité pour les hackers éthiques ou pentesters.
Plusieurs cas de figures s'ouvrent à nous pour la création de ces outils :

- Réalisation de plan détaillé déjà créé avec software et hardware.
- Réalisation de plan détaillé déjà créé avec software et hardware en adaptant le hardware pour des microcontrôleurs ou microprocesseurs moins coûteux (avec adaptation simple du software si nécessaire).
- Création de système embarqué pour servir de hardware à un software déjà créé.
- Création de système embarqué et du software.

Dans tous les cas, chaque outil créé durant l'année fera l'objet d'une réalisation technique, de la création d'une notice détaillée pour reproduire chaque étape de l'installation software ainsi que de l'assemblement hardware (et des circuits électroniques si besoin est).

2 Listes d'outils potentiels

- Badusb
- Usbkiller
- Pineapple clone
- Bashbunny clone
- Screen clab clone
- Keylogger
- RFID cloner
- MSKB sniffer / Keysweeper
- Wifi deauther
- Wifi jammer
- Bluetooth jammer (?)
- Open sesame

- MagSspoofer
- Netsplit
- OMG cable/Usb samurai

Cette liste n'est pas exhaustive, et seulement certains outils pourraient finir par être choisis.

3 Détails techniques

Le choix de chaque outil donnera lieu à la création d'un cahier des charges et une notice séparés, contenant notamment mais pas exclusivement :

- Le détails pièce par pièce et références du hardware
- Un lien vers un gist ou repository github avec le code
- Une notice de soudure avec un circuit électronique (si nécessaire)
- Une notice d'installation
- Une notice d'utilisation