Préparation du WHID :

Préparer l'environnement Arduino

Dans le cadre de l'utilisation du WHID Injector en France, il convient de le flasher avec un firmware compilé avec la Keymap AZERTY. Pour ce faire, il faut recompiler ce nouveau firmware via l'IDE Arduino. **Ce tutoriel est à réaliser sur Windows**, des modifications sur la board ou Linux ayant modifié le support Linux pour les ATmega32u4.

Pour commencer, il convient d'installer l'IDE Arduino, disponible sur http://www.arduino.cc

Pour obtenir le support pour la board concernée, il faut ajouter dans Fichiers -> Préférences dans le champs "URL de gestionnaire de cartes supplémentaires" l'URL suivant :
http://arduino.esp8266.com/stable/package_esp8266com_index.json

Dans Outils => Type de Carte => Gestionnaire de carte, installer *esp8266 by ESP8266 community version 2.3.0.*

De plus, dans Croquis => Inclure une bibliothèque => Gérer les bibliothèques, rechercher "json". Dans les résultats devrait apparaître "*ArduinoJson by Benoit Blanchon*", qu'il convient d'installer dans sa version 5.11.0.
Une fois l'installation réussie, télécharger :

- https://github.com/exploitagency/esp8266FTPServer/archive/feature/bbx10_speedup.zip

Pour ensuite ajouter cette bibliothèque à l'IDE, utiliser la fonction Croquis => Inclure une bibliothèque => Ajouter la bibliothèque .ZIP, et sélectionner le fichier précédemment téléchargé.

L'IDE est désormais préparé pour la compilation des firmwares WHID, il est donc temps de commencer par modifier la keymap dans les fichiers Arduino.
Pour ce faire, modifier dans C:/Program Files (x86)/Arduino/libraries/Keyboard/keyboard.cpp la variable _asciimap, il est possible d'en trouver des versions AZERTY sur internet.

Compilation et mise en place du firmware

Nous pouvons désormais commencer la compilation des firmwares du WHID injector.

Télécharger la dernière release de https://github.com/exploitagency/ESPloitV2, puis ouvrir avec Arduino IDE le fichier ESPloitV2-master/source/Arduino_32u4_Code/Arduino_32u4_Code.ino.
Il convient désormais de brancher le WHID Injector s'il ne l'est pas.
Ensuite, dans le menu Outils => Type de Carte, sélectionner LilyPad Arduino USB. Dans Outils => Port, sélectionner celui ou est écrit (LilyPad Arduino USB).
Il est désormais possible d'utiliser Croquis => Téléverser de manière à mettre le firmware en place.

Maintenant, nous allons procéder à la mise à jour d'ESPloitV2 sur la clef, en enlevant au passage de potentielles backdoors présentes à l'achat (ces devices étant flashés en Chine et dédiés à des professionnels de la sécurité, il est mieux de procéder à ce flash).

Pour ce faire, ouvrir ESPloitV2-master/source/ESP_Code/ESP_Code.ino.
Ensuite, dans le menu Outils => Type de Carte, sélectionner Generic ESP8266 Module. Dans Outils => Flash Size, sélectionner "4M (3M SPIFFS)".
Il est ensuite possible d'exporter le binaire dans Croquis => Exporter les binaires compilées. Ce binaire sera exporté dans %temp% dans un dossier nommé arduino_build_XXXXXX.

Pour mettre ce firmware sur la clef, nous allons utiliser la fonction d'upload de firmware proposée par ESPloitV2.

Il convient donc de se connecter au réseau créé par le WHID Injector avec les informations suivantes :

- SSID "Exploit"
- Password "DotAgency"

Pour accéder à l'interface web du device, se rendre sur 192.168.1.1. La fonction d'upgrade du firmware est située sur la partie administration, dont les identifiants par défaut sont :

- username "admin"
- password "hacktheplanet"

Sélectionner le firmware, l'uploader, et l'interface devrait indiquer que le device redémarre.

Une fois le redémarrage effectué, la keymap devrait avoir changé, et le device envoyer les commandes en AZERTY.

Utilisation dans le red team :

- Prepare scripts
    - Have a collection of scripts

- have a webserver with a malware ready to serve