WE DON'T KNOCK

Miscreant Crèche

Activities Guide
General Information

Background

The Short Version

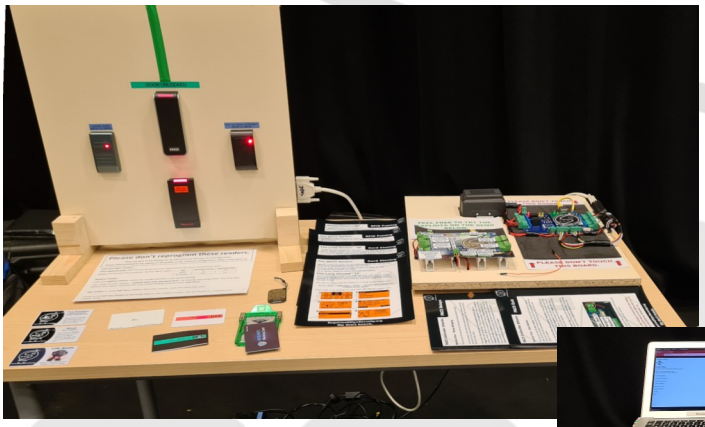
An activities evening for hacker-types who have bought tools like HackRF, Flipper, Proxmark but don't have a way experiment with them legally.

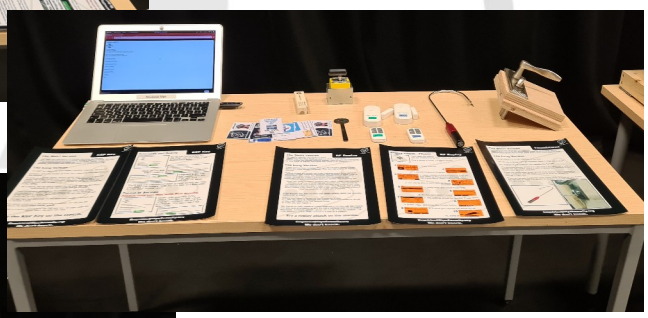
The Long Version

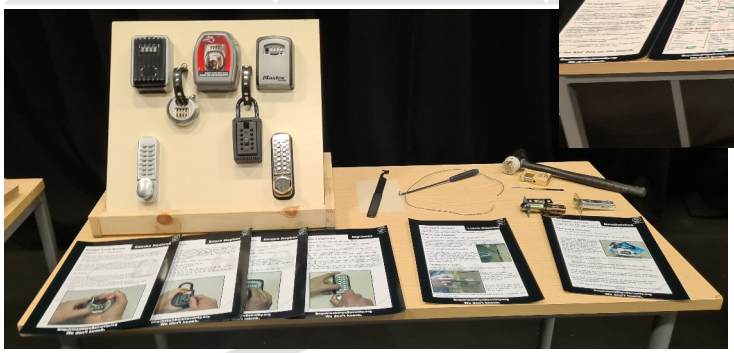
The idea came from a conference where Styx Security hosted the "Covert Entry Play Centre and Miscreant Crèche". It featured a few stands with various covert entry tools, an access control system, alarms, etc. Most of it came from training gear. Photos below.

It went down so well, we decided to make it a proper event where people could bring their own Flippers and other kit to play with.

There are instructions and there will be technical help available but this is explicitly not to be considered formal training.







There will be a limited number of Flippers available on the evening so we ask people bring theirs along and be willing to work in groups.

Enquiries@StyxSecurity.org

We don't knock.

Activities List

Activities

The list of activities will potentially change
as new things are added, old things drop out (or break) and whether something decides to stop working between testing and event…
Limited numbers of Flippers may limit some activities.

PACS Activities

Physical Access Control Systems are the kind of tappy tap card readers and associated hardware you get in commercial buildings. They consist of a door controller, locking system, card reader and a server. We have a few of these and two are used in the Crèche.

Low Frequency RFID:
- **Card cloning**
- **Card emulating**
- **Reader fuzzing**

High Frequency RFID:
- **Card cloning (easy)**
- **Card cloning (harder)**
- **Card cloning (yeah right)**

General PACS:
- **Wiegand sniffing / MITM**
- **Direct controller approaches**

Alarms Activities

A variety of alarms and ways to mess with them are on offer.

There is some overlap with the radio activities.

PIR alarm:
- **Try to evade the PIR sensor**
- **Clone the remote**

Door contact alarms:
- **Bypassing solid state sensors**
- **Clone the remote**
- **Bypassing mechanical sensors**

Enquiries@StyxSecurity.org

We don't knock.

Activities

Combination Locks

There are lots of different types of combination lock and Styx has far too many of each. Below is a list of the locks that come to the Crèche:

Key Safes:

- **Master Lock Heavy Duty**
- **Master Lock Standard 5401**
- **Generic 4 wheel**
- **Knock off Master Lock 5401**
- **Master Lock push button**
- **Supra push button**

Digilocks:

- **Digital brand digilock**
- **Codelocks brand digilock**
- **Generic digilock**

Padlocks:

- **Master Lock heavy duty disc padlock**

Other:

- **My wife's re-appropriated laptop lock**
- **Bike lock**
- **Any others that come to hand whilst packing**

RF / SubGHz Activities

A collection of some easy and some harder to mess with RF systems. We make use of the Flipper "Rolling Flaws" app to simulate a rolling codes system that can easily be reset.

Radio and SubGHz:

- **Raw static code clone**
- **Static code clone**
- **Garage door receiver**
- **Flipper Rolling Flaws**

Hopefully we'll be adding some old car fobs to this section, but without the receiver side...

Enquiries@StyxSecurity.org

We don't knock.

Activities

Misc Physical Locks

There's often lock picking at these types of events, but it's the sort of thing you need to sit down quietly for an hour and focus on. It's not really a pub activity. As a result, there will be some clear locks and basic picks but only enough to let people try out picking.

General Physical Locks:

- **Shutter lock**
- **Hand cuffs**
- **Clear locks to pick**
- **Padlock raking**
- **Briefcase decode**
- **Commercial lock**

Competition

At the end of the evening, there's likely to be a competition. Entrants will be randomly selected from a hat to compete in some ridiculous and unlikely scenario, combining many of the skills and techniques from the different activities.

General

General Information

Age limits will be dictated by the venue. Evening events in pubs may be limited to over 18s and, where under 18s are permitted, the policy will be at the discretion of the venue.

The Miscreant Crèche is not to be considered formal training and the selection of activities reflects security vulnerabilities which have been commonly known for years. The activities are based around readily available, hobbyist grade hardware.

Advanced techniques and equipment will not be provided at this event. If you want to bring a Proxmark, HackRF, or other kit, you're more than welcome, but instruction won't be provided.

Our aim is education and experimentation. **If we think you're sketchy and just want to learn how to break into things, you will be asked to leave.**

Enquiries@StyxSecurity.org

We don't knock.