Proxmark3

•••

06.2022

Paulina Pacura

Jaką wersję proxmark3 wybrać?

Agenda samouczka:

- Co to jest Proxmark3;
- Dostępne urządzenia;
- Parametry urządzeń, na które warto zwrócić uwagę;
- Dostępne oprogramowania oraz ich wady/zalety;
- Instrukcja użytkowania;

Co to jest Proxmark3?

- czytnik RFID ogólnego przeznaczenia
- “szwajcarski scyzorek” do RFID

First version of Proxmark3 originally designed by Jonathan Westhues

Date invented	2007
FPGA	Xilinix Spartan®-II
Processor	Atmel AT91SAM7S64
Memory	64 kB flash

Grupa docelowa

- Pentesterzy
- Naukowcy

Dostępne urządzenia (½)

Proxmark 3 RDV4.01

—----------2018—----------
-mała obudowa,
-wymienne anteny modułowe,
-aplikacja na Androida, która umożliwia zdalne łączenie się i interakcję z urządzeniem za pomocą pełnej wersji terminala klienckiego,
-obecnie najmniejszy PM3 na rynku,
- wymaga co najmniej 20 minut czasu konfiguracji oraz znacznej ilości badań i praktyki z urządzeniem.

ProxmarkPro

—----------2019—----------
- stosunkowo łatwy w użyciu,
- uproszczony interfejs użytkownika zamiast skomplikowanego terminala klienta,
- wbudowany wyśw. LCD i pad nawigacyjny,
- przeznaczony do użytku w terenie lub przy biurku bez połączenia z klientem lub konfiguracji (bez pełnej wersji terminala),
- nie został zaprojektowany do użytku jako narzędzie programistyczne.


RyscCorp.
0008517240 00129,63596
45°

Dostępne urządzenia (2/2)

Proxmark3 RDV2

-działa w trybie autonomicznym bez komputera,
-nie opensource,
-wymienne anteny modułowe.

Proxmark3 Easy

- tani,
- opensource,
- jest to wersja przeznaczona wyłącznie na chiński rynek krajowy, więc usunięto kilka funkcji, np. mniejsza pamięć
- kompaktowe anteny LF i HF - da się używać, ale podobno może być z tym problem.

Parametry, na które warto zwrócić uwagę

Anteny	• Każdy Proxmark3 wspiera LF, ale niektóre gorzej • Jeśli chcemy dużo podsłuchiwać to lepiej niech ma wymienne
Rozmiar	• Niewielkie rozmiary są bardziej dyskretne • A wolimy żeby nikt nie domyślił się co to robi
OpenSource	• OpenSource to jak wszędzie, wady i zalety • Ale zwykle więcej ludzi umie naprawić
Cena	• Cytat z forum: “jak Cię stać, to kup lepsze, ale jak nie to wcale dużo nie stracisz”

Dostępne oprogramowanie

> Stock firmware with HF standalone mode

> “Modded” firmware with LF standalone emulation/cloning

> Proxbrute ported to the new CDC bootloader/current firmware(Standalone Brute Forcer)

> Matty’s Mifare Standalone Mode

> Iceman’s Fork

> Marshmellow’s Fork

Instrukcja użytkowania

- jak zhackować RFID?

Klonowanie HID ProxCard z RDV2

Karta HID ProxCard, która będzie kopiowana

Źródło: https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/

Klonowanie HID ProxCard z RDV2

Wyszukanie tagu za pomocą “lf search”

```
proxmark3> lf search
#db# DownloadFPGA(len: 42096)
Reading 30000 bytes from device memory
Data fetched
Samples @ 8 bits/smpl, decimation 1:1
NOTE: some demods output possible binary
  if it finds something that looks like a tag
False Positives ARE possible
Checking for known tags:
HID Prox TAG ID: 2004263f88 (8132) - Format Len: 26bit - FC: 19 - Card: 8132
Valid HID Prox ID Found!
```

Źródło: https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/

Klonowanie HID ProxCard z RDV2

Skanowanie pozostałych informacji z karty

```
proxmark3> lf hid fskdemod
#db# TAG ID: 2004263f88 (8132) - Format Len: 26bit - FC: 19 - Card: 8132
#db# Stopped
```

Źródło: https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/

Klonowanie HID ProxCard z RDV2

Kopiowanie RFID na nową, czystą kartę

Źródło: https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/

Klonowanie HID ProxCard z RDV2

Kopiowanie RFID na nową, czystą kartę

```
proxmark3> lf hid clone 2004263f88
Cloning tag with ID 2004263f88
#db# DONE!
```

Teraz tag T5577 powinien działać jako identyczny klon oryginalnej karty ProxCard!

Źródło: https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/

Zespół

Paulina Pacura,
wykonawca

Przygotowała materiały,
złożyła prezentację oraz
przedstawiła ją
(zdjęcie niezwiązane)