Workshop - Live Hacking

P4wnP1 A.L.O.A. - Der Rapsberry Pi Zero W als Bad USB Device

Tom Gries

Dokumenten URL: http://docs.tx7.de/TT-PPA
Autor: Tom Gries <TT-PPA@tx7.de>
@tomo@chaos.social

Version: 7.2.0 vom 02.02.20243

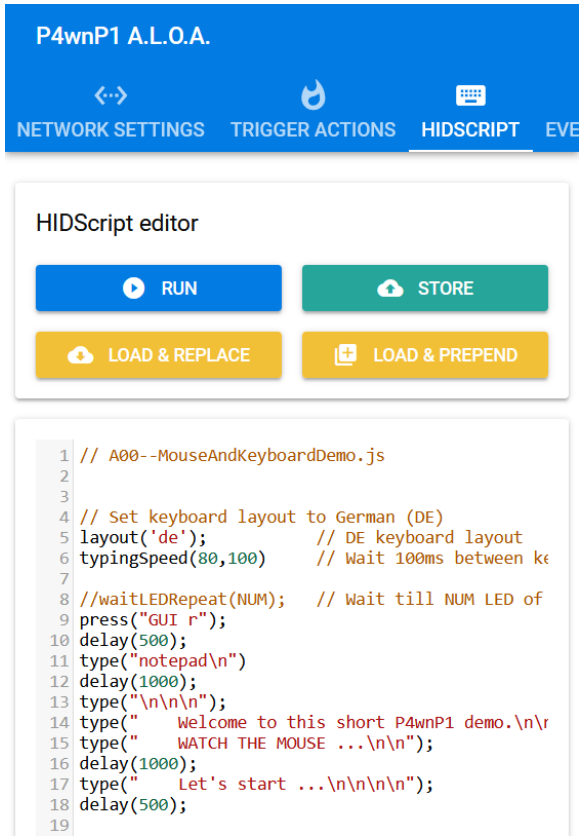
Legal Disclaimer - Hackerparagraf

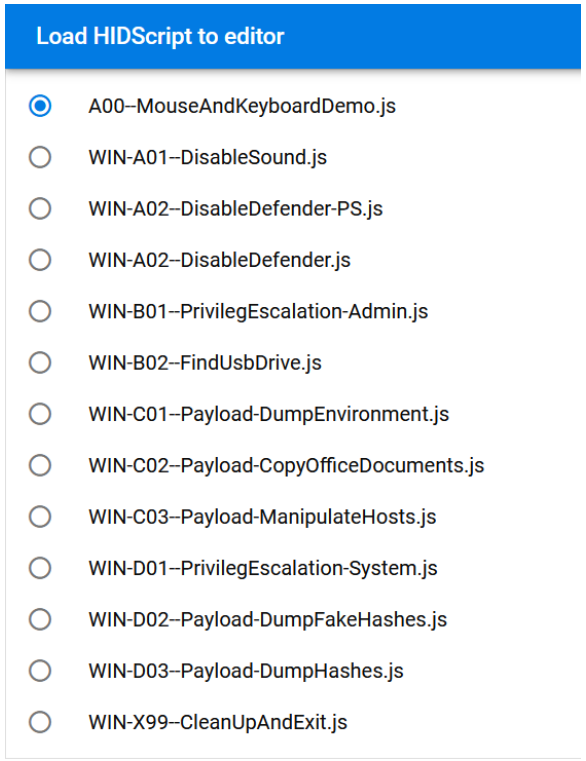
Die hier vorgestellten Methoden und Tools dienen zum Schutz der eigenen Systeme. Das Knacken fremder Passwörter ebenso wie das Eindringen in Systeme kann eine Straftat darstellen. Die vorgestellten Tools können unter den Hackerparagrafen 202c StGB fallen. Entsprechend dürfen Sie nur auf eigene Kennwörter oder Testsysteme losgehen, beziehungsweise sich schriftlich die Erlaubnis des Systembesitzers einholen.

Zudem können Cracking-Tools die getesteten Systeme stark beeinträchtigen oder außer Funktion setzen. Entsprechend vorsichtig sollten Sie bei Produktivsystemen sein.

P4wnP1 A.L.O.A. - kurz vorgestellt

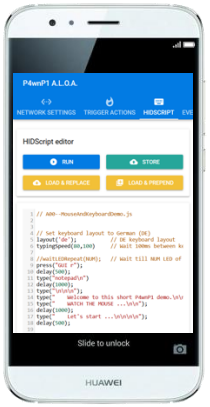
Ich bin eine Tastatur, eine Maus, ein USB Speicher, ein WiFi Access Point, kann auch LAN over USB und hab die Kali-Tools im Gepäck …





Der Aufbau

Angreifer



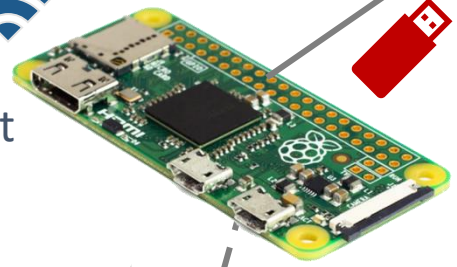
Mobiltelefon zur Steuerung des P4wnP1 A.L.O.A (zum Starten der Scripte)

Das Opfer

Angreifer

Optional: Laptop anstelle des Mobiltelefons

Raspberry Pi Zero W mit P4wnP1 A.L.O.A.



Optional: Mobiler Internet Router und Powerbank

Mögliches Szenario mit dem P4wnP1 A.L.O.A.

⇒ P4wnP1 A.L.O.A. (PPA) anschließen.

⇒ Vorbereitung: Sound und Defender deaktivieren

⇒ Vorbereitung: Privileg escalation zum Admin (Eingabeaufforderung)

⇒ **Payload: Umgebungsvariablen dumpen**

⇒ **Payload: Office Dokumente auf P4wnP1 kopieren**

⇒ **Payload: Hosts-Datei manipulieren**

⇒ Vorbereitung: Privileg escalation zum System-User (NT-Autorität)

⇒ **Payload: Passworthashe dumpen**

⇒ Aufräumen und P4wnP1 A.L.O.A. entfernen.

Los geht’s …

Anmerkungen oder Fragen?