

Workshop - Live Hacking

P4wnP1 A.L.O.A. - Der Raspberry 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

Lizenz:

Creative Commons BY-NC-ND

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 ...



P4wnP1 A.L.O.A.

NETWORK SETTINGS TRIGGER ACTIONS HIDSCRIPT EVENT ACTIONS

HIDScript editor

RUN STORE

LOAD & REPLACE LOAD & PREPEND

```
1 // A00--MouseAndKeyboardDemo.js
2
3
4 // Set keyboard layout to German (DE)
5 layout('de'); // DE keyboard layout
6 typingSpeed(80,100) // Wait 100ms between ke
7
8 //waitLEDRepeat(NUM); // Wait till NUM LED of
9 press("GUI r");
10 delay(500);
11 type("notepad\n")
12 delay(1000);
13 type("\n\n\n");
14 type(" Welcome to this short P4wnP1 demo.\n\r
15 type(" WATCH THE MOUSE ... \n\n");
16 delay(1000);
17 type(" Let's start ... \n\n\n\n");
18 delay(500);
19
```

Load HIDScript to editor

- ☒ A00--MouseAndKeyboardDemo.js
- ☐ WIN-A01--DisableSound.js
- ☐ WIN-A02--DisableDefender-PS.js
- ☐ WIN-A02--DisableDefender.js
- ☐ WIN-B01--PrivilegeEscalation-Admin.js
- ☐ WIN-B02--FindUsbDrive.js
- ☐ WIN-C01--Payload-DumpEnvironment.js
- ☐ WIN-C02--Payload-CopyOfficeDocuments.js
- ☐ WIN-C03--Payload-ManipulateHosts.js
- ☐ WIN-D01--PrivilegeEscalation-System.js
- ☐ WIN-D02--Payload-DumpFakeHashes.js
- ☐ WIN-D03--Payload-DumpHashes.js
- ☐ WIN-X99--CleanUpAndExit.js





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?