[Fecha]

Proyecto ShellSpark

Jonathan Garcia Peramo y Roberto Alaya Mallagray

Índice

Contenido

[Introducción 3](#_Toc8647867)

[Ataques HID 3](#_Toc8647868)

[Planificación del ataque 3](#_Toc8647869)

[Configuración de la RaspberryPi 4](#_Toc8647870)

[Configuración de SSH 4](#_Toc8647871)

[Punto de acceso 5](#_Toc8647872)

[NextCloud 11](#_Toc8647873)

[NextCloudPi 11](#_Toc8647874)

[Instalación 11](#_Toc8647875)

[DigiSpark 14](#_Toc8647876)

[Conclusiones 15](#_Toc8647877)

[Bibliografía 16](#_Toc8647878)

# Introducción

Nuestro proyecto consiste en el estudio sobre los ataques basados en HID, “Human Interface Devices” y en las medidas que se pueden tomar para proteger un equipo ante este tipo de amenazas.

## Ataques HID

En el mercado existen varias herramientas que simulan el funcionamiento de un teclado o ratón para vulnerar la seguridad de un equipo. Estos ataques son especialmente difíciles de detectar mediante software, ya que no escriben en disco y pocos programas hacen una monitorización activa sobre las señales que se reciben de un HID.

Para una persona con conocimientos de informática, este tipo de ataque no tiene apenas éxito, ya que el usuario se dará cuenta de que se está llevando a cabo un ataque y desconectará rápidamente el dispositivo, pero para una persona que haya dejado su equipo desbloqueado o que no sepa de informática no sabrá identificar el ataque hasta que sea tarde.

## Planificación del ataque

Para ejemplificar un ataque HID, vamos a utilizar dos componentes:

1. DigiSpark
2. RaspberryPi

El DigiSpark es un dispositivo con entrada USB que permite emular un teclado, reproduciendo una serie de comandos proporcionados previamente. El código que va a ejecutar con el DigiSpark se escribe mediante el IDE de Arduino y cuenta con un lenguaje propio.

La RaspberryPi se usará como servidor de archivos en línea y será donde vamos a almacenar los payloads que queremos introducir en el equipo objetivo. El software que utilizara es NextCloudPi.

Una vez se conecte el DigiSpark a un puerto USB del equipo de la víctima, este abrirá una línea de comandos y descargará un payload desde nuestro servidor NextCloud. Con el payload ya descargado, el DigiSpark lo ejecutara, infectando el equipo.

# Configuración de la RaspberryPi

**Instalación de Raspbian**

## Configuración de SSH

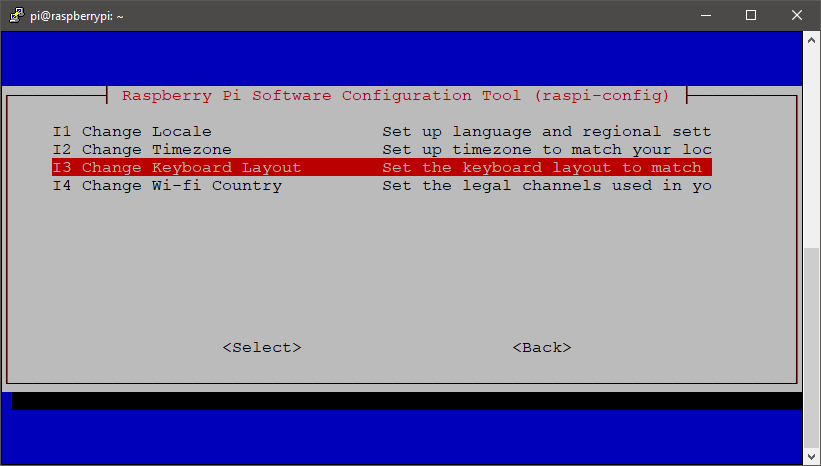
Configuraremos el servicio SSH en nuestra RaspberryPi para administrarla fácilmente y de forma remota.

El comando que se utiliza en Raspbian para entrar al menú de configuración es:

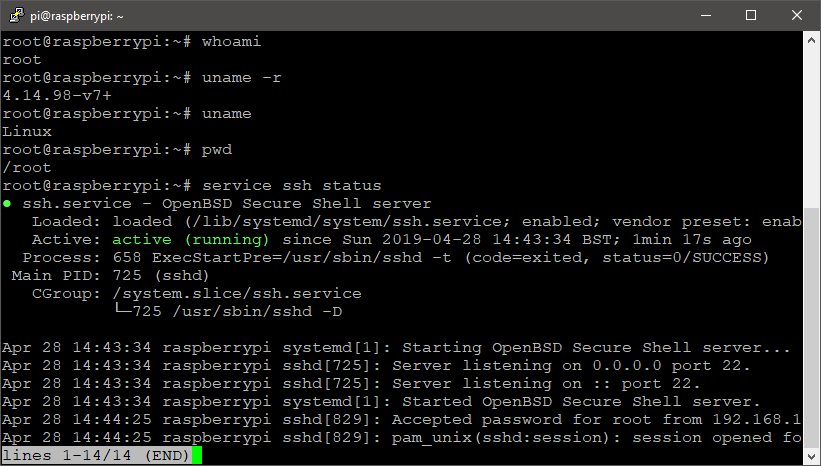




Es importante elegir la distribución del teclado correcta



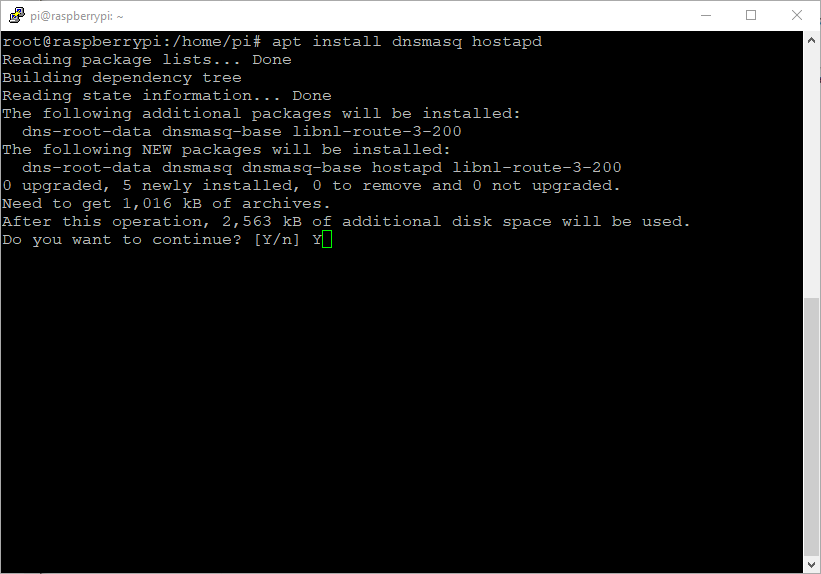
Podemos ver como el servicio de SSH se ejecuta correctamente



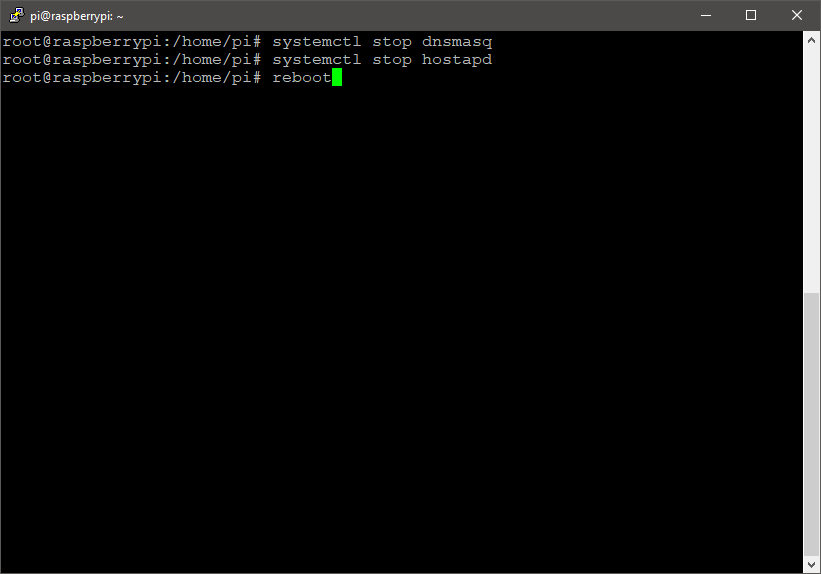
## Punto de acceso

Para mostrar cómo vamos a realizar el ataque, no vamos a poder utilizar una conexión a través de internet hacia nuestro servidor NextCloud, así que accederemos de forma local mediante un punto de acceso Wi-Fi integrado en nuestra RaspberryPi.

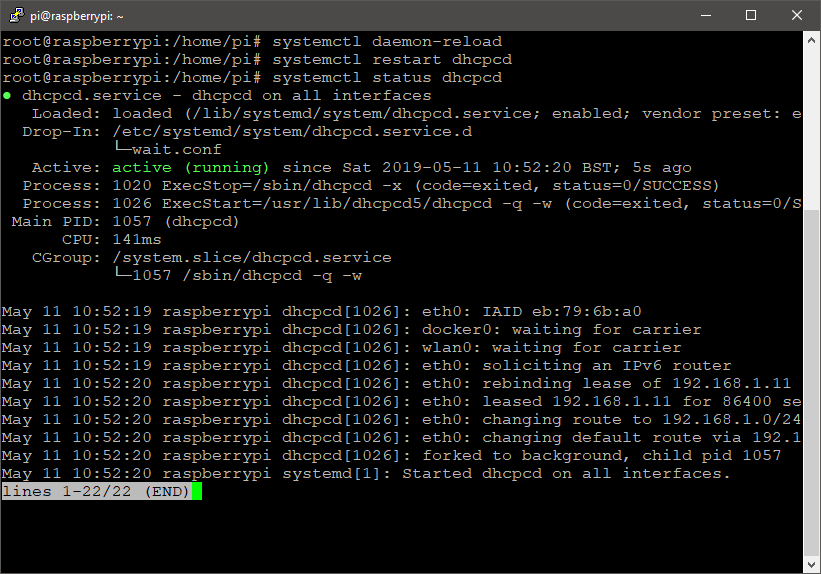
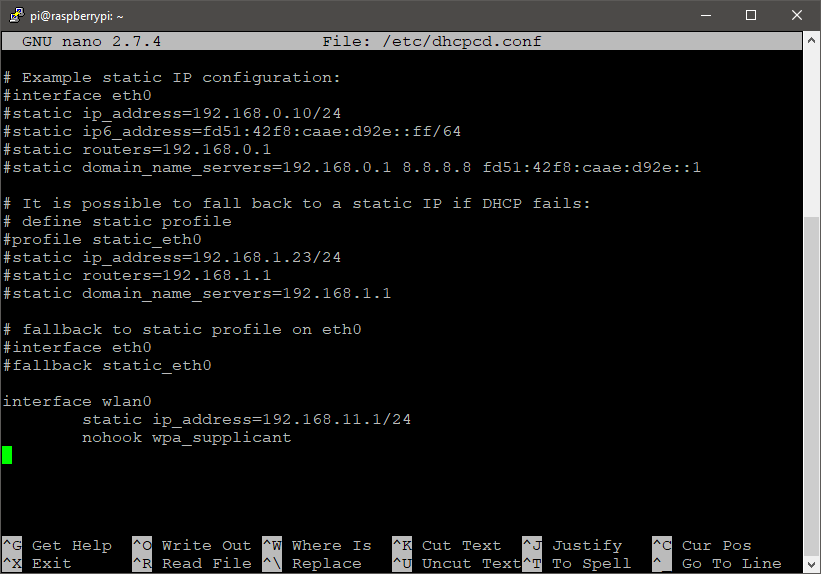
Para que nuestro punto de acceso funcione correctamente, tenemos que instalar dnsmasq y hostapd. Ambos se encuentran en los repositorios oficiales de raspbian.



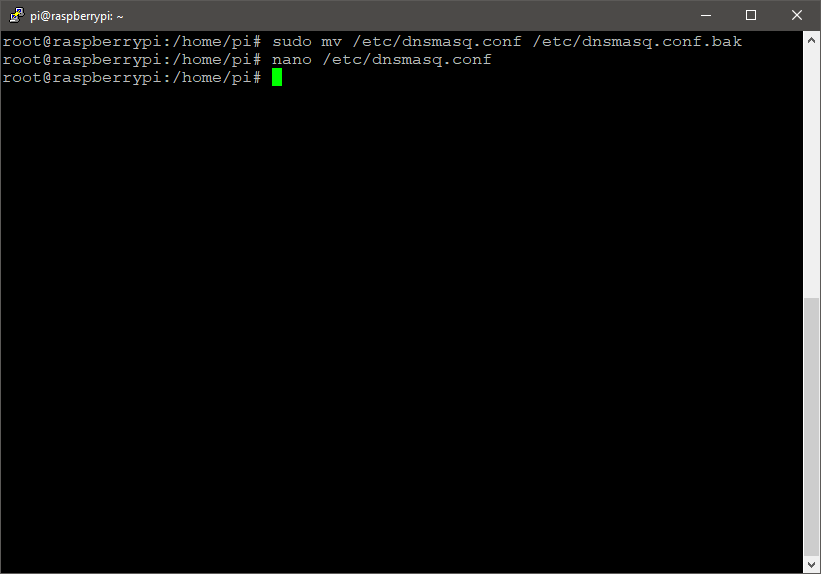
Como vamos a estar configurando estas utilidades, vamos a detener los servicios.



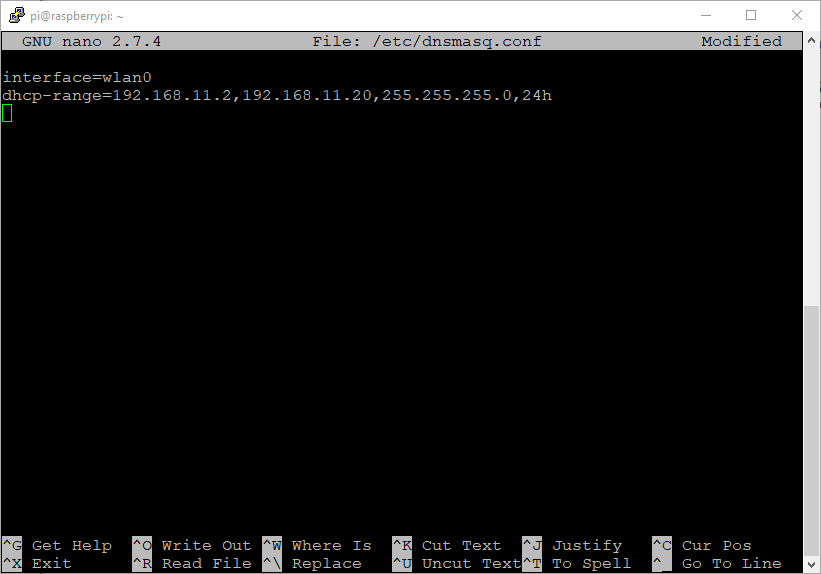
Lo primero que vamos a configurar es la interfaz de red wlan0, modificando el fichero dhcpd.conf y adaptándolo a nuestras necesidades.



Ahora configuraremos el servicio de dhcp, con dnsmasq, haciendo primero una copia de seguridad.

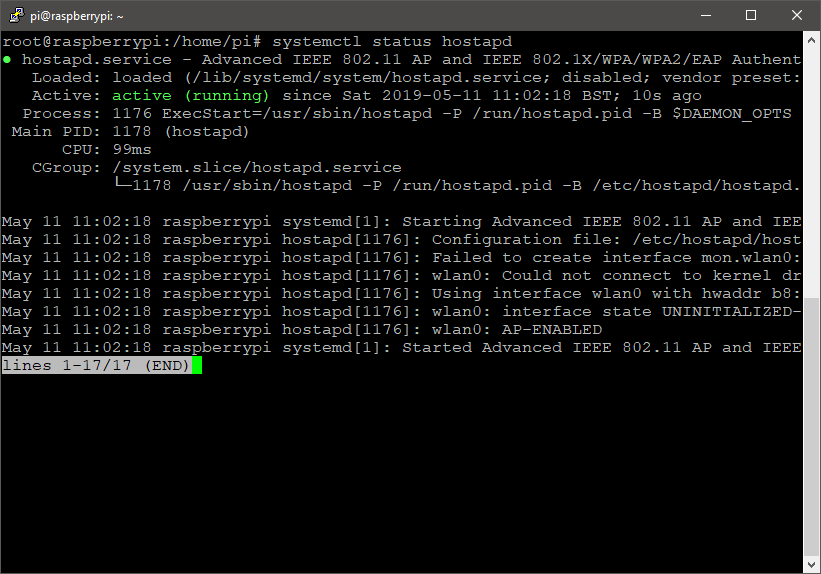
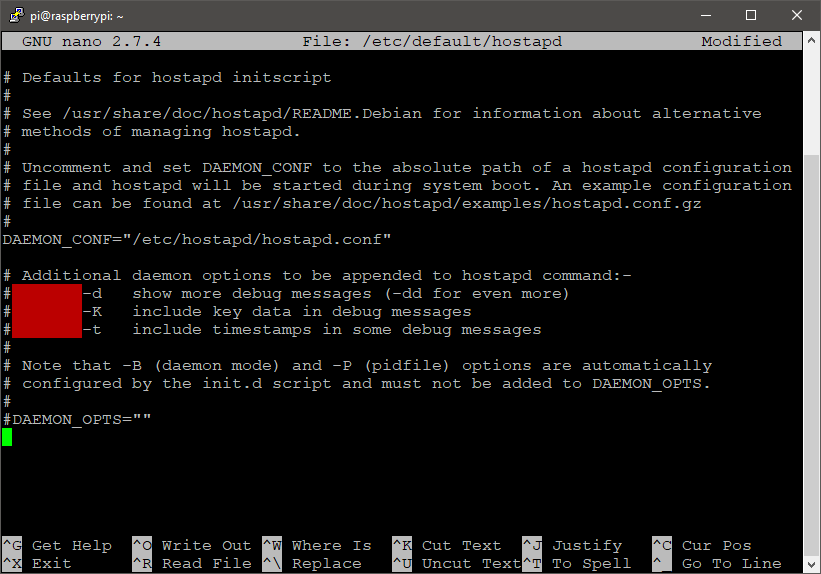
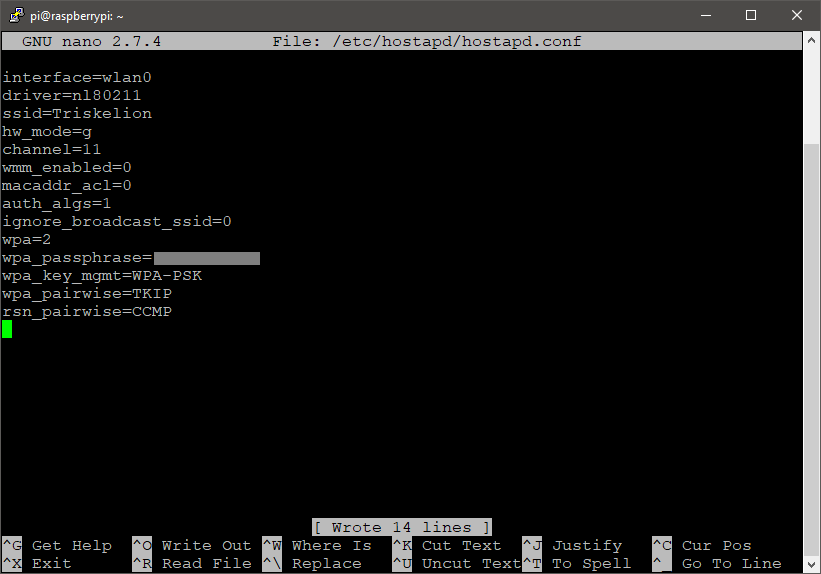


Ya que este punto de acceso solo lo vamos a utilizar para tareas sencillas, nos vale con simplemente asignar un rango de direcciones de lease.



\*Captura de DHCP funcionando\*

El hostapd, se encarga de crear el propio punto de acceso Wi-Fi y con el podemos modificar parámetros como el canal y la frecuencia en la que se transmite.



Si se quiere habilitar el punto de acceso tras iniciar el Sistema Operativo habría que ejecutar el siguiente comando:



# NextCloud

El problema que tienen los DigiSpark es que no cuentan con una memoria interna, por lo que tenemos que encontrar un método para pasar los payload al equipo víctima.

La solución que hemos planteado es la de proveer nuestro propio sistema de almacenamiento, uno que nos permita descargar directamente los archivos que necesitamos y que se adapte a nuestras necesidades.

Nextcloud es de código libre y es compatible con un buen número de dispositivos. Además, es compatible con RaspberryPi y con Docker, otra tecnología que es interesante investigar.

## NextCloudPi

NextCloudPi es una instancia de NextCloud preconfigurada que incluye un portal web con múltiples herramientas de administración.

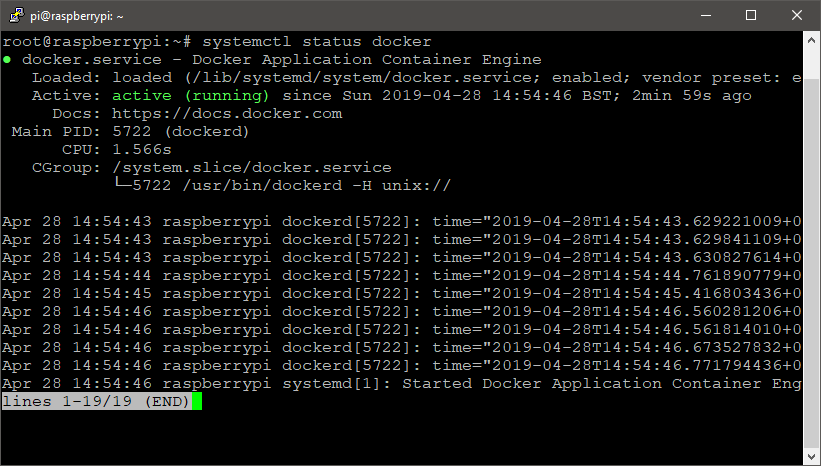
Esta distribución de NextCloud se puede instalar a través de Docker con una imagen especial para sistemas basados en ARM, teniendo como ventaja que, al estar limitado a un contenedor, no se requiere utilizar una RaspberryPi limpia únicamente para instalar NextCloud.

## Instalación

El primer paso para instalar nuestro NextCloudPi es instalar Docker, para ello usaremos el siguiente comando:



Una vez se haya instalado, podemos comprobar que funciona correctamente con systemctl.



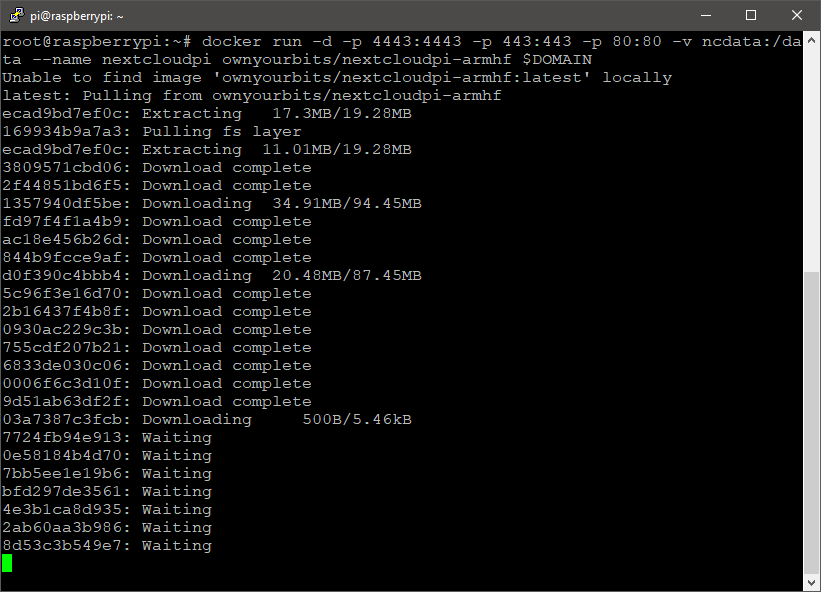
Para el correcto funcionamiento de Docker, es necesario descargar los paquetes de instalación de Python



Y también la herramienta de Docker-compose (ya a través de pip)

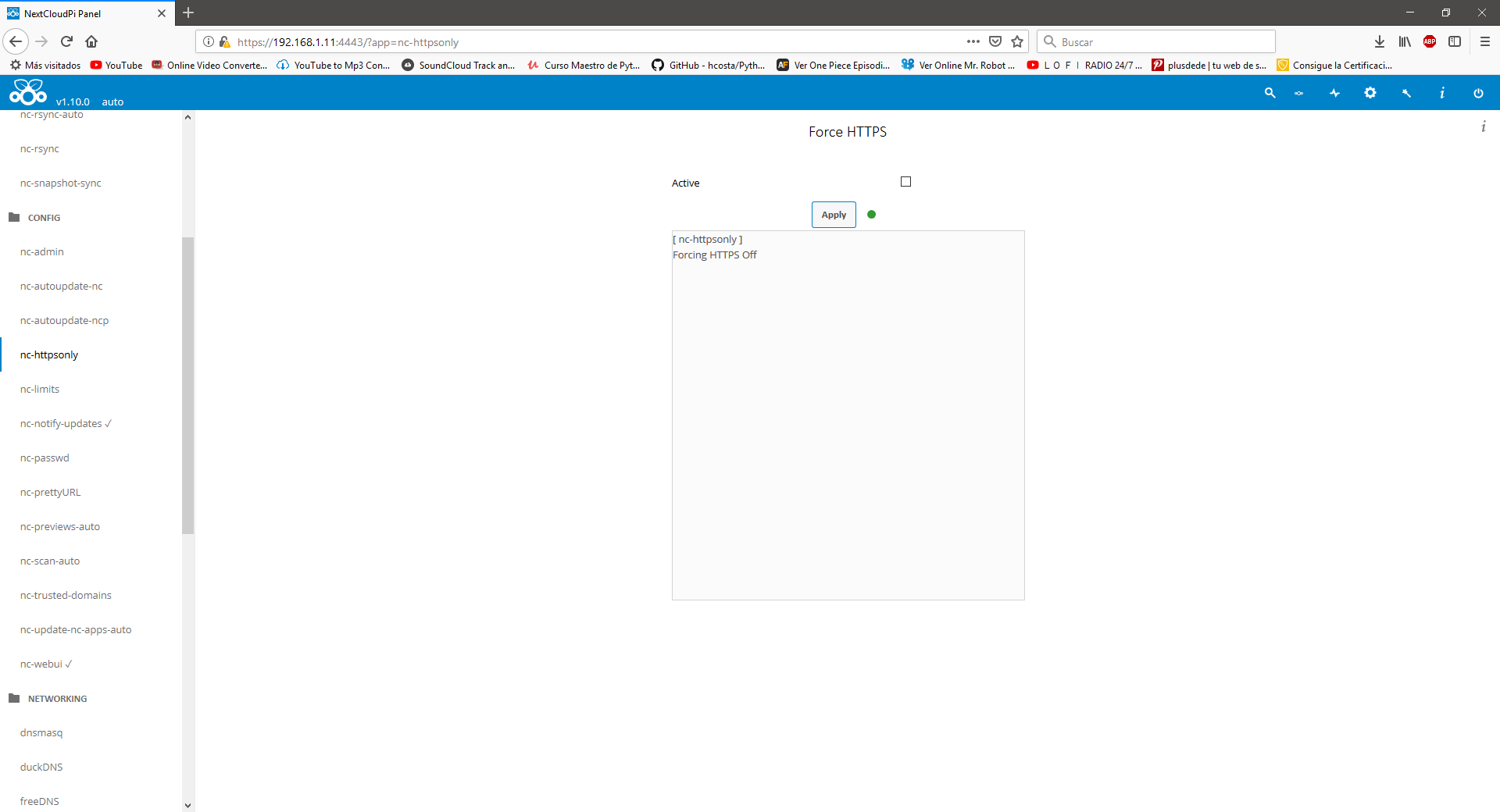


Una vez ya tenemos a Docker preparado para funcionar, descargaremos la imagen de NextCloudPi.

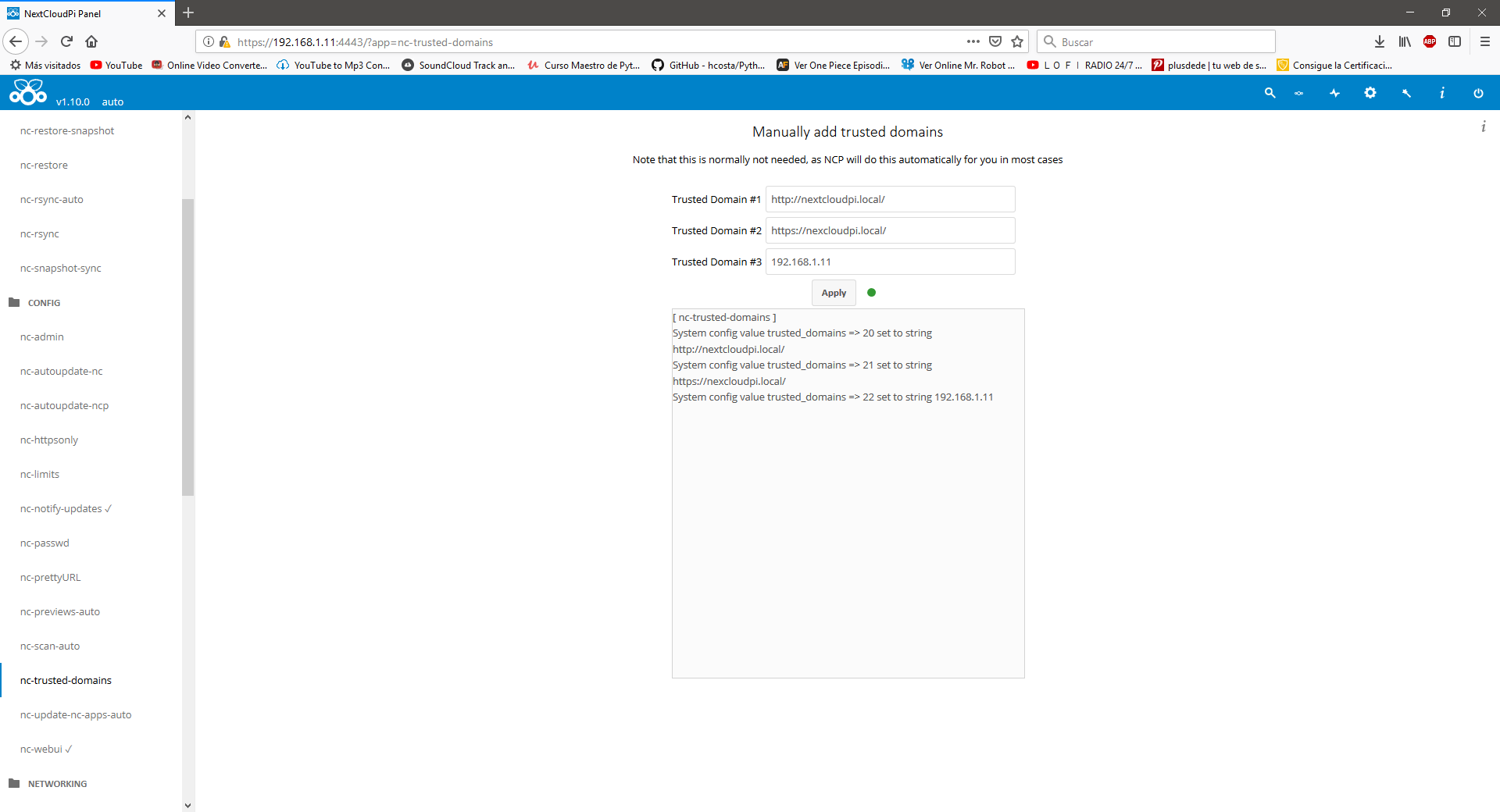


Cuando termine el proceso, el contenedor ya estará listo para usarse, a si que abriremos el navegador de internet en un ordenador en la misma red que nuestra RaspberryPi y accederemos a la siguiente dirección: <https://nextcloudpi.local:4443>

Para poder descargar el payload desde la maquina cliente, tenemos que deshabilitar el forzado https, ya que no tenemos un certificado valido y powershell no nos permitirá descargar un archivo por https si la conexión no es segura.



También aprovecharemos para definir los dominios de confianza del NextCloudPi



# DigiSpark

# Securizacion de puertos

Ahora que ya nos hemos puesto en el lado del atacante, podemos pensar de qué forma podemos proteger nuestros equipos contra un ataque por HID.

En cuanto a seguridad, podemos contemplar los siguientes aspectos: aspecto físico, el aspecto social y aspecto de software.

En cuanto al aspecto social, es importante concienciar a los empleados sobre los riesgos que puede provocar dejar su equipo desbloqueado o de no usar contraseña y de que no pueden conectar cualquier pendrive que se encuentren. De ser posible no debería utilizarse ningún pendrive que se traiga de casa, para prevenir la posible propagación de virus informáticos.

Mirando el aspecto físico, se pueden deshabilitar los puertos USB desde la BIOS, si se encuentra en un entorno en el que no se deban usar y solo mantener los estrictamente necesarios (teclado y ratón en la mayoría de los casos).

Hay múltiples soluciones a nivel de software para prevenir este tipo de ataques, en cuanto a Windows, podría desactivarse la línea de comandos del Símbolo del Sistema y de powershell o mantener un control más estricto sobre las cuentas de usuario.

En internet se pueden encontrar programas como DuckHunter, que son capaces de detectar un dispositivo de estilo RubberDucky (un emulador de teclado más avanzado que DigiSpark) mediante la monitorización de las pulsaciones del teclado, descubriendo si se está escribiendo a una velocidad excesiva y de detectar un ataque, desactivara temporalmente el teclado y registrara el ataque. Esta solución parara la mayoría de los ataques de este tipo, pero se puede evitar fácilmente, bajando la velocidad de escritura del dispositivo



DuckHunter por Pmsosa 1

# Conclusiones

# Bibliografía

**Documentación sobre Cloud de Archivos**

[**https://ownyourbits.com/2017/11/15/nextcloudpi-dockers-for-x86-and-arm/**](https://ownyourbits.com/2017/11/15/nextcloudpi-dockers-for-x86-and-arm/) **(versión actualizada)**

[**https://ugeek.github.io/blog/post/2019-01-06-nextcloudpi.-nextcloud-en-raspbian-con-docker.html**](https://ugeek.github.io/blog/post/2019-01-06-nextcloudpi.-nextcloud-en-raspbian-con-docker.html)

[**https://www.redeszone.net/2017/06/13/nextcloudpi-docker-instala-y-utiliza-nextcloud-en-tu-raspberry-pi-gracias-a-docker/**](https://www.redeszone.net/2017/06/13/nextcloudpi-docker-instala-y-utiliza-nextcloud-en-tu-raspberry-pi-gracias-a-docker/)

**Documentación sobre RubberDucky**

[**https://null-byte.wonderhowto.com/how-to/automate-hacking-raspberry-pi-with-usb-rubber-ducky-0177088/**](https://null-byte.wonderhowto.com/how-to/automate-hacking-raspberry-pi-with-usb-rubber-ducky-0177088/)

[**https://null-byte.wonderhowto.com/how-to/load-use-keystroke-injection-payloads-usb-rubber-ducky-0176829**](https://null-byte.wonderhowto.com/how-to/load-use-keystroke-injection-payloads-usb-rubber-ducky-0176829)

**Documentación sobre Raspberry**

[**https://thepi.io/how-to-use-your-raspberry-pi-as-a-wireless-access-point/**](https://thepi.io/how-to-use-your-raspberry-pi-as-a-wireless-access-point/)

[**https://www.raspberrypi.org/**](https://www.raspberrypi.org/)

**Documentación sobre prevenir el ataque USB**

[**https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/usbview**](https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/usbview)

[**https://hackaday.com/2016/10/28/duckhunting-stopping-rubber-ducky-attacks/**](https://hackaday.com/2016/10/28/duckhunting-stopping-rubber-ducky-attacks/)

[**https://www.nirsoft.net/utils/usb\_devices\_view.html**](https://www.nirsoft.net/utils/usb_devices_view.html)

[**https://www.fwhibbit.es/matando-al-patito-proteger-puertos-usb**](https://www.fwhibbit.es/matando-al-patito-proteger-puertos-usb) **(Bloqueo con whitelist)**

[**https://www.solvetic.com/tutoriales/article/2935-como-bloquear-dispositivos-usb-en-el-dominio-con-gpo/**](https://www.solvetic.com/tutoriales/article/2935-como-bloquear-dispositivos-usb-en-el-dominio-con-gpo/) **(Con GPO)**

**Documentación sobre ataques por USB**

[**https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads**](https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads)

[**https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload--Fast-Meterpreter**](https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload--Fast-Meterpreter)

[**https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---download-mimikatz%2C-grab-passwords-and-email-them-via-gmail**](https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---download-mimikatz%2C-grab-passwords-and-email-them-via-gmail)

[**https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---WiFun-v1.1**](https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---WiFun-v1.1)

**Documentación sobre compilar scripts en Digispark**

[**https://seytonic.com/ducky/**](https://seytonic.com/ducky/) **(Online)**

[**https://github.com/CedArctic/digiQuack**](https://github.com/CedArctic/digiQuack)

[**https://github.com/toxydose/Duckyspark**](https://github.com/toxydose/Duckyspark)

[**https://ducktoolkit.com/payload/windows**](https://ducktoolkit.com/payload/windows) **(Creador de código personalizado Online)**

**Documentación sobre BadUSB**

[**https://www.quora.com/Which-USB-drives-contain-Phison-2251-03-2303-controller-type**](https://www.quora.com/Which-USB-drives-contain-Phison-2251-03-2303-controller-type)

[**https://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/**](https://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/)

**Documentación sobre creación de Payload**

[**https://www.flu-project.com/2012/08/msfvenom-la-cosa-va-de-payloads-y\_28.html**](https://www.flu-project.com/2012/08/msfvenom-la-cosa-va-de-payloads-y_28.html)

[**https://underc0de.org/foro/hacking/curso-metasploit-part-5-hablemos-de-msfvenom/**](https://underc0de.org/foro/hacking/curso-metasploit-part-5-hablemos-de-msfvenom/)

[**https://underc0de.org/foro/hacking/curso-metasploit-part-5-1-creando-un-paylodad-basico/**](https://underc0de.org/foro/hacking/curso-metasploit-part-5-1-creando-un-paylodad-basico/)

**Ocultación de Payloads**

[**https://underc0de.org/foro/hacking/t23851/**](https://underc0de.org/foro/hacking/t23851/)

[**https://underc0de.org/foro/criptografia-253/t28569/**](https://underc0de.org/foro/criptografia-253/t28569/)

[**https://securityhacklabs.net/articulo/metasploit-y-windows-10-creando-un-payload-indetectable-evadiendo-software-antivirus**](https://securityhacklabs.net/articulo/metasploit-y-windows-10-creando-un-payload-indetectable-evadiendo-software-antivirus)

[**https://github.com/trustedsec/unicorn**](https://github.com/trustedsec/unicorn)