Bash Bunny

The best penetration testers know that with the right tools and a few seconds of physical access, all bets are off.

It opens up attack surfaces that weren't possible before in one single device. Penetration testing attacks and IT automation tasks are all delivered in seconds with the Bash Bunny. By emulating combinations of trusted USB devices – like gigabit Ethernet, serial, flash storage and keyboards – computers are tricked into divulging data, exfiltrating documents, installing backdoors and many more exploits.

Exploiting local network attack vectors, the Bash Bunny emulates specialized Ethernet adapters.

Each attack, or payload, is written in a simple «Bunny Script» language consisting of one or more text files. These payloads can be found from the central repository – a library of community developed attacks. Staying up to date with all of the latest payloads is just a matter of downloading a zip file from git. Loading these payloads onto the Bash Bunny is as simple as copying files, just as you would to any ordinary flash drive.

More information

https://hakshop.com/products/bash-bunny