Top Hacking Gadgets

1. Wi-Fi Pineapple
   A tool designed for analyzing and exploiting wireless networks. It can be used for Man-in-the-Middle (MITM) attacks, detecting and exploiting vulnerabilities in Wi-Fi networks.

2. USB Rubber Ducky
   A device that looks like a common USB stick but can execute pre-programmed keyboard commands when plugged into a computer. It is used for automated attacks and injecting malicious code.

3. Raspberry Pi
   A small and affordable computer that can be programmed for various hacking activities, such as wireless network experiments, network attacks, and custom penetration testing projects.

4. Proxmark3
   A device for analyzing and attacking RFID systems. It is used for reading, copying, and simulating RFID cards commonly found in access control and contactless payment systems.

5. Hak5 LAN Turtle
   A tool that looks like a USB Ethernet adapter, designed for remote access and network analysis. It can be used for network attacks and gaining remote access.

6. HackRF One
   A platform for Software Defined Radio (SDR) that can be used for analyzing and attacking wireless signals across a wide range of frequencies. It is used for experiments and attacks on wireless protocols like GSM, Bluetooth, and Wi-Fi.

7. Keyllama USB Keylogger
   A device that records all keystrokes on a computer. It is used for monitoring and analyzing the commands typed on a target system.

8. Alfa Network Adapter
   A powerful USB wireless adapter used for analyzing and attacking Wi-Fi networks. It offers high range and sensitivity, making it ideal for network scanning and WPA/WPA2 encryption attacks.

9. O.MG Cable
A seemingly ordinary USB cable that actually contains malicious software and wireless communication capabilities. It can be used to send malicious commands and gain remote access to systems.

10. Signal Hound BB60C
A portable spectrum analyzer used for analyzing and monitoring wireless frequencies. It helps in detecting and analyzing hidden signals and interferences across various frequencies.

11. Throwing Star LAN Tap
A small tool that connects between two network devices to monitor data traffic on a network. It is used for packet analysis and understanding network protocols and traffic.

12. Ubertooth One
An open-source platform for developing and analyzing Bluetooth devices. It is used for detecting, monitoring, and analyzing Bluetooth communications and protocols.

13. HackRF Blue
A cheaper alternative to the HackRF One, used for experiments and analysis across a wide range of wireless frequencies.

14. Bash Bunny
A tool that looks like a USB stick but offers a full Linux computer. It is used for automated attacks, such as credential harvesting, network attacks, and payload delivery.

15. RFIDler
A tool for reading, writing, and simulating RFID cards. It is mainly used for researching and exploiting vulnerabilities in RFID systems.

16. Flipper Zero
The Flipper Zero is a versatile, open-source, multi-tool device designed for penetration testing and exploring digital interfaces. Shaped like a toy dolphin, it features a variety of modules that allow it to interact with RFID, NFC, infrared, Bluetooth, and GPIO interfaces.