

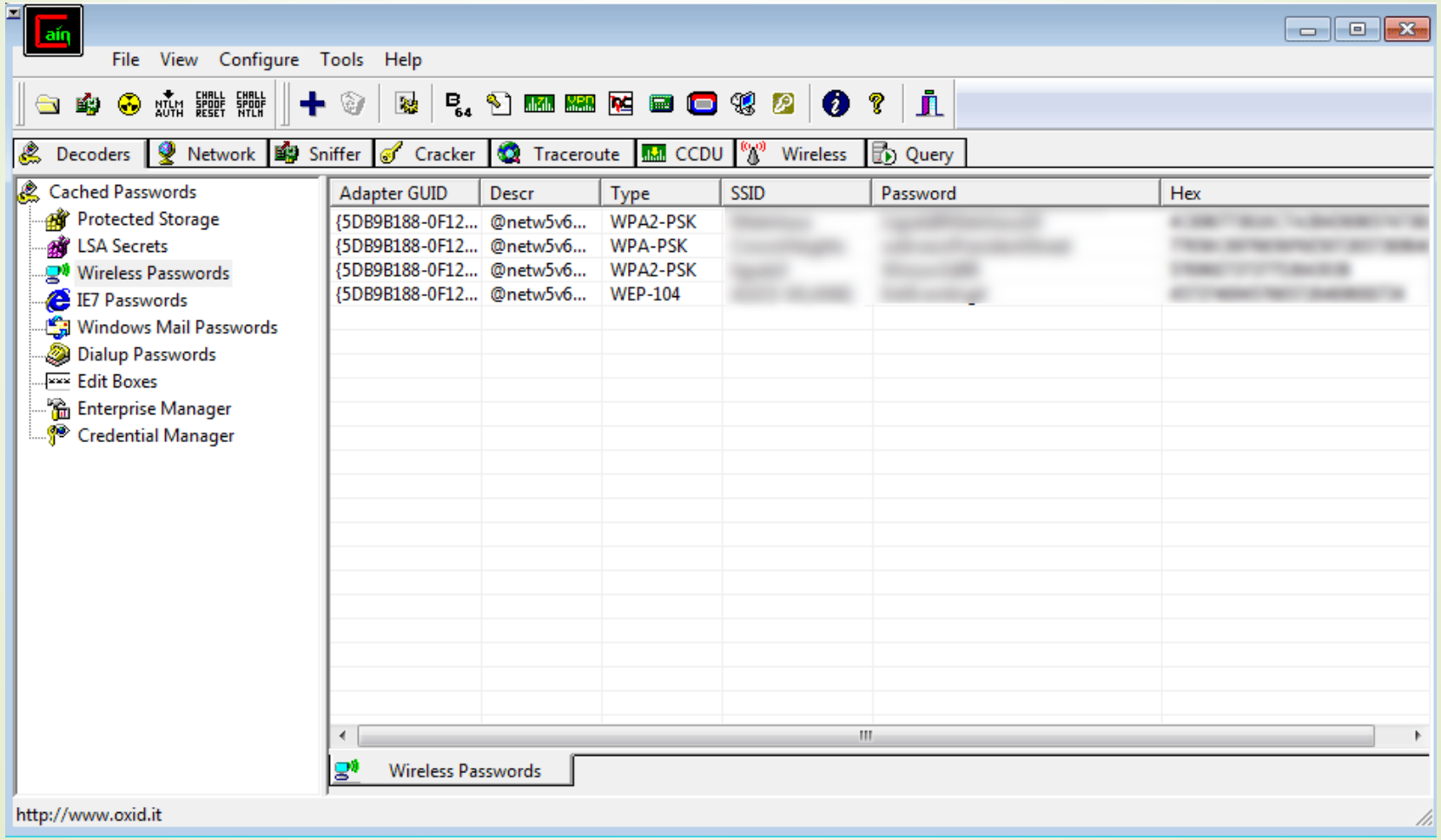
Herramientas Hardware de Hacking

César Granda Fernández

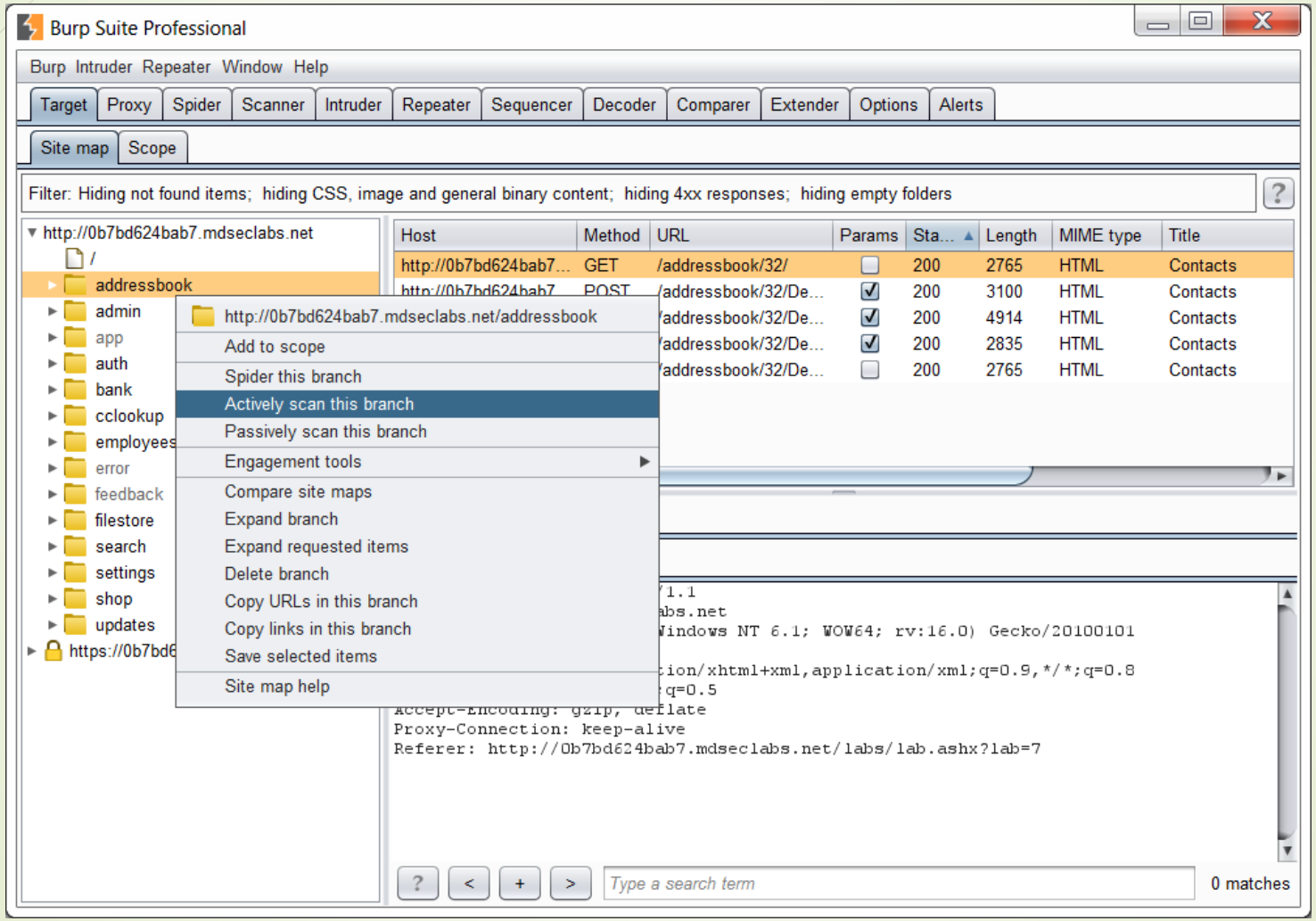
Sara Cayuela Rodríguez

Cyberworking 2018

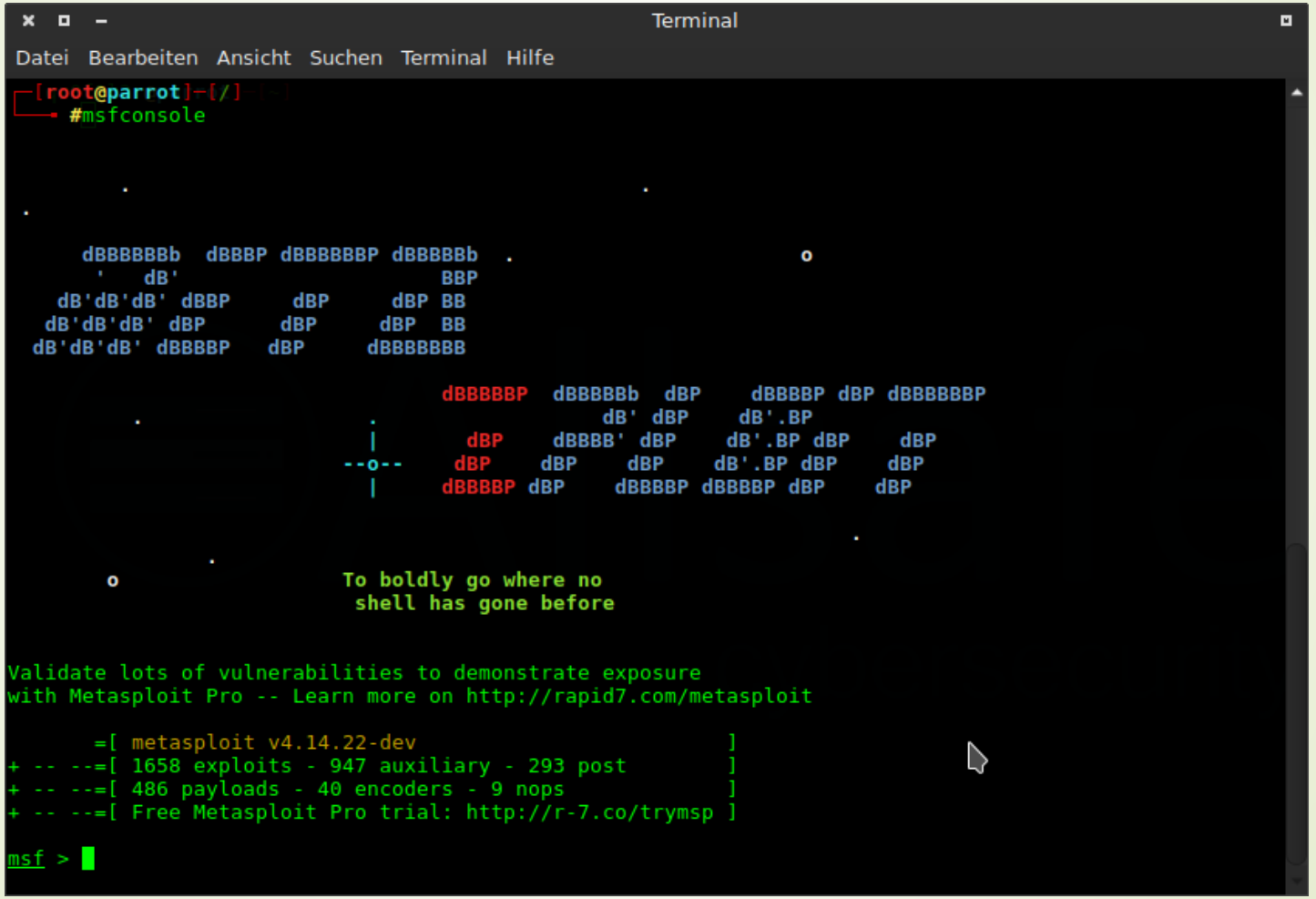
Tipos de herramientas-Software



Tipos de herramientas-Software



Tipos de herramientas-Software



Tipos de herramientas-Software



Tipos de herramientas-Software



Tipos de herramientas-Humanos



Tipos de herramientas- Hardware

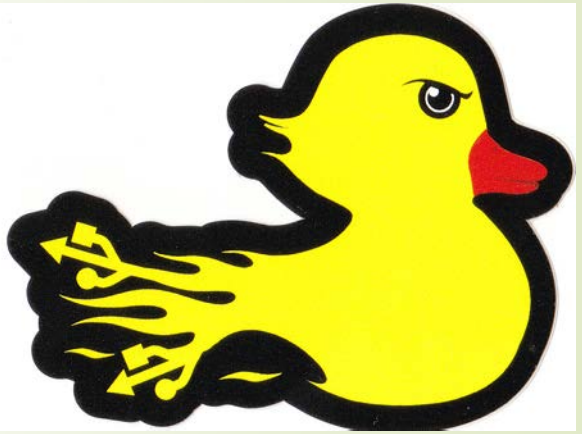
- Tipos
  - Bad USB
  - Dispositivos destinados a Redes.
  - Dispositivos WIFI

Tipos de herramientas- Hardware

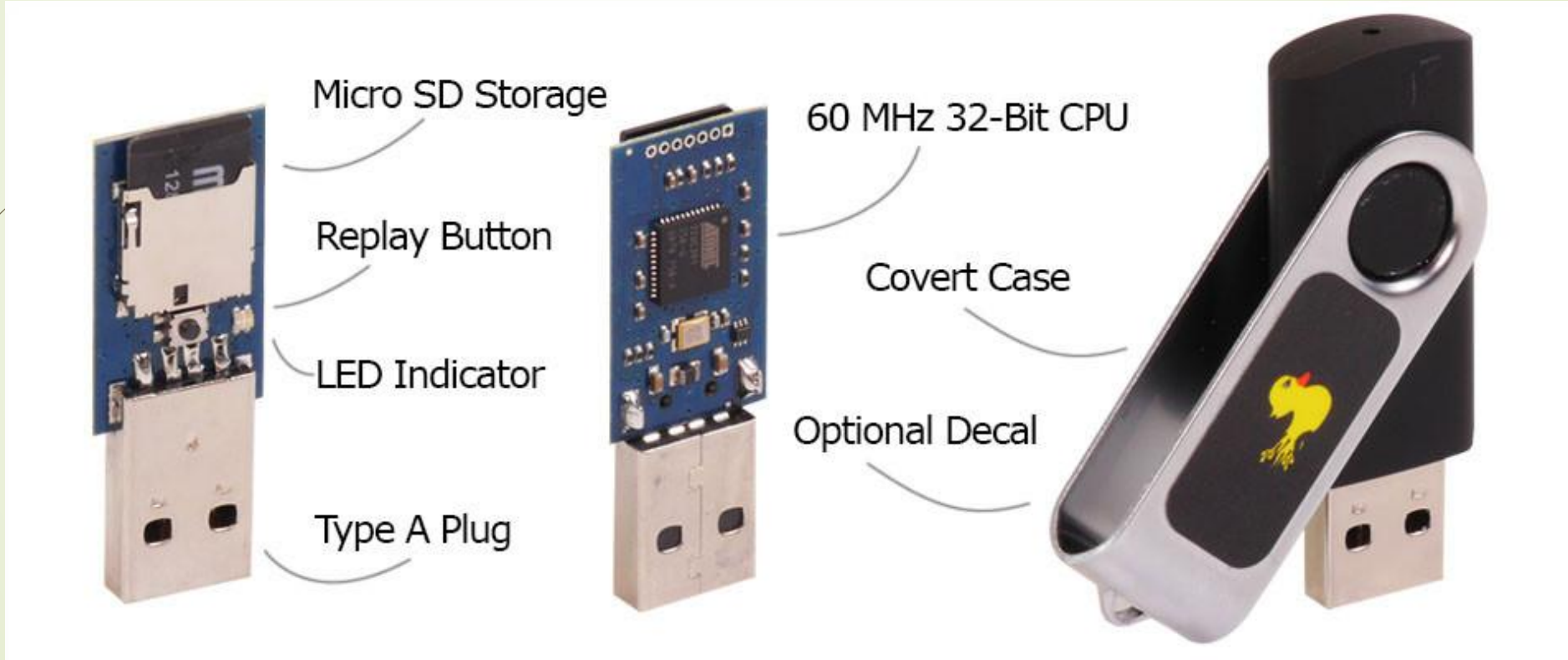


Rubber Ducky

- Hardware
  - Atmel 32bit AVR Microcontroller AT32UC3B1256
  - MicroSD card reader
  - Micro push-button
  - Multi-color LED indicator
  - Standard “Type A” USB connector
- Amtel AT32UC3B1256 Features
  - Amtel AT32UC3B1256
  - Performing up to 1.39 DMIPS / MHz
  - Memory Protection Unit
  - Internal High-Speed Flash

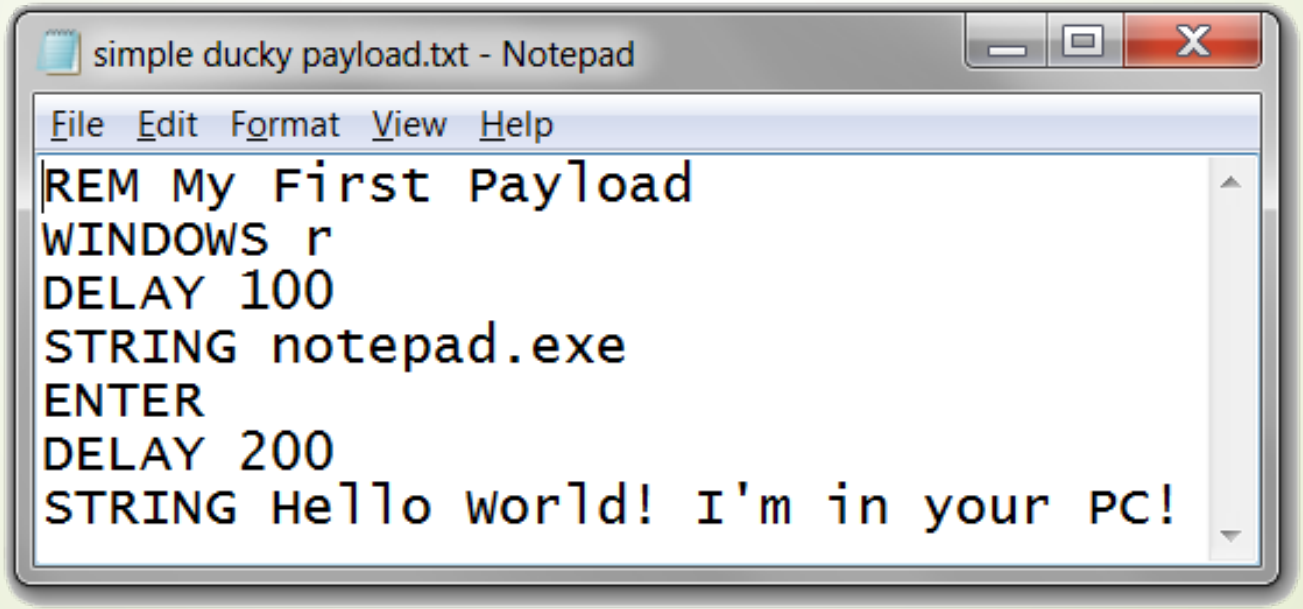


Rubber Ducky(II)



Rubber Ducky(II)

- Mi primer Payload.

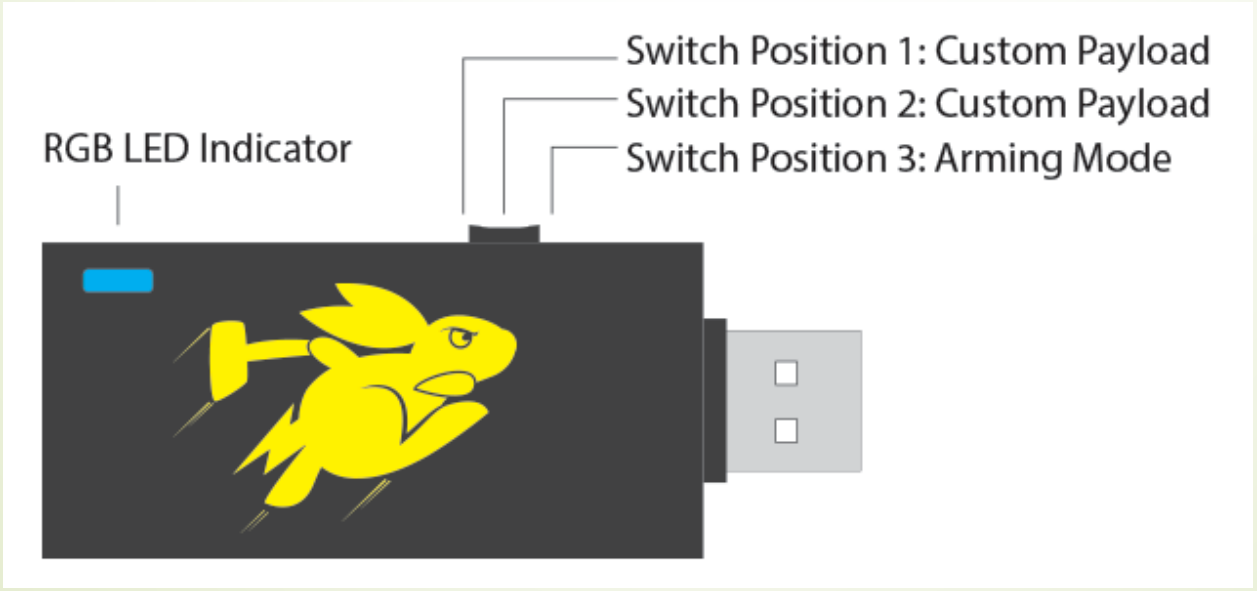


Rubber Ducky(II)

- Generar Payloads
  - https://ducktoolkit.com/
  - Mediante la librería .jar “Dunkencoder”

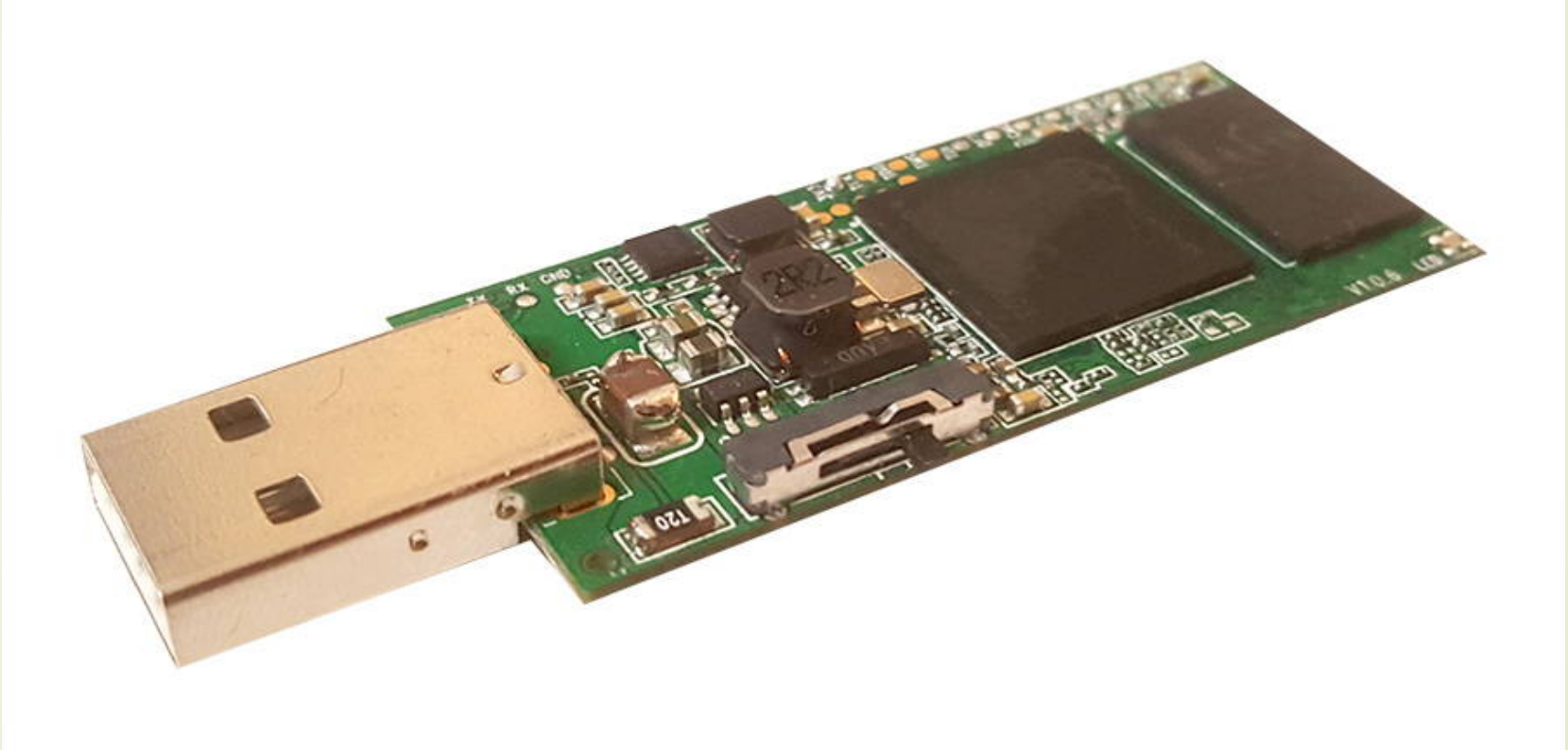
Bash Bunny

- Specifications
  - Quad-core ARM Cortex A7
  - 32 K L1/512 K L2 Cache
  - 512 MB DDR3 Memory
  - 8 GB SLC NAND Disk





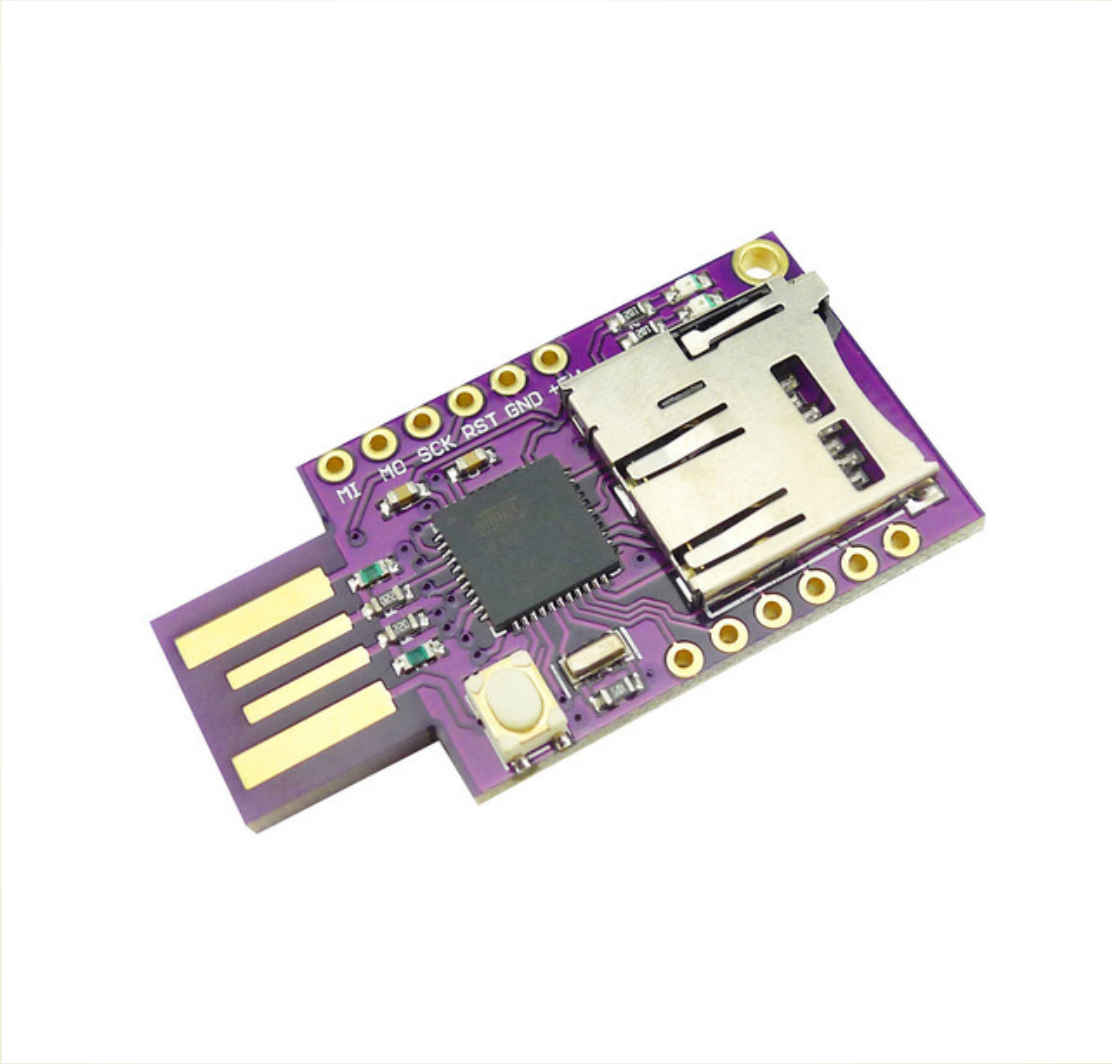
Bash Bunny(II)



Bash Bunny(II)

- Demo
  - https://github.com/hak5/bashbunny-payloads

Bad USB

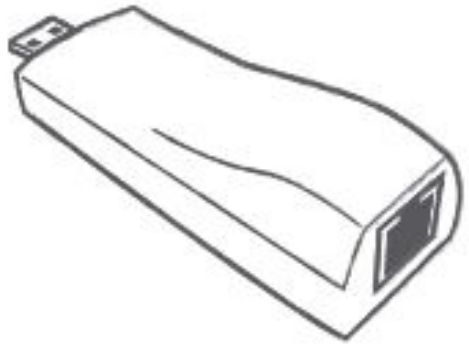


Lan Turtle

- Specifications
  - Atheros AR9331 SoC at 400 MHz MIPS
  - 16 MB Onboard Flash
  - 64 MB DDR2 RAM
  - 10/100 Ethernet Port
  - USB Ethernet Port – Realtek RTL8152
  - Indicator LED (Green Power, Amber Status)
  - Button (inside case for Factory Reset / Firmware Recovery)
  - Dimensions: 95 x 23 x 31 mm



Lan Turtle



CONFIGURE

Set it up for Remote Access, Man-in-the-Middle or Network Reconnaissance.

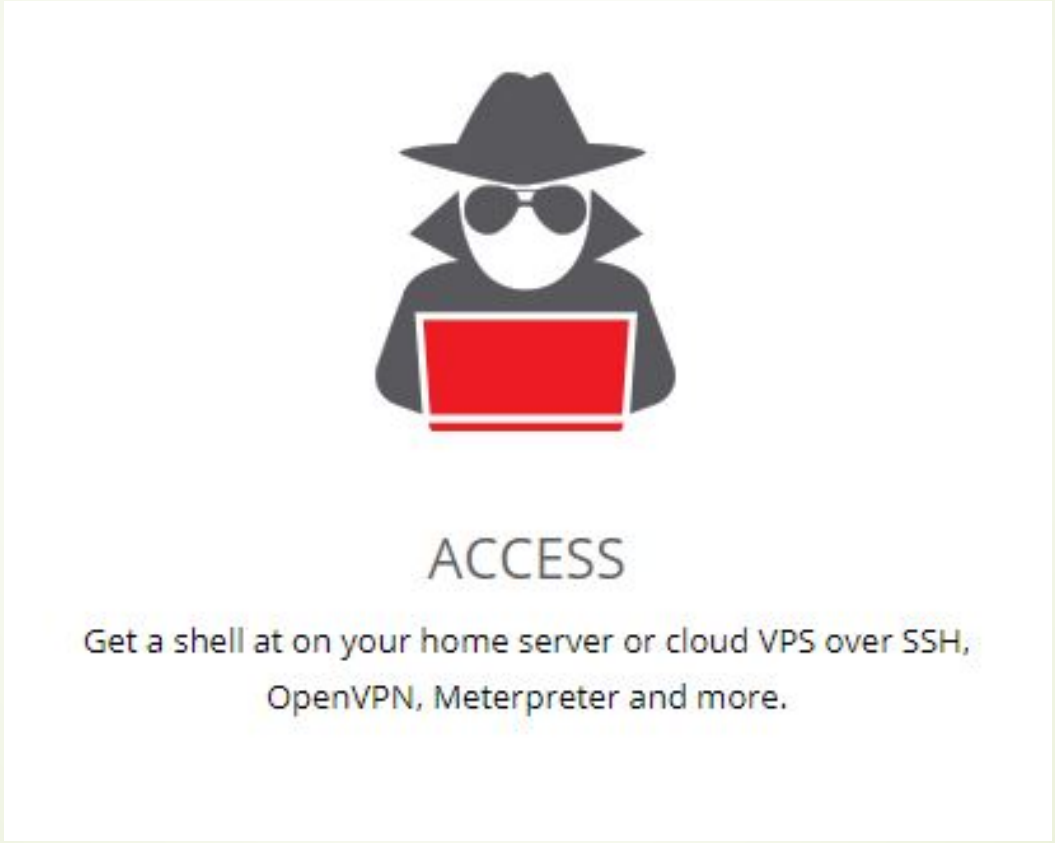
Lan Turtle



DEPLOY

Disguised as a USB Ethernet Adapter, it easily blends in with your target network.

Lan Turtle

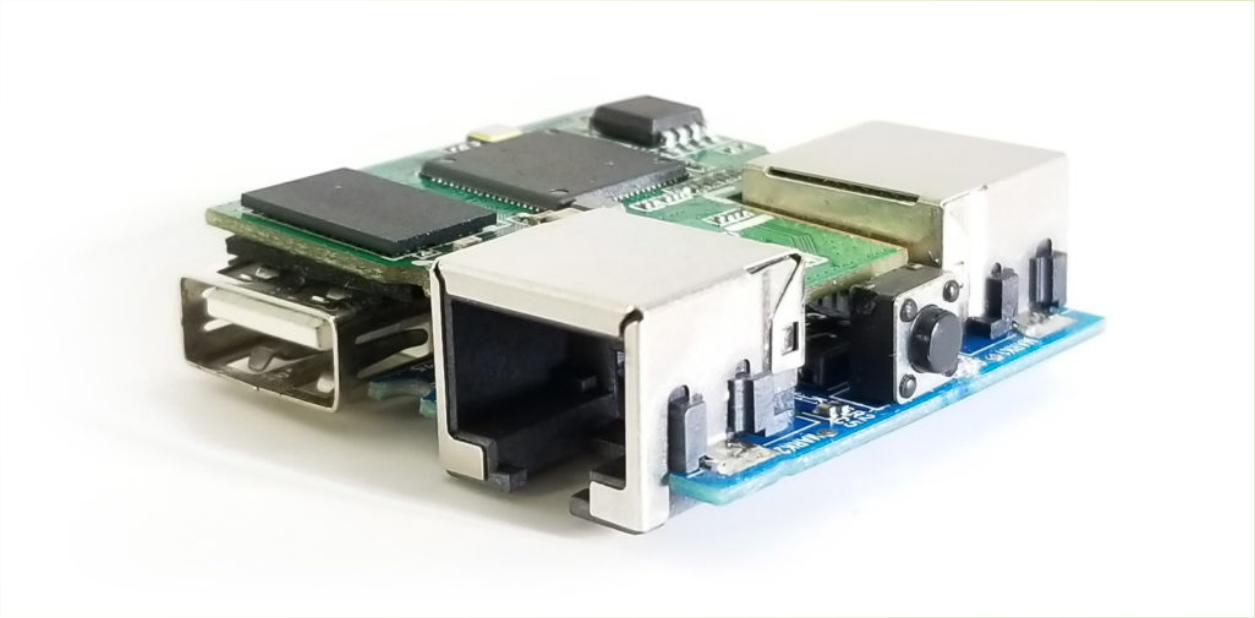

ACCESS
Get a shell at on your home server or cloud VPS over SSH,
OpenVPN, Meterpreter and more.

Lan Turtle

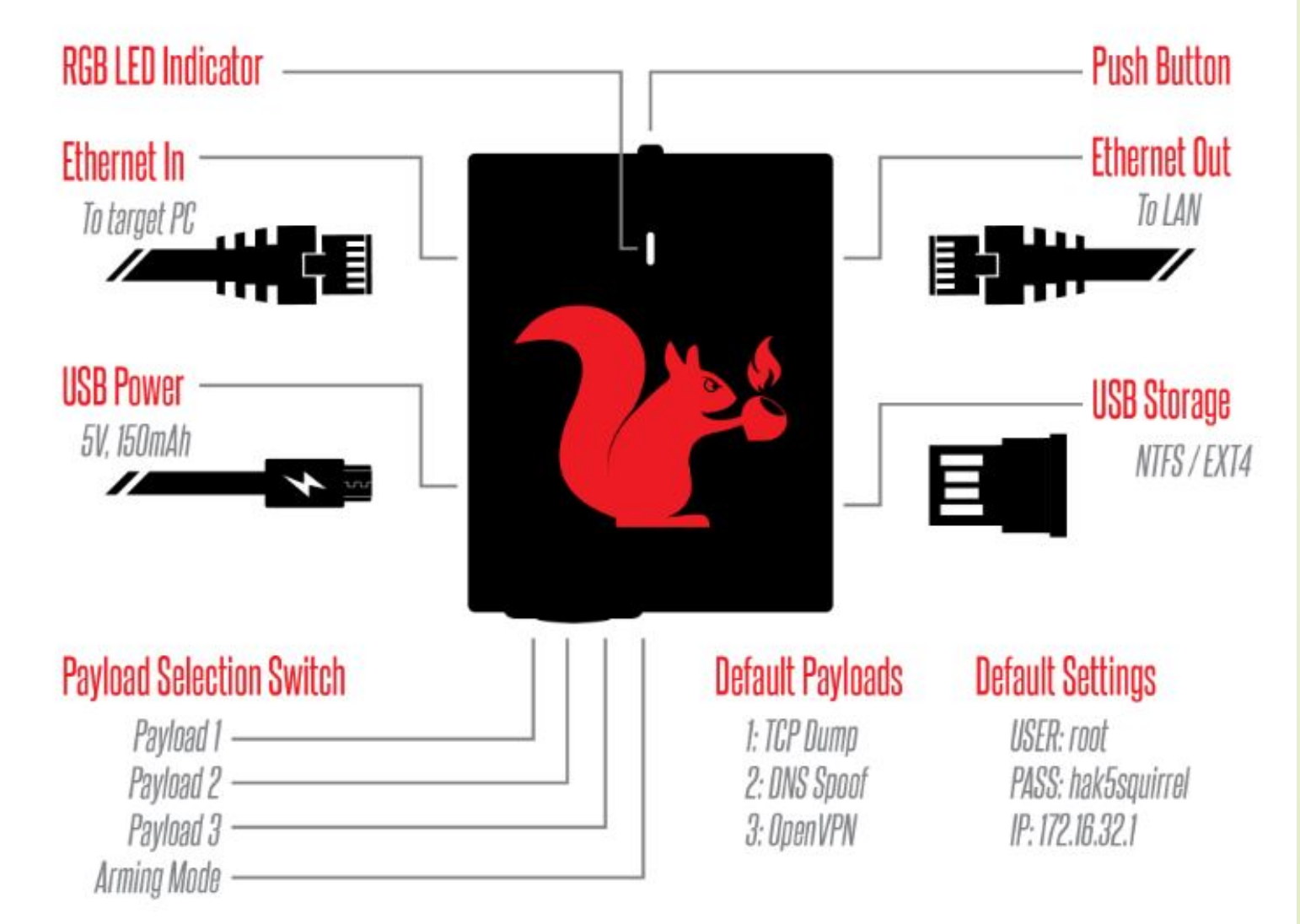


Packet Squirrel





Packet Squirrel



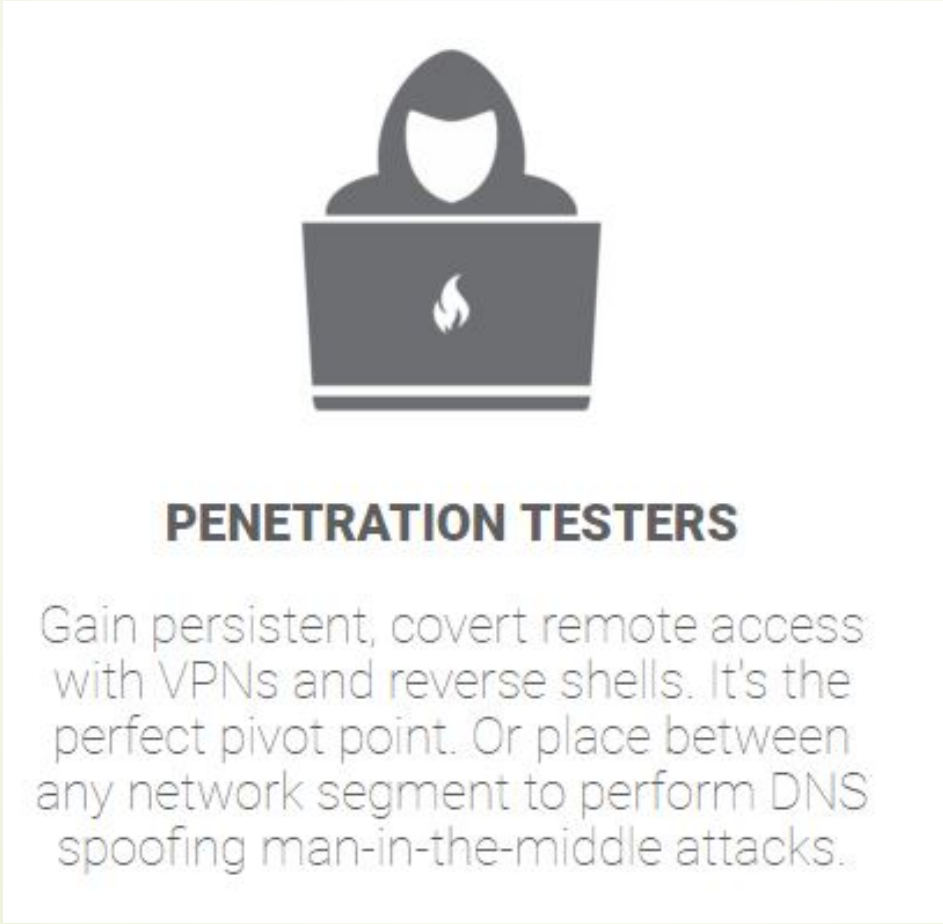
Packet Squirrel



SYSTEMS ADMINISTRATORS

Easily capture packets between any network endpoint. Save standard .pcap files to ordinary USB flash drives for later analysis with open source tools like Wireshark.

Packet Squirrel



Packet Squirrel



PRIVACY CONSCIOUS

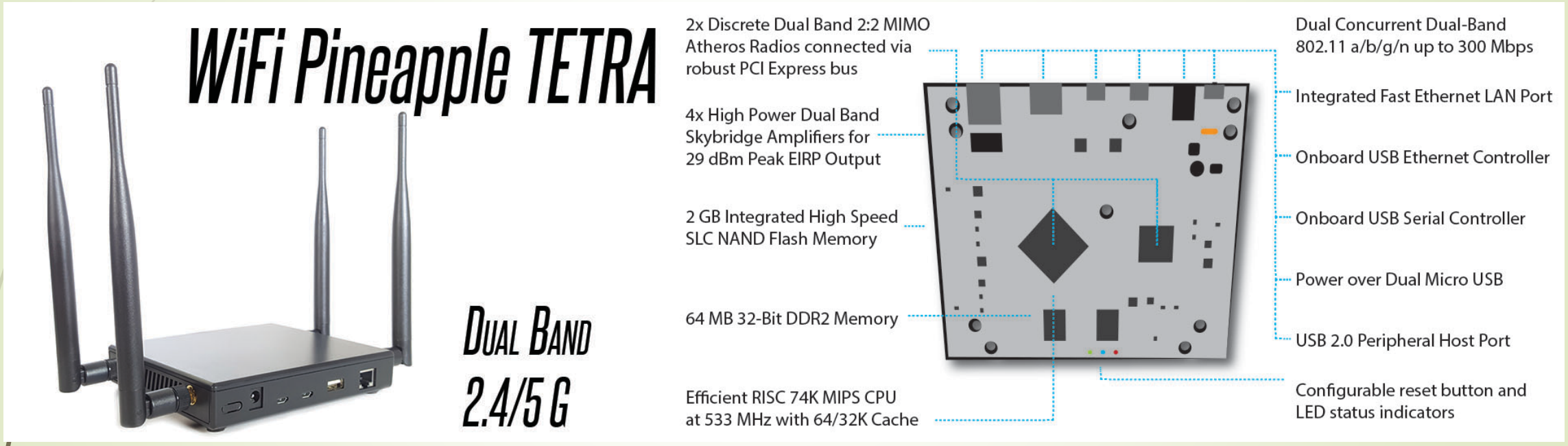
Confidently maintain privacy with this advanced hardware firewall and VPN router. All network traffic can be securely passed through encrypted OpenVPN-based tunnels with ease.

Wifi Pineapple TETRA



- **Specifications**
  - CPU: 533 MHz MIPS 74K Atheros AR
  - Memory: 64 MB DDR2 RAM
  - Disk: 2 GB NAND Flash
  - Wireless: Atheros AR9344 + Atheros AR9580, both IEEE 802.11 a/b/g/n with quad integrated skybridge amplifiers and included 5 dBi antenna for a high 29 dBm gain EIRP
  - Ports: (4) SMA Antenna, RJ45 Fast Ethernet, Ethernet over USB, Serial over USB, USB 2.0 Host, 12V/2A DC Power

Wifi Pineapple TETRA



Wifi Pineapple NANO

- CPU: 400 MHz MIPS Atheros AR9331 SoC
- Memory: 64 MB DDR2 RAM
- Disk: 16 MB ROM + Micro SD (not included. up to 200GB)
- Wireless: Atheros AR9331 (wlan0) + Atheros AR9271 (wlan1), both IEEE 802.11 b/g/n
- Ports: (2) RP-SMA Antenna, Ethernet over USB (ASIX AX88772A)
- USB 2.0 Host, Micro SD card reader

Wifi Pineapple NANO



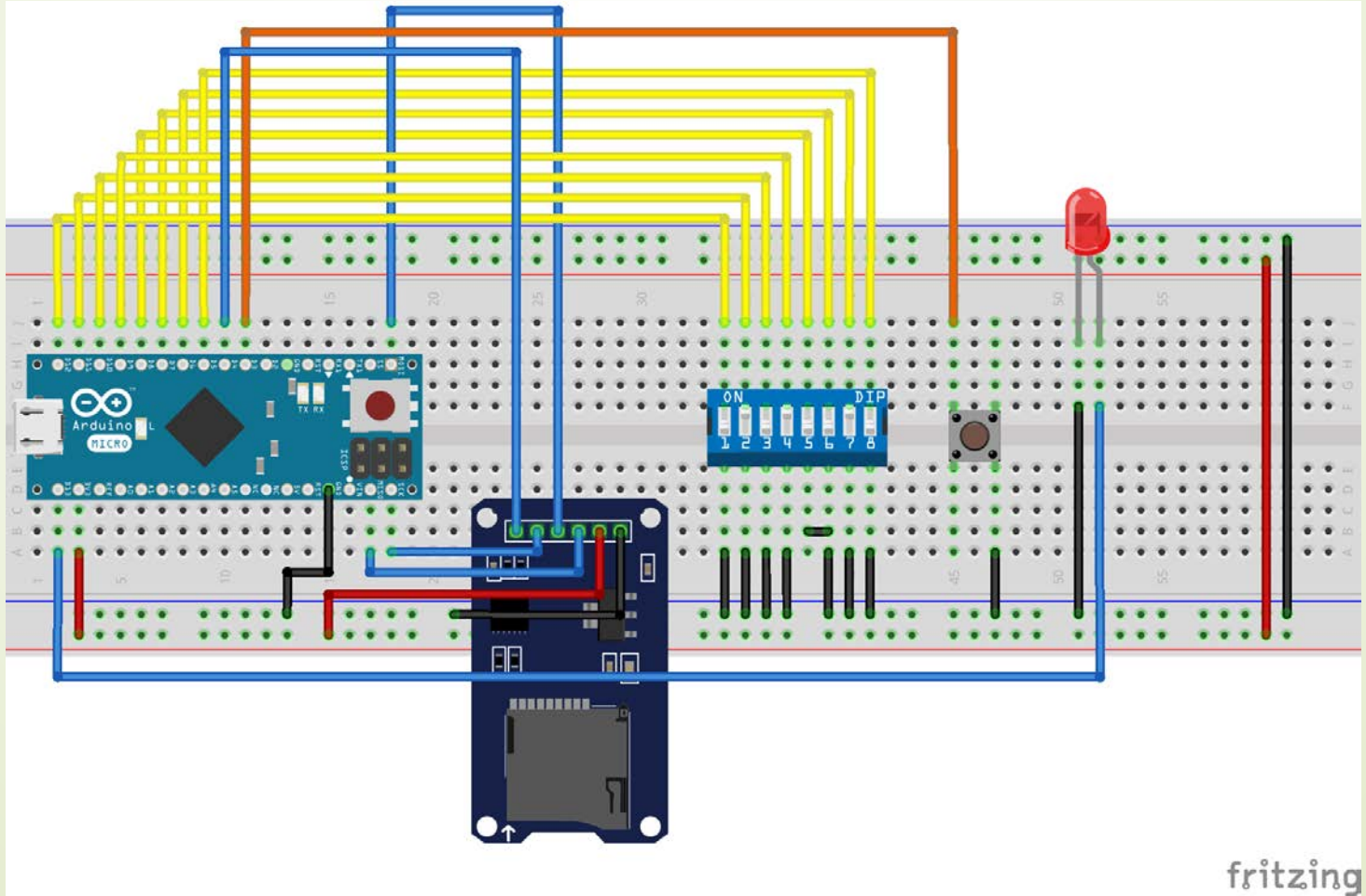
USB Killer

- **Killer Specifications:**
  - Input voltage: 4.5 - 5.5 VDC
  - Output voltage: -215 VDC
  - Pulse Frequency: 8 - 12 times / second
  - Pulse current: ≥180A
  - CE & FCC Approved, allowing you to test in complete safety.



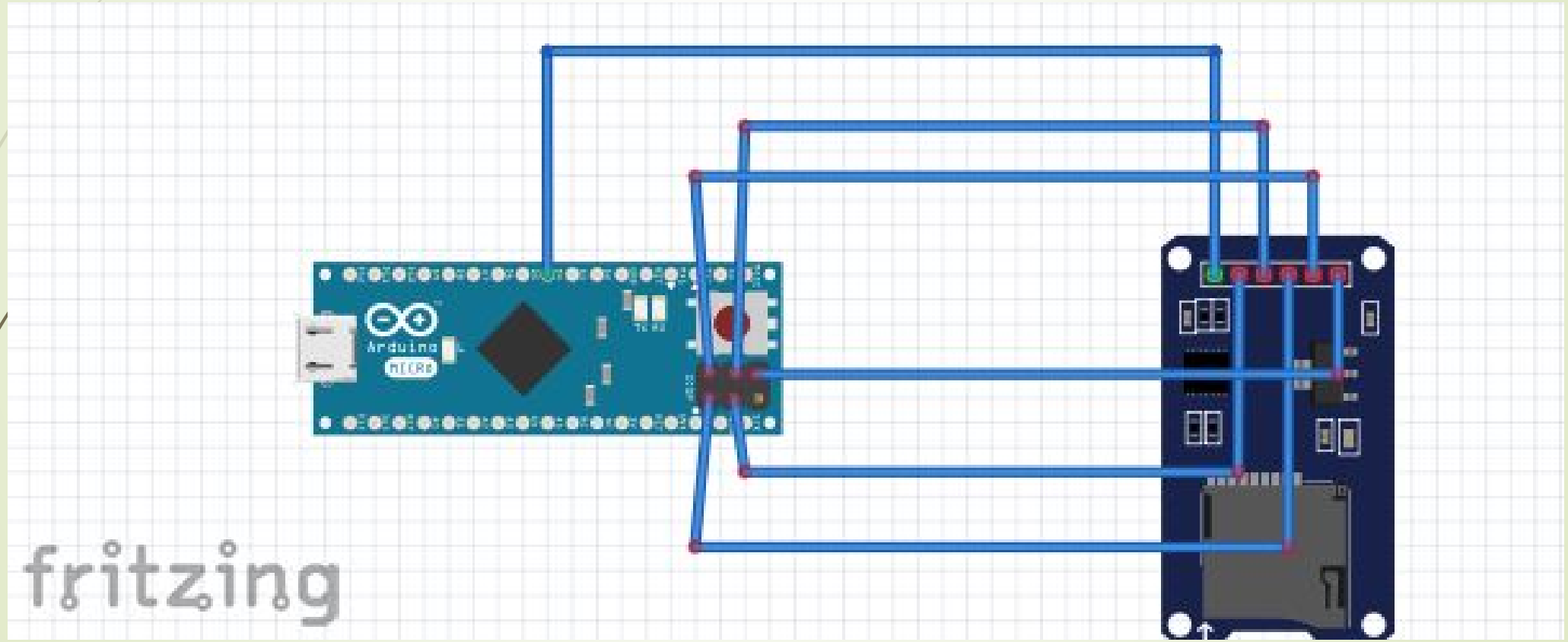
Taller

- https://github.com/toolsprods/ArDucky

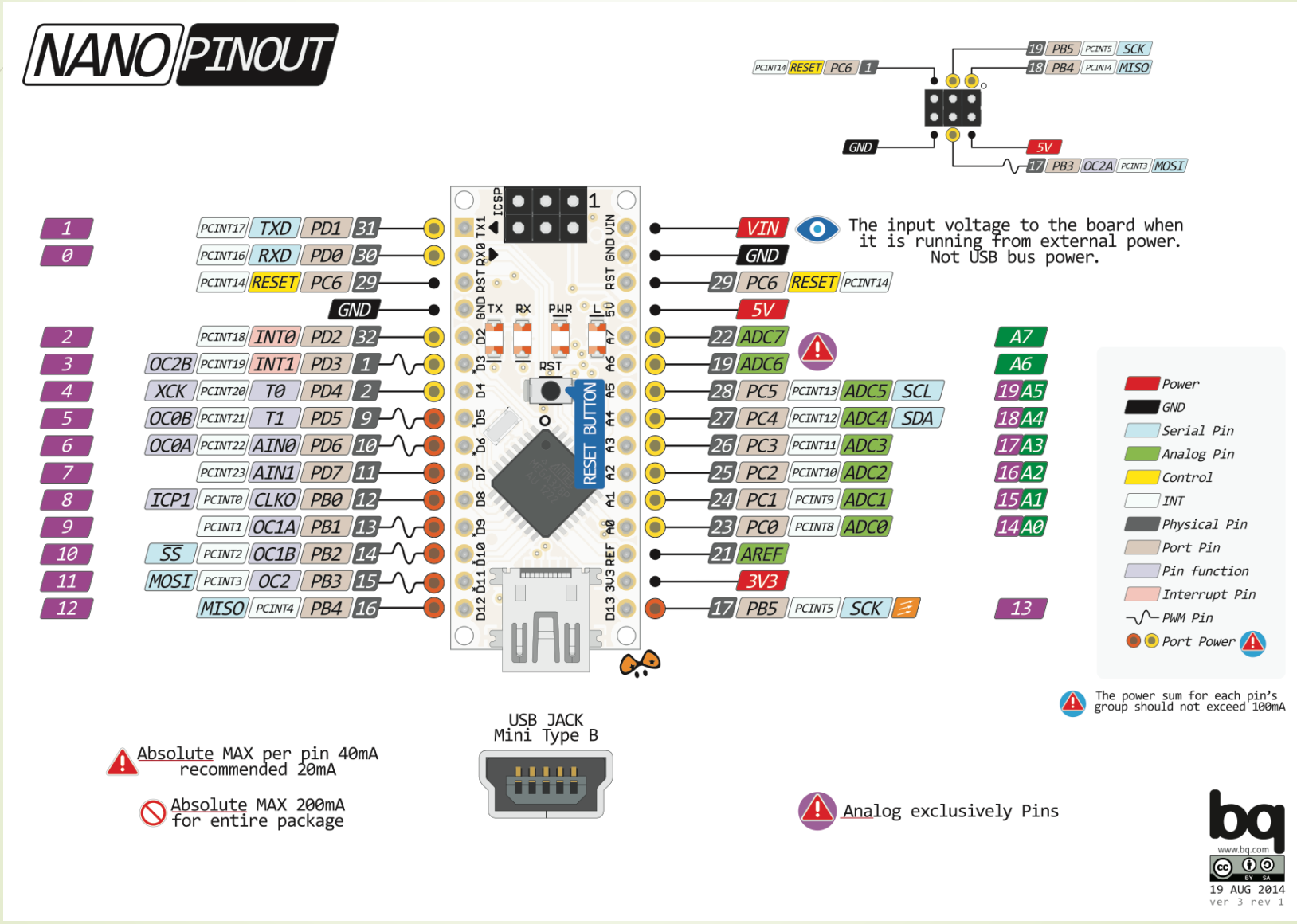


Taller

- https://github.com/toolsprods/ArDucky



Taller


NANO PINOUT
PCINT14 RESET PC6 1
19 PB5 PCINT5 SCK
18 PB4 PCINT4 MISO
GND
5V
17 PB3 OC2A PCINT3 MOSI
ICSP
1
TX RX PWR L
RST
RESET BUTTON
1 PCINT17 TXD PD1 31
0 PCINT16 RXD PD0 30
PCINT14 RESET PC6 29
GND
2 PCINT18 INT0 PD2 32
3 OC2B PCINT19 INT1 PD3 1
4 XCK PCINT20 T0 PD4 2
5 OC0B PCINT21 T1 PD5 9
6 OC0A PCINT22 AIN0 PD6 10
7 PCINT23 AIN1 PD7 11
8 ICP1 PCINT0 CLKO PB0 12
9 PCINT1 OC1A PB1 13
10 SS PCINT2 OC1B PB2 14
11 MOSI PCINT3 OC2 PB3 15
12 MISO PCINT4 PB4 16
VIN
GND
29 PC6 RESET PCINT14
5V
22 ADC7
19 ADC6
28 PC5 PCINT13 ADC5 SCL
27 PC4 PCINT12 ADC4 SDA
26 PC3 PCINT11 ADC3
25 PC2 PCINT10 ADC2
24 PC1 PCINT9 ADC1
23 PC0 PCINT8 ADC0
21 AREF
3V3
17 PB5 PCINT5 SCK
A7
A6
19 A5
18 A4
17 A3
16 A2
15 A1
14 A0
13
The input voltage to the board when it is running from external power. Not USB bus power.
Power
GND
Serial Pin
Analog Pin
Control
INT
Physical Pin
Port Pin
Pin function
Interrupt Pin
PWM Pin
Port Power
The power sum for each pin's group should not exceed 100mA
USB JACK
Mini Type B
Absolute MAX per pin 40mA
recommended 20mA
Absolute MAX 200mA
for entire package
Analog exclusively Pins
bq
www.bq.com
19 AUG 2014
ver 3 rev 1