Menu

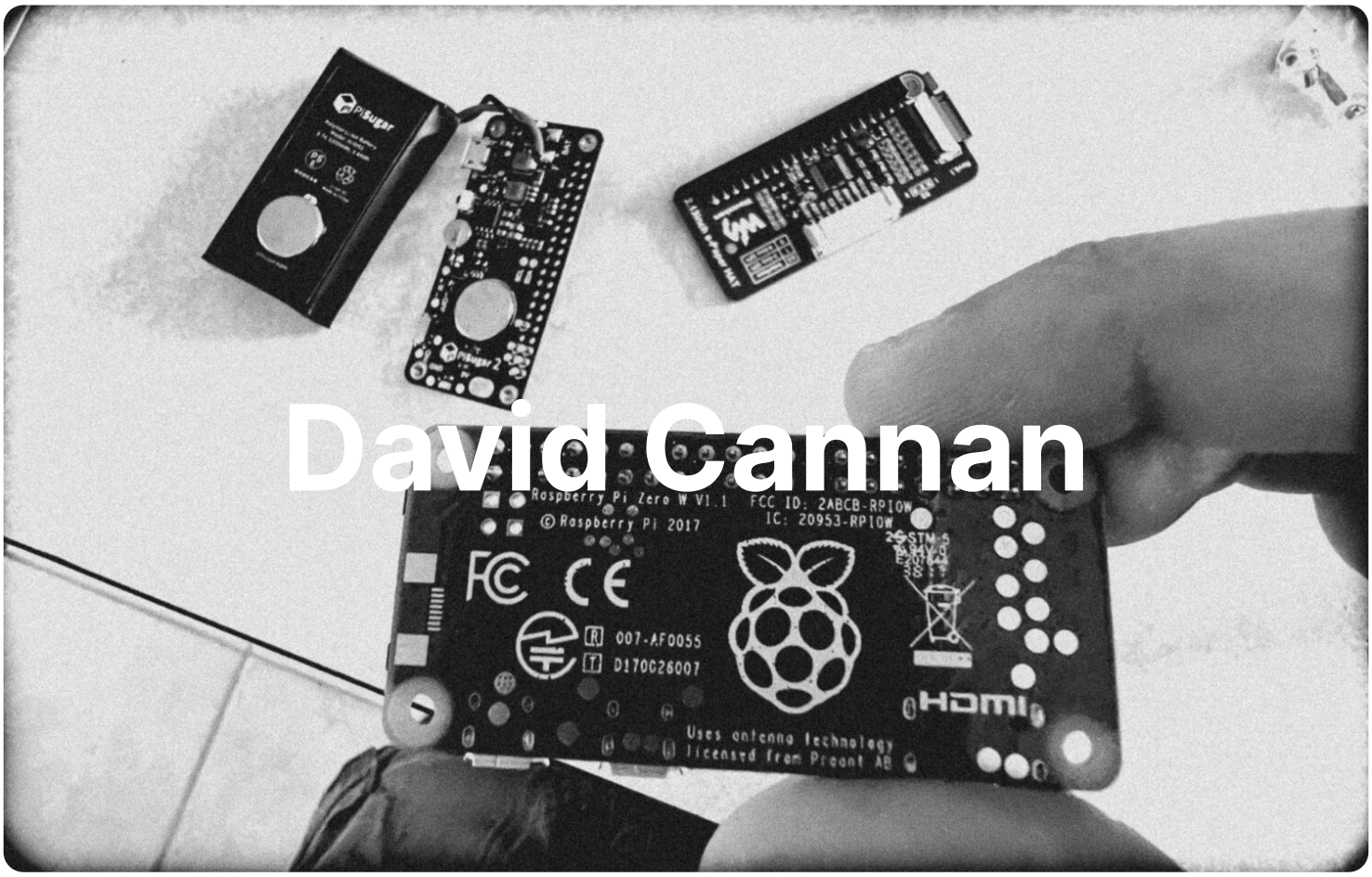
## David Cannan

Pwnagotchi... the ultimate handshake generator! Local Payload Injector via USB-C

Wi-Fi... GPS Coordinate's... and Python! OnePlus 7 Pro – Root & Nethunter CNC Build

Kali RasPi – OTG OnePlus 7 Pro – Root & Nethunter

## David Cannan




## David A. Cannan

> **Offensive Security|Network Enthusiast**

**Pn:** (404)358-4338

**Em:** cdasmkt@gmail.com

**Fb:** https://facebook.com/1492603121

**Website:** wp.cdaworkstation.com

# whois

First and foremost, I am dad to triplet boys, who gave me the opportunity to become something great; as well as someone who has the potential, drive, and the ability that is required to make a future for myself and my children.

Highly capable SE, observing and analyzing social behavior; 10+ exciting years of social engineering, rapport building, and risk taking experiences.

I found it necessary to go out and find the information in order to learn the things I am interested in.

> *A couple of traits that I proceeded to learn were portrait photography, and classical woodworking. In both instances I used my ability to focus as well as resources from internet, to learn the skills necessary to make a grind for myself.*
>
> *I've now had several small business ventures as well as work full time as a cabinetmaker at T&T Caseworks. I was sought out and offered a job, having never stepped in a cabinet-shop before; where I quickly established myself as a highly effective employee, by challenging myself and tirelessly aiming for quality.*

Looking to shift my career path to that of security testing, and I believe that the amalgam of my experiences are best suited for that of a risk assessment. I am studying for the CompTIA Security+ & Juniper (JNCIA) certifications.

# Skills, framework, and method.

- A curious and creative, critical thinker. Excellent problem solving skills, and a goal oriented learner. Have an understanding of security methodologies and big picture ideas.

- An an excellent learner, in that I absorb any knowledge that I can manage to be exposed to; over several months I have learn more than I learned I was capable of. My next step in life is to proceed in finding a job that will help me grow my knowledge and meet other likeminded people.
- Great with Linux command line, and understand how the Linux filesystems are structured.
- Top notch communication skills; patience, empathy, and understanding. Self-aware and capable of challenging own my beliefs (mental flexibility).
- I know the basics of coding languages, and over several months I've come to know some: BASH, Python, C++, HTML, JSON, as well as how to format things like YAML and Dockerfiles.

---

# Creating Practical Experience for myself build target and replicate environments to hack.

- **Implementing attacks using *ESP32 microcontrollers* at home, to build target and replicate environments to hack.**
  - ***Example Setting:*** *1 host device, and 2 or more clients (host programmed to have a WPA2/hidden network & clients communicate with each other).*
  - ***Example Attack:*** *Preforming a beacon attack to retrieve the hosts hidden SSID. Using the gathered information to spoof/intercept handshakes from the client devices and crack the hash to gain the credentials needed to access the host from the threat device.*
    - ***Result:*** *Access has been gained to the network; from here ARP or DNS spoofing can be implemented to direct traffic and phishing can begin.*
- **Building Labs in "the cloud"**Using *Linode Cloud Computing* (and other *SaaS*) for building and securing my domains and servers behind services like *Cloudflare*.
  - Allows me to practice penetration testing from the comfort of any browser that I have access too.
  - Spinning up *Linux servers* to learn *backend* and teach myself how to create and manage *VMs*.
  - Using *Docker Container's* to host entire networks all on one server and practicing my attacks.
    - *Portainer, Kasm, Kali Linux, Parrot OS, Metasploitable, WordPress, Tor, etc…*
- ***Reverse Engineering* IoT hardware to learn about *UART*, *serial connections* and *data streams*.**
  - Currently learning about onboard memory and recovering firmware from everyday devices with the goal obtaining root privileges.
- **OSINT and Recon**

    - Google dork and scraping APIs with tools like Maltego.
    - I've had several successful OSINT searches and found information on targets (gov salaries, police records, and property searches) for friends and family members.
    - Ran home network through vulnerability scans using tools like NMAP and Metasploit and patched the problems that I found.
- **Familiar with *Cross-Site Scripting* (XSS) and web application attacking.**
    - Successfully "hooked" browsers by copying trusted HTML pages and injecting *BeEf's* JavaScript webhook.
    - Stress tested and exploited my own domains and servers through BurpSuite.
- WI-FI Data Collection
    - WI-FI is so open air, it's important to be precise when throwing out attacks, the Wi-Fi Pineapple is great for that, makes EvilTwinPortals super easy and AP enumeration is incredibly easy with its GUI.
    - Built a Pwnagotchi from a Raspberry Pi, great for generating WI-FI hashes.
    - Built a WarDriving rig from an ESP8266 and a GPS module designed for a drone.
        - Allows me to plot Wi-Fi signals with its GPS coordinates. Great for collecting the data needed in order to overlay WI-FI targets on a map (using Python).
- **Home lab (Home network)**
    - Flashed my home router with *open source firmware* ( OpenWRT)
    - Setup multiple *VLANs* which are categorized by device.
    - Followed the rule of least privilege.
    - Hardened *default passwords* and hostnames.
    - Adjusted *wireless signal power* to prevent outside connections.
    - *Synology NAS* server running docker to host things like Minecraft servers, and hosting other in house hosting.
    - Assembled *Windows Active Directory* and *Domain Controller*.
        - Setup an environment in a as VMs, using *Windows Server 2019* as *domain controller* and *Windows 11*clients.

---

# Employment

**T&T Caseworks**

Head of Lamination/Finisher

*(May 2021 — Current)*

*• I am for all intensive purposes the only person in my department.*

*• The laminator position is best described as: laminating (in shop) the design/textured finishes*

*onto cabinets, countertop, custom displays and features; that have been chosen by people in the design and architecture industry. Almost always jobs are built-to-order and no two jobs are the same.*

*• Serving clients such as: Wellstar Kennestone, Grady Hospital, Kenestone Hospital, Children' Healthcare of Atlanta, Multiple Sclerosis Center of Atlanta, to name a few.*

*• Being able to prepare and manage many small but intricate tasks which all come together as an end product.*

*• I had to create a method that works for me, in helping sort my day and complete jobs.*

*• I was sought out and offered a job, having never stepped in a cabinet-shop before; where I quickly established myself as a highly effective and sufficient employee, by challenging myself and aiming for quality.*

**CDA Woodworks**

Woodworker/ Small Business Owner

*(May 2018 — Current)*

*Heirloom quality, hardwood joinery, self employment.*

*Build custom cabinets, shelving, flooring, tables, desks, panel doors, drawers, and such.*

*Set up, operate & tune a variety of woodworking tools and machinery: bandsaw, tablesaw, lathe, thickness planers and sanders, circular saw and hand tools (chisels, saws, hand planes).*

**David Cannan Photography**

Photographer/Small Business Owner

*(August 2017 — Current)*

*Accustom to providing services such as, family sessions, individual portraiture, and product photography. Both environmental and studio style portraiture.*

*Experienced with: Adobe creative cloud, digital photo/video, camera rig, monitor, 3-axis stabilizer, strobe lighting, and continuous lighting.*

**Grace Baptist Christian School**

Maintenance Worker/Janitorial

*August 2015 — October 2019*

*Routine cleaning, maintenance, and similar required work.*

# Associations

David Cannan Photography

CDA Woodworks