From Recon to Root

The Journey of an Offensive Security Professional

whoami

- Greg Oldham, Owner of Cape Fear Information Security.
- Ethical hacker and network security consultant operating out of the Wilmington, NC.
- Over 30 years of experience in the field.
- Veteran of the United States Army
- Core Member of the Red Team Village, a non-profit organization focused on teaching security professionals new tactics, techniques, and procedures in offensive security.

(Twitter)X: @hax4coffee

Linkedin: www.linkedin.com/in/greg-oldham-cfis github: https://github.com/Hax4Coffee

Why This Talk

Becoming a professional in offensive security is a journey that requires knowledge, skills, certifications, hands-on experience, but above all an insatiable curiosity.

This presentation will outline the steps to take, the best certifications to pursue (in my opinion), a few essential tools to master, and the importance of practical experience and networking with like-minded people.

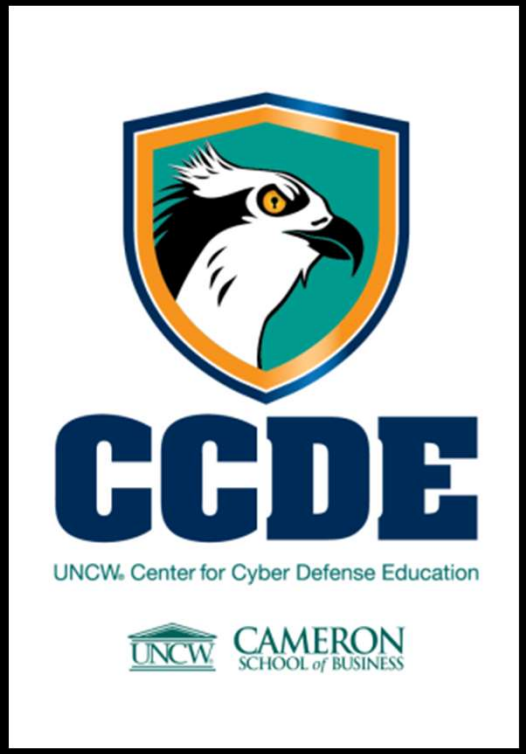
Education Pathways

There are a myriad of ways to get to where you need to be in the constantly evolving landscape of Cyber Security.

Every hour there are new threats and new exploits discovered all around the world.

Your mission, should you choose to accept it, is to do the very best you can to thwart your adversary. Knowledge and experience are your best allies.

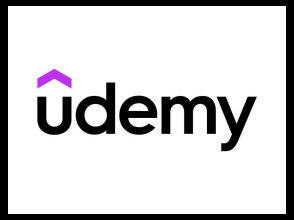
Formal Education



A formal education in cybersecurity provides several key benefits:

- Comprehensive understanding of cybersecurity
- Enhanced career opportunities
- Ultimately making individuals more valuable in the job market

Self-Taught Learning



- Online Courses
- Cybersecurity Books
- YouTube Tutorials
- Independent Research

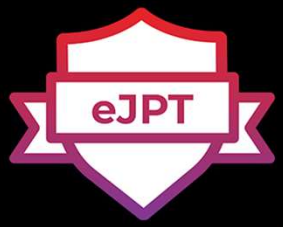
Bootcamps & Training Programs

- SANS Institute
- OffSec
- eLearn Security (INE)
- ISC²

Essential Certifications (In My Opinion)

Certifications validate your knowledge and skills, making you a more attractive candidate for jobs. Here are some of the best certifications for an offensive security professional

Beginner Level Certs



- CompTIA Security+
- CompTIA Pentest+
- eLearnSecurity Junior Pentester
- Cisco CyberOps Assoc.
- GIAC Security Essentials

Intermediate Level Certs

- OSCP (Offensive Security Certified Professional)
- PNPT (Practical Network Penetration Tester)
- CEH (Certified Ethical Hacker)
- CISSP (Certified Information System Security Professional)

Advanced Level Certs

- OSWE (Offensive Security Web Expert)
- OSEP (Offensive Security Experienced PenTester)
- CRTO (Certified Red Team Operator)

Must-Know Software Tools

In offensive security, knowing your tools is crucial because they serve as force multipliers, allowing you to exploit vulnerabilities, bypass defenses, and simulate real-world attacks efficiently.

Reconnaissance

When doing recon for offensive cyber operations, you want tools that help gather as much target information as possible with minimal noise. Here's a breakdown of some essential tools by category:

Passive Recon (Stealthy, OSINT-based)

1. Shodan – Finds internet-facing devices, services, and vulnerabilities.
2. Censys – Similar to Shodan but more research-focused.
3. theHarvester – Gathers emails, subdomains, IPs, and more from public sources.
4. Amass – Comprehensive subdomain enumeration using OSINT and active techniques.
5. Maltego – Visual OSINT tool that maps relationships between entities.
6. GHunt – Extracts intelligence from Google accounts and services.
7. FOCA – Extracts metadata from public documents.
8. Recon-ng – A framework for automating OSINT data collection.
9. SpiderFoot – Automated OSINT collection for threat intelligence.
10. OSINT Framework – Not a tool, but a great reference for OSINT techniques.

Reconnaissance

Active Recon (More Direct Interaction)

1. Nmap – The gold standard for network scanning and fingerprinting.
2. Masscan – High-speed port scanning (like Nmap but faster).
3. Zmap – Another ultra-fast network scanner.
4. Subfinder – Fast passive and active subdomain discovery.
5. Dnsrecon – DNS enumeration tool.
6. Aquatone – For mapping and visualizing websites.
7. Gobuster / Dirsearch – Directory and subdomain brute-forcing.
8. WhatWeb – Identifies web technologies.
9. Wappalyzer – Similar to WhatWeb but has a browser extension.

Exploitation

Exploitation Frameworks:

1. Metasploit Framework – The go-to for exploit development, payload generation, and post-exploitation.
2. ExploitDB & SearchSploit – Fast access to public exploits and POCs.
3. Fuzzbunch (NSA's Exploit Framework) – Used for legacy exploits like EternalBlue.

Privilege Escalation:

1. LinPEAS & WinPEAS – Automated privilege escalation enumeration.
2. PowerUp & PrivescCheck – Windows privilege escalation scripts.
3. BeRoot – Windows/Linux privilege escalation scanner.

Web Exploitation:

1. Burp Suite – Proxy for web application security testing.
2. SQLmap – Automated SQL injection exploitation.
3. XSStrike – Automated XSS detection and exploitation.

Password Cracking & Credential Dumping:

1. John the Ripper & Hashcat – Fast password cracking.
2. Mimikatz – Windows credential dumping.
3. LaZagne – Extract stored passwords from local systems.

Shells & Payloads:

1. Chisel & Ligolo – Reverse tunneling & pivoting.
2. nishang & PowerShell Empire – PowerShell-based post-exploitation.
3. Sliver & Cobalt Strike – Red teaming C2 frameworks.

Network Exploitation:

1. Responder – LLMNR, NBT-NS, and MDNS poisoning for credential capture.
2. Impacket – SMB, Kerberos, and remote execution tools.
3. CrackMapExec (CME) – Automate Active Directory exploitation.

Memory & Binary Exploitation:

1. GDB, PEDA, Pwntools – Binary exploitation toolkits.
2. Radare2 & Ghidra – Reverse engineering and debugging.
3. ROPgadget & one_gadget – Finding ROP chains for binary exploitation.

Wireless Attacks:

1. Aircrack-ng – Wi-Fi network cracking.
2. Bettercap – MITM attacks for network exploitation.
3. Wifiphisher – Evil twin phishing for Wi-Fi credential harvesting

Post-Exploitation

Post-exploitation is where the real fun begins in offensive security—once you've gained access, you need to escalate privileges, maintain persistence, and extract valuable information. Here are some essential post-exploitation tools you should have in your arsenal:

Persistence Tools:

1. Evil-WinRM – Remote administration via Windows Remote Management.
2. PowerShell Empire – Post-exploitation and C2 framework with persistence modules.
3. Koadic – JScript-based RAT with post-exploitation capabilities.
4. Nishang – PowerShell scripts for maintaining access.

Data Exfiltration & Enumeration:

1. CrackMapExec – Automates SMB and Active Directory attacks.
2. Impacket – Python scripts for network protocol exploitation.
3. PSExec – Remote command execution on Windows.
4. SharpHound – BloodHound data collection for AD.
5. Shad0w – Lightweight post-exploitation framework.

Lateral Movement:

1. Cobalt Strike – APT-style post-exploitation framework.
2. Metasploit Post-Exploitation Modules – Various built-in modules for maintaining access.
3. WMIC / WMIExec – Executes commands remotely using WMI.
4. RDP Hijacking / tscon.exe – Hijack existing RDP sessions.

Evasion & Defense Bypass:

1. Shellter / Veil – Payload obfuscation to evade AV.
2. Obfuscation techniques (AMSIBypass, Invoke-Obfuscation) – PowerShell-based AV evasion.
3. Donut – Converts PE files and scripts into shellcode.
4. C2 Frameworks (Mythic, Covenant, Sliver, Havoc) – Alternative to Cobalt Strike for advanced operations.

Custom Scripting

Custom scripting in offensive security is crucial because it allows you to tailor attacks, automate tasks, and bypass defenses that standard tools might not evade. Here's why it's so important:

Bypassing Defenses

Many security tools detect common exploits and payloads from well-known frameworks like Metasploit. Custom scripts help you evade these detections by modifying payloads or creating new attack vectors.

Automation of Repetitive Tasks

Offensive security involves a lot of scanning, enumeration, and exploitation. Writing scripts can automate these tasks, making engagements more efficient and reducing manual workload.

Custom Exploits & Payloads

Publicly available exploits may not work in every scenario. Custom scripts allow you to tweak or write new exploits tailored to specific vulnerabilities.

Adapting to Unique Environments

Every target environment is different, and pre-built tools may not always work as expected. Custom scripts allow you to adapt to different operating systems, applications, and network architectures.

Custom Scripting

Obfuscation & Evasion

Antivirus (AV) and Endpoint Detection and Response (EDR) systems rely on signatures and behavior analysis. Writing your own scripts can help you avoid detection by using unique execution methods or encryption techniques.

Privilege Escalation & Lateral Movement

Custom scripts help in crafting exploits that escalate privileges, automate persistence mechanisms, or move laterally within a network in a stealthy manner.

Red Team Operations

During Red Team engagements, operational security is key. Custom scripts allow for stealthier operations, avoiding common Indicators of Compromise (IoCs) that blue teams look for.

Improved Learning & Understanding

Writing your own tools forces you to deeply understand vulnerabilities, exploit development, and security mechanisms. This enhances your problem-solving skills and creativity.

Hands-On Experience is Vital

Hands-on experience in offensive security is critical because cybersecurity is a highly practical field where theoretical knowledge alone won’t cut it.

Hands-On Experience is Vital

Bridges the Gap Between Theory and Reality

Reading about exploits or pentesting methodologies is one thing, but actually executing them in a lab or real-world environment is entirely different. Hands-on experience teaches you how attacks work in practice, not just on paper.

Develops Problem-Solving Skills

Offensive security engagements rarely go as expected. You'll run into network segmentation, AV/EDR defenses, and unexpected system configurations. Practical experience helps you build the troubleshooting mindset needed to pivot and adapt.

Improves Tool Proficiency

Tools like Metasploit, Burp Suite, Cobalt Strike, BloodHound, and others require real-world application to master. Learning their intricacies through use in labs or real-world environments makes you much more effective as a security professional.

Builds Muscle Memory for Attacks

Just like an athlete needs repetition to perfect movements, a pentester needs repetition to execute attacks efficiently. Running through buffer overflows, lateral movement, privilege escalation, and AD exploitation regularly makes these techniques second nature.

Enhances Situational Awareness

Every environment is different. Real-world experience helps you recognize patterns in network defenses, detect anomalies, and make informed attack decisions. This skill set is crucial for Red Teaming and real-world pentests.

Hands-On Experience is Vital

Strengthens Report Writing & Communication
Running an exploit is easy; explaining its impact to a CISO or a client is much harder. Hands-on testing helps you learn how to document findings clearly and provide actionable recommendations.

Prepares for Certifications (Like OSCP, CRTO, etc.)
Certifications like the OSCP, CRTO, and OSEP demand hands-on skills, not just theoretical knowledge. The OSCP, for example.

Increases Employability & Credibility
Companies prefer candidates who can demonstrate real-world offensive skills over those who just list certifications. Building a home lab, participating in HTB, TryHackMe, or CTFs, and contributing to open-source security projects make you stand out.

Simulates Real Adversarial Thinking
The best way to think like an attacker is to act like one. By conducting real-world engagements, you develop the adversarial mindset, understanding how attackers bypass defenses and what security controls work in practice.

Validates Knowledge with Real-World Impact
Finding a zero-day, discovering a new bypass technique, or successfully executing a full kill chain attack in a Red Team assessment shows real impact. It’s what separates a good offensive security professional from a script-kiddie.

Practice Platforms

TryHackMe (tryhackme.com)

- Beginner-friendly learning paths
- Guided & self-paced challenges
- Great for structured learning (especially for students)

Hack The Box (hackthebox.com)

- Free & paid labs
- Active Directory, web app, and network-based challenges
- OSCP-style and real-world boxes

Over The Wire (overthewire.org)

- Text-based CTF-style war games
- Good for learning Linux privilege escalation

Capture The Flag (CTF) Competitions

Root Me (root-me.org)

- Hundreds of challenges with walkthroughs
- Web, crypto, reverse engineering, and more

Hack This Site (hackthissite.org)

- Good for learning basic security concepts
- Legal hacking exercises

CTFlearn (ctflearn.com)

- Good for beginners with easy-to-medium challenges
- Covers multiple cybersecurity domains

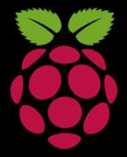
Red Team Village (redteamvillage.io)

- Hosts CTFs at major security conference

CTF Time (ctftime.org)

- Tracks all upcoming and ongoing CTFs
- Has rankings for CTF teams and competitions

Home Lab Setup | A solid home lab for offensive security should be versatile, allowing you to test network penetration, exploit development, malware analysis, and Active Directory attacks.



- Any modern system with minimum 16GB RAM (more is better for virtualization)
- VMware Workstation or VirtualBox
- Raspberry Pi / Mini PC for pivoting, C2 servers, or IoT pentesting
- Virtual Machines (VMs) Vulnerable VMs can be downloaded from VulnHub
- Offensive tools – Kali Linux and Parrot OS for All-in-one distros
- Commando VM – Windows-based pentesting environment
- Metasploitable 2 – Vulnerable Linux for basic pentesting
- Windows 10/11 (Enterprise) – To practice post-exploitation
- Windows Server 2019/2022 – For Active Directory (AD) attacks
- PfSense Firewall VM
- C2 Frameworks (Cobalt Strikeneeds a license) Sliver, Mythic, Havoc
- Obsidian/Cherry Tree for note taking and tactic playbooks
- GitHub/GitLab to store payloads, recon scripts, and automation

Remember to setup Host-only / NAT VMs: to Isolate vulnerable VMs from your network. Best practice is to have dual NICs in your attack machine.

Home Lab Setup | A solid home lab for offensive security should be versatile, allowing you to test network penetration, exploit development, malware analysis, and Active Directory attacks.

WebSploit Labs | websploit.org

- **WebSploit Labs** is a learning environment created by Omar Santos for different Cybersecurity Ethical Hacking, Bug Hunting, Incident Response, Digital Forensics, and Threat Hunting training sessions. WebSploit Labs includes several intentionally vulnerable applications running in Docker containers on top of Kali Linux or Parrot Security OS, several additional tools, and over 9,000 cybersecurity resources.

  It comes with over 500 distinct exercises!

Attend Conferences and Meetups

1. Learning Cutting-Edge Techniques

- Conferences like **DefCon, Black Hat, BSides, and Red Team Village events** showcase **zero-days, new TTPs (Tactics, Techniques, and Procedures), and innovative exploits** before they become mainstream.
- You'll see **live demos** of techniques that aren't yet in books or courses.

2. Networking with Experts

- You get to **meet red teamers, pentesters, malware devs, and security researchers** who share your passion.
- Many job offers and collaborations happen through these events, especially in **hallway talks** and **after-parties**.

3. Hands-On Competitions (CTFs & Labs)

- **Capture The Flag (CTF) events** and **red team vs. blue team challenges** let you **test your skills in real-world attack scenarios**.
- It's a **great way to practice offensive security** in a controlled environment.

Attend Conferences and Meetups

4. Staying Updated on Security Trends

- Offensive security is constantly evolving—what worked last year might be patched or outdated now.
- Conferences help you stay ahead of blue teams and adapt to changing security landscapes.

5. Showcasing Your Work

- Presenting your own research at a conference boosts your reputation in the community.
- You can publish a new tool or exploit, which can get you recognized by top companies (like Cisco or nCino) or security groups.

6. Access to Exclusive Research

- Some security researchers and APT (Advanced Persistent Threat) analysts only present their work at conferences.
- You'll gain insights into cyber warfare, red teaming methodologies, and real-world cyber attacks.

7. Career Growth & Certifications

- Many conferences offer OSCP, CRTO, and other cert prep sessions.
- You can connect with hiring managers or get mentorship from seasoned pros.

Conferences & Online Communities

Discord is a great place to meet and learn from professionals and students.

There are multiple cybersecurity conferences in ILM & RDU

- **Techno Security & Digital Forensics Conference 2025** Scheduled for June 3-5, 2025, at the Wilmington Convention Center, this conference brings together professionals in cybersecurity, digital forensics, and eDiscovery. Attendees can expect educational sessions, networking opportunities, and insights into the latest industry developments.
- **Annual UNCW Cybersecurity Conference** is an opportunity to explore the latest in cybersecurity trends, challenges and innovations. The two-day event brings together industry leaders, government officials, small business owners and academics. Register to connect with experts and gain insights into cybersecurity.

Conferences & Online Communities

- **Bsides RDU 9/12/2025** @ The McKimmon Conference and Training Center at NC State. A community-driven framework for building events for and by cybersecurity community members.

- **Cackalackycon 5/16-5/18** @ Doubletree Hilton RDU a community partnership to provide a hacker conference in the Research Triangle Park (RTP) area of North Carolina

- **DEF CON Thu, Aug 7, 2025 – Sun, Aug 10, 2025** is a hacker conference that focuses on computer security, privacy, and emerging technology. It's the world's largest and longest-running underground hacking conference

Conclusion

The path to becoming an offensive security professional requires a mix of education, certifications, hands-on experience, and networking. **Stay curious**, continuously learn, and engage with the cybersecurity community to grow in this field.

The journey from recon to root is challenging but rewarding!

My life in a meme...

The end