**Carlos Palencia**

Portfolio: [www.carlosmpalencia.com](http://www.carlosmpalencia.com/) | carlos.m.palencia@icloud.com

Recent computer science graduate, ethical hacker, and passionate life-long learner with penetration testing experience in lab environments. Currently practicing offensive security using my own homemade lab while also pursuing the CompTIA Security+ and CCNA certifications. Check out my portfolio website at: [www.carlosmpalencia.com](http://www.carlosmpalencia.com/).

Additionally, I possess the following:

* Experience with security tools such as Kali Linux, Metasploit, and Burp Suite.
* Python and shell scripting experience.
* Proficiency in translating technical information to non-technical people (both verbally and in writing).
* Excellent research abilities for finding solutions to problems on my own.

# EducatioN

## B.S. Computer Science (May 2023), The University of the District of Columbia — 3.7/4.0 GPA

# projects

**[Homemade Penetration Testing Lab](https://carlosmpalencia.com/projects/penetration-testing-lab/):
Attacking Networks, Web Applications, CTF Machines, and Exploiting Buffer Overflows**

Ethical Hacker, April 2023 – Now

* Performed reconnaissance, scanning, and enumeration using the following tools:
Nmap, Nessus, OWASP Amass, PowerView, Bloodhound, Airodump-ng, directory busting tools, OSINT tools, and more.
* Performed [network penetration testing against Active Directory](https://carlosmpalencia.com/projects/penetration-testing-lab/part-5-active-directory/). Attacks/exploits used include:
EternalBlue (MS17-010), LLMNR poisoning, intercepting hashes, hash cracking, SMB relays, IPv6 DNS takeovers, pass-the-pass, hash dumping, pass-the-hash, token impersonation, Kerberoasting, GPP/cPassword attacks, URL file attacks, PrintNightmare (CVE-2021-1675), credential dumping from memory, Golden Ticket attacks using Mimikatz, ZeroLogon, and more.
* Performed [web application penetration testing](https://carlosmpalencia.com/projects/penetration-testing-lab/part-6-web-apps/) with an emphasis on the OWASP Top 10 vulnerabilities. Attacks performed include:
SQL injections, XML external entity (XXE) attacks, cross-site scripting (XSS), credential stuffing, password spraying, brute forcing, and more.
* Performed [exploit development against a server](https://carlosmpalencia.com/projects/penetration-testing-lab/part-4-exploit-development/) by identifying a buffer overflow vulnerability and writing a manual Python exploit for it.
* Successfully compromised multiple CTF (capture the flag) machines.
* Currently using the lab to continue experimenting with other new attacks, tools, and tactics.

# Experience

## Front-End Web Developer, Washington, DC

Self-Employed, January 2017 – Now

* Comprehensive website deployment both from scratch and via tools like WordPress.

## Center for Reverse Engineering and Assured Microelectronics Research Lab(Morgan State University), Baltimore, MD

## Research Assistant, June 2021 – August 2021

## Performed vulnerability scanning and enumeration in medical network environments.

## Researched security vulnerabilities in CPAP medical machines.

## Researched security vulnerabilities in Internet-of-Things (IoT) networks.