

ARPIT DHAMELIYA

New York, NY | (201) 850-2908 | arpitdhameליya7@gmail.com
[LinkedIn](#) | [GitHub](#) | [Credly](#)

Summary

OSCP+ certified penetration tester with 1+ year of professional offensive security experience across web, API, and Active Directory environments, plus an MS in Cybersecurity from Pace University. Demonstrated tradecraft in exploitation, post-exploitation, AD attack chains, and physical/wireless red teaming, with hands-on competition record and active CTF practice.

Certifications

Offensive Security Certified Professional+ (OSCP+) · eJPT (INE Security) · CompTIA Security+ · CompTIA Network+ · Certified Cybersecurity Technician (EC-Council) · API Security Analyst

Languages & Technologies

Offensive Security: Burp Suite, Metasploit, Nmap, BloodHound, Impacket, CrackMapExec, Mimikatz, Responder, Hashcat, John the Ripper, OWASP Top 10, OWASP API Top 10

Active Directory Attacks: Kerberoasting, AS-REP roasting, NTLM relay, ACL abuse, ADCS exploitation, cross-forest trusts, lateral movement, privilege escalation

Wireless / Physical / RF: Aircrack-ng, RFID/NFC cloning, wardriving, Sub-GHz/2.4GHz radio attacks, ESP32, embedded systems, IoT

Scripting & Languages: Python, Bash, PowerShell, C/C++

Platforms: Windows Server, Windows 10/11, Linux, Active Directory, Docker, Git, VMware; Wireshark, MITRE ATT&CK

Professional Experience

Penetration Tester (Cybersecurity Analyst), Cyber Octet Pvt. Ltd.

January 2023 – November 2023
Ahmedabad, India

- Led VAPT engagements across web applications, REST APIs, and Active Directory environments for **3 banking clients**, chaining **15+ critical OWASP Top 10 vulnerabilities** into proof-of-concept exploit paths and demonstrating **20%** reduction in unauthorized access risk post-remediation.
- Authored **Python proof-of-concept exploits** covering injection, deserialization, broken auth, and AD abuse, then walked **5+ business stakeholders** through attack paths and impact in executive-level briefings.

Penetration Testing Intern, Cyber Octet Pvt. Ltd.

October 2022 – December 2022
Ahmedabad, India

- Performed wireless penetration tests with Aircrack-ng and static malware analysis, translating **30+ findings** into prioritized exploitation reports for senior consultants.
- Conducted reconnaissance, enumeration, and exploitation using Nmap, Burp Suite, and Metasploit across **2 client networks**, identifying exposed services, misconfigurations, and exploitable vulnerabilities.

Projects

Multi-Domain Active Directory Attack & Defense Lab · VMware, BloodHound, Impacket, CrackMapExec Aug 2024 – Present

- Built a **5-VM multi-domain Active Directory environment** (sevenkingdoms.local / essos.local) and chained **20+ attack scenarios** including Kerberoasting, AS-REP roasting, NTLM relay, ACL abuse, ADCS exploitation, and cross-forest trust attacks to achieve full domain compromise.
- Mapped attack paths with **BloodHound** and automated exploitation with **Impacket and CrackMapExec**, reinforcing OSCP+ tradecraft and replicating real-world red team operations end to end.

PhishArk: Automated Social Engineering Simulation Framework [GitHub] · Python, Bash, Cloudflared May 2024 – Apr 2025

- Co-developed a modular Python framework with **70+ phishing templates** and Cloudflared tunnel automation for authorized red team initial-access engagements, increasing operator deployment speed by **50%**.

Bruce Smoochie: Wireless and Embedded Auditing Tool [GitHub] · ESP32-S3, C++, Embedded Systems Jul 2024 – Dec 2025

- Designed a portable, battery-powered multi-radio attack platform integrating **CC1101 (Sub-GHz)**, **nRF24L01 (2.4GHz)**, and **PN532 (NFC)** modules for physical pentests and red team engagements; firmware (Bruce framework) supports **RFID/NFC cloning**, **signal replay (IR/RF)**, and **GPS-based wardriving** with **3+ hours** untethered operation.

Achievements & Competitions

- National Cyber League (NCL) Top 6%**, Team Game, Fall 2024 and Fall 2025; CyberSEED 2025 competitor; SANS Holiday Hack Challenge 2025 participant; active on Hack The Box, TryHackMe, PicoCTF, and OSCP Proving Grounds.
- Selected for EC-Council's **Certified Cybersecurity Technician (CCT)** beta testing committee.

Education

Pace University, New York, NY · M.S. Cybersecurity (Security Operations) · GPA: 3.65 · Jan 2024 – Dec 2025

Dharmsinh Desai University, India · B.E. Electronics and Communication · GPA: 3.4 · Jun 2019 – May 2023