

ADHISHRI KOTHIYAL

<https://www.linkedin.com/in/adhishrikothiyal/>

Santa Clara, CA, 95054

+1(475)-228-3040 | kothiyal@terpmail.umd.edu

<https://www.hackthebox.eu/home/users/profile/84253>

<https://github.com/AdhishriKothiyal>

EDUCATION

Master of Engineering, Cybersecurity University of Maryland	GPA – 3.55	College Park, MD Aug'18 - May'20
Bachelor of Technology, Computer Science & Engineering Jaypee University of Information Technology	GPA – 3.33	Solan, HP, India Aug'13 - May'17

SKILLS

SECURITY TOOLS	Burp Suite Scanner, testssl.sh, Metasploit, Nmap, Wireshark, GDB, Netcat, Kibana (ELK), FireEye HX, CrowdStrike Falcon, Autopsy, Ghidra, IDA Pro
OPERATING SYSTEMS	Kali Linux, Windows, MacOS
PROGRAMMING LANGUAGES	C, Python3, 32-bit x86 Assembly Language, Bash Scripting, SQL, Web Technologies
OTHER	Understanding of OWASP top 10 webapp attacks, Gathering or Open-Source Intelligence (OSINT), Reverse Engineering

WORK EXPERIENCE

Associate Security Consultant – Leviathan Security Group	Santa Clara, CA Aug '20 – Mar'21
<ul style="list-style-type: none">Ensured quality as a Third-Party Organization (3-PAO) and provided assessment support by evaluating the security and compliance of clients.Performed white box (SAST) and black box (DAST) penetration testing and security audits that focused on web applications, network security (internal/external) & secure code analysis and review for the clients.Contributed to OAuth 2.0 and SSL/TLS encryption testing.	
Information Security Operations Intern – Synopsys Inc.	Mountain View, CA May'19 – Aug'19
<ul style="list-style-type: none">Designed and simulated test cases to test NGAV as a possible replacement for traditional AV.Analyzed outbound RDP for BlueKeep vulnerability over the port 3389. Developed bash script for the analysis of port 3389 of a bunch of logs using Kibana.Assisted with hardening of email security by developing Python script for Proofpoint cleanup.	
Incident Response Support student employee – Security Operation Center (SOC) - Division of IT, UMD	College Park, MD Feb'19 – May'20
<ul style="list-style-type: none">Single handedly managed incident tickets of phishing mails received by the students/faculty of university and actively monitored and analyzed systems and network logs for intrusion with 24/7 incident response.Performed passive reconnaissance, network forensics and webapp pentesting using EDR, vulnerability scans, burp proxy and OSINT to escalate incidents to concerned departments and help them understand security controls and how they should be positioned.Prepared weekly executive incident reports highlighting attacker trends and technical briefs for management, administrators and end user liaison with other cyber analysis entities using Splunk.	

PROJECTS

Tech Fellow at CodePath (Cybersecurity) partnered with Facebook	Present
<ul style="list-style-type: none">Leveraging expertise from OWASP's Security Shephard to develop offensive and defensive skills in web application pentesting through hand-on experience.IDOR, XSS, Broken Session Management, SQLi, CSRF, Crypto, Authentication, Hashing.	
Buffer Overflow Attack	Aug'18 – Dec'18
<ul style="list-style-type: none">Disassemble compiled code and looked for any possible vulnerabilities.Exploited vulnerabilities of functions like 'strcpy' to introduce shell code to the program or run dead code.	
Python Implementation of Cipher Systems	Aug'18 – Dec'18
<ul style="list-style-type: none">Ciphers implemented: Caesar, Hill, Playfair, Feistel, DES, AES, Hashing.	

ACTIVITIES

Conference: Blackhat'19 Defcon'19 WiCyS'19,'20 GHC'19 BSidesDC'19	2019
Won, Blue Team CTF by Facebook at WiCyS'19 conference	Mar'19
Won, CTF 4 Noobz by Women's Society of Cyberjutsu at WiCyS'19 conference	Mar'19