+3 | @gmail.com | linkedin.com/in/

SUMMARY

I am a computer science engineer and a Cyber Security Enthusiast!!! Presently, I'm pursuing my Masters in Applied Cybersecurity from TU Dublin. In the past, I worked as a cyber threat intelligence analyst at ***PwC (PricewaterhouseCoopers)*** and have about **two years of MSSP experience** well-versed in threat intelligence, cyber threats and vulnerabilities.

PROFESSIONAL EXPERIENCE

PwC Acceleration Centers **Bengaluru, Karnataka, India**
Cyber Threat Intelligence Associate 2 *September 2022 - August 2023*

- Threat Hunting to support technical analysis of malicious cyber security events.
- Analysing various dark web records including Credit/Debit card details and Compromised credentials.
- Analysing Data Breaches and Marketplace events.
- Brand monitoring and Takedown assistance.
- Evaluating risk and alerting customers accordingly.
- Creating various advisories and reports on emerging threats.
- Skills: Cyber Threat Hunting (CTH) · Malware Analysis · Cyber Threat Intelligence(CTI) specialising in Threat Actors, Attack Vectors, Campaigns, TTP's · Mitre's Framework · Cyber Kill Chain Framework

PwC Acceleration Centers **Bengaluru, Karnataka, India**
Cyber Threat Intelligence Associate *September 2021 - August 2022*

- I was a part of some highly confidential engagements, performed Security Monitoring, delivered quality work and received appreciations from the client and on-shore teams for detecting some critical exploitation attempts
- Involved in Threat Research, OSINT gathering, Intelligence Analysis
- Mentored interns/new hires at the firm and helped provide KT to them in my areas of expertise
- Skills: SOC analyst · Cyber Threat Intelligence (CTI) · Security Research documentation and engaging with both technical and non-technical audiences

BETSOL **Bengaluru, Karnataka, India**
Product Security Intern *March 2021 - June 2021*

- During the course of internship, I have worked on
- Threat modeling (STRIDE)
- Attack surface analysis
- API security
- Implementing TLS1.2 for remote APIs

EDUCATION

Technological University Dublin, Ireland **September 2023 - September 2024**
Master's, Cybersecurity

JSSATE, Bangalore, India **August 2017 - August 2021**
Bachelor's, Computer Science *GPA: 8.99*

PROJECTS & OUTSIDE EXPERIENCE

IDS Evasion | SNORT **Dublin, Ireland**
November 2023 - January 2024

- This project delves into the deployment of open-source Intrusion Detection and Prevention systems (IDS/IPS) such as Snort to understand the internal operations of such cyber defense systems. In addition, research and implement various approaches to evade these IDS defenses to understand the threat actor's point-of-view. Further, train the IDS to detect such evasion techniques to build efficient defense mechanisms to prevent future attacks. This project gives a fair knowledge of open-source IDS i.e. Snort, about its purpose, modes of operations, its implementations and applications.
- The Intrusion detection system i.e. Snort was setup in Ubuntu 22.04.3 LTS (Jammy Jellyfish) and 'snort.conf' file crucial for Snort's working, specifying rules, and defining network settings, encapsulating the system's detection and prevention parameters was suitably configured. In this project, we emulate a few attack scenarios, where threat actors can find a flaw in the victim's machine and exploit it to carry out an IDS evasion technique to go undetected by existing defence mechanisms.
- These attack scenarios included SSH Brute Force Attack for Payload Encryption Evasion via Nmap recon tool and brute force HYDRA tool and TCP/SYN Flooding Attack – a tactical DDoS via Hping3 tool.
- *Link to project*

T-Pot Honeypot **Dublin, Ireland**
September 2021 - January 2024

- Executed an independent project involving the deployment, configuration, and implementation of a honeypot on multiple Google Cloud Platform (GCP) instances based in London (As per reports, the United Kingdom (UK) suffers more cyberattacks compared to any other European country), Israel region (Tel Aviv) amidst the heightened tension between Israel and Palestine, Korea region (constant conflict between North and South Korea) to gain insights into threat actor's tactics, techniques, and procedures (TTPs) and malware behavior.
-

Honeypots have been considered in such a way that they help the security analyst learn and understand various fields of cybersecurity. Email security (Mailoney), Mobile Security (ADBhoney), and Network Security (Citrix honeypot, Ddospot) have been analysed in this project. In order to allow traffic into our instance's individual honeypot ports, ingress traffic rules/VPC firewall rules were customised. All this traffic data is logged using Logstash (ELK stack) and visualized using Kibana dashboards. To analyse the data visualisation of the threat landscape, the Kibana Dashboard and Discover components of the ELK stack were utilised. Additionally, I utilized tools such as VirusTotal, AbuseIPDB, MITRE Attack and Defend framework to swiftly generate comprehensive reports for efficient analysis.

- Interpreted the TTPs used by threat actors in the case of observed ADBhoney-Mailoney attacks and mapped them to MITRE Attack and Defend framework provided actionable threat intelligence in the form of TTPs and security recommendations.
- *Link to project*

Arp Spoofer **Remote**

- Man-in-the-Middle attack
- A Python script CLI tool for Arp spoofing, implementing the Scapy module to perform a Man-in-the-Middle (MitM) attack against someone else on your local network for educational purposes.
- *Link to project*

SKILLS

Skills: Cyber Threat Hunting (CTH), Cyber Threat Intelligence (CTI), Malware Analysis, Digital Forensics, MITRE framework, Cyber Kill Chain Framework, Python, Cybersixgill Darkweb Monitoring, SOCRadar, Digital Shadows, BitSight, SOC

CERTIFICATIONS

Bagged 13th rank in CTF at ShellCon Cybersecurity conference.
Cleared TCS Codevita round1 with all India rank 13655.
Foundations of Operationalizing MITRE ATT&CK v13
Fortinet NSE 1 & NSE 2 - Network Security Associate certified by Fortinet (Issued Aug 2020)
Cyber@ANZ Program – Virtual Internship with ANZ Banking Group
CYBER SECURITY AND DIGITAL FORENSICS - Indian Institute of Information Technology, Kota, India
Introduction to Cybersecurity - Cisco
Digital Acumen - PricewaterhouseCoopers (PwC)
Human-Centered Design – PricewaterhouseCoopers (PwC)
CSI Accredited Student - Computer Society of India (Issued Feb 2019)