Shivam **Kapoor**

Software Engineer · Cyber Security Enthusiast

67/143 Pratap Nagar, Sanganer, Jaipur-302033, INDIA

(+91) 952-1458-982 | mailme@shivamkapoor.me | www.shivamkapoor.me | ConanKapoor | ConanKapoor

Work Experience

The European Organization for Nuclear Research (CERN)

Geneva, Switzerland

Openlab Security Intern

Jun. 2018 - Aug. 2018

- Selected among 41 candidates out of 1800+ applicants to work closely with industry leaders on real-world problems faced by CERN
- Worked with the CERN Computer Security Team on automated sandbox analysis of quarantined malware reaching CERN through email traffic
- Utilized components involved Joe Sandbox Cloud, FireEye EX appliances and open source threat intelligence platform MISP
- The project is now an addition to the other security and defence strategies deployed at CERN for email security
- **Technologies Used** - Python, Flask, Web development technologies

Cyware Labs

Bangalore, India

Cybersecurity Research Intern

May. 2017 - Jul. 2017

- Worked directly under co-founder and CTO of Cyware Labs on various cybersecurity and information security related problems
- Developed a whole module of *Cyware Mobile Application* which is being used by thousands of employees around the world
- Collaborated on a project to develop a middleware that can prevent OWASP top 10 vulnerabilities in a real-time production environment
- Utilized security tools and frameworks like Metasploit, Burpsuite and OWASP Zap for various pentesting assignments
- **Technologies Used** - Python, Django, Android Studio, NetBeans, Web development technologies

Publications

Malware Analysis Management (M.A.M.) : Automated sandbox analysis of quarantined emails at CERN.

DOI: 10.5281/zenodo.1470452

Shivam Kapoor

Jun. 2018 - Aug. 2018

- Focuses on the design, implementation and deployment of M.A.M. on CERN email security infrastructure
- The cornerstone of this strategy is the use of FireEye EX appliances to quarantine malicious attachments reaching CERN through email traffic
- Advanced sandbox technologies like Joe Sandbox Cloud are utilized in the project to deep analyse malware samples for a detailed report
- Open source threat intelligence platform MISP is utilized in the project to report Indicators of Compromise (IOCs) as security events
- M.A.M., a real-time daemon running persistently on a dedicated VM, is now an addition to the CERN email security infrastructure
- The report can be accessed here on public domain - **https://doi.org/10.5281/zenodo.1470452**

Extracurricular Activity

GameJam 1.0 and 2.0

VIT University, India

Head Organizer & Instructor

Sep. 2016 - PRESENT

- The event was co-located with International Symposium of Big Data and Cloud Computing Solutions '17.
- Organised workshops & hackathons to train over 100 participants to build games from scratch using Unity 3D game engine
- Successfully managed & coordinated a team of six talented fellow game developers

VITCMUN'17

VIT University, India

Marketing & Sponsorship

Sep. 2016 - Mar. 2017

- Participated in Marketing and Sponsorship team for 2 editions of VITCMUN over a year
- Attracted a total of 700+ students for both editions combined from all over India
- Got Rs. 50,000 in sponsorship for the event and accounted for 1/4th of the budget

Certifications and Training

Nov. 2017	**Bitcoin and Cryptocurrency Technologies,** Princeton University
Feb. 2017	**Introduction to Cyber Security,** The Open University
Jan. 2017	**The Complete Ethical Hacking Course: Beginner to Advanced!,** By Ermin Kreponic, IT Expert
Nov. 2016	**Learn Ethical Hacking from Scratch,** By Zaid Sabih, Ethical Hacker, Pentester & Computer Scientist

Education

VIT University, Chennai Campus *Chennai, India*

B.Tech. in Computer Science and Engineering *Jul. 2015 - Jun. 2019*

- **Major GPA:** 9.13 / 10.0
- **Cummulative GPA:** 8.95 / 10.0
- **Relevant Coursework:** Cybersecurity (A Grade - 9/10); Networks & Communication (A Grade - 9/10); Operating Systems (S Grade - 10/10); Database Management Systems (S Grade - 10/10)

Notable Projects

All projects can be seen on my Github profile: https://github.com/conankapoor

TorScrapper *Project URL*

Cyber Security *Oct. 2017 - PRESENT*

- A python based scrapper used to crawl the Deep and Dark web over Tor network to scrape Indicators of Compromise (IOCs)
- The scraped threat intelligence can be converted into STIX/TAXII format for reporting as security events
- Some of the integrated libraries include BeautifulSoup and Tor Stem controller library
- The work in progress will be published as a research paper once substantial threat intelligence has been gathered
- **Programming Languages** - Python

Protecting Democracy from Election Fraud using Blockchain Technology *Project URL*

Cyber Security *Sep. 2017 - PRESENT*

- A foolproof, secure and transparent system to legitimize Indian elections and bridge the trust gap between the voter and the election body
- Blockchain technology is incorporated in this project to remove malpractice and tampering in the voting process
- Challenging part of the project involved implementing proof of work and incentive for no monetary benefit
- **Programming Languages** - Python

Network Monitoring Tool *Project URL*

Networks and Communication *Feb. 2017 - May 2017*

- A lightweight and effective terminal based network monitoring tool with colourful and user-friendly interface
- Show results for the parameters like packet loss, CPU usage, memory usage, bandwidth analysis (upload and download), and node graphs
- The developed tool can be easily deployed on Linux distributions that are based on Debian operating system
- **Programming Languages** - Bash, C, Python

NeuroImpression *Project URL*

Machine Learning *Nov. 2017 - Dec. 2017*

- A facial recognition tool primarily designed to derive the psychological personality of an individual in accordance with the Big Five personality traits model
- Useful in banking sector to personalize banking for every customer and thus helpful in increasing trust between bank and the customer
- LSTM and various other machine learning algorithms were used to achieve the results
- **Programming Languages** - Lua, Python, nodeJS

Skills

LANGUAGE PROFICIENCY

Industrial Experience	Python
Project Experience	C, C++, Go

SECURITY TOOLS

Network Mappers	Nmap, Zenmap, Angry IP Scanner
Vulnerability Scanners	OWASP Zap, Burp Suite, Sqlmap
Password Audit and Exploits	Aircrack, Hashcat, Metasploit
Other Softwares and OS	Tor Project, OpenSSH/PuTTY/SSH, Kali Linux, Backtrack 5

TOOLS & FRAMEWORKS

Large-scale projects	Django, Flask
Medium-scale projects	BeeGo, Android Studio, MATLAB, R Studio