Nishit Majithia

SECURITY ENGINEER

OSCP(Feb-2019) · Bengaluru, India

☐ (+91) 9727092127 | ✉ nishit.nm@gmail.com | nishitm.github.io | nishitm | nishit-majithia

Work Experience

Goldman Sachs

Bengaluru, India

SECURITY ARCHITECT - ASSOCIATE

Jul. 2021 - Present

- Examine application state machine to validate assumptions and identify vulnerabilities
- Understand, highlight and articulate risk to product owners and present alternate designs to the teams in order to help them reduce risks
- Develop and run application security tools such as fuzzers, scanners, debuggers, decompilers, proxies, simulators, etc.
- Analyse protocols, flows and interactions in a design to evaluate gaps

VMWare

Bengaluru, India

SECURITY ENGINEER-II

Sep. 2019 - Jul. 2021

- Identifying and assessing all threat vectors impacting VMWare products and the production infrastructure
- Investigate software vulnerabilities and evaluate risk using industry standard metrics such as CVSSv3 and provide corresponding recommendations based on this evaluation
- Report findings and work closely with development teams to implement security controls; relate findings to real-world risks and provide specific, actionable recommendations for resolution
- Design and conduct proof-of-concept tests to replicate third-party findings and propose solutions to resolve discovered security issues by external entities
- Perform research activities to investigate vulnerabilities and technologies which may impact VMware products, and present findings at industry conferences and tradeshows

Walmart Labs

Bengaluru, India

SECURITY ENGINEER

Aug. 2017 - Sep. 2019

- Perform web application, network, hardware and mobile application peneration testing on internally Walmart developed applications
- Design and develop security services in modern programming language like GoLang or Python to make Walmart's internal environment more secure
- Develop automation tools to fasten the penetration testing process
- Patent filed for Walmart on Identifying malware compromises on computing devices

Cyber Security Lab

IIT Kanpur, India

PROJECT EMPLOYEE

Jun. 2017 - Jul. 2017

- Perform threat analysis and penetration testing to find various vulnerabilities on SCADA control system
- Report these issues and notify CERT-In to make these issue fix

Samsung R&D Institute

Delhi, India

INTERN

Jun. 2016 - Aug. 2016

- Developed **Client HoneyPot** and honeypot server to detect malicious domain
- Implemented a idea of modifying the client honeypot to integrate with Tizen TV kernel in order to create sandbox environment for browser
- The client honeypot was capable enough of identifying malware that tries to access or modify file system or process tree of underlying operating system

CSTC, ISRO
Ahmedabad, India

INTERN, RESEARCH SCIENTIST — *Jan. 2014 - May. 2014*

- Implemented a payload called "Wireless Sensor Netowrk" for **IMS1A** satellite
- Configured and programmed a ZigBee device for communicating with all sensors available in satellite wirelessly to transfer control signal received from earth

Research

M.Tech, Thesis HONEYPOTS FOR IIT, KANPUR
Jan. 2016 - May. 2017

- Build an intelligent research **Honeypots for IITK** applications and web-hosting servers
- Major idea was of securing honeypots in order to make it undetectable by advance attackers
- With use of these honeypots, we collected various malware related to variety of services which helped us to analyze the pattern of attack that happen everyday on any education institute from internet

Education

Indian Institute of Technology Kanpur
Kanpur, India

MASTER OF TECHNOLOGY, MAJOR IN COMPUTER SCIENCE AND ENGINEERING

CGPA- 7.7/10

2015 - 2017

Charusat University
Gujarat, India

BACHELOR OF TECHNOLOGY, MAJOR IN COMPUTER SCIENCE AND ENGINEERING

CGPA- 8.7/10

2010 - 2014

Projects

wotop: Web on top of any protocol
OPEN SOURCE — *Feb. 2020*

- WOTOP is a tool meant to tunnel any sort of traffic over a standard HTTP channel.
- Useful for scenarios where there's a proxy filtering all traffic except standard HTTP(S) traffic. Unlike other tools which either require you to be behind a proxy which lets you pass arbitrary traffic (possibly after an initial CONNECT request), or tools which work only for SSH, this imposes no such restrictions.
- Github: wotop

goBox: Sandbox to run untrusted code
OPEN SOURCE — *Jan. 2020*

- GO sandbox to run untrusted code.
- goBox uses Ptrace to hook into READ syscalls, giving you the option to accept or deny syscalls before they are executed.
- Github: goBox

RTS: Real time scanner
OPEN SOURCE — *Nov. 2019*

- Sometime external researchers don't want to report security bugs of any products to security team of respective companies, instead, they prefer to go out to the public and disclose.
- Real time scanner is capable of fetching data in real time from Twitter, Github, Reddit, Gist and many pastie websites and report the information back to response security team in no time, so that team can take actions based on that.
- Github: RTS-go

Framework for finding Kubernetes security mis-configurations
WALMART LABS — *Oct. 2018 - Aug. 2019*

- The project aimed to check and identify the security mis-configurations in any kubernetes cluster.
- It checks compliance of master-worker nodes using **CIS benchmarking for Kubernetes**, container image analysis using **Anchore**, POD and container mis-configurations and lastly runtime analysis using **Sysdig Falco**.

Content Security Policy

WALMART LABS *Feb. 2018 - Oct. 2018*

- Content Security Policy(CSP) is a computer security standard introduced to prevent cross-site scripting, click-jacking and other code injection attack resulting from execution of malicious content in the trusted web page context.
- This project aimed to develop CSP environment, including backend and header injection as a part of security measures.

File Integrity Monitoring

WALMART LABS *Aug. 2017 - Feb. 2018*

- File Integrity Monitoring(FIM) is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification between the current file state and a known, good baseline
- This project aimed to implement file monitoring system across Walmart PCI environment network as a part of security concerns

Talks & Conferences

2020	**Speaker**, MooseCon, VMware Security Conference	*Sofia*
2019	**Speaker**, LasCon-X, OWASP Conference	*Texas*
2019	**Speaker**, DefCon Meet-up 0x03	*India*
2018	**Speaker**, DefCon Meet-up 0x02	*India*

Awards & Achivements

2018	**Received AOM(Associate of the Month) award for my exception contribution in the month of October to the InfoSec team of the Walmart**,
2017	**Received prize money award from SIDBI Incubation Center for Innovative Project across all branches**,
2017	**Received Best Innovative Project Award amongst Graduating Students, 2017, across all branches of IITK, for the M.Tech Thesis project**,
2017	**Received Honorarium from Dr. Rajat Mittal, ACA Head, IITK for effective teaching for the course titled ”System Security And Exploitation Techniques” in Summer School, 2017**,
2016	**Earned Google APAC rank 361 in competitive coding competition**,
2015	**AIR 476 in GATE for Computer Science**,
2013	**University Second Rank in 2nd year B.Tech**,

Publications

Open-source tools recognised by KitPloit and published: Wotop and GoBox *2020*

Co-Author of a book Cyber Security in India *2020*

- This book focuses on cyber security research, education and training in India, and work in this domain within the Indian Institute of Technology Kanpur.
- Providing glimpses of the work done at IIT Kanpur, and including perspectives from other Indian institutes where work on cyber security is starting to take shape, the book is a valuable resource for researchers and professionals, as well as educationists and policymakers.

Position of Responsibility

CTF Contest
Oct 2017 & 2018

- One of the member of the team of two who were responsible for organising a Security CTF contest across the entire WalmartLabs on Security Awareness Month

Summer Mentor-ship
May. 2017 - Jun. 2017

- Mentored one internship projects called **Secure SMTP** which is PGP integrated implementation of SMTP with kerberos Authentication server

Instructor of System Security and Exploitation Techniques Course
May 2017

- Nominated by CSE Dept as one of the three Instructors for the course. Managed a class of around 30 students with regular assignments, quizzes and lab sessions. Awarded Honorarium for the same.

Instructor of ”Introduction to C/C++” Course
May 2016

- Nominated by CSE Dept as one of the two Instructors for the course. Managed a class of around 40 students with regular assignments, quizzes and lab sessions.

Coordinator ACA
2016 - 2017

- One of the two coordinators amongst PG-Y15 batch. Instrumental role in organization of ACA summer School-2016 and Freshers for Y16.

Coordinator INFOSEC(System Security Group)
2016 - 2017

- Organized System Security related lectures, workshops and CTF for IITK students. Organized ”Crypto” CTF event in Takneek-2016

Skills

Security	Web Security, System Security, Smart contract audit, Blockchain security
Programming	C/C++, Golang, Python, Java, Ruby, JavaScript, Embedded(Arduino) Programming
Utilities	Linux shell utilities, Git, Docker, Kubernetes, GDB, ElasticSearch, LaTeX

Miscellaneous

- Blog about programming topics and poems at nishitmajithia.blogspot.com
- Contribute to open source projects like Zentral, logrus, maintain some well appreciated projects on my Github.