



TANOY BOSE

OFFENSIVE SECURITY RESEARCHER, RED TEAM, EX-BIG4
CONSULTANT

EXECUTIVE SUMMARY

- I am a security researcher with 6 years of industry experience with specialization in offensive security research with over 20 High Risk CVEs and regarded as a subject matter expert on the domain of red teaming
- I have been awarded by the Prime Minister of India for winning Global Cyber Challenge SCADA CTF and Director of U.S. Airforce Research Labs to Hack-A-Sat DEFCON CTF
- I have provided consultation to 30+ clients located at EU, Middle East and Asia across Finance, Industrial, Pharmaceutical and Technology sectors
- I have led teams of 10+ sizes
- I have created business, managed and delivered projects worth millions of dollars

STATISTICS

CVE: 28 (20+ High)
CTF Wins: 3 (Finalist in 7)
Bug Bounties: 10+
Conference talks/ research papers: 6
Tools built: 4

PUBLIC WORK

Vulnerability Advisories:
<https://vuln.shellcoder.party>
Published research:
<https://repo.shellcoder.party>

OFFENSIVE SECURITY EXPERIENCE

- Active Directory Environment
- Windows user-land
- Linux user-land
- Android user-land
- Software and Protocol Fuzzing
- Web application
- Mobile application (Android)
- Protocols (802.1X, SIP, TLS, UART)
- Firmware
- Satellite Software Stack

CONTACT ME

Website: <https://shellcoder.party>
Phone: +971 52 122 1005
Email: connect@shellcoder.party
Twitter: @TanoyBose
LinkedIn: /in/tanoybose/

RELEVANT EXPERIENCE

Security Resesarcher, Abu Dhabi

xen1thlabs, Digital14 LLC (former Darkmatter LLC) | Jan 2019 - present

- Lead the assessment of in-house developed security products (Mobile applications, VPN box, Windows applications) - Build custom fuzzing harness, source code review, dynamic testing
- Established the process of integrating security into SDLC (SSDLC) - Threat modeling, Agile Security Engineering Modeling
- Built a scale-able fuzzing framework
- Researched popular software stacks on Android, Windows, Protocols, and IOT- Built tools, custom fuzzers, exploitation techniques, and identified 20+ discovered zero-days on popular software
- Trained clients on advanced vulnerability discovery and exploitation techniques
- Managed and delivered projects worth AED 40,000,000+

External Security Consultant, Mumbai

PricewaterhouseCoopers | July 2018 - Jan 2019

- Led the region's red team practice and managed projects of 10,000,000 INR
- Pentested India's largest 4G provider's network - Developed custom fuzzers for multiple protocols
- Red Teamed on Middle East's largest Bank's network - Developed a NAC bypass utility to hack ATMs and endpoints

Senior Security Consultant, Mumbai

Ernst and Young LLP | March 2015 - June 2018

- Established red team practice and led the read team for the Mumbai region in the Industrial Sector winning and managing projects over 100,000,000 INR with 20+ clients globally
- Established SCADA pentest and red team for a client (India's biggest Oil and Gas organization) and was appointed to consult as an independent technical advisor to the CISO
- Led the multi-nation red team for a project across 7 countries, building a red-team collaboration framework
- Built new attack techniques, discovered new 0-days, and developed new research during challenging client engagements
- Innovated, developed and sold new cybersecurity offerings like cyber drills, purple teaming, honeypots, threat intelligence

MOST VIEWED RESEARCH

PHDays 2021

Satellite Software Hacking

VulnCon 2020

Fuzzing Windows Applications

Hack-In-The-Box Armory

Raspberry powered Network Access Control bypass toolkit with active injection capability

Hack-In-The-Box Workshop

Windows AD Hacking

BalCCon 2018

Hacking Hybrid (Azure) Cloud

36 Chaos Computer Congress

Locating users with Google APIs (Lightning talk)

SCHOOL BACKGROUND

Amrita Vishwa Vidyapeetham (Amrita University)

*Bachelor of Technology, Electronics and Communication Engineering
Jun 2010- May 2014*

- Completed the degree with a 'First Class' score
- Worked as a Teaching Assistant