Sathwik Mohan Vallala

Herndon, VA, USA
+1(571) 373 6079
sathwikv143@gmail.com
linkedin.com/in/sathwik-mohan
sathwikv143.github.io

EXPERIENCE

Security Response Engineer – *VMware, Inc,* Reston, VA
APR. 2021 – PRESENT
- Triage external reports, identify core issues in code, and provide fixes.
- Validated and reviewed open source software vulnerabilities.
- Created unique innovative solutions that increased our efficacy and greatly improved our efficiency.

Digital Forensic Researcher – *ADF Solutions Inc,* Reston, VA
DEC. 2020 – PRESENT
- Research various OS's & Apps for critical evidence.
- Write python scripts to extract/parse the artifacts.
- Test and validate triage tools and evidence extractors.

Bug Bounty Hunter – *Freelance,* International
OCT. 2019 – OCT. 2020
- Discover vulnerabilities in web-applications using Burpsuite or ZAP Proxy.
- Automate vulnerability scanning with Python & Open Source Tools.
- Report any found vulnerabilities to the website owners.

Security Analyst Intern – *SOC Experts,* Bangalore, India
JUL. 2019 – OCT. 2019
- Use different SIEM tools for organisational defense..
- Tools like Splunk, LogRhythm are used to perform log analysis/monitoring.
- Investigate and manage Incidents and Events on Windows Servers.
- Use basic digital forensics for incident investigations.

EDUCATION

MS in Digital Forensics – *George Mason University,* Fairfax, VA
JAN. 2020 – DEC. 2021
- GPA: 3.88/4.0

PROJECTS

Autopsy WhatsApp Plugin
APR. 2020 – MAY 2020 – *GMU*
Github
- A plugin developed as a plugin which supports popular forensics tool *Autopsy*.
- Extract and parse evidence from *WhatsApp* application in *Windows*.

Chat over network with Python
JUN. 2018 – JUL. 2018 – *Self*
Github
- A project developed to with *privacy* as main focus.
- Chat between parties are encrypted from end to end.
- Server can be self hosted and can be connected from anywhere.

SKILLS

Professional
Ethical Hacking
Vulnerability Assessment
Web Application Penetration Testing
Network Penetration Testing
Mobile Application Penetration Testing
Incident Response
Digital Forensic Analysis
Network Forensics & Memory Forensics
Malware Reverse Engineering
Security Incident & Event Management
Threat Hunting
Open Source Intelligence

Tools
EnCase, FTK, Autopsy, Falcon, WinHex, Black Bag, X-Ways, AXIOM, Volatility, IDA, Ghidra, Tcpdump, OllyDbg, Snort, Zeek, Hashing, Yara, Write Blocker, Splunk, IBM QRadar, LogRhythm, SOC, SIEM, DFIR, IOC, OSI Layers, Metasploit, Burpsuite, ZAP, OWASP, MITRE ATT&ACK, Nmap, Wireshark, Ettercap, TCP/IP, IDS/IPS, IPSec, Aircrack-ng, SQLMap, Hydra, John the Ripper, Nikto, Commix, Nessus, Kali, Linux

CERTIFICATIONS

Digital Evidence Investigator
ADF Solutions
DECEMBER 2020

Certified Autopsy User
Basis Technology
OCTOBER 2020

Certified Ethical Hacker
EC Council
OCTOBER 2017

VOLUNTEERING

Instructor
JAN 2019 – MAY 2019
KMIT Cyber Security Club

Vice President
JAN 2016 – NOV 2016
HYA - Street Cause