NIHALKUMAR PARSANIA

DIGITAL FORENSIC, MALWARE ANALYSIS, VULNERABILITY ASSESSMENT, SOC ANALYSIS, PENETRATION TESTING, THREAT INTELLIGENCE

Phone: 08780502507

Email: nihalparsania@gmail.com **LinkedIn:** www.linkedin.com/in/nihalkumar-parsania-517936119

PROFESSIONAL SUMMARY

Hard-working, I have currently pursuing my master's degree with a **M.Sc. Digital Forensic and Information Security** in Cyber Security ([7.75/10] GPA). I have completed my bachelor degree in **Computer Application (BCA)** with 8.89 CGPA. I have also completed some certification which is help me to improve my knowledge into the field of cyber security. Aiming to leverage academic experience and a proven knowledge of troubleshooting, programming, and routing to successfully fill the **Digital Forensic, Malware Analysis, Vulnerability Assessment, Penetration testing, SOC** role. Frequently praised as focused by my peers, I can be relied upon to help your company achieve its goals. Hands-on, successful Software, Tools with decades of verifiable success leading teams in delivering appropriate technology solutions for desktop and mobile products. Innovative change agent with a unique mix of high-level technology direction and deep technical expertise.

EDUCATION

Master of Science: M.Sc. Digital Forensics and Information Security

- Gujarat Forensic Sciences University - Gandhinagar, Gujarat

Bachelor **of Science: Bachelor of Computer Application**

- Parul Institute of Computer Application - Vadodara, Gujarat

IT Project Management

- Indian School of Business

WORK EXPERIENCE

Mindtree Ltd. (Malware Researcher and Analyst) **2019 – Present Hyderabad, Telangana**

When customer sends the suspicious file and I have to analyse that file and need to give the conformation whether that file is malicious or not and for that I have to analyse file first and according to that I need to write a signature for the testing. I also have a hands-on technology like Splunk, Threat Intelligence, Q-Radar, AlienVault or Accunetix for the system log analysis, Event log, network log etc. In log analysis I also used a regular expression for investigate the suspicious activities.

- Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures.
- Monitor current reports of computer viruses to determine when to update virus protection systems.

Microsoft (Windows Defender Researcher) **Dec. 2019 – Present Hyderabad, Telangana**

I was working with the Mindtree and Microsoft is the main client of the company. My job is to analyse the files and set the determination. According to my determination windows defender take the decision whether file is being execute or not in the windows machine.

Anti-Corruption Bureau (Forensic Advisor) **April. 2019 – August. 2019 Junagadh, Gujarat**

Here in bureau when the case is under investigation and that case is relevant to the cyber related crime then I need to give an idea how the case can be resolved. I have also worked with the District Forensics Lab of Junagadh, Gujarat. Here, I have also used hardware level integration system which used for maintaining an integrity of the evidence.

- Answer user inquiries regarding computer software or hardware operation to resolve problems.
- Set up equipment for employee use, performing or ensuring proper installation of cables, operating systems, or appropriate software.

CERTIFICATION

1. Introduction to Cyber Security Tools & Cyber Attacks by IBM
2. Technical Support Fundamentals by GOOGLE
3. Cyber Security and It's Ten Domains by University of Georgia
4. Blockchain Basic by University of Buffalo

5. Cryptography and Hashing Overview by University of California
6. International Cyber Conflicts by The State University of New York
7. Network Cybersecurity by Palo Alto
8. Web Application Security Testing OWASP ZAP by rhyme.com
9. Mobilyze Tool Training by BlackBag
10. Autopsy 8 hours of Training by Autopsy
11. Microsoft Certified Solutions Associate (MCSA) from IIHT
12. Cisco Certified Network Associate (CCNA) in Routing and Switching from IIHT
13. Cisco Certified Network Associate (CCNA Security) form IIHT
14. Optical Fiber Technician from Government of Gujarat
15. Splunk 7.x Fundamentals Part 1
16. Splunk User Behaviour Analytics
17. Stay anonymous online at Darknet, TOR, WHONIX, Tails and kali.
18. Certification of Phishing from Udemy Learning Site.

EXTRA CURRICULAR ACTIVITIES

1. Attended the JAVA Training Program conducted by IIT Bombay.
2. Attended the PHP Training Program conducted by IIT Bombay.
3. Attended the MySQL Training Program conducted by IIT Bombay.
4. Attended the LINUX/ UNIX Training Program conducted by IIT Bombay.
5. Attended NASSCOM training.
6. I had given the training to the government L1 class officers on Cyber security at Gandhinagar Sachivalaya.
7. I have attended the seminar of Rakshit Tondon on Cyber Security and Awareness Program.
8. Attended the NULLCOM meet in Hyderabad.

SKILLS

Malware Analysis	Memory Forensic	Analytics
Yara Signature	Network Forensic	Adaptability
Reverse Engineering	Digital Forensic	Troubleshooting
Network Security	Splunk	Critical observation
Penetration Testing	Log Analysis	Team Work

TOOLS AND TECHNOLOGY

Digital Forensic

- Dc3dd
- Autopsy
- FTK Imager
- John the Ripper
- PasteBin
- Bulk_extractor
- EnCase
- Guy_mager
- WebSlayer

Malware Analysis

- Peid, peview,pestudio
- Pdf parser
- Olly dbg
- Gidhra
- Pdfid
- MITRE ATT&CK
- Proc Dot
- IDA PRO
- Sysinternals
- Pdfstream dumper
- Procmon
- Snort
- MeltaGo

Vulnerability Assessment

- Nmap / Zenmap
- OWASP
- W3af
- sqlmap
- Wayback Machine
- Metasploit
- Wireshark
- Zap
- Burp Suite
- SilkRoad

SOC Analysis

- Splunk
- IBM Q-Radar
- Accunetix
- Threat Intelligence
- AlienVault

TRAINING

1. SANS Webcast - YARA - Effectively using and generating rules
2. SANS Webcast: Practical OSINT - Six Tips for Starting an Effective Investigation
3. SANS Webcast: Web Hacking with Burp Suite
4. SANS Webcast: Password Cracking - Beyond the Basics
5. NPTEL: Introduction to Information Security co-ordinate by IIT Madras
6. NPTEL: Information Security Module IV co-ordinate by IIT Madras
7. Certification or training of Build your own lab at home from the Udemy Learning Site.

PROJECTS

1. Gate-Pass Management System using C language.
2. Travel Management System using Asp.net for web portal as well as use Android for Application.
3. Fuel Saving System using Arduino Uno, sensors etc.
4. Comparative Analysis of SQL injection Tools.
5. Mobile Data Acquisition Tool.
6. Malware Analysis of Non- Portable Executable.
7. Log Analysis using AlienVault, Snort and Splunk