Prachi Oza

Hyattsville, Maryland

240-384-8773 | prachi.oza92@gmail.com | linkedin.com/in/prachi-oza | prachi-oza.github.io

EDUCATION

University of Maryland — *College Park, Maryland*
Master of Engineering in Cybersecurity — **Aug, 2021 – May, 2023**
- Grader Assistant for Machine Learning Techniques applied to Cybersecurity — **Feb, 2023 – May, 2023**
- Coursework: Hacking of C programs and Unix binaries; Penetration testing; Cloud Security; Networks and Protocols; Network Security; Secure Coding for Software Engineering; Digital Forensics and Incidence Response

Nirma University — *Ahmedabad, India*
Bachelor of Technology in Computer Engineering — **Sept, 2016 – June, 2020**
- Coursework: Software Engineering, Database Management Systems, Web Security, Advanced Data Structures

WORK EXPERIENCE

Bonum Technologies LLC — *College Park, Maryland*
Network Specialist — **July, 2022 – Aug, 2022**
- Day-to-day monitoring of the company's network server and infrastructure- including the firewall and network configurations, reducing downtime by 35%.
- Troubleshooted issues quickly and observed performance data in order to research and create detailed performance reports.
- Regular maintenance of the networks and update firewall as required.

Feynman Technologies Pvt. Ltd. — *Ahmedabad, India*
Apprentice Software Engineer — **June, 2020 – May, 2021**
- Developed and modified various modules of the company's user application, Tilt, using concepts such as token-based authentication resulting in a 25% decreased log in time.
- Programmed the listings page, bookings module as well as the user sign in/sign up page.
- Assisted in creating a scalable web application and back-end infrastructure to create a suitable and optimal database.

Proclink Consulting Services LLP — *Ahmedabad, India*
Cybersecurity Intern — **Jan, 2020 – June, 2020**
- Designed a vulnerability scanner for industrial control systems using tools from Kali Linux and Python language by incorporating 3 scanning techniques.
- Developed and executed a comprehensive plan to conduct penetration testing on a small scale, leveraging vulnerability exploitation techniques to test system resiliency.
- Performed research on control systems such as ICS, SCADA, and DCS.

PROJECTS

Cloud Security | *AWS, Azure Active Directory* — **Aug, 2022 – Dec, 2022**
- Performed analysis of the given scenario and provided recommendations to safely transition to the AWS Cloud. Provided NACL and security groups as per requirements and a technical documentation showcasing how to make use of each recommended service by making use of AWS CLI in Windows and Ubuntu operating systems.
- Additionally, integrated AWS Cloud with Azure and made use of Azure Active Directory.

Secure Code Review | *Mitre CWE, SonarQube, Vulnerability Assessment, Git* — **Aug, 2022 – Dec, 2022**
- Performed a secure code review of a software and analyzed it to find weaknesses associated with any CWEs. Made use of tools such as SonarQube, Snyk and Roslyn analyzer to detect the issues; making use of Docker to initialize an analyzer.
- Also conducted secure code review on a consumer-ready software application to detect any vulnerabilities present; was successfully able to make appropriate recommendations to improve security by 70% for the same.

Penetration Testing | *Nmap, Metasploit, Threat Hunting* — **Aug, 2021 – Dec, 2021**
- Made use of various penetration testing tools and frameworks such as Nmap, Metasploit Framework, Wireshark and Hashcat in order to gain access to an admin account.
- Additionally, used the Remote Desktop Protocol to log into the admin account from the host machine and using some commands pertaining to AWS S3 bucket, were able to obtain all the flags.

TECHNICAL SKILLS

Languages: Java, Python, C, C#, SQL, JavaScript, HTML/CSS, Shell Scripting
Frameworks: Bootstrap, Wireshark, .NET, AWS IAM
Tools & Software: Nmap, Metasploit, BurpSuite, Nessus, Splunk, GDB, SonarQube, Snyk, Git, Docker, Visual Studio
Security: NIST, Network Protocols, Vulnerability Analysis, Penetration Testing, Cryptography
CompTIA Security+ : Expected July, 2023