Neelkumar Patel

Linkedin: https://www.linkedin.com/in/neelkumarpatel
Github: https://github.com/neelpatel05

Email : nnpatel@terpmail.umd.edu
Mobile : +1-908-829-4298
Address : Hyattsville, College Park, MD

Education

- **University of Maryland** — College Park, MD
  Masters in Cybersecurity — *Anticipated May 2021*
  Courses: Hacking of C Programs and UNIX binaries, Networks and Protocols, Penetration Testing.
- **Gujarat Technological University** — Anand, India
  Bachelor of Engineering, Information Technology; GPA: 3.85 (9.25/10.00) — *Aug 2015 - May 2019*

Skills Summary

- **Languages & Databases**: Python, C, C++, Java, Go, Unix scripting, Javascript, SQL, NoSQL, MongoDB
- **Assembly Languages**: x86 IA-32, IA-64 (Familiar)
- **Networking**: TCP/IP, OSI Model, Firewall, Port Forwarding, Implementation of DNS, FTP, SSH, Proxy Server
- **Web-App Exploitation**: SQL Injection, XSS Attack, Command Injection, File Inclusion, Deserialization Attack, Brute Forcing
- **Hacking Tools**: Wireshark, NMAP, Burpsuite, Metasploit, Dig, Hashcat, John the ripper
- **Operation Systems & Tools**: Linux, macOS, Windows, Riverbed Modeler, Docker, GIT, Android Studio, Xcode
- **Other**: Rest APIs, Flask, Machine Learning, Deep Learning, Keras, Tensorflow

Experience

- **OpenEyes Technologies** — Vadodara, India
  Intern - Product and Project — *Jan 2019 - Apr 2019*
  - **Convolution Neural Network Developer**: Researched latest technologies to construct a Convolution Neural Network (CNN) platform "Anti-Smokify" achieving 92% accuracy.
  - **Amazon Web Services**: Performed Identity Access Management (IAM) for development of platform utilizing Amazon Web Services (AWS). Utilized DynamoDB for backend development.
  - **Security**: Inspected and resolved API request and response errors employing Wireshark sniffing tool to capture and rectify faults. Diagnosed and exposed critical software vulnerabilities to propose solutions to augment software security.
- **Gujarat Alkalies and Chemicals Limited** — Vadodara, India
  Software Development Trainee — *May 2017 - June 2017*
  - **ERP Development**: Led alongside 2 senior managers of Management Information System (MIS) department to develop a Decision Support System platform "Hydrogen Utilization" to analyse and measure hydrogen usage and production on production site.
  - **Documentation**: Completed 38-page report on Decision Support System platform 1 week ahead of schedule.

Projects

- **Exploiting Buffer Overflow in Cherokee Webserver - C, IA-32, Python**: Developing Exploits in python to buffer overflow the cherokee webserver which leads to crashing. Overwriting argv[0] to insane length causes the webserver as well as admin panel to carsh and fails to bind the port (In progress)
- **Network Sniffer - Python**: Structured a network sniffing tool to monitor or capture TCP, UDP, ICMP, DNS and IP packets from data communication over computer network links in real-time and over internet using python. (Sept '19)
- **Brute force SSH - Go, Python, Wireshark**: Designed and created a brute force attacking software to gain remote access of machines through Secure Shell (SSH) protocol. Integrated project with crunch penetration testing tool to generate word-list according to specifications of attacker (Aug '19)
- **Brute force ZIP - Go, Python**: Implemented a terminal program to perform a brute force attack on password-protected zip files on a local computer or remote machines. Scripted Python code generates word list and Golang script performs brute force attack with each password in generated word list (July '19)
- **JSON Web Tokens, JWT - Go, Python, Postman, REST API**: Built a secure REST API implementing JSON web tokens to assert claims between two parties or endpoints complying with RFC 7519 industry standard. Utilized REST API project to ensure secure authentication and integrity of information in various types of projects and software (Mar '19)
- **Cryptographic Algorithm - Python**: Devised a novel encryption and decryption cryptographic algorithm operating with metadata of input information for safe transmission of data over physical transmission media preventing from active and passive attack. Formulated algorithm randomly generates key from input data of different length and embeds key into transmitted information (Mar '18)

Honors and Awards

- Ranked Third among batch of 72 students in my Information Technology Engineering Department.
- Received Excellency Award by "NASSCOM" as being top ranker and best project in Information Technology Department
- Acquired government funding for a national level project from Student Start-Up & Innovation Policy (SSIP)