Neelkumar Patel

Graduate Teaching Assistant

Email: nnpatel@umd.edu
Address: Hyattsville, College Park, MD
GitHub: github.com/neelpatel05

Summary

An enthusiastic Cyber-security Engineer focused on Red Teaming and Offensive Security. Strong expertise in Reverse Engineering Software and Malware along with Exploit Development. Highly dedicated to develop a proof-of-concept by exploiting vulnerabilities in an application.

Education

- **University of Maryland** — College Park, MD
  Masters of Engineering, Cybersecurity; GPA: 4.00 — *Anticipated May 2021*
  - **Coursework**: Hacking of C Programs & UNIX Binaries, Networks & Protocols, Penetration Testing, Network Security, Embedded System Security, Secure Software Construction & Testing, Reverse Engineering, Cloud Security, Cryptography
- **Gujarat Technological University** — Ahmedabad, India
  Bachelors of Technology, Information Technology; GPA: 3.85 — *Aug 2015 - May 2019*
  - **Coursework**: Data Structure & Algorithms, Operating System, Information Security & Cryptography, Computer Architecture, Computer Networking, Python Programming

Experience

- **A. James Clark School of Engineering, University of Maryland** — College Park, MD
  Graduate Teaching Assistant — *Jan 2020 - Present*
  - **Teaching**: Graduate Teaching Assistant for ENPM691 - Hacking of C Programs and UNIX Binaries. Spearheaded over 20 graduate students in Hacking of C Programs and UNIX Binaries class
  - **Logistics**: Conducted Office Hours for mentoring students over Class Projects and to clear technical doubt regarding the course
  - **Course Contribution**: Contributed to course development and developed Linux Based Ubuntu 64-bit Docker container specifically for Reverse Engineering Binaries with all tools and technologies. Deployed the docker image to Docker Hub and GitHub package repository
- **WiSSR Lab, Department of Computer Science, University of Maryland** — College Park, MD
  Graduate Research Assistant — *Jan 2020 - Oct 2020*
  - **Research Topic 1**: Researched novel and innovative technique called "Honey-Maze", by merging low level IoT honeypots with intelligence. Integrated Markov Decision Process with hacker's behavioural pattern to leverage total time spent by the attacker on honey-maze
  - **Research Topic 2**: Programming Assembly code in ARM and x86 to introduce structural and data hazards in the processor. Researched side-channel analysis for defence mechanism and investigated hazards through thermal imaging techniques
- **OpenEyes Technologies Inc.** — Vadodara, India
  Software Development Intern — *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.

Skills Summary

- **Programming, Databases & OS**: Python, C, C++, Java, Go, SQL, NoSQL, macOS, Windows, Linux, Kali
- **Reverse Engineering**: x86 (32 and 64 bit), ARM, MIPS, Ghidra, Radare2 Tools, Binutils, Cutter, GDB
- **Cloud AWS**: VPC, EC2, DynamoDB, S3, IAM, API Gateway, Security Group
- **IDS/IPS & Firewall**: Snort, OSSEC, SIEM, Splunk, Iptables, Cisco Firewall, UFW
- **Network & Application Security**: OWASP Top 10, MITM Attacks, DNS poisoning, IP Layer Attacks, ARP poisoning
- **System Security**: SAST, DAST, Buffer Overflow, Format String, Meltdown, Spectre, Shellshock, ROP
- **Web Exploitation/Security**: SQL Injection, XXE, Deserialization Attack, LFI, XSS, CSRF, Command Injection, RCE
- **Networking & Hacking Tools**: PCAP Analysis, TCP/IP, NMAP, Wireshark, John-the-ripper, Hashcat, Metasploit, Dig, Nikto, Gobuster
- **Certification**: Offensive Security Certified Professional (Pursuing OSCP)

Projects

- **Exploiting Buffer Overflow in Cherokee Webserver - C, IA-32, Python, GNU Debugger**: Developed exploit 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.
- **TP-Link Firmware Exploitation - C, Cutter, radare2, Binwalk, Qemu, Firmware Mod Kit**: Exploited TP-Link firmware with backdoor to get a reverse shell during boot of operating system facilitating to launch networkwide attacks on machines connected to router. Collaborated with a team of 5 and reversed engineered TP-Link firmware binaries to explore existing vulnerabilities.
- **Securing Tiny Web Server - C, CMake, Python**: Patched tiny web server developed by professors of Carnegie Mellon University in Pittsburgh from security vulnerabilities like Integer overflow, Buffer Overflow, Format String Vulnerability, Command Injection, Local File Inclusion. Created a detailed and professional vulnerability assessment report along with the defined patches for vulnerability.
- **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.
- **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.
- **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
- **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.

Honors and Awards

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