Neelkumar Patel

+1 (240)-505-8107 | nnpatel@terpmail.umd.edu | 3404 Tulane Dr. Apt 14, Hyattsville, MD
LinkedIn: https://www.linkedin.com/in/patelneeln | GitHub: https://www.github.com/neelpatel05

EDUCATION

University of Maryland, College Park, MD Aug 2019 - May 2021
Master of Engineering, Cybersecurity, GPA: 4.00

- 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 Aug 2015 - May 2019
Bachelor of Technology, Information Technology, GPA: 3.85

- Secured academic excellence award for being 3rd rank and for best project in Information Technology Department

EXPERIENCE

Graduate Teaching Assistant at A. James Clark School of Engineering, University of Maryland Jan 2020 – Present

- Spearheaded over 50 graduate students in Hacking of C Programs and UNIX Binaries class
- Conducted office hours to help students to understand course theory and mentored to implement class projects

Graduate Research Assistant at Wireless Systems and Signal Research Lab, University of Maryland Jan 2020 – Oct 2020

- Researching a novel technique called “Honey-Maze”, by merging low level Internet-of-things honeypots with intelligence
- Integrating Markov Decision Process with hacker’s behavioural pattern to leverage total time spent by attacker on honey-maze
- Combined intelligent system with decoy system fooling attacker to give its attacking methodology by “honey-mazing” attacker

Software Development Intern at OpenEyes Software Solutions Limited, Vadodara, India Jan 2019 - Apr 2019

- Led alongside 2 peers to research and build a Convolutional Neural Network (CNN) platform called “Anti-Smokify”
- Performed AWS Identity Access Management (IAM) and configured cloud environment to mitigate potential security risks
- Diagnosed and exposed critical software vulnerabilities to propose mitigation plans to augment software security
- Adopted transfer learning and utilized ResNet50 neural network model to achieve 96% accuracy from as low as 70%

SKILLS

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/IDP and Firewall	Snort, OSSEC, SIEM, Splunk, Iptables, Cisco Firewall, UFW
Network 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

Cherokee Web Server Exploitation (CVE-2019-1010218) - *C, IA-32, Python, GNU Debugger*

- Constructed exploit to overflow buffer leading to Denial-of-Service (DoS) and disrupting “Availability” among CIA triads
- Managed to overwrite arguments to insane length with system call causing webserver as well as admin panel to crash by port-service binding error
- Proposed a patch to effectively eliminate the vulnerability and submitted merge request to the creator of web server on GitHub

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 network-wide 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

Penetration Testing of Virtual Network

- Performed professional penetration testing on virtual network to discover vulnerabilities and exploit it to compromise system
- Documented captured exploit and vulnerabilities to craft technical and executive report to present security of Virtual Network

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 attacks