SWAPNIL PATHAK

+1 (617)-840-2797 | pathak.s@husky.neu.edu | linkedin.com/in/swapnil-pathak/ | swapnil-pathak.github.io

EDUCATION

Master of Science – Research (Cybersecurity) | Northeastern University, Boston | GPA: 3.5/4.0 Dec 2019

Activities: Northeastern University Collegiate Cyber Defence Championship (NUCCDC) team – **Blue team**

Courses: Network Security, Computer System Security, Software Vulnerabilities and Security, Digital Forensics

Bachelor of Engineering – (Computer Engineering) | University of Pune | GPA: 3.8/4.0 May 2017

Certificates: Computer Security Fundamentals (Microsoft), PHP, MySQL

Courses: Cyber Security, Cloud Computing, Operating System Administration, Software Engineering

PROFESSIONAL EXPERIENCE

Cybersecurity Intern | Commonwealth of Massachusetts Jan 2019 – Present

- Performed application and system **penetration test**, manual and automated vulnerability scanning, generated exploits in **C language** and reported to management with findings
- Reviewed code for vulnerabilities in 13 applications (**1 million** lines of code) and categorize based on the severity
- Monitored and assessed threats and presented findings and suggestive measures for mitigation
- Examined network packets, application and network logs, system logs and responded to security events
- Automated IP address blocking on firewall efficiently using a **Python** script
- Investigated malware, phishing attempts, DDoS attacks on 5 domains using Crowdstrike, Splunk and Symantec
- Audited users' access to admin rights, VPN, ActiveSync, and OWA, revoked unnecessary access
- Served as a point of contact between network team, developers and infrastructure team
- Assisted in deployment of tools including Splunk, Ensilo, Manage Engine, and HPE Fortify

ACADEMIC EXPERIENCE

Graduate Teaching Assistant | Northeastern University Sep 2019 – Dec 2019

- Instructed students on Python programming, Bash scripting, and penetration testing
- Designed labs to teach Kerberos authentication, vulnerability scanning, buffer overflow, and cryptography

Graduate Research Assistant | Northeastern University Jan 2018 – Aug 2018

- Identified **5 critical buffer overflow vulnerabilities** using fuzzing (AFL) in system libraries and firmware
- Implemented peripheral device models in Qemu for ARM Cortex M by analyzing memory-mapped registers
- Formulated MMIO collected from datasheets in JSON format compatible with the model learning algorithm
- Fixed issues in interrupt handling, attachment of fuzzer to an emulated environment and design decisions
- Tested the automated bug finding system using Python scripts and obtained **100%** precision and recall

TECHNICAL PROFICIENCY

Programming Languages:	C, C++, Python, Bash, Powershell, Assembly (x86, MIPS)
Technologies:	SIEM, PKI (Public Key Infrastructure), Git, TCP/IP
Security Tools:	Burp Suite, Wireshark, Nmap, Metasploit, Kali Linux tools
Core Competencies:	Penetration testing, Vulnerability assessment, Security Operations Centre (SOC)

PROJECTS

Discovery and Registration for IoT Devices |**National Security Agency (NSA)** | NEU Sep 2018 – Dec 2018

- Developed a mechanism to securely provision Wi-Fi Access in C and Android by reverse engineering Smart Config technology, resulting in the mitigation of risks for over **70%** IoT devices

Checkpointing of Docker Containers using DMTCP | NEU Feb 2019 – Mar 2018

- Led a **team of 4** and engineered 3 approaches to create a checkpoint and restart a process running in a Docker container using C code also deployed RESTful services using Python Flask framework

System and Network Hardening | NEU Jan 2018 – Feb 2018

- Configured Splunk, OpenVAS, Security Enhanced Linux, Extended Internet Service Daemon, IDS (Suricata) and firewall (iptables) to allow vulnerability scanning and defense-in-depth on a Linux server

ACTIVITIES

- Ranked **Pro-Hacker** on HackTheBox (Profile link) – Position top **300** out of **125k** users in Hall of Fame
- **Runner-up** at IBM CTF competition and participated in online CTFs on CTFtime