Nabeel Mahdi Abid Mehdi Sayed

snmahdi97@gmail.com | 703-341-9688 | www.github.com/nixonion | www.linkedin.com/in/nabeelsayed/

Summary

A penetration tester and cloud security enthusiast with background in secure programming, security audit and compliance, network security, operating system security and vulnerability assessment. An excellent communicator and team player with a liking for sharing knowledge with the team. Skills in network and systems programming, PCAP analysis, SIEM, AWS, Azure and Scripting.

Education

Master of Science (Information Security and Assurance) — *Aug 2019 – May 2021*

George Mason University | GPA 3.72/4.0 | Graduating May 2021

Bachelor of Engineering (Information Technology) — *July 2015 – May 2019*

Mumbai University | GPA 3.5/4.0 | Graduated May 2019

Certifications

Microsoft Certified: Azure Security Engineer Associate — *Estimated Completion: Jan 2021*

AWS Certified Security Specialty, AWS — *Jul 2020 – Jul 2023*

Certified Ethical Hacker (CEH), EC-Council — *Jul 2019 – Jul 2022*

Experience

Graduate Teaching Assistant | George Mason University, Fairfax, VA — *Jan 2020-Present*

- Lab assistant for the course "Security Laboratory" and instructed students on setting up and using security tools and technologies like **SIEM (Splunk),** Firewalls (**Pfsense**, IPTables), OSINT tools (Shodan, Maltego, etc), **IDS (Snort**), Windows and Linux logging (Sysmon), Macro based pattern matching (YARA, Olevba), SQL Injection, XSS, **Windows Active Directory Administration**, LLMNR poisoning, SMB Relay attacks, Golden ticket attack (Mimikatz) and Command and Control communications (Covenant).
- Responsible for assessing assignments and assisting students with course related queries and **troubleshooting** their labs.

Penetration Tester | Token Metrics, DC — *June 2020-Aug 2020*

- Performed weekly penetration tests and secured the beta versions of web applications by pointing out the vulnerabilities using **OWASP ZAP, Selenium, Burpsuite**, **penetration testing tools** and drafted vulnerability reports.
- **Implemented User Segmentation** by implementing structured IAM rule base, altering Security Groups and NACL for application and task specific VPN access.
- Conducted system scans using **AWS** inspector, drafted a list of IOCs for WAF and analyzed logs in AWS Cloudwatch.
- Enhanced source code security by **performing dynamic and static analysis** using Sonarqube, Gitsecrets and Jshint installed and ran it using Containers and Kubernetes.
- Performed internal social engineering attacks to spread awareness and assisted in drafting user guides for clients on key security related enhancements.

Cybersecurity Intern | Protechmanize Solutions Pvt Ltd, Mumbai, India — *June 2019-June 2019*

- Performed vulnerability scans over the network of in scope firms. Employed **Nessus professional** and Kali Linux based penetration testing tools for vulnerability assessment on networks. E.g., Aircrack-ng, Burpsuite, Sqlmap, nikto, etc.
- Facilitated the development of **vulnerability reports** and created analysis and visualization of the reports for reporting needs.

Projects

Security Audit and Compliance testing | George Mason University — *Nov 2020*

- Created an IT security policy for a large Organization that is in accordance with **COBIT/PCI-DSS** guidelines and drafted a **Security Audit Program** and Compliance testing policy.

Runtime system call monitoring using Loadable Kernel Module | George Mason University — *Oct 2020*

- Developed my own custom **system call** for Linux kernel and added a dynamic runtime system call monitoring mechanism using **Loadable Kernel Module**.

Network enabled secure game | George Mason University — *Feb 2020 – May 2020*

- Developed a client server model game secured from **SQL injection, DoS Attacks, buffer overflow, snooping, data leaks, resource exhaustion** and **input validation attacks**, and removed all vulnerabilities through static and dynamic analysis of source code.