NIDA ILYAS, B.S.

Mobile: (703) 371-3036 | Email: nsum280@gmail.com | linkedin.com/in/nida-ilyas-4aa49528b

OBJECTIVE

Recent Information Technology graduate with a Cybersecurity concentration, holding CompTIA Security+ (SY0-701) certification. Exposure to key areas including threat analysis, vulnerability management, SIEM tools, incident response, access control, cloud security, and scripting.. Seeking an entry-level cybersecurity role to apply analytical skills and contribute to strengthening an organization's security posture.

EDUCATION & CREDENTIALS

GEORGE MASON UNIVERSITY

Information Technology (Concentration in Cyber Security), BS

Relevant Coursework: Network Security · Applied Cyber Threat Analysis · Digital Forensics and Auditing · Information Security Fundamentals · Data and Application Security · Security Accreditation of Information Systems · Information Defense Technologies · Operating Systems Fundamentals · Data Communications & Networking Principles · Database Fundamentals · Python and Java Programming · Object-Oriented Design · IT Problem Solving

CERTIFICATION

CompTIA: Security+ (SY0-701)

Technical Experience

MALWARE ANALYSIS - GitHub

- This project involves setting up a Virtual Machine (VM) sandbox in VirtualBox for malware analysis and examining a Remote Access Trojan (RAT).
- Performed static and dynamic analysis using Process Monitor, Process Explorer, Autoruns, and Regshot to monitor system behavior, registry changes, and persistence techniques.
- Captured and analyzed malicious traffic with Wireshark, identifying command-and-control (C2) communications and outbound connections.
- Documented Indicators of Compromise (IOCs), behavioral findings, and system impact in a detailed technical report.
- Demonstrated hands-on malware analysis skills, including behavioral inspection, threat detection, and safe lab configuration.

SIMPLE VULNERABILITY MATCHER - GitHub

- Developed a Python-based tool that scans installed Windows software and checks for known vulnerabilities using the NVD API.
- Integrated severity filtering and export functions for generating reports in CSV, JSON, and PDF formats.
- Demonstrated skills in API integration, Python scripting, vulnerability management, and secure automation.

ELYSIUM IT INTEGRATION

- Established a secure IT environment for a small business transitioning from a fully paper-based system
- Performed risk assessment, configured access controls, and built a secure web framework to protect customer data and enable secure transactions.

SKILLS

Security & Threat Analysis: Threat Detection, SIEM (Splunk, QRadar), IDS/IPS (Snort, Suricata), Risk Assessment
Incident Response & Forensics: Incident Response, Threat Intelligence, Log Analysis, Malware Detection, Auditing
Vulnerability Management: Vulnerability Scanning (Nessus, OpenVAS), Patch Management, Security Policies & Compliance
Network Security: Firewalls (Palo Alto, Cisco ASA), VPN, Wireshark, TCP/IP, Encryption, Network Hardening
Endpoint & Cloud Security: EDR Solutions, AWS Security, IAM Policies
Programming & Scripting: Python (Security Automation), Bash, PowerShell, SQL, Java
Frameworks & Compliance: NIST, MITRE ATT&CK, CIS Controls, ISO 27001, SOC 2, Cybersecurity Principles