

Tasin Naveed

New Jersey, USA

tan7@njit.edu | +1-862-235-7825 | [linkedin.com/in/tasin-naveed/](https://www.linkedin.com/in/tasin-naveed/) | [t-naveed.github.io/myself-naveed/](https://github.com/t-naveed/myself-naveed/)

SUMMARY

I am a skilled IT professional with a broad base of experience in Information Security, System Administration and IT Support. I can resolve problems quickly, delivering high levels of customer satisfaction. I have excellent knowledge of technical support and operations.

WORK EXPERIENCE

Infosys — Cyber Security Intern

June 2022 - August 2022

- Collaborated with Senior Technology Architect and Senior Security Associate for completing daily tasks.
- Researched on Threat Hunting: analysis and possibilities of automation.
- Automated Threat and Vulnerability Management, raising incident tickets and attaching reference files to ServiceNow.
- Worked with OWASP ASVS framework to test and verify security measurements of web applications.

EDUCATION

New Jersey Institute of Technology

B.S. in Information Technology — Specializing Network and Security

GPA 3.80 - Dean's List

Newark, New Jersey

Sep 2020 - May 2023

Relevant Coursework: Ethical Hacking for System Administrator, Computer Forensics, System and Network Security, Privacy and Law, Cyberpsychology, Digital Crime, Advanced Programming, System Administration, Internet Application.

TECHNICAL SKILLS

Expertise: Threat Intelligence and Vulnerability Management, Security Operations and Monitoring, Incident Response and Forensics, Malware Analysis and Vulnerability Research, Web and Network Penetration Testing, Data Analytics (Python Streamlit), Automation with Python, Web Technologies, System Administration, IT Support.

Languages: Python, Powershell, Bash, JavaScript, SQL, PHP, HTML/CSS.

OS: Windows, MAC, Ubuntu, Centos 7, Kali Linux, VMWare.

Tools/Platforms/Software: Cisco Talos, Burp Suite, Zeek, Networkminer, Brim, Wireshark, Splunk, MISP, OpenCTI, Wazuh, Hive, Tenable Nessus, Rapid7, Sysinternals, Sysmon, Snort, Metasploit, OpenVAS, Zap, Nikto, Nmap, Maltego, Autopsy, Office 365.

ACADEMIC PROJECTS

CyberSentry - Aim to assist security Analysts

System Integration (IT490)

- A Complete and Modern Threat Intelligence Dashboard to assist security analysts in protecting their organizations.
- Key features: Cyber threats from across the world, Analytics of threats categorized by countries, in depth details of each threat, rule generator for IDS/IPS or Firewall.
- Technology stack: Python, OTX API, Rabbitmq, MySQL, Streamlit Analytics Framework.

Astia - A Smishing Platform

Capstone Project (IT491)

- A Complete and Modern Platform built to enhance cybersecurity awareness training.
- Key Features: smishing campaign simulation and documentation of those attacks, identifying employees at risk of social engineering, generating comprehensive analytical views.
- Technology Stack: Bootstrap, Javascript, Python, Twilio API, SQL, Nginx, rsyslog.

Penetration Testing and Computer Forensics Investigation

Final Project (IT430 & IT330)

- Learned ethical hacking, conducted penetration tests and wrote reports in ethical hacking class (IT430).
- I was lead investigator of computer forensics class (IT330) where I conducted a forensics investigation to find the possibility of industrial espionage which includes collecting evidence, computer forensics and writing reports.

Computer System Security

Hands-on Lab (IT230)

- Completed hands-on lab on Vulnerability Scanning, Malware Analysis, and Cryptography.