

MITWA MISTRY

Clifton, NJ | 929-544-8382 | mistrymitwa23@gmail.com | [LinkedIn](#)

PROFILE

Aspiring Cybersecurity Professional | Cisco Certified Network Associate | Preparing for CompTIA Security+ | Passion for Protecting Corporate Environments from Malicious Actors | Experience in Analyzing & Mitigating Suspicious Incidents from Cyber Threats

EDUCATION

Pace University, Seidenberg School of Computer Science & Information Systems **New York, NY**
Master of Science (MS) in Cyber Security | **Concentration:** Cybersecurity | **GPA:** 4.00 August 2021 - May 2023

LDRP-ITR, KSV University **Gandhinagar, India**
Bachelor of Engineering (BE) in Computer Engineering | **GPA:** 3.6 August 2016 - May 2020

RELEVANT COURSEWORK

Cryptography & Network Security | Operating Systems | Network Security & Defense | Ethical Hacking & Penetration Testing | Computer & Internet Forensics | Information Security Auditing & Risk Management | Information Security Planning & Policy

TECHNICAL SKILLS

Operating Systems: Windows, Linux/Unix, Ubuntu

Programming Languages: Java, Python, C/C++, HTML/CSS, MySQL, Shell Scripting

Platforms: PhishER, Datalake/Exabeam, CarbonBlack EDR & App Control, KnowBe4, Cisco Talos, AWS, Opsgenie, Dynatrace

Ethical Hacking: Burpsuite, WebGoat, Metasploit, SIEM, Snort, Netcat, Powershell, Nmap, Wireshark, Nessus, John-Ripper, Kali Linux

Tools: ThreatStream, Cherwell Service Management, JIRA, Crowdstrike, SIFT Workstation, History Viewer, Autopsy

Security Management: NIST Cybersecurity Framework, ISO 27001, OWASP Top 10, Risk Assessment, OSINT, Threat Modeling

Network Security/Protocols: TCP/IP, ARP, OSPF, BGP, EIGRP, RIP, SSH, IPSEC, DHCP, HTTPS, TLS, SSL, VPN, IDS/IPS

PROFESSIONAL EXPERIENCE

Black Hills Energy, Rapid City, SD June 2022- August 2022
Cyber Security Intern

- Designed phishing campaign using PhishER & KnowBe4 to evaluate employee response to illegitimate communications.
- Leveraged TOR to create hypothesis for new threat hunting project & performed OSINT on ALPHV ransomware group across multiple vendors, determining third party/supply chain risks to avoid potential business dealings.
- Analyzed DHS threat intelligence to identify risks or threats associated with environment & participated in InfraGard program with FBI to share attack, vulnerability, & threat information.
- Collaborated with Incident Response team to analyze executables & run through joes' sandbox.
- Evaluated client websites for malicious intent & leveraged Cherwell vendor solution for whitelisting approved sites & adding users to Active Directory (AD) group with defined policies to grant specific-site access.

Aries Systems Pvt. Ltd, India August 2020 – June 2021

L1 Network Administrator | 8 months

- Deployed policies to safeguard confidential data against threat agents to ensure data integrity.
- Provided customer support resolving technical issues, improving device performance by 25%.
- Analyzed & resolved critical alerts within SLA timings to fortify problem resolution in timely manner.
- Evaluated, escalated, & troubleshooted errors & alerts from servers hosted on Dynatrace using Sciencelogic & Opsgenie.

Network Engineer Intern | 3 months

- Implemented network monitoring & configuration of security devices (firewalls & ACLs) preventing unauthorized access.
- Created runbooks for violations occurring in network & shared with team, reducing violations by 15%.

ACADEMIC PROJECTS

Security Audit for Black Hills Energy November 2022

- Established security audit criteria, evaluated vulnerabilities, & developed strategy to mitigate enterprise's inherent risks.
- Aligned strategy to ISO 27002 control framework to enable compliance to ISO 27000 Series, Sarbanes-Oxley, HIPAA, & PCI-DSS.

SQL Injection and XSS March 2022

- Performed SQL injection, gaining access to user information, allowing login bypass & enabling modification to database storage.
- Applied countermeasure to SQL injection using Prepared Statement to prevent vulnerabilities caused by SQL injection.
- Inserted malicious script using XSS injection to gain access to sensitive information.
- Created malicious webpage infected with clickjacking frame, redirecting users to alternate websites.

ACHIEVEMENTS

Graduate Cybersecurity Scholar Award, Pace University, Recognized for Academic excellence in Cybersecurity May 2023