# Gage Neumaier

Madison, Wisconsin|gage.neumaier@gmail.com|(608) 333-9955|linkedin.com/in/gage-neumaier-239ab21a5


## PROFESSIONAL SUMMARY


IT Help Desk Technician with hands-on experience in technical support, troubleshooting, and customer service. Skilled in resolving hardware and software issues, maintaining Windows and Apple operating systems, and supporting networking and Microsoft business applications. Strong problem-solving abilities, excellent communication skills, and a client-first mindset. Passionate about delivering high-quality IT support in fast-paced environments and ensuring seamless user experiences.


## EDUCATION

**University of Wisconsin-Madison**
Cybersecurity Professional Program – Madison, Wisconsin (Jan 2025)

- Relevant Courses: Computer Networking Fundamentals, Microsoft Security System Administration

**University of Wisconsin-Madison**
B.S. Biological Systems Engineering – Mechanical Systems – Madison, Wisconsin (May 2022)

- Relevant Courses: Introduction to Operating Systems, Data Structures, Machine Organization & Programming

## CERTIFICATIONS & TECHNICAL SKILLS

**Certifications:**

- CompTIA Security+
- JPMorgan Chase & Co. - Cybersecurity Job Simulation

**Security Operations & Threat Monitoring:**

- SIEM (Splunk), IDS/IPS (Suricata), Log Analysis, Threat Intelligence, Incident Response
- Windows Event Log Analysis, Firewall Configuration (pfSense), Malware Detection

**Network Security & Protocols:**

- TCP/IP, UDP, DNS, DHCP, VPN, Cisco IOS, Windows Command Line
- Network Traffic Analysis (Wireshark, Zeek), Packet Inspection, Firewall Rules

**Operating Systems:**

- Windows, Linux (Kali, Debian 12, Ubuntu), Unix

**Digital Forensics & Incident Handling:**

- Memory & Disk Analysis (FTK Imager, Autopsy), Log File Investigation, Open Source Threat Intelligence (OSINT)
- Digital Artifact Examination, Endpoint Security Strategies

**Programming & Automation:**

- Python, Bash, PowerShell (for security automation, log parsing, and threat detection)

**Cloud Security & Virtualization:**

- AWS Security, Windows Server Security Policies, Virtual Machine Hardening

## CYBERSECURITY PROJECTS & SIMULATIONS

**IT Help Desk Technician (Home Lab) | Madison, WI | 2024 – Present**

- Provided technical support for end users, diagnosing and resolving hardware and software issues.
- Troubleshot network connectivity issues, including DNS, DHCP, and VPN configurations.
- Documented technical issues and resolutions in Git to track and improve service efficiency.

**Security Information and Event Management (SIEM) & Threat Detection:**

- Configured Splunk Enterprise on Linux to collect and analyze security logs from Windows OS and pfSense IDS alerts.

- Created automated SIEM alerts and dashboards to monitor security events and detect anomalies.

**TryHackMe SIEM Simulation:**

- Completed hands-on SIEM training using Splunk, analyzing security logs, detecting anomalies, and configuring alerts to respond to security incidents.

**Endpoint Detection & Incident Response:**

- Deployed Suricata IDS/IPS for real-time network intrusion detection and prevention.
- Configured firewall rules in pfSense to block unauthorized traffic and analyze logs for threats.
- Investigated suspicious processes and files using SysInternals Suite on Windows.

**Network Traffic Analysis & Forensics:**

- Captured and analyzed PCAP files in Wireshark, identifying malicious traffic and extracting files from network packets.
- Utilized Zeek-cut in Linux for advanced traffic filtering and log analysis.
- Performed forensic log analysis of an Apache2 web server to detect signs of compromise.

**Cloud Security & Virtualization:**

- Created AWS EC2 instances running Windows Server 2016 and Ubuntu, configuring security settings and RDP access.
- Applied security hardening techniques to virtual environments.

**Penetration Testing & Ethical Hacking**:

- Conducted Nmap scans to discover open ports and assess vulnerabilities.
- Performed brute-force attacks using John the Ripper and Hashcat on NTLM and MD5 hashes.
- Exploited vulnerabilities in a controlled environment using the Metasploit framework.

**Digital Forensics & Incident Handling:**

- Created and analyzed forensic disk images using FTK Imager, performing memory acquisition and analysis.
- Conducted live forensic investigations on Linux and Windows, collecting system and network data
- Examined browser artifacts using Autopsy, analyzing cached data, cookies, and history for forensic evidence.

## ADDITIONAL SKILLS & STRENGTHS

---

- Strong analytical and problem-solving abilities
- Customer Service-Oriented: Adept at explaining complex IT concepts in a clear and user-friendly manner.
- Problem-Solving Mindset: Ability to diagnose and resolve technical issues efficiently.
- Process Improvement: Experience with IT documentation and ticketing systems to track and enhance support services.
- Time Management: Able to prioritize multiple tasks, handle urgent technical requests, and meet deadlines.
- Strong Communication: Skilled in collaborating with end users, IT teams, and vendors to resolve technical issues.