**Jimmy Neutron**

704-555-555 | neutronj@gmail.com

Charlotte, NC

**SUMMARY OF QUALIFICATIONS**

Information technology and security professional with experience in penetration testing, endpoint security, network security, and incident response. Dedicated to continual learning through training and certification courses, as well as daily practice in a home lab. Exceptional communication and prioritization skills.

Active member of InfraGard, OWASP, and QC Skiddies (monthly MeetUp focused on learning penetration testing techniques, security soft skills, Hack the Box, and Capture the Flag activities).

**AREAS OF EXPERTISE**

Security Best Practices, Policies, & Tools Incident Response Security Breach Mitigation

Multifactor Authentication (Okta/OAuth/SAML) PCI & ISO Compliance Endpoint Protection/Logging

Scripting (PowerShell, Python) Firewall Management RDS Management

OpenVPN & WireGuard VPN Configuration VMware Management Ticket Queue Management

Network Security Tools & Practices Cloud Security Secure Messaging/Communication

**SECURITY EDUCATION & PROFESSIONAL TRAINING**

**Neural University** Bachelor of Science, Cybersecurity (expected 2021)

**CompTIA** Security+

**Dept. of Homeland Security** Operational Security (OPSEC) for Control Systems

**Microsoft** MTA: Security Fundamentals

**Cybrary** PenTest Fundamentals – Sniffing, Insider Threats, & Intro to PowerShell Scripting

**PROFESSIONAL EXPERIENCE**

**Science Labs LLC**, Location August 2018- Present

***IT Infrastructure Analyst (2019 – Present)***

* Served as the lead and final escalation point for the company’s global internal IT helpdesk, responding directly to customers and other technicians needing assistance. Continued all Level II Infrastructure Technician responsibilities.
* Created and maintained all helpdesk processes and documentation including SOPs, on-call rotations, and resolutions to common issues; drove SLAs and productivity within the IT Support Team.
* Liaison between the Helpdesk Team and Infrastructure, Network, and Security Teams; acted as backup to each team.
* One of two technicians primarily responsible for security incident response and assisted in the mitigation of four company-wide security breaches. Acted as primary technician testing new software and configurations.
* Created new Windows 10 workstation images monthly to be deployed company-wide with proper driver and application integration and OS configuration. Managed VMWare and Citrix appliances and access.
* Assisted with patching security vulnerabilities and implementing driver and functionality updates on Windows and Linux servers and workstations company-wide using WSUS.
* Collaborated with Information Security to ensure endpoint and network security and implemented necessary changes.
* Assisted with ensuring compliance of internal helpdesk ticket queue, asset lists, Active Directory, and network and endpoint security with PCI and ISO Certifications and participated in audits.
* Assisted managing the following security applications: BitLocker Administration and Monitoring, Cisco Umbrella, Forcepoint Proxy, Okta MFA, Rapid7 Insight, Symantec Endpoint Protection, and SEPM

***Level II Infrastructure Technician (2018 – 2019)***

* Served as second tier of escalation in the company’s internal global helpdesk, responding directly to customers and other technicians needing assistance. Imaged new machines with the company image for new users.
* Responsible for security incident response and assisted in the mitigation of two company-wide security breaches.
* Created and modified accounts, devices, and mailboxes as necessary in Active Directory and Exchange.
* Provided Network Team support in providing consistent corporate network speed and reliability. Collaborated with the Information Security Team to ensure endpoint and network security on current software solutions and legacy systems.

***Science Labs continued***

* Managed the following security applications: Cisco Umbrella, Forcepoint Proxy (before replaced by Cisco Umbrella), Rapid7 Insight, Symantec Endpoint Protection, SEPM
* Worked with the Server Team to deploy software updates, both security and functionality patches, to Windows endpoints company wide. Assisted the Server Team to ensure consistent availability of services, applications, and data globally.
* Microsoft Products: Windows 7, Windows 10, Server 2012, Server 2012 R2, Server 2016, Active Directory
* BitLocker Administration and Monitoring, Exchange, Office 365, and Skype for Business
* Cisco: AnyConnect VPN, Unified Call Manager, Jabber, Umbrella, Unity, WebEx; Apple Products: iOS and MacOS

**CYBERSECURITY PROJECTS**

***Principles of Cybersecurity***

* Implemented risk management and risk assessment to manage, prioritize, and reduce risks for organizations.
* Researched and examined numerous advanced persistent threat (APT) groups and their anatomy.
* Designed and performed IT system security evaluations, reviews, and assessments.
* Developed policies and procedures to ensure confidentiality, integrity, and availability of IT systems.
* Studied and performed different forms of social engineering to learn mitigation techniques.
* Performed cybercrime investigations to identify and eliminate threats.
* Conducted reconnaissance on targets to identify assets, collect human intelligence, and assess vulnerabilities.

***Network Technologies and Network Security***

* Used command-line tools (ping, ipconfig, ifconfig, netstat, tracert, arp) to troubleshoot and analyze system connectivity issues and to identify the security posture of a network.
* Learned about, implemented, and configured protocols (SRTP, FTP, SFTP, FTPS, SSH, TLS, IPsec, SMTP, POP3, IMAP4, HTTP(S), Kerberos, LDAP, NTP, DHCP, RDP) to support different use cases.
* Studied, Installed, and configured switches, routers, and firewalls to create a secure and efficient network.
* Understood and utilized different security zones (DMZ, intranet, extranet) and network separation (airgaps,

VLANs, proxy servers) to construct secure networks.

* Installed and configured IDSs/IPSs (Snort) to monitor networks in order to detect and analysis potential attacks.
* Studied and implemented wireless cryptographic protocols (WPA, WPA2 in PSK and Enterprise modes, TKIP, CCMP) to discover vulnerabilities, which led to understanding how to design secure wireless networks to thwart wireless attacks.

***Cyber Operations***

* Performed XXS attacks to redirect targets and grab cookies, SQLi attacks to exfiltrate usernames and password hashes.
* Carried out buffer overflows to create new user accounts and change login session owners.
* Used TELNET and Metasploit to obtain remote access on Metasploitable VMs.
* Implemented rapid triage to identify and categorize issues into four priority levels: low, medium, high, and critical.
* Employed the concept of order of volatility to preserve forensic data.

***Steganography and Data Hiding***

* Concealed and extracted payloads from images with LSB steganography Hid and extracted payloads in WAV files.
* Employed cyber forensic software to view anomalies between virgin and modified images.
* Applied forensic hashing concepts to create a list of known file filters (KFFs) to identify and isolate suspicious files.
* Employed Python to extract and analyze metadata to reveal malicious payloads in MP3 files.
* Created a TCP/IP covert channel to send a concealed message.

***Malware Analysis***

* Created a malware analysis network using a Zero Wine Tryouts VM connected to Windows 8 VM. Employed a sandbox (Sandboxie) and a sandbox analyzer (BSA) to examine changes that malware made to the OS in a VM environment.
* Set up and employed an INETSIM VM to simulate the Internet in a controlled environment for malware network communication analysis.
* Employed static malware analysis tools (PEid, PEview, and Resource Hunter) to examine malware packers, DDLs, Windows functions, and resource sections.