John Poblete

+30 6971846510 | jpoblete@vnoproject.com | github.com/0xscorpio | linkedin.com/in/0xscorpio

Northeastern University, D'Amore-McKim School of Business Boston, MA

Bachelor of Science Degree in Business Administration May 2019

Major: Management Information Systems / Minor: Computer Science

Languages: English, Greek and Filipino. Limited working proficiency in French.

Certifications: AZ-900, Qualys VM, CEH, PJPT, arcX FTIA

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst | Accenture (Greece) Feb '21 – Present

- Ran internal AD exploitation penetration tests to remediate basic weaknesses and improve AD security baselines (SMB relay, LLMNR poisoning, WSDigest, Kerberoasting, NTLMv2, password policies, account tiering, LAPS, LNK file attacks, IPv6 MitM, DCSync attack).
- Conducted monthly vulnerability scans (Nessus) and tracked them (Azure DevOps) for scheduled patch management and reporting.
- Utilized threat intelligence platforms (SOCRadar, MISP) to search for leaked employee credentials & set up threat hunting queries (Defender XDR) to search for common enumeration tactics, suspicious events/anomalies and analysis of current security baselines.
- Wrote security hardening scripts for servers (SUSE, RHEL, Ubuntu, Windows) via TLS/SMB/GPO using PowerShell, Bash & Python.
- Analyzed system logs (Event Viewer, QRadar), network traffic data and endpoint protection client logs (CheckPoint) for incidents.
- Participated in the design and implementation of secure network/server architectures (DMZ, WAF) and business processes (SAP).
- Configured and set up entire two-tier PKI infrastructure on test environments with security baselines along CA clustering and load balancing (AIA/CRL, NDES, OCSP, SCEP, SSL/TLS certificates, SAN, iSCSI) as well as issued custom TLS certificates (OpenSSL).
- Configured HSMs and utilized Azure Key Vault for efficient storage of cryptographic keys & secrets.
- Managed Azure VMs, Defender for incidents & Purview for adherence to security regulations/frameworks (ISO-27001, NIST 800-53).
- Configured Azure RBAC rules, Conditional Access policies, MFA & PIM to control user authorization on various cloud applications.
- Ran phishing campaigns to test employee security awareness & support the building of user security-awareness training programs.
- Documented technical processes, training wikis and security best practices (GitHub, Jira, SharePoint, Confluence).
- Participated in various security training bootcamps within Accenture (CISSP, CCSP, GSEC, CEHv12, Security+).

DevOps Support Specialist | Cogo Labs (Cambridge, MA) Sept '19 – July '20

- Supported and maintained in-house email sending infrastructure to ensure deliverability for 6 incubating companies.
- Maintained Linux (CentOS, RHEL, Ubuntu) servers via network configurations such as proxies, SSH whitelisting, NAT dressing, cron jobs, network interface troubleshooting and set proper permissions for different user/admin groups.
- Purchased and managed domains by configuring proper A records, PTRs, DKIM generations, SPF set ups and DMARC policies and ensuring WHOIS information for each domain was compliant to FTC standards (CAN-SPAM act).
- Wrote automation scripts (Python, Bash) for DNS setups, database APIs and Kubernetes environments for in-house programs.

Systems Administrator | Anaqua (Boston, MA) July '18 – Dec '18

- Wrote scripts (PowerShell) to automate new-hire onboarding, termination tickets and general admin tasks on AD.
- Liaise with both on-site & remote clients (NA, EMEA, APAC regions) to resolve networking issues, server troubleshooting, NAS deployments and server room rack management while adhering to security best practices (ISO-27001).

IT Support Technician | Harvard Law School (Cambridge, MA) July '17 – Dec '17

- Triaged and resolved tickets in categories such as asset management and deployment, software upgrades, network issues, technical consulting, laptop imaging, OS migrations, hard drive decommissions (DBAN, Degauss) and desktop builds.
- Utilized Splunk to monitor for network security intrusions, track IPs and resolve for HLS user-associated hostnames.