Ebube Nnaemeka

Junior Systems Administrator | IT Administrator | SOC Analyst
Toronto, ON, Canada | nnaemekaelyon17@gmail.com | ebube-nnaemeka.pages.dev | github.com/EbubeNnaemeka

SUMMARY

Entry-level IT and cybersecurity candidate targeting Junior Systems Administrator, IT Administrator and Security Operations Center (SOC) Analyst roles. Built a public homelab portfolio of 8 projects covering Windows Server and Active Directory administration, PowerShell and Ansible automation, Zabbix infrastructure monitoring, vulnerability management, and Security Information and Event Management (SIEM) detection engineering in Splunk mapped to MITRE ATT&CK. Advanced Diploma in Accounting from Seneca Polytechnic adds a business and finance perspective. Strong troubleshooting, documentation and communication skills.

SKILLS

Systems Administration: Windows Server 2022, Active Directory (AD DS), Group Policy (GPO), DNS, DHCP, user account management, identity and access management (IAM), role-based access control, least privilege, patch management, Windows 10/11, Linux (Ubuntu, Kali Linux)

Security Operations: SIEM, Splunk, SPL, log analysis, threat detection, alert triage, incident response runbooks, Windows Event Logs, Sysmon, Security Onion, Zeek, Suricata, intrusion detection system (IDS), network security monitoring, malware analysis, indicators of compromise (IOC), MITRE ATT&CK, Atomic Red Team

Vulnerability Management: vulnerability scanning, OpenVAS/GVM, Nessus Essentials, Nmap, CVSS scoring, risk prioritization, remediation reporting

Scripting and Automation: PowerShell, Ansible, Bash, Git, GitHub, Docker

Monitoring: Zabbix, infrastructure monitoring, service availability alerting, performance thresholds

Networking and Virtualization: TCP/IP, subnetting, ports and protocols, host firewall rules, network segmentation, Proxmox VE, VMware

PROJECTS

Homelab Portfolio (Independent Projects) | *github.com/EbubeNnaemeka* Sep 2026 – Present

Active Directory Enterprise Lab | *Windows Server 2022, AD DS, Group Policy, PowerShell*

- Designed a two-domain-controller Windows Server 2022 forest with AD-integrated DNS and DHCP for redundancy, modelled on a mid-size company with 5 departmental organizational units (OUs) and delegated admin rights.
- Wrote PowerShell scripts to provision 500+ user accounts from CSV and configured Group Policy for password and account lockout baselines, departmental drive mappings and software restriction.

SIEM Detection Engineering Lab | *Splunk, SPL, Sysmon, Windows Event Logs*

- Authored 3 Splunk SPL detections for brute force (T1110), PsExec lateral movement (T1021.002) and encoded PowerShell (T1059.001) using Windows Event IDs 4625, 4688 and 7045 plus Sysmon telemetry.
- Documented false-positive sources and a triage step for each detection; configured Sysmon and the Splunk Universal Forwarder.

Purple Team Lab: Attack Simulation and Detection Validation | *Atomic Red Team, MITRE ATT&CK, Splunk*

- Planned attack simulations with Atomic Red Team for Kerberoasting (T1558.003), LSASS credential dumping (T1003.001) and encoded PowerShell to validate SIEM detection coverage against the Active Directory lab.
- Authored a new Kerberoasting detection to close a coverage gap, with an attack log of commands, expected telemetry and results.

Vulnerability Assessment Lab | *OpenVAS, Nessus, Kali Linux, DVWA, Docker*

- Built a vulnerability management workflow against intentionally vulnerable targets: OpenVAS scanning, manual verification and a CVSS-scored report template with prioritized remediation.

IT Automation Scripts | *PowerShell, Ansible*

- Wrote PowerShell tools for patch-compliance reporting, disabled-account audits and stale computer object cleanup (dry-run by default), plus an Ansible playbook for mixed Windows and Linux patch inventory.

Infrastructure Monitoring Lab | *Zabbix, Docker*

- Configured Zabbix in Docker to monitor domain controllers and endpoints, with triggers for AD DS, DNS and DHCP service failure, low disk space, sustained high CPU and unreachable hosts.

Network Security Monitoring and Malware Analysis | *Security Onion, Zeek, Suricata, PEStudio, Wireshark*

- Documented Security Onion network alert triage and a sandboxed malware analysis process: static and dynamic analysis, IOC extraction, ATT&CK mapping.

EDUCATION

Advanced Diploma, Accounting | Seneca Polytechnic, Toronto, ON