Kiante Nolen

Dallas, TX • me@kiantenolen.com • kiantenolen.com • linkedin.com/in/kiante-n • github.com/kl-nln

PROFESSIONAL SUMMARY

CompTIA Security+ certified cybersecurity professional with hands-on experience in Python security automation, AWS cloud security, Active Directory IAM, network forensics, and threat detection. Built 18+ production-ready security tools and completed real-world labs spanning SIEM (Splunk), EDR (Wazuh), network packet analysis (Wireshark), and Active Directory lifecycle management. Developed a Python-based AD IAM auditor that connects live to Active Directory via LDAPS and generates professional PDF/HTML audit reports. Operates a multi-OS homelab (Kali, Parrot OS, Ubuntu, Windows Server 2025) for continuous offensive and defensive security practice. Certified in Google AI Essentials and Google Prompting Essentials with practical experience using AI tools for security automation, workflow optimization, and technical documentation. Pursuing AWS Certified Cloud Practitioner with a long-term focus on Cloud Security Engineering and AI Security.

CERTIFICATIONS & TRAINING

- CompTIA Security+ (SY0-701) — Passed (April 2026)
- Google AI Essentials — Completed (April 2026)
- Google Prompting Essentials — Completed (April 2026)
- AWS Certified Cloud Practitioner — In Progress (Target: August 2026)
- TryHackMe Pre-Security Path — Completed
- TryHackMe Cyber Security Path — In Progress (80% Complete)
- TryHackMe Active Labs: network scanning, log analysis, Linux fundamentals, threat hunting, OSINT
- Jason Dion Cybersecurity / Security+ Course — Completed
- Professor Messer Security+ Video Series — Completed
- SoloLearn Python — Beginner, Intermediate, and Developer paths completed
- CompTIA SecAI+ (CY0-001), AWS Security Specialty, AWS Solutions Architect, AWS ML Specialty — Roadmap targets

TECHNICAL SKILLS

Programming & Scripting: Python (Advanced) — boto3, ldap3, reportlab, jinja2, socket, concurrent.futures, hashlib, regex, psutil; Bash; PowerShell; HTML; CSS; Git, GitHub

AWS: EC2, S3, IAM, Cost Explorer, boto3 SDK

Cloud Security: S3 misconfiguration detection, IAM auditing, security group analysis, cloud cost monitoring

IAM & Identity: Active Directory, LDAPS, RBAC, Group Policy, JML lifecycle management, access auditing, privilege drift detection

Security Tools: Splunk (SPL queries, log ingestion, threat hunting), Wazuh (EDR, endpoint agents, alert triage), Wireshark (packet capture, display filters, malware PCAP forensics), Nmap, Nessus, MITRE ATT&CK

Cybersecurity: Threat detection, log analysis, brute-force detection, file integrity monitoring (SHA-256), IOC extraction, C2 traffic analysis, incident response, vulnerability scanning, firewall ACL configuration

Networking & Protocols: TCP/IP, DNS, DHCP, SSH, HTTP/HTTPS, Kerberos, NBNS, SAMR, MX records, port scanning, banner grabbing, OS fingerprinting, CIDR notation, Google Workspace, GoDaddy DNS

Operating Systems & Tools: Linux (Kali, Ubuntu, Parrot OS), Windows Server 2025, Windows 10/11 — administration and troubleshooting; VirtualBox, WSL2; VS Code, virtual environments, pip

AI TOOLS & SKILLS

Certifications: Google AI Essentials (April 2026), Google Prompting Essentials (April 2026)

Prompt Engineering: Iterative refinement, context management, structured output generation for technical documentation and reporting

AI-Assisted Automation: Workflow design and optimization using large language models; AI-assisted Python development and debugging

LLM Evaluation: Output quality assessment, bias identification, response accuracy evaluation

Tools: Claude, ChatGPT — used as collaborative technical tools for security automation, documentation, and code development

PROJECTS

Wireshark Network Traffic Analysis Lab | github.com/kl-nln/wireshark-lab May 2026

- Performed live network packet capture on Parrot OS (Wireshark 4.4.14), analyzing protocol hierarchy across TCP, TLS, DNS, ICMP, and ARP traffic

- Applied 7 display filters to identify port scan activity (2,012 SYN packets from Nmap), RST rejections, plaintext HTTP exposure, and DNS queries
- Conducted forensic analysis of a real-world NetSupport Manager RAT malware PCAP — independently identified all 5 victim IOCs (IP, MAC, hostname, username, full name) via NBNS, Kerberos, and SAMR protocol analysis before checking answers
- Produced a professional SOC-style incident report documenting C2 beaconing traffic to 45.131.214.85 over TCP 443, attack timeline, and remediation recommendations

Active Directory IAM Lab | github.com/kl-nln/active-directory-iam-lab 2026

- Deployed Windows Server 2025 Domain Controller in VirtualBox, configured AD DS, and built domain corp.local with 4 OUs (IT, HR, Finance, Terminated) and 3 RBAC security groups
- Provisioned 10 users via PowerShell bulk script and executed full JML lifecycle: Joiner provisioning, Mover access transfer with old access revoked, Leaver account disabled and moved to Terminated OU
- Ran PowerShell access audit identifying 2 critical findings: cross-department privilege drift (Bob Harris in Finance group, David Kim in IT Admins) — documented with severity ratings and remediation steps

AD IAM Auditor — Python Security Tool | github.com/kl-nln/ad-iam-auditor 2026

- Built a modular 4-file Python tool that connects live to Active Directory via LDAPS (port 636) and runs 4 automated IAM security checks: cross-department memberships, disabled accounts in active OUs, accounts with no group memberships, and inactive accounts (90+ day threshold)
- Resolved 7 distinct technical challenges including LDAP signing enforcement, LDAPS certificate binding to NTDS registry store, and Python 3.14 MD4 removal breaking NTLM auth (fixed via pycryptodome)
- Generates timestamped professional PDF and HTML audit reports via reportlab and jinja2; architecture separates audit logic from report generation for extensibility
- Scanned 14 users against corp.local — identified 2 cross-department violations (Critical/High) and 10 inactive accounts

Python Security Automation Portfolio | github.com/kl-nln/python-automation-labs 2025 – Present

- 18 production-ready security automation tools spanning cloud security, threat detection, and network reconnaissance

AWS Cloud Security Suite

- S3 security auditor with risk scoring (CRITICAL/HIGH/MEDIUM/LOW) — detects misconfigurations behind the Capital One breach ($190M settlement)
- IAM permission analyzer flagging missing MFA, excessive admin access, and unused credentials
- EC2 inventory tool with public IP exposure, default security group, and missing SSH key detection
- Cost monitoring system with trend analysis and month-end forecasting

Network Reconnaissance Tools

- Concurrent TCP port scanner (100 threads) — 1,000 ports in 10 seconds (100x speedup vs sequential)
- Service detection via banner grabbing and OS fingerprinting
- Ping sweep with CIDR notation for network discovery and asset mapping
- Unified scanner combining host discovery, port scanning, and service enumeration

Cybersecurity Automation

- Brute-force detector with 3-layer detection: velocity attacks, distributed IPs, account enumeration
- Real-time file integrity monitoring using SHA-256 cryptographic hashing
- Authentication log parser with regex-based threat correlation
- Multi-format security reporter (CSV, Markdown, JSON)

Technologies: Python, boto3, AWS (EC2, S3, IAM, Cost Explorer), concurrent.futures, socket, regex, psutil, cryptographic hashing, Git

HOMELAB

- Splunk SIEM Lab: Deployed Splunk, ingested endpoint and authentication logs, performed threat hunting with SPL queries — identified failed login patterns, off-hours auth, and privilege escalation attempts; documented findings in incident report format
- Wazuh EDR Lab: Deployed Wazuh across a multi-OS homelab environment (Parrot OS and Windows), configured endpoint agents, triggered and analyzed security alerts including failed logins and file integrity changes
- Virtualized Attack/Defense Lab: VirtualBox running Kali Linux (attacker), Parrot OS, Ubuntu (analyst), and Windows (victim) for penetration testing and log analysis
- Firewall & Log Analysis Practice: Hands-on Security+ PBQ scenarios including ACL configuration and threat indicator identification

EXPERIENCE

IT & Administrative Systems Specialist | International Harvest Fellowship Ministries Aug 2017 – Present

- Serve as sole IT resource — manage, maintain, and troubleshoot all networked PCs, AV equipment, and PA systems
- Configure and administer Google Workspace accounts, user permissions, and domain settings for all staff

- Perform routine hardware maintenance and software updates to ensure uptime during weekly services
- Oversee audio engineering and signal chain configurations for all live services

Freelance Web Developer & Digital Systems Consultant | Independent — Arkansas & DFW Area Jul 2017 – Present

- Design, build, and maintain websites and digital infrastructure for small business clients
- Resolved critical Google Workspace misconfiguration for a logistics client: identified root cause, corrected MX records — restoring full email functionality
- Advise clients on domain management, DNS configuration, email deliverability, and cloud service selection

Remote IT & Operations Coordinator | Thrive Behavioral Health Services 2020 – Present

- Managed scheduling, client documentation, and records handling in a HIPAA-adjacent setting with strict attention to data privacy and access control
- Coordinated communication across clinical and administrative staff to maintain accurate and timely records
- Maintained digital workflows and provided technical support to ensure operational continuity for a remote-first team

Pharmacy Technician / Machine Operator | All Care Pharmacy Mar 2016 – Jul 2017

- Selected as sole daily operator of the Omnicell M5000 (beta unit — one of five in existence), trained directly by Omnicell systems engineers
- Collaborated with Omnicell engineering team to identify and resolve OS-level bugs during live beta deployment
- Flown to NJ to evaluate Synmed Multimed machine pre-purchase; became first tech trained and lead operator
- Processed high-volume cycle-fill medication orders for nursing home patients with zero-error tolerance

EDUCATION

Computer Science / Engineering — Completed 1.5 Years | University of Arkansas Aug 2011 – Jan 2013

High School Diploma — 3.0 GPA | Malvern High School May 2011