Vasty Kervens Guivaldo Desir

dkervensguivaldo@gmail.com 845-364-1303 United States LinkedIn Portfolio

Core Skills

Offensive Security

Internal & **External** Network, **Web App Testing**, **Kali Linux**, **Metasploit**, Burp Suite, **BloodHound**, **NetExec**, **Impacket**, Nmap, **Nessus**, Gobuster, Enum4linux

Adversary Simulation, Privilege Escalation, Lateral Movement, Pivoting, Domain Dominance, **GOADv2**, **MITRE ATT&CK TTPs**, C2 Frameworks (**Cobalt Strike**, Sliver)

Defensive Security

Threat Hunting, Alert Triage, **Log Analysis**, **Incident Response**, Malware Analysis, Threat Intelligence, IOCs, **Splunk**, **Elasticsearch(ELK)**, **Microsoft Sentinel**, **Defender XDR**, Wazuh, **Zeek**, **Volatility**, **FTK** Imager, **Microsoft Defender XDR**, **Sentinel SIEM**

Azure/Entra ID, Authentication, **Zero Trust**, External ID, Azure VM, Intune, MDM

Networking & System

TCP/IP, **VLANs**, **Subnetting**, **Routing & Switching** (OSPF, BGP basics), STP, EtherChannel, DHCP, **DNS**, NAT, **ACL**, **VOIP**, **Firewall management**, Web filtering, **IPS/IDS**, VPN (WireGuard / OpenVPN), **Network segmentation**

Active Directory administration

Basic **Linux server** administration

Virtualization

Proxmox, Hyper-V, VMware

Professional Experience

Chestnut Ridge 06/2025 – Present | USA

IT Contractor

- Deployed and configured Grandstream VoIP desk phones across 6+ sites, coordinating cabling, SIP trunk provisioning, and dial plan configuration for end-to-end telephony rollout
- Installed and configured new network equipment and workstations at multiple sites performed cabling, switch configuration, VLAN setup, and end-user onboarding

Farmatrix S.A 11/2023 – 01/2024 | Haiti

Sr. IT Support Engineer

- Managed enterprise network infrastructure supporting 70+ users maintained Windows and Linux servers, enforced firewall policies, and configured VLAN segmentation for network security
- Deployed and maintained Hyper-V virtualization infrastructure for 10+ remote workers, reducing hardware costs and improving availability
- Configured WireGuard VPN for secure remote access applied firewall rules and network segmentation to reduce attack surface
- Delivered security awareness training to 70+ staff on phishing, social engineering, and password hygiene implemented internal security policies reducing incident reports

Papillon Technique 10/2018 – 11/2023 | Haiti

Helpdesk Support Technician

- Installed and configured Windows systems and network equipments

- Performed hardware/software troubleshooting on laptops, desktops, and peripherals for 80+ clients (remote and on-site)
- Managed onboarding documentation and first-line ticket resolution maintained high client satisfaction through systematic issue tracking

Projects & Home Lab

Enterprise Security Home Lab 2022 – Present

- Conducted full Red Team exercises on GOADv2 lab environment covering initial access, privilege escalation, lateral movement, pivoting, and domain dominance simulating real-world APT tradecraft aligned to **MITRE ATT&CK** framework
- Designed and deployed a **multi-VLAN** enterprise-grade network using Cisco 2900 routers, Catalyst 2960/3750 switches, MikroTik routers, Zyxel switches, FortiGate and WatchGuard firewalls configured VLAN segmentation, **inter-VLAN** routing, trunking, HSRP failover, STP, and EtherChannel (LACP)
- Built a dedicated **SOC & DFIR** lab on **Proxmox** deploying Splunk, **Elasticsearch (ELK Stack),** Wazuh, Zeek, **Volatility3**, and **FTK** Imager performed alert triage, log analysis, malware investigation, and **threat hunting** workflows
- Deployed and administered Active Directory on Windows Server 2019/2022/2025 configured Users, Groups, GPOs, DNS, DHCP, and practiced AD attack paths including **Kerberoasting**, **Pass-the-Hash**, **Pass-the-Ticket**, and **DCSync** using **Impacket** and **BloodHound**
- Deploying lab in the cloud setting up **Microsoft Sentinel** and **Defender XDR** for cloud-native **SIEM/SOAR** practice built detection rules, alert playbooks, and incident response workflows mapped to **MITRE ATT&CK TTPs** Using **KQL**
- Configured VoIP system using Grandstream desk phones with Cisco routing infrastructure across multiple simulated sites
- Documented network topology, IP addressing schemes, VLAN assignments, and security configurations

Certifications

- Microsoft Certified Identity and Access Management (SC-300)... In progress
- Cisco Certified Network Associate (CCNA)
- Fortinet Certified Associate (FCA)
- Certified Defensive Security Analyst (CDSA)
- Microsoft Certified Security, Compliance and Identity Fundamentals (SC-900)
- Junior Penetration Tester (PT1)
- Certified Red Team Operator (CRTO)
- Certified Red Team Professional (CRTP)
- Practical Network Penetration Tester (PNPT)
- Certified Red Team Analyst (CRTA)
- eLearnSecurity Junior Penetration Tester v2 (eJPTv2)

Professional Development

- Continuous learning on platforms such as **OffSec**, **HackTheBox**, **TryHackMe**, **CyberDefenders**, **CyberWarfare** Labs and personal homelab
- Actively monitoring threat intelligence feeds, **CVE** disclosures, and **MITRE ATT&CK** updates to stay current on adversary **TTPs**, detection gaps, and emerging attack techniques