WYLIE BAYES

Email: me@wyliebayes.com **Phone: 719-680-0913**

QUALIFICATIONS

Accomplished, talented Network/Systems/Security Engineer with experience in the corporate market and in the Government, U.S. Navy onboard two naval warships, U.S. Air Force global AFNET deployments, and Missile Defense Agency operations. Dynamic Leader with excellent communication skills, easily interacts with executives, senior, and junior-level staff. Received two Navy Achievement Medals, and two Flag Letters of Accommodation for network management resulting in increased network performance and user efficiency during a single activity duty enlistment. Received the Atlas Technologies Sextant award for outstanding technical achievements. Technically proficient with Cisco routers / switches, Alcatel-lucent switches, and knowledgeable of many operating systems and numerous software and security applications. **Proficient in both Powershell and Shell scripting**. **Top Secret Active Security Clearance**. **Discovered Hyper-V host route hijack method, and new ways to abuse Tenable Nessus vulnerability scanning products.**

TECHNICAL SKILLS

Software Applications: Office 2016, Notepad++, VIM, MySQL, MSSQL, MariaDB, Ghost platform, Wordpress, Node.JS, Apache, Nginx, vSphere, Sysinternals, Git, Jira, Confluence, Keycloak.
Operating Systems: Windows 2003/XP, 2008/R2/Win7, Windows 8/2012 Server, Windows 10/2016 Server, **Kali Rolling**, Linux (Debian/**Redhat** based), FreeBSD, and **OpenBSD**.
Networking: LAN, WAN, POP, SMTP, DHCP, **TCP/IP**, WINS, DNS, LDAP, Samba, L2/L3, **OSPF,** 802.1q, 802.1s, 802.1w, 802.1x, 802.11a/b/g/n/ac, and VPN.
Security: Snort, Wireshark, Nmap, Tcpdump, Tenable Nessus / Security Center, Arcsight ESM/Logger, Netscout, FireEye, McAfee NSM/EPO, Barracuda, Bluecoat, BurpSuite, Metasploit Framework, Gobuster, Nikto, Alienvault OTX, MISP, Twistlock, Anchore, and OSCAP.
Programming Languages: Experience in PHP, XML, **Powershell**, C, and **Shell** Scripting.
Virtualization: VMware Workstation/ESX/ESXi/vCenter 4x, 5x, and 6x. Microsoft Hyper-V, and Redhat Openshift/Kubernetes.

PROFESSIONAL EXPERIENCE

Penetration Tester/Red Team Senior Associate (Dark Wolf Solutions LLC. (May 2018-Present)

- DoD Platform One Red Team Anchor
- Manages and assists with all Red Team operations within the DoD Platform One IL2/IL4/IL5 and classified cloud environments.
- Assists in performing penetration tests for other commercial and government clients.

Senior IT Cyber Range Infrastructure SME (Boecore/US Air Force 50th SCS), (May 2018-Present, Part time)

- Designs, engineers, implements, and maintains virtualized environment in support of Defensive Cyber Operations (DCO) training and exercise requirements.
- Installs and configures software to support DCO training environment to included, but not limited to: Elastic search (ELK), Logstash (ELK), Kibana (ELK), Snort, Bro, McAfee ePO, Tenable Security Center/Nessus, Sysmon, Elastic Beats, Linux, Windows, OpenBSD, VMWare ESXi 6.5 + vCenter, and Cisco iOS.

- Configures event log/syslog ingestion and parsing from all assets to feed Logstash/SIEM(ELK)
- Develops lab scenarios to support DCO Fundamentals, Detect, Protect, Respond, and Crew Commander Course delivery.
- Implements offensive / red team style compromises in support of threat hunting activities.
- Implements CTF style Capstone challenges to support all DCO training classes.
- Implements automation wherever possible with Powershell/PowerCLI and shell scripting for efficiency.
- Assists with the development of course content to correspond with lab activities.
- Ensures classes and labs are designed with DoD 6510 framework in mind.

Network Security Analyst III (ERC/Missile Defense Agency Tier II CSSP), (Nov 2017-May 2018) (Lateral Move)

- Provides DCO coverage for MDA's 4 principle, 10 major and 139 remote sites consisting of 266 network enclaves and 14,000 users to protect and defend MDA from state and non-state cyber threat actors
- Conducts attack sensing and warning and continuous monitoring activities by analyzing cybersecurity event logs from defensive sensors, network infrastructure and mission critical server devices for cyber-attack patterns and indicators of compromise.
- Develops and disseminates DCO alerts and notifications to inform MDA Tier 3 organizations and provide direction to implement countermeasures to protect against cyber threat activity.
- Reviews data originating from or reflecting status of ongoing intrusions or cyber security incidents and documents the findings according to established procedures.
- Reviews and assesses the enterprise cyber-threat environment and disseminates guidance to improve network defensive posture.
- Responds to cyber security incidents by reporting all pertinent details utilizing internal and external data management systems.
- Supports digital forensic investigations by collecting and safeguarding potential evidence, preserving chain of custody, providing inputs/data to reports and/or investigation lead.
- Supports the development, establishment, review and update of CND procedures processes, manuals, and other (CERT) documentation.
- Develops custom PowerShell solutions for OSINT integration from threat feed APIs into MDA's SIEM environment.
- Builds custom PowerShell solutions for endpoint data collection to support investigations.
- Pivotal team member in the MDA Tier 2 CSSP-CERT winning the 2017 MDA Cybersecurity Team of the Year Award

Cyber Security Engineer III (CSRA), (Oct 2017-Nov 2017) (Lateral Move)

- Cyber security engineer for Missile Defense Agency security information and event management (SIEM), endpoint protection platform (EPP), and vulnerability and compliance scanning systems(VCS).
- Engineers and maintains SIEM suite infrastructure ensuring event management for all priority systems within the agency.
- Creates custom automation solutions in multiple scripting languages for integration of different system components.
- Provides subject matter expert backend support and troubleshooting for CERT engineers and analysts on all cybersecurity products within the MDA.
- Provides design input and support of new products coming into the environment allowing for expedited integration into all cybersecurity applications.
- Architects security solutions for integration of remote networks to include SIEM, EPP, and scanning solutions.

- Integral engineer for event monitoring solution that identifies issues proactively rather than reactively.

Cloud Operations Engineer III (CSRA), (June 2017-Oct 2017)(Lateral Move)

- Manages large virtual environment on both unclassified and classified networks consisting of VMware vSphere 6x, EMC Vmax Storage, and HP C7000 (G9) infrastructure.
- Provides scripting design and support to automate tasks within the environment with Powershell/PowerCLI and shell scripting on unix like appliances.
- Completes design reviews, impact assessments, environment updates, associated with changes/updates as well as project implementation activities that impact the Cloud and other Virtual Environments (VE).
- Overseas VE baseline configuration with respect to product upgrades and standardization of release methodology.
- Conducts deep-dive analysis on systemic issues; supporting the problem manager in follow-up and proactive activities to prevent service interruptions and improve VE stability.
- Troubleshoots outages and performs break/fix as needed.
- Conducts research into problematic deployment stoppages.
- Creates and improves procedures and other duties as assigned.

Virtualization Engineer III (Agile Defense Inc), (Oct 2015-June 2017)

- Administers and maintains 8 VMware vCenters and corresponding NetApp storage resources.
- Daily tasks include reviewing syslog and SNMP messages for clustered NetApp filers, VMware vSphere 5.5, HP C7000 blade enclosures, CISCO fiber channel switches (MDS 9000 series), and CommVault backup system.
- Troubleshoots performance issues and service outages for virtual/storage/fiber channel/Ethernet infrastructure including VMware High Availability, NetApp storage aggregate/volume/qtree/LUN capacity, HP C7000 enclosure connectivity (FLEX-10), and CISCO Fiber Channel Zones and connectivity.
- Provides performance and asset reporting and automation of administrative tasks via PowerShell, PowerCLI, HPOA modules, and DataONTap modules including: virtual hardware utilization, snapshot existence, LUN ID assignment for Datastores, log shipping tasks, daily monitoring checks for all enclosure/storage controllers, vCenter host/datastore/VM alarms, and over-provisioning at Netapp and VMWare levels.
- Provisions storage, virtual hardware, and modifies fiber channel network connectivity for new systems.
- Reviews vulnerability reports, maintains patch compliance, collaborates with tenant groups for successful deployment and implementation of systems, and troubleshoots outages.
- Opens support tickets with vendors for hardware replacement. NetApp models: FAS6070, FAS6080, FAS3070, and FAS6250's. Cisco MDS model 9000 series. HP c7000 enclosures with G1, G6, G7, and G8 blades.
- Maintains Commvault backup system to include: proper tenant retention levels, new storage policies for new systems, recurring disk/aux(tape) backups, presents and increases storage where necessary on W2k8 R2 media agents, and completes tape swaps for continuation of Auxiliary copies.

Network Technician III (Atlas Technologies Inc), (June 2014-Oct 2015)

- Installs and troubleshoots Integrated Shipboard Network Systems, Automated Digital Network System (ADNS) to include SCIP-IWF (VOIP) services, CENTRIXs networks, and COMPOSE networks under SPAWAR direction.
- Experience in configuring and integrating KG-175D, E-100, and Classic TACLANES.

- Configures Cisco 2800, 3600, and 2800 series routers, Alcatel 7700/9700/6600/6850 Gig-E switches, and IBM Blade Centers.
- Integrates newly installed sub-systems into ADNS and ISNS environments.
- Implements many different switching environments such as Link Aggregate groups, inter-vlan routing, multiple spanning tree regions, and integrated networking with many different sub-systems.
- Configures networks utilizing Windows 2008 R2 servers/Exchange 2010 on multiple hardware platforms.
- Provides sustainment engineering and subject matter support for Server 2003/XP environments that still exist.
- Responsible for completion of SOVT's (Ships Operational Verification Tests)
- Responsible for configuring and testing off-ship paths of communication, as well as internal LAN communication across all paths, and all levels of redundancy.
- Re-designed San Diego office lab environment to include 21 ESX hosts in a datacenter cluster with multiple IBM blade centers (HS-21's, and HS-20's,) with Netapp FAS 270, and FAS 2020 storage, and Alcatel 9700 and 6850 switching infrastructure.
- Completed ADNS INC III SP2 installation and SOVT onboard USS Ronald Regan CVN-76.

Systems Engineer II (Lead Subject Matter Expert) (NCI Information Systems), (Sept 2012-May 2014)

- Provides engineering and design support to the Air Force ACAS (Assured Compliance Assessment Solution) program at several sites within the United States.
- Provides script/signature development, new script testing, script and system update development, system maintenance, and other engineering support as required for the AF ACAS Systems.
- Liaise with ESC and the ACAS PMOs on a regular basis.
- Creates, implements, and maintains standards for maintaining Redhat Enterprise Linux 5.x servers within the Virtual Infrastructure on both Classified and Unclassified networks.
- Helps create and maintain documentation for training and review purposes.
- Maintains all RHEL 5.x virtual servers and databases at Tier 2 West AF location to include but not limited to: Patch management, Certificate management, Script design, and network troubleshooting.
- Created custom patch management solution during Phase 1 roll-out.
- Lead Subject Matter Expert for ACAS AFIN (Air Force Information Network) Deployment.
- Deployed maintained 300+ RHEL 5.9 servers at Tier 2 (INOSC) and Tier 3 (Base Level) locations.

Network Technician II (First National Bank in Trinidad), (Mar 2012-Sept 2012)

- Responsible for user experience and system availability of end-user systems, internal security, and helps facilitate business continuity.
- Systems responsible for:
    - Virtualization Infrastructure (Emphasis on branch locations.)
    - Citrix/RDP services.
    - Active Directory Domain Controllers (Server 2003)
    - Anti-virus, WSUS, and Netwrix change reporting server.
    - BackupExec 10 server.
    - SQL 2005 database server for Lansweeper/Netwrix databases.
    - Surveillance systems (Emphasis on branch locations)
    - Debian servers providing file storage.
    - FreeNAS servers providing file storage.
    - Hardware – Servers, switches, routers, and communication equipment.
- Business Continuity **-** Develops, documents, and tests fail over of end-user services including AD, file/printer services and banking software applications.

- Research and Development – Helps to research, develop, and implement new ideas and technology to improve system performance, availability, efficiency, and continuity.
- Partially responsible for after hours and weekend availability.(On-call 24/7)

Automation Technician (XTO Energy), (Dec 2010- Nov 2011)

- Troubleshot, designed, commissioned, and maintained all control systems, electrical, hydraulic, motor controls, and communications equipment. VDF, SCADA, EFM, radios and solid state controllers. Assisted in controlling inventory of automation equipment and purchases. Worked with operation's assisting in the daily operating needs of the field. Primary functions were doing calibrations and performing plate inspection and tank and level testing.

Network Technician I (Atlas Technologies Inc), (Aug 2008-Nov 2010)

- Installed and troubleshoots Integrated Shipboard Network Systems, Automated Digital Network Systems, CENTRIXS networks, and COMPOSE networks under SPAWAR direction.
- Configured Cisco 2800, 3600, and 3800 series routers, Alcatel 7700/9700/6600/6850 Gig-E switches, and IBM Blade Center servers.
- Implemented many different switching environments such as Link Aggregate groups, multiple spanning tree regions, and integrated networking with many different sub-systems.
- Experiencing configuring and integrating KG-175 E100, and classic TACLANES.
- Configured networks on Windows 2003 server/Exchange 2003 on multiple hardware platforms.
- Responsible for one to four ships at a time.
- Networks configured: USS Wasp, USS Nassau, USS George H.W. Bush, USS Carl Vincent, USS Donald Cook, USS Hue City, USS Nitze, USS Vicksburg, USS Hurricane, USS Winston Churchill, USS Oscar Austin, USS Car, USS Makin Island, USS McFaul, USS Barry, USS Cole, USS Ashland, USS Mitcher, USS Anzio, USS Mahan, USS Monterey, USS Kearsarge, USS George Washington, USS Gettysburg.
- Responsible for completion of SOVT's (Ships Operational Verification Tests.)
- Responsible for configuring and testing off-ship paths of communication, as well as internal LAN communication across all paths, and all levels of redundancy.

U.S. NAVY, Norfolk, Virginia 2004 – 2008

Network Administrator/Information Systems Security Officer (USS PONCE LPD – 15), (Mar 2005-Aug 2008)

- Managed the Classified and Unclassified networks, 4 Intranet sites, and their operations providing guidance to both senior and junior-level personnel.
- Consulted with executive personnel regarding equipment, and application statuses.
- Configured and maintained 6 Fast Ethernet Alcatel switch stacks, 8 Windows 2000 Servers, 7 Windows 2003 Servers, 2 Linux servers, 1 HP-UX server, and 1 OpenBSD server.
- Lead the effort to ensure security compliance meets Navy standards.
- Maintained network resources, ensuring that it efficiently meets the needs of the user groups.
- Served as Lead Network Administrator with supervisory responsibility of 5 staff members including training them regarding network administration techniques.
- Implemented network security policies resulting in increased customer satisfaction.

Network Administrator (USS SAIPAN LHA-2), (Aug 2004-Mar 2005)

- Responsible for the supervision of ten junior–level personnel in the naval division, provide network administration training and implementation of new initiatives to meet goals and objectives; write evaluation reports.

- Managed ADP help desk services such as trouble tickets, routing calls, and face-to-face customer service interaction.
- Responsible for equipment updates for any type of network failure, maintenance or upgrades.
- Created USS Saipan command intranet website; configured and maintained 17 Alcatel gigE switch stacks, 6 Windows NT servers, 4 Windows 2000 servers, 4 HP-UX servers, and 2 Linux servers.
- Maintained database of user accounts and agreement forms in addition to equipment inventory.
- Prepared and documented five System Operating Procedure Manuals.

EDUCATION & TRAINING

C|eH v9 (Certified Ethical Hacker) 312-50 CERTIFIED ***February 11th 2021 – Certification# ECC52461577905***	Currently Pro Hacker on https://hackthebox.eu (Username: wyliebsd)
CASP (CompTIA Advanced Security Practitioner) CAS-002 CERTIFIED ***November 4th 2023 – Candidate ID# COMP001020485273***	DISA CND Analyst 301 ***February 1st 2018 - DISA CND Training***
SECURITY+ SY0-301 CERTIFIED ***November 4th 2023 – Candidate ID# COMP001020485273***	DISA ASSURED COMPLIANCE ASSESMENT SOLUTION. ***November 11th 2017 - DISA ACAS Training***
CySA+ (Cybersecurity Analyst) CS0-001 CERTIFIED ***November 4th 2023 – Candidate ID# COMP001020485273***	DISA HBSS Admin(201)/Advanced(301)/Analyst(501 Training. ***November 14th 2017 - DISA HBSS Training***
Pentest+ PT0-001 CERTIFIED ***Julyr 22nd 2023 – Candidate ID# COMP001020485273***	U.S. NAVY (2735 NEC). ***Journeyman Networking Core – Systems Administration Course,*** 2007
SecurityOnioin 2019 Conference Speaker https://wyliebayes.com/building-a-detection-lab-with-security-onion/	WESTWOOD COLLEGE ONLINE. ***Bachelors of Science – Computer Network Management,*** 2008 – 2011
DISA CND Analyst 101 ***January 26th 2018 - DISA CND Training***	HOEHNE HIGH SCHOOL ***Diploma – 2004***