# John Ellwood Saurbaugh

703-634-3576 / ellwood@thesaurbs.com


**Information Security / Cybersecurity Engineer**

Active Top Secret/SCI cleared senior IT engineer with over 15 years of professional and personal experience in systems security engineering, vulnerability assessments, penetration testing, network deployment, and administration of physical and virtual environments.

Key skill set:

- Type 1 and Type 2 hypervisors (VMware / Hyper-V)
- Linux / Windows
- Scripting (Bash / Powershell / Python)
- Recon and exploitation techniques
- Wireshark, nmap, MetaSploit
- Vulnerability assessment / NIST auditing

## Education, Training and Certifications

**Master of Science in Cyber Security and Information Assurance** Mar 2015
Specialization in Ethical Hacking & Pen Testing

**Bachelor of Science degree in Information Systems Security** May 2011

Recent Training:

- SANS SEC617 Wireless Penetration Testing course (Sept 2020)
- Offensive Security's Cracking the Perimeter (CTP) (Offensive Security Certified Expert) (Jan 2021)

Certifications:

- GIAC GPEN, GWAPT, GXPN
- ISC$^2$ Certified Information Systems Security Professional (CISSP)
- EC-Council Certified Ethical Hacker (CEH)
- CompTIA Network+, Security+, Server+
- Security University: Qualified Security Assessor (Q/SA) Qualified Penetration Tester (Q/PTL)
- Other certs related to System Administration / Network Administration
- Offensive Security OSCP, OSCE

## Experience

**Penetration Tester** July 2018 – Present
*Department of Energy*, Enterprise Assessments

- Leads and participates in external and internal penetration testing assessments.
- Creates reports based on technical and programmatic observations of sites throughout the DoE agency.
- Discovers new vulnerabilities and submits for CVE listing.

**Security Assessor** April 2015 – July 2018
*Internal Revenue Service*, FISMA Compliance

- Leads FISMA audits for IRS Computer systems and programs.
- Evaluates local policies, procedures and security controls.
- Develops System Security Plans with stakeholders, updates documentation as required for compliance.
- Documents results of security controls assessment (SCA) activities in Security Assessment Reports.
- Advises on security best practices, research current threats and trends, and relay information as required.
- Analyzes network, webapp, and database vulnerability assessment reports, and source code scan reports.

**Senior Integration Engineer (Dual Role)** August 2012 – April 2015
*US Navy SSCPAC*, Joint Space Operations Center (JSpOC) Mission Systems (JMS), San Diego, CA

- Created VMWare PowerCLI scripts using PowerShell, Bash, and Python for administration
- Led multi-domain integration effort using Agile Software development Scrum/Sprint process.
- Deploy and integrate web services utilizing Oracle middleware and Oracle RAC databases.
- Engineered EMC Avamar backup solution for VM-level and file level backups using EMC DD670 hardware.
- Deploy and manage VMware technologies (ESXi, vCenter, Hyperic, Horizon View) on Cisco UCS equipment.

**Senior Information Assurance Engineer (Dual Role)** August 2012 – April 2015
*US Navy SSCPAC*, JSpOC Mission Systems, San Diego, CA

- Detected and mitigated vulnerabilities and threats for JMS.
- Maintained secure posture using DoD baselines, security auditing tools, and responding to emerging vulnerabilities.
- Deployed Tenable Nessus and Security Center within enterprise environment.
- Identified security concerns to high level government representatives in a dynamic environment.
- Utilized DoD 8500 series, NIST 800 series Risk Management Framework, OWASP documentation, and best practices.
- Updated documentation as required to maintain current baselines.

**Network Security Professional** May 2010 – August 2012
*The Pentagon*, Vulnerability Assessment Branch (VAB), Arlington, VA

- Led vulnerability assessment teams in network and system level audits of connection approval and C&A missions; conforms to DoDI 8500, NIST 800-53 guidance.
- Developed new scanning techniques and procedures increasing the chance of detecting security threats.
- Ensured audits adhered to best practices outlined within DISA Security Technical Implementation Guides (STIGs), Security Readiness Review (SRRs) and DISA Gold Disk.
- Audited and accredited database servers, web servers, LDAP and AD, and workstations of Windows or Linux operating systems.
- Established IT vulnerability reporting criteria; audit reports directly briefed to senior executives on state of vulnerabilities for over 250 DoD organizations connecting to the backbone.
- Engineered Eeye Retina deployment covering 15 separate scan zones utilizing Retina Events Manager Army ITA Pentagon backbone.
- Architected upgrade and migration plan for moving branch assets from physical Windows 2003 servers to virtual Windows 2008 environment within VMware vSphere.

**Windows System Administrator** March 2008 – April 2010
*U.S. Capitol Police*, Technical Countermeasures Division, Washington, DC

- Pioneered creation and organization of IT department budget; implemented future upgrade path and life-cycle replacement plan for entire division of 75 people.
- Designed and executed $350K migration project from aging hardware and software to updated equipment using Windows 2003 server and initiated Windows 7 deployment to new machines.
- Created baselines for consistent user environment utilizing Windows Deployment server, Microsoft Deployment Toolkit, Windows Automated Installation Kit (AIK), and System Center Configuration Manager (SCCM) for post install applications.
- Excelled at non-job-related training to support the TCD mission; learned radio theory and technical countermeasures.

**Prior experience information available upon request:**

**Senior System Administrator (Tier 2)** November 2007 – January 2008
*Federal Bureau of Investigation*, Enterprise Operations Center, Washington, DC

**Special Weapons Maintenance Team Chief** December 2001 – Dec 2007
*United States Air Force*, Albuquerque, NM

**Network Systems Administrator** July 2000 – May 2001
*Saiontz, Kirk and Miles, P.A.,* Baltimore, MD