

# Resume

Arthur (Bo) Weaver  
12 Left Turn Rd.  
Blue Ridge, Ga 30513  
404-921-7663  
[bo@boweaver.com](mailto:bo@boweaver.com)  
<http://www.boweaver.com>

Systems/Network Security Engineer with over twenty years experience providing R&D, engineering and design, testing, build-out and maintenance of computer systems LAN and WAN networks in a global enterprise environment. My first systems/networking experience was in the US Navy in 1972 doing research work on ARPANET and the TCP/IP stack. At my present position I am the Senior Penetration Tester for Compliancepoint a security consulting firm which conducts PCI/DSS, HIPPA, and Sarbanes-Oxley QSA consulting services for small businesses to fortune 500 companies. In my work I preform both internal and external black box penetration testing of networks and a team leader or our Red Team of Pen Testers. I preform R&D work on the latest vulnerabilities and exploits and help with training of our younger Pen Testers. All testing results are then written in a fully detailed report for the customer.

My pen testing skills are not limited to networks and systems but I am also well skilled in physical penetration analysis and Social Engineering. I am highly skilled in finding Open Source solutions for low cost but secure and efficient networks and network services.

I have been doing network engineering, design,vulnerability and penetration testing of networks and systems for over 18 years. Also highly skill with vulnerability scanning and exploitation tools such as Nessus/OpenVAS, Qualsys, Nexpose, Metasploit, Nmap, and toolsets such as Kali Linux.

I have recently co-authored a book soon to be published by Packet Publishing called "*Kali Linux Windows Penetration Testing*". The book is written for Windows Systems Administrators who are not familiar with working with Linux and pen testing so they can do their own in house testing of their networks.

## **Objective:**

Penetration Tester, Network/Systems Security Engineer, Network/Systems Security Analyst, Information Security Engineer, Senior Systems Engineer, Systems Engineer

## **Education:**

2 years UT at Chattanooga

Blaze IT Collage  
Texas A&M online courses.

**Training/Certifications:**

MCP, MCSE (out-dated)  
A+ Network+  
Certified Smoothwall Firewall Security Engineer  
CISSP (In progress)  
DHS certification Network Assurance  
DHS certification Cyber Incident Analysis and Response  
DHS certification Cyber Ethics  
DHS certification Digital Forensics  
DHS certification Cyber Law and White Collar Crime

**Teaching:**

Visiting Security Expert ITT Tech Atlanta, GA

**Writings:**

Moderator on <http://www.point2security.com/>  
Soon to be published Co-Authored book by Packet Publishing "*Kali Linux Windows Penetration Testing*"

**Technical Skills:**

Experience in the following:

**Operating Systems:**

Linux (RedHat, CentOS, Fedora, Debian, Ubuntu, Vyatta, Kali Linux ) UNIX (Solaris 9 10 11)  
Windows Server (NT3.51 to Windows Server 2008R2)

**Firewalls and Network Security Devices:**

Vyatta, Smoothwall, Snort, OSSEC, Splunk, Zabbix, Nagios. Firebox devices, Checkpoint Firewall, Sonicwall, Juniper, Cisco ASA, IPSec VPN, L2TP, OpenVPN

**Pentesting Tools:**

Nmap, Wireshark, Etherape, Ettercap, Tcpdump, OpenVAS, Nessus, Metasploit, Kali Linux, OWASPZap, Burpsuite, SQLmap. Custom built toolsets

**Network Services:**

BIND DNS, IPSec, L2TP, LDAP, Windows AD, Windows DNS, NFS, CIFS, Postfix Mail, SendMail, Jabber, IPAM, DHCP, NAT, Load Balancing, Apache Web, Postgres DB, MysqL DB, BGP, OSPF, EIGRP, RIP, Static routing

**Server Applications:**

SSH, BIND, LAMP Stack Web Services with Load Balancing, MySQL, Postgres, Jabber Server, Postfix, Sendmail, Zabbix Distributed Network Monitoring, Java Messaging Server, Zimbra Messaging Server, OTRS Ticketing System, Telnet, Vmware, Critx, Xen Server, Terminal Server, Rsync, IPSec

**Compliance protocols:**

HIPPA, Sarbanes-Oxley Act, PCI, ISO 27001, ISO 17799/27002, ITIL

**Experience:**

Present to February 2014  
Compliancepoint  
Senior Penetration Tester

In my role at Compliancepoint I work with the Compliance Team in black box pen-testing of internal and external networks of our customers. It involves exploitation of any expose in-scope running services on the network. This involves using network vulnerability scans to footprint the victim network and compiling a plan of attack against the expose network services. Once a system is compromised sample confidential data is looted from the system as evidence of the compromised. Once testing is completed a full detailed report is written to be sent to the customer for evaluation and sent to the QSA for use in any certifications needed. Most testing is preformed for PCI/DSS certification for our customers. However a large part of testing I have done is also for HIPPA testing within the health industry. Some testing during my time at Compliancepoint has also been for companies in other high security fields which cannot be discussed due to NDA agreements.

My job duties also include in training and mentoring the younger members of the Red Team to help enhance their skill levels and training.

I also preform R&D work on new vulnerabilities and exploits to be used in further testing. This includes research on security tools, hardware, software, security related appliances and new attack vectors.

**Experience:**

February 2014 to April 2013  
Contractor (Fiserv)  
Senior Vulnerability/Compliance Engineer

On contract to Fiserv performing PCI/DSS vulnerability assessments to the networks and assets of the company and their customers.

- Research and analyzing Vulnerability Scans and collect data.
- PCI/ROC data collection, ROC interviews and data presentation
- Penetration testing of internal and external networks and reporting finding with remediation of the vulnerabilities.
- Penetration testing of web applications. Tools used Metasploit, Nikto, Webcarb, Websploit, Wpscan, OpenVAS, Wireshark, OWASPzap, Custom built tools. Expert in the use of the Kali Linux Toolkits.
- Research new vulnerabilities and attack vectors

April 2013 to March 2006  
 Astila Corporation  
 Chief of Network Security  
 Senior Systems/Network Engineer

Astila's main business model is to supply remote computing solutions to the Health care, Law and Investment industries. One of my responsibilities is to maintain compliance of our customer's networks to State and Federal regulations regarding these fields and to monitor and report and compliance issues. This involved regular scans, tests, and reports of these networks for compliance.

- Conducted pen testing on remote networks and on one time contract basis on client networks.
- In charge of research & development, design, set up and security of a Data Center in Atlanta, Ga. This includes set up, maintaining and testing of redundant power systems, redundant network routers and firewalls, with connections to several other DCs and a private VPN network to over 60 remote locations.
- Maintained Public Authoritative Root DNS servers for company and client domains. Maintained all internal DNS structure.
- Designed, built and maintained company network/systems monitoring service. This system monitors both the internal data center systems but also systems at remote locations secured through IPSec tunneling.
- Built and maintained ITIL compliant Operations/HelpDesk ticketing system.
- Maintained ,monitored and kept secure all firewalls both at the data centers and client remote locations.
- Supervised engineering staff which included but limited to project assignments, time management, training and tech support for tier 1 Technicians, project reports, monthly network reports, network security management.
- Worked directly with customers to design cost effective custom systems/network services for their needs.
- Experience with using Open Source applications and operating systems to deliver stable

and secure systems at an affordable price.

- Handled Tier 3 support tickets either sent in by the customer or escalated up by Tier 1 staff. Troubleshooting and repair of high level systems/network issues.
- Design, develop and implement information security architecture in a large global multi-geography enterprise environment
- Develop, implement, monitor and enhance data security policies, procedures and standards
- Test and evaluate new technologies that will enhance the security of the enterprise
- Partner with business units and various groups within Interface to define secure technology solutions
- Performs information security risk assessments and serves as the internal auditor for information security processes including risk identification, risk mitigation, and documentation
- Work with data owners, IT teams, compliance and legal to classify all data and maintain appropriate access restrictions
- Participate in the testing and development of the organizations disaster recovery plan on an annual basis to ensure data and information security practices are maintained
- Initiates, facilitates and promotes activities to foster information security awareness within the organization by developing and/or deploy Education and Awareness Programs
- Direct and provide hardening guidance in operating system, databases and application security
- Leads incident response team and facilitate incident management and response across all platforms and generate management reports
- Monitors advancements in information security technologies, and changes in the industry that affect information security
- Administer and maintain network security systems such as Firewalls, IDS (intrusion detection system), A/V (anti-virus) and incident management
- Leads forensic / security investigations under the direction of legal and human resource departments
- Conduct vulnerability assessments (network, server, databases, application, etc.) and drive remediation
- Define and validate system security requirements.
- Implement secure systems / standards using ISO 27001 and ISO 17799/27002
- risk assessments, provide technical security support to projects, and assist with incident investigations.
- Audit and monitor IT Security Best Practices including:
  - Firewall/Network Design
  - Anti-Virus Strategy
  - Platform Maintenance
  - Intrusion Detection Monitoring
  - System access ID

- Logon procedures and policies
- File transfer protocols
- Procedure and practices
- Identify and manage remediation efforts on vulnerabilities
- Develop Security awareness and training programs
- Provide guidance and advocacy regarding prioritization of infrastructure investments that impact security
- Develop, publish and maintain comprehensive company-wide information privacy and security strategy, plans, policy, procedures, and guidelines
- Ensure departments consider information security risks in both ongoing and planned operations
- Maintain relationships with local, state, and federal law enforcement and other related agencies
- Work with outside consultants as appropriate on required security and risk audits
- Create selection criteria for vendor products, tools and services related to information security Monitor and report on our client's risk management activities and compliance
- Demonstrated critical, independent thinking; demonstrated ability to conceive and present creative solutions.

March 2006 – February 2005

MTPros.

Atlanta, GA

Senior Systems/Network Engineer

Maintained operations and security of a Data Center in Atlanta, Ga. This includes set up of redundant network routers and firewalls.

- Maintained Authoritative Root DNS servers for company and client domains. Maintained all internal DNS structure.
- Designed, built and maintained company systems monitoring service. This system monitors both the internal data center systems but also systems at remote locations secured through IPSec tunneling.
- Built and maintained Operations/HelpDesk ticketing system.
- Maintained ,monitored and kept secure all firewalls both at the data centers and client remote locations.
- Troubleshooting and repair of systems.
- Network Administration
- Network Architecture
- Application Development

- Server Administration
- Network Security (performing network or application scans, Firewall/IDS Administration, VPN etc.)
- Application Security (development/review of secure code, performing application scans etc.)
- Server Security (system hardening, etc.)
- Strong Information Security experience with a solid knowledge of distributed, Internet and mainframe systems; distributed and web-based applications; and a knowledge of Internet-based threats and risks.
- Strong hands-on experience implementing, administering and managing security solutions
- Analytical skills
- Strong follow-up skills
- Strong documentation skills and detail-oriented
- Ability to evaluate information security controls and identification of potential risk as well as mitigating controls
- Ability to work in an independent capacity
- Strong relationship building skills and ability to interact with all levels of employees and management
- Strong research and problem solving skills
- Strong investigative skills to lead complex incidents
- Strong time management skills and the ability to work on numerous projects/activities at the same time
- Strong communication skills, both written and verbal including presentation skills in order to address small or large groups of all levels of employees or management
- Leadership skills to coordinate project tasks and activities
- Ability to communicate complex, technical concepts to business/executive management in a clear, understandable way
- Handled Tier 3 support tickets either sent in by the customer or escalated up by Tier 1 staff. Troubleshooting and repair of high level systems/network issues.

February 2005 – March 1999

Self Employed

Security Consultant, Application Development

Worked as a consultant with various businesses designing and developing business systems and applications. Also did consulting doing pen testing of businesses and business networks, forensic data inspection, analyzing network penetrations footprinting and documentation of network hacks. Reported to owners of any security issues and solutions to these issues.

- Reseller network/security products
- Audit and monitor IT Security Best Practices
- Firewall/Network Design
- Anti-Virus Strategy
- Platform Maintenance
- Intrusion Detection Monitoring
- System access ID
- Logon procedures and policies
- File transfer protocols
- Procedure and practices
- Identify and manage remediation efforts on vulnerabilities
- Develop Security awareness and training programs
- Provide guidance and advocacy regarding prioritization of infrastructure investments that impact security
- Develop, publish and maintain comprehensive company-wide information privacy and security strategy, plans, policy, procedures, and guidelines
- Ensure departments consider information security risks in both ongoing and planned operations
- Maintain relationships with local, state, and federal law enforcement and other related agencies
- Work with outside consultants as appropriate on required security and risk audits
- Create selection criteria for vendor products, tools and services related to information security
- Monitor and report on our client's risk management activities and compliance

November 1992 - March 1999

Personal time off.

March 1985 – November 1992

Culet Communications

Atlanta, GA

Systems/Network Engineer

Maintained systems and network services including email, web hosting, DNS. Troubleshooting and repair of network and computer systems.

- Perform testing of computer systems to monitor effectiveness of security.



- Analyzing information security threats, requests and audits findings, provides solutions, and audits remediation as directed.
- Works primarily within IT and occasionally with end-users to ensure understanding and adherence to established data and computer security policies.
- Assists with troubleshooting of applications or infrastructure related to security technology.
- Works with external vendors and partners as necessary to resolve incidents.

1971 – 1972

US Navy

Electronics Technician

Worked research and development on ARPA NET during school at Dam Neck VA. Work involved the development of the TCP/IP stack and LAN/WAN networked computer systems. Maintenance and repair of computer systems at base data center.