

# Arthur (Bo) Weaver

• bo@boweaver.com

## **Professional Summary**

Dynamic Offensive Cybersecurity Technical Lead with over 20 years of experience in penetration testing and cybersecurity assessments. Proficient in conducting comprehensive internal and external tests, including Wi-Fi security, phishing campaigns, and vulnerability scanning. Successfully mentored junior testers and improved client security postures by remediating critical vulnerabilities. Demonstrated expertise in PCI/DSS and HIPAA compliance testing. Committed to enhancing security measures and driving innovative solutions that align with organizational goals.

## **Work Experience**

### **01/2026-Present**

#### **Cyber Ethics and Malicious Network Activities Expert, ScaleAI**

- Conducted authorized red-team evaluations of large language model (LLM) agents to identify security vulnerabilities, jailbreaks, prompt injection risks, and unsafe behaviors.
- Designed and executed adversarial test cases aligned with industry frameworks (including OWASP Top 10 for LLM Applications) to evaluate model robustness and security controls.
- Developed and refined prompt injection, output manipulation, and social engineering test scenarios to assess AI agent resilience.
- Analyzed agent behavior, documented vulnerabilities, and produced detailed technical reports with reproducible findings and remediation recommendations.
- Evaluated authentication, authorization, data leakage, and privilege escalation behaviors in AI-powered applications and agentic workflows.
- Collaborated with AI safety teams to improve model alignment by validating security mitigations against real-world attack techniques.
- Performed structured testing using isolated Docker-based environments, Kubernetes deployments, and intentionally vulnerable applications to verify model behavior under controlled conditions.
- Authored clear technical documentation summarizing evaluation methodology, attack paths, observed behaviors, and security impact for engineering teams.
- Leveraged Python, REST APIs, Linux, Docker, and command-line tooling to automate portions of AI security assessments and evidence collection.

- Applied over two decades of offensive cybersecurity experience to evaluate emerging AI systems while maintaining strict adherence to authorized testing and responsible disclosure practices.

**04/2022 – 02/2025**

### **Offensive Cybersecurity Technical Lead, Schneider Downs**

#### **Pittsburgh PA**

- Executed advanced internal and external penetration testing for both public and private sector clients.
- Conducted Wi-Fi testing, managed phishing campaigns, and orchestrated social engineering attacks.
- Collaborated with the Blue Team on client projects to identify and validate vulnerabilities, collaborating directly with clients to remediate identified issues.
- Performed comprehensive firewall configuration reviews, addressing security gaps and misconfigurations discovered during assessments.
- Conducted reconnaissance on clients utilizing OSINT techniques.
- Conducted vulnerability scanning and assessments on client targets.
- Led internal and external penetration testing initiatives.
- Carried out Wi-Fi security assessments.
- Executed testing and audits on SCADA/OT networks.
- Engineered and deployed phishing campaigns.
- Facilitated social engineering operations.
- Mentored junior penetration testers, elevating their skills and knowledge.
- Conducted research and development on emerging exploits.
- Maintained lab network infrastructure for testing purposes.
- Conducted client meetings to review findings and recommendations comprehensively.
- Delivered training sessions on new exploits and methods of exploitation.
- Performed thorough firewall security audits, ensuring compliance and optimal security.

**08/2021 – 02/2022**

### **Security Team Lead, Lockstep Technology Group**

#### **Atlanta GA**

- Managed the security team while overseeing various related projects.
- Assigned tasks to team members, monitored their progress, and coordinated meetings to review project outcomes with both team members and clients.
- Executed internal, external, and wireless penetration testing on customer networks, along with ad-hoc testing to validate identified vulnerabilities.

- Captured forensic images from compromised systems and analyzed data to identify potential threats.
- Managed team operations and project timelines effectively.
- Developed report templates for consistency and clarity.
- Reviewed team member reports before submission to customers.
- Performed internal and external penetration testing with a focus on thorough analysis.
- Led wireless penetration testing initiatives, ensuring the security of client wireless networks.
- Conducted SCADA and OT network testing to identify vulnerabilities and risks.
- Executed rigorous vulnerability scanning and analysis across various platforms.
- Performed forensic analysis on infected systems to ascertain breach causes.
- Conducted physical security audits to evaluate on-site security measures.

**02/2014 – 07/2021**

**Senior Penetration Tester, CompliancePoint**

**Atlanta GA**

- Collaborated with the Vulnerability and Penetration Testing team to perform black box penetration testing on both internal and external customer networks.
- Exploited vulnerabilities found in in-scope running services on the target network effectively.
- Initiated the process with network vulnerability scanning to map the target network, followed by the development of a targeted attack plan based on exposed services.
- Extracted sample confidential data from compromised systems as evidence of breaches during assessments.
- Drafted comprehensive reports post-testing for customer evaluation, facilitating review by QSAs for any necessary certifications.
- Focused primarily on PCI/DSS certification testing while also conducting significant HIPAA compliance testing in the healthcare sector.
- Collaborated on projects for organizations in other high-security sectors, adhering strictly to NDA agreements.
- Took on leadership responsibilities, mentoring and training junior Red Team members to enhance their skill sets.
- Conducted extensive R&D on emerging vulnerabilities and exploits, researching new security tools to strengthen our testing capabilities.
- Performed research and analysis of scanning data for thorough assessments.
- Executed footprinting and OSINT intelligence gathering for project effectiveness.
- Executed full network stack penetration testing on internal and external networks, including routers, switches, and various operating systems.
- Maintained detailed documentation of projects and evidence for auditing purposes.
- Produced comprehensive reports for client review.

- Worked directly with customer engineering teams to address vulnerabilities effectively.
- Executed wireless hacking techniques and conducted SCADA/OT network testing.
- Performed extensive penetration testing on Android applications.

**01/2013 – 02/2014**

**Senior Vulnerability/Compliance Analyst, Fiserv**

**Atlanta GA**

- Served on contract for Fiserv conducting PCI/DSS vulnerability assessments across company and client networks.
- Researched and analyzed vulnerability scans while collecting critical data.
- Oversaw PCI/ROC data collection and conducted ROC interviews, presenting findings with recommended remediation strategies.
- Performed penetration testing on both internal and external networks, delivering detailed reports of findings and vulnerabilities.
- Executed web application penetration testing, utilizing tools such as Metasploit, Nikto, WebScarab, Websploit, Wpscan, OpenVAS, Wireshark, and OWASP ZAP.
- Demonstrated expertise in utilizing the Kali Linux toolsets effectively.
- Conducted research on new vulnerabilities and attack vectors within the industry.
- Performed both physical and network intrusion testing across the corporate campus.

**03/2006 – 02/2012**

**Chief of Security, Astila Corporation**

**Atlanta**

- Oversaw cybersecurity operations focusing on remote computing solutions for the healthcare, legal, and investment sectors.
- Ensured that customers' networks remained compliant with relevant state and federal regulations through regular scans, tests, and assessments, generating detailed compliance reports.
- Conducted penetration testing on remote networks, as well as on client networks on a project basis.
- Led research and development initiatives, designing, setting up, and securing a data center in Atlanta, GA.
- Oversaw setup and maintenance of redundant power systems, networking equipment, and firewalls, connecting to multiple data centers and a private VPN network to over 60 remote locations.
- Managed public authoritative root DNS servers for company and client domains.
- Maintained the entire internal DNS structure.

- Designed, created, and oversaw operations for a comprehensive systems monitoring service for both data center systems and remote secure systems via IPSec tunneling.
- Established and managed an ITIL-compliant Operations/HelpDesk ticketing system for efficient issue tracking and resolution.
- Supervised engineering staff, providing project assignments, time management oversight, training, and technical support for Tier 1 technicians, in addition to project reporting and monthly network assessments.
- Collaborated directly with customers to design secure, cost-effective custom systems and network services tailored to their needs.
- Leveraged open-source applications and operating systems to deliver stable and secure solutions affordably.
- Handled Tier 3 support tickets escalated from Tier 1 staff, troubleshooting high-level systems and network issues as needed.
- Designed, developed, and implemented an enterprise-level information security architecture relevant to a global, multi-geography environment.
- Developed, monitored, and enhanced data security policies, procedures, and standards, and conducted risk assessments while serving as an internal auditor for information security processes.
- Collaborated with data owners, IT teams, and compliance/policy departments to classify sensitive data and ensure appropriate access controls are maintained.
- Participated annually in testing and developing the organization's disaster recovery plan to ensure high data security standards are upheld.
- Initiated and promoted activities to foster information security awareness throughout the organization, deploying education and awareness programs.
- Provided direction and hardening guidance for operating system, database, and application security initiatives.
- Led the incident response team, facilitating incident management across all platforms while generating management reports for analysis.

**02/2005 – 09/2006**

**Senior Systems/Network Engineer, MTPros.**

**Atlanta GA**

- Maintained operation and security protocols for a data center in Atlanta, GA, including the setup of redundant network routers and firewalls.
- Managed authoritative root DNS servers for both company and client domains, ensuring reliable performance.
- Oversaw the internal DNS structure to maintain functionality and security.
- Designed, built, and maintained a systems monitoring service, ensuring both internal data center systems and remote systems secured by IPSec tunneling are effectively monitored.

- Developed and maintained an Operations/HelpDesk ticketing system to enhance support ticket management.
- Ensured security measures were upheld across firewalls at data centers and client remote locations, continually monitoring for vulnerabilities.
- Handled troubleshooting and repair of various systems.
- Proficient in network administration, architecture, application development, server administration, and security management.
- Conducted application security assessments, development, and review of secure coding practices, performing application scans and implementing server security measures.
- Possessed robust information security experience with in-depth knowledge of distributed systems, Internet-based applications, and web security.
- Demonstrated strong analytical skills, effective follow-up, and robust documentation capabilities.
- Recognized for the ability to evaluate information security controls, identify potential risks, and design mitigating controls swiftly.
- Possessed strong relationship-building skills, able to interact with diverse levels of management and employees effectively.
- Utilized problem-solving and research skills to address complex incidents and ongoing security challenges.
- Exhibited strong communication skills, adept at conveying technical concepts to non-technical audiences, and presented to both small and large groups.
- Supervised project tasks, ensuring on-time delivery while managing multiple initiatives.

**03/1999 – 02/2005**

**Security Consultant, Application Development, Network Intranet**

**Atlanta GA**

- Provided consulting services to various businesses, focusing on the design and development of business systems and applications.
- Conducted security assessments of business networks through penetration testing and forensic data analysis, identifying breaches and attack footprints effectively.
- Reported directly to business owners, highlighting security vulnerabilities, threats, and providing viable solutions for remediation.
- Performed audits to monitor IT Security Best Practices, focusing on firewall/network design, anti-virus strategies, system access, and security procedures.
- Developed and implemented security awareness and training programs tailored to client needs, promoting effective security practices.
- Engaged with local, state, and federal law enforcement agencies as necessary to strengthen security protocols.

## **Education and Certifications**

1973 – 1975

**University of Tennessee**

Structural Engineering

Chattanooga TN

1992 – 1993

**Blaze IT College**

Systems Engineering

Atlanta GA

2013

**Texas A&M**

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

## **Skills**

### **Operating Systems**

Linux RedHat, CentOS, Fedora, Debian, Ubuntu, Vyatta, Kali Linux, UNIX (Solaris 9 10 11), Windows Server (NT3.51 to Windows Server 2022)

### **Firewalls and Security Devices**

Vyatta, Smoothwall, Snort, OSSEC, Splunk, Zabbix, Nagios, Firebox devices, Checkpoint Firewall, Sonicwall, Juniper, Cisco ASA, Tripwire

### **Protocols and Services**

IPSec VPN, L2TP, OpenVPN, DNS, IPSec, L2TP, LDAP, Windows AD, Windows DNS, NFS, CIFS, Postfix Mail, SendMail, Azure AD, Intune, O365, Microsoft Defender, Proofpoint, Jabber, IPAM, DHCP, NAT, Load Balancing, Apache Web, Postgres DB, Mysql DB, BGP, OSPF, Static routing

### **Vulnerability Scanners**

Qualsys, Nexpose, Openvas, Nessus,

### **Penetration Tools**

Nmap, Wireshark, Etherape, Ettercap, Tcpdump, Metasploit, Kali Linux toolsets, OWASPZap, BurpsuitePro, SQLmap, Rapid7 tools, Netexec, Impacket toolsets,

Crackmapexec, MFSvenom, John the Ripper, HashCat, Maltego, Evil-winrm, Nikto, Bettercap, Hydra, StegHide, Wpscan, Netcat, Responder, MitM6, Eyewitness, Wifi Pineapple, Bash Bunny, Dirbuster, Aircrack-ng, Masscan, Bloodhound, to mention just a few tools that I use

## **Compliance Standards**

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

## **Skill Sets**

Analytical skills

Strong follow-up skills

Strong documentation skills

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

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

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

critical thinking

independent thinking

creative solutions

## **Writings and Talks:**

- 2015 Moderator on <http://www.point2security.com/>
- June 27, 2016 Packet Publishing "Kali Linux Windows Penetration Testing" <https://www.packtpub.com/networking-and-servers/kali-linux-2-windows-penetration-testing>
- September 5, 2016 Hackin9 "Fear not the Penguin" <https://hakin9.org/fear-not-penguin-interview-wolf-halton-bo-weaver-book-kali-linux-2-windows-penetration-testing/>
- Dec 16 2016 Rapid7 "Security Nation" Podcast "What Pen Testing Teaches You, for 40 Years Strong" <https://www.rapid7.com/resources/podcast-what-pen-testing-teaches-you/>
- Sept 12, 2017 Rapid7's Conference UNITED Summit in Boston "Keep It Simple, Stupid" <https://blog.rapid7.com/2017/09/12/keeping-it-simple-at-united/>
- October 10, 2017 Packt Publishing "Penetration Testing: A Survival Guide" Kindle Edition <https://www.amazon.com/Penetration-Testing-Survival-Wolf-Halton-ebook/dp/B01N35OHY0>
- Jun 15, 2018 Rapid7 blog article "How to Create a Secure and Portable Kali Installation" <https://blog.rapid7.com/2018/06/15/how-to-create-a-secure-and-portable-kali-installation/>
- October 24, 2018 Packet Publishing "Kali Linux 2018: Windows Penetration Testing - Second Edition" <https://www.packtpub.com/networking-and-servers/kali-linux-2018-windows-penetration-testing-second-edition>

- January 19, 2019 Packt Publishing Interview “Bo Weaver on Cloud security, skills gap, and software development in 2019” <https://hub.packtpub.com/bo-weaver-on-cloud-security-skills-gap-and-software-development-in-2019/>
- January 19, 2019 Packt Publishing Interview “Kali Linux 2018 for testing and maintaining Windows security” <https://hub.packtpub.com/kali-linux-2018-for-testing-and-maintaining-windows-security-wolf-halton-and-bo-weaver-interview/>
- January 23, 2019 Podcast Guest “Destination Linux EP105 - Bo Knows Hacking” <https://www.youtube.com/watch?v=pgvFxsNZKck>
- February 5, 2019 Podcast Guest “Ethical Hacking with Bo Weaver” <https://podcast.asknoahshow.com/113>
- June 14, 2019 Southeast Linuxfest (SELF) Talk “Keeping the Pen Tester and Bad Guys Out. K.I.S.S them. <http://www.southeastlinuxfest.org/pdfs/SELF-2019-Schedule.pdf> Video Link (bad audio) <https://www.youtube.com/watch?v=DbRwz6zJBdg>