Ben S. Knowles **Information Security Engineer and Educator**

Associate of Science, Computer Science | Associate of Science, Psychology
Black Box Software Tester | CISSP | SANS GIAC GSEC, GCIA, GCIH | ITILF | Linux Professional
Mail: adric adric net **Mobile**: 1-404-936-7473

Certifications:

Global Information Assurance Council (GIAC)
GIAC Security Essentials Certification Gold (GSEC), awarded Mar 2014

PeopleSoft
Information Technology Infrastructure Library (ITIL) Foundations (**ITILF**) Apr 2013

International Information Systems Security Certification Consortium (ISC²)
Certified Information Systems Security Professional (**CISSP**) Sep 2012

Global Information Assurance Council (GIAC)
GIAC Certified Intrusion Analyst Silver (**GCIA**) Aug 2012

Black Box Software Testing Project (BBST) / Association for Software Testers (AST)
Black Box Software Tester (**BBST**) Nov 2011

Global Information Assurance Council (GIAC)
GIAC Certified Incident Handler Silver (**GCIH**) July 2011

Linux Professional Institute (LPI)
Level One Certification (**LPIC-1**) Dec 2010

Recent Classes Taught:

Association for Software Testing
FND101: Black Box Software Testing: Foundations, as Asst. Instructor June – July 2014

SANS Institute
SEC504: Hacker Techniques, Exploits, and Incident Handling (GCIH), as Mentor May – July 2014

SANS Institute
SEC504: Hacker Techniques, Exploits, and Incident Handling (GCIH), as Mentor April – July 2013

SANS Institute
SEC401: Security Essentials (GSEC), as Mentor Oct – Dec 2012

Recent Computer Work:

Security Engineer, Web.com Oct 2013 – current
- SOC and CSIRT tools and processes design and deployment
- Senior Incident Handler and Incident Coordinator
- Incident handling and analysis education: brownbags and workshops

Security Analyst, CISO Threat Resistance**:** Dell SecureWorks May 2012 – Sep 2013
- Prevent and respond to security events and incidents on global enterprise network
- Develop, deploy, tune state of the art Network Security Monitoring (NSM) and hunting technology
- Artifact triage and analysis with automated tools including Cuckoo Sandbox and Mastiff

Lead Analyst, CISO Countermeasures**:** Dell SecureWorks Sep 2011 – May 2012
- Threat focused internal incident response and information security
- Direct, perform, track, report, and analyze all counters to threat activity
- Maintain and operate defensive security technologies including IPS and proxies

NOC Lead, IT Service Management: SecureWorks Mar 2010 – Sep 2011
- Track, report, analyze incidents: outages and investigations
- Work with IT, Operations, Research, and Risk Management leadership
- Building out full service NOC and Service Desk functions

Systems Administrator, NOC **:** SecureWorks Nov 2009 – Sep 2011

- Administration of hundreds of RHEL, Debian, and BSD servers, physical and virtual
- High security environments across multiple sites in a regulated industry
- Incident Response, Triage, and Escalations, Manage ticketing and alerting infrastructure
- Made NOC Lead, March 2010

Independent Contracting, Community, and Volunteer Work **:** ongoing

- Presenter, DC404
  - ***Breaking into Information Security****: some infosec career tips* Feb 2014
  - ***Sift your … before you Autopsy****: Learn digital forensics with free tools* July 2014
- Technical Reviewer for SANS 2012 - 2014
- Exam question author for GIAC 2011,2013
- Participant: WTST 2012 : Workshop on Teaching Security Related Software Testing
  - ***Vulnerability Lifecycle for Testers*** Jan 2012
- Web application/LMS consulting, BBST , Education SIG, AST
- System Integration of Win, Mac, Linux Servers running open source software

System Administrator II **:** National Net, Inc: Oct 2006 – Feb 2009

- Part of a small SA team at a big Linux web host: Data center with more than 1600 hosts
- Software and Hardware troubleshooting, Live incident response
- Shift lead on weekend nights for more than a year

Network Administration : MMI -> Contexo Media : Aug 2004 – Sep 2006

- Designed, rebuilt, developed, and supported a mixed Linux/Mac office network for two years
- Production Web, Mail, DNS services, VPN, File Shares, Databases, Revision Control, Printing, Remote Access, Ticketing, et al
- Defense in depth, proactive patching, least privilege

Hands On Training : H & H Computer Education : 2004-2005

- Taught Intro to PC Tech part time to diverse groups at local computer shops
- Helped students prepare for the A+, Net+, MCSA, and MCSE certification tests.
- Used Linux boot media and open source tools including *memtest86* and *lspci* to teach troubleshooting

Formal Education:

Associate Of Science, Computer Science
Georgia Perimeter College, Clarkston, Georgia, USA May 2002

Associate Of Science, Psychology
Georgia Perimeter College, Clarkston, Georgia, USA Aug 2002

Academic Diploma with Honors
Chamblee High School, Chamblee, Georgia, USA June 1995

Computer Skills and Knowledge Domains:

System Administration:

- Linux, Windows, Macintosh platforms
- Basic scripting in shell, Perl, Python, ruby
- VMWare, kvm, VirtualBox
- Support sysadmins, developers, researchers, testers, and users

Security Domain Knowledge:

- vulnerability lifecycle
- defense in depth strategies
- host, network, and web application security
- incident response and forensics
- secure software development

Security Tools:

- Wireshark, tcpdump
- nmap, netcat, nessus
- snort, snorby, Bro
- Sleuth Kit, Autopsy, FTK
- Volatility Framework
- Cuckoo Sandbox
- Security Onion