Ben S. Knowles

Associate of Science, Computer Science | Associate of Science, Psychology
Black Box Software Tester | SANS GIAC GSEC, GCIH | Linux Professional Institute Certified

Mail: adric adric net **Mobile**: 1-404-936-7473

Recent Certifications:

Black Box Software Testing / AST

Black Box Software Tester (**BBST**) Nov 2011

SANS Global Information Assurance Council (GIAC)

GIAC Certified Incident Handler Silver (**GCIH**) July 2011

Linux Professional Institute

Level One Certification (**LPIC-1**) Dec 2010

SANS Global Information Assurance Council (GIAC)

GIAC Security Essentials Certification Silver (**GSEC**) Sept 2010

Recent Computer Work:

Lead Analyst, CISO Countermeasures: Dell SecureWorks — Sep 2011– present

- 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 and Volunteer Work : — ongoing

- System Integration of Win, Mac, Linux Servers running open source software
- Independent Developer of MooCash: ZenCart - Moodle software: http://moocart.sf.net/
- Exam question author, GIAC 2011
- Web application/LMS consulting, BBST , Education SIG, AST
- Participant: WTST 2012 : Workshop on Teaching Security Related Software Testing
- Technical Reviewer, SANS 2012

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
- Administration of production virtual, dedicated, and co-located customer servers
- 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

Recent Coursework:

Association for Software Testing (AST)
Black Box Software Testing (BBST) Test Design Nov 2011

Association for Software Testing (AST)
Black Box Software Testing (BBST) Bug Advocacy Apr 2010

Association for Software Testing (AST)
Black Box Software Testing (BBST) Foundations Feb 2009

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:

System Administration:

- Linux, Windows, Macintosh platforms
- Basic scripting in shell, Perl, python, ruby
- MySQL, SQLite, PostgreSQL, MSSQL
- Support administrators, developers, researchers, testers, and users

Security:

- Broad security domain knowledge including:
  - vulnerability lifecycle
  - defense in depth strategies
  - host, network, and web application security
  - incident response and forensics
  - secure software development
- security tools usage: wireshark, nmap, nessus, snort, nagios