Volume 5, Issue 4
April 2002—The Software Quality Advisor

April, 2002

The Software Quality Advisor Online

April, 2002

Am I Getting Through to You? Exploring Penetration Testing

This article examines some of the basics of performing a type of security testing called penetration testing.

- Penetration testing requires special skills.
- A high level of communication is required to prevent false alarms and to keep the tester from getting in trouble.

This article is taken from Rice Consulting Services' newest course, "Security Testing for the Enterprise and the Web." You can find details at www.riceconsulting.com/training_center.htm.

Inside this issue:

Am I Getting Through to You? Exploring Penetration Testing

By Randall W. Rice, CSQA, CSTE

The objective of penetration testing is to validate the degree of difficulty in breaking into a system from the outside. This type of test generally has two typical major purposes:

- To demonstrate to management there are security problems and the potential consequences of an attack.
- To test intrusion detection and response capabilities.

We need to keep in mind that penetration testing is a snapshot - what is seen today may be different tomorrow! Penetration testing is also more than just running a vulnerability scanner. While vulnerability scanners may be helpful, they are often too generalized to achieve a full penetration test. Manual "white hat" hacker tests can find holes in your security defenses, but manual tests have the limitation of time and resources. In this article, we will discuss the issues and challenges of penetration testing with the goal of at least raising awareness of this type of testing.

Who can perform penetration testing?

Penetration testing can be performed by people with adequate training, supervision, tools and planning. However, it takes a very unique type of person to perform penetration testing or other types of security testing for that matter. A security tester must have a mindset that allows them to think like an attacker. Finding this type of person in an organization can be quite a challenge. For this reason, some organizations have hired "white hat" hackers to perform the test. An expert may perform a more complete test, but there is debate about the security risk posed by hiring outside firms to have access to your most secure systems.

Penetration testing is a process

This process of penetration testing also includes tools and best practices. Penetration testing is more than just guessing at how to break into a system. You can learn much about penetration testing by keeping up with the links and resources listed in this module.

(Continued on Page 2)

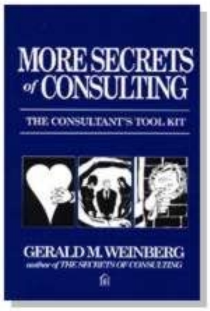
Book Review—More Secrets of Consulting by Gerald Weinberg

More Secrets of Consulting delivers on its title as a sequel to the book I regard as the best guide to consultants around, *The Secrets of Consulting*.

I was fortunate to read *The Secrets of Consulting* when it first came out in 1985 and when I was early in my journey as a consultant. The lessons contained in the first *Secrets of Consulting* book have served me well over the past ten years and have helped me serve my clients well.

In *More Secrets of Consulting*, Weinberg presents a tool kit that can be used to see client needs from a variety of perspectives. In addition, in *More Secrets of Consulting* you will learn how to serve your clients with integrity and to take care of yourself in the process.

(Continued on Page 2)


MORE SECRETS of CONSULTING
THE CONSULTANT'S TOOL KIT
GERALD M. WEINBERG
author of THE SECRETS OF CONSULTING

Book Review (Cont'd.)
The Secrets of Consulting by Gerald Weinberg

Examples of the tools that Weinberg presents are:

The Golden Key, which allows you to open up new areas for learning and practicing and to close them, if necessary.

The Detective Hat (an Magnifying Glass), which helps you to examine data and reason about those data, and

The Oxygen Mask, which reminds you to take care of yourself before attempting to help others.

Weinberg also adds a new extension to The Law of Raspberry Jam, which says that "the wider you spread it the thinner it gets." The Law of Strawberry Jam, which says "as long as it has lumps, you can never spread it too thin." As Weinberg explains "Young visionaries are discouraged by The Law of Raspberry Jam because they would like to believe that their message would remain thick as they spread it far and wide. But they need not be discouraged, even though no vision retains uniform thickness as it spreads." He goes on to say, "In strawberry jam, the lumps are strawberries. In your Great Message, the lump is you. What lumps are to strawberry jam, you are to your Great Message. As long as your medium of communication involves your own body in the flash—speaking, writing, hugging—your message cannot be infinitely diluted.

Although the primary audience for this book is consultants, anyone who is involved in providing advice (for example, internal consultants and project managers) will find this book enlightening and helpful.

For independent consultants, the tools in this book and the first Secrets book will set you apart from other consultants and will position you to provide great value to your clients.

Reviewer: Randy Rice

> ***"As long as your medium of communication involves your own body in the flash—speaking, writing, hugging—your message cannot be infinitely diluted."***
>
> ***Gerald Weinberg***

Am I Getting Through to You? (Continued from Page 1)

Important Warning

Penetration testing requires caution not to cause damage to data or to raise suspicion. When performing security testing, be aware that the test can look like a real attack. To avoid getting fired and/or arrested, make sure that your test is scheduled, planned and has management approval. Also, network and security administrators need to know about the test. Penetration testing must be planned and authorized so that you will not be fired and/or arrested for attempted computer crime. The element of surprise may be a real-life factor in security attacks, but in testing it can get you in trouble.

> ***"Penetration testing requires caution not to cause damage to data or to raise suspicion."***

The Kinds of Attacks Simulated

Penetration testing typically simulates the following kinds of attacks:

- War-dialing – In this type of attack, the attacker has tools that try many different telephone numbers until they get a hit on a data line. Then, they use password cracking tools to guess user name and password combinations.
- Network-based attacks – In a network-based attack, an attacker uses a scanning or mapping tool to identify the IP addresses and other information about the target system. Specific computers on the network can then be targeted. Like the war-dialing attack, password cracking tools are used to guess user names and passwords.
- Application-based attacks – In this type of attack, the attacker takes advantage of known security holes in applications to gain entry into a system.
- Password hacks – In all of the above attacks, the attacker needs a way to gain entry through a logon process. Typically, a password cracking tool is used to rapidly try many different user name and password combinations. However, sometimes the attackers don't even need to be very creative as users will keep default passwords and use common words such as "password", the name of the month, their kid's name, etc. for passwords. Even when users are required to change passwords each month, they will often just toggle between one or two passwords.

Although penetration testing may reveal vulnerabilities, it is not a substitute for security reviews and preventative measures. When comparing relative effectiveness, security reviews and preventative measures get higher marks from security professionals than penetration testing. This is to be expected, as we see the same type of effectiveness increase in finding functional defects when software inspections are used in addition to functional testing. Penetration testing is a validation that security measures are in place and working effectively.

Manual or Automated?

Penetration testing can be performed manually using planned tests and intuition, or it can be performed using specialized tools. The tool-based approach requires a multi-tool solution with tools such as network scanners, vulnerability scanners and password cracking tools. Even the best commercial tools often do not allow you to test all attacks and the freeware tools often have bugs and could even introduce a security risk.

Continued on Page 3

The Role of the Test Team Leader in Facilitating Change

By Randall W. Rice, CSQA, CSTE

Rapid change is one of the major challenges of software testing and because of the instability that rapid change brings, many testers and test team leaders often oppose change in general. However, there are many types of change that should result from testing, such as the need to change a process for the purpose of improving efficiency or defect prevention. Interestingly, it seems that many times testers are resistant to the things that development and users want to change, while development and users are resistant to things that testers want to change.

The fact remains that the greatest value of testing is not to find defects, but to provide information to management for the purpose of process improvement. This may be a direct contradiction to what many people in management and in testing believe to be the purpose of testing, but if finding defects is the only value of testing, then a lot of resources are being expended for a single-use purpose with a one-time return on investment.

In my course, Becoming an Effective Test Team Leader, I discuss that test team leaders are ideal agents of change for software processes in an organization.

Here are some things to consider when you want to be a change agent in your organization.

1. The first person to change is you!

We often see how others need to change, but fail to make personal application first. A true leader makes the trip in front of others, not from a perspective of observation from the outside. For example, a test team leader has many opportunities to change personal processes and testing processes.

2. You must focus on what you have in common, not differences. It is tempting to view others by their differences, such as age, ideas, energy, personality, and culture.

(Continued on Page 6)

> ***"The fact remains that the greatest value of testing is not to find defects, but to provide information to management for the purpose of process improvement."***

Am I Getting Through to You? (Continued from Page 2)

Black box and White Box Penetration Testing

Like other forms of testing, there are two major views of a penetration test:

A zero-knowledge attack, which is like a "black box" test, in that the tester that has no knowledge of the target system. This type of test is one that would be performed by an independent third party and simulates the type of attack that an external attacker would perform.

A full-knowledge attack, which is like a "white box" test, in that the tester has complete knowledge of the target system. This simulates the kind of attack an employee or former employee could mount.
As mentioned earlier, testers must exercise great care when performing penetration testing. There are many examples of damage caused during penetration testing. Many other cases are never publicized to avoid embarrassment to the victim companies.

Another issue in penetration testing is exposing your security vulnerabilities to outside people. The question comes to mind, "How much can you really trust an "ethical" hacker who works for someone else?"

A Penetration Testing Process

Step 1 - Define the Test Strategy

In this step you lay the foundation of the test by defining "what" is to be tested. This step has the following tasks:

Task 1 - Define the objective

In this task, you identify the overall objective of the test. One major objective could be to prove security threats to management. Another major objective could be to validate intrusion detection and response.

Task 2 - Define the target

The targets are the points in the system infrastructure you plan to test. Targets can include networks, application systems, data, client PCs, etc.

Task 3 - Define the attacker profile/level

This might be one of the most difficult aspects of security testing, as you never know for sure who will try to attack your systems. Typical attacker profiles are:

- Script kiddies – These people are outsiders who lack the technical skills to create attacks on their own, but they are adept at running attacks created by others. While the name "script kiddie" sounds innocent enough, don't underestimate these people. There are plenty of attacks freely available that can cause a lot of damage.
- Malicious insider – These are the people who work for you that are out to damage your system, but hide it. These people can also leak sensitive internal information to outside attackers.
- Temporary employee – These people can be a problem because they may need a basic level of system access to do their job. These people may also learn enough about your company to perform an external attack once they leave the company.
- Professional attacker – These are the people who create the new attacks. They are often skilled programmers with a lot of time of their hands.

Continued on Page 5

Links

Yahoo Coverage on Hacks and Attacks

http://fullcoverage.yahoo.com/fc/Tech/Hackers_and_Crackers/

Security White Papers from TruSecure

http://www.trusecure.com/html/tspub/whitepaper_index.shtml

Draft Guidelines for Network Security Testing

http://csrc.nist.gov/publications/drafts/security-testing.pdf

Database Testing

http://www.ppc.pims.org/Projects/CE/CE99/WG/DatabaseTesting.htm

http://www.dallaway.com/acad/dbunit.html

PROTOS - Security Testing of Protocol Implementations

http://www.ee.oulu.fi/research/ouspg/protos/

Security Links

http://www.krazee.unstman.btinternet.co.uk/page11.html

The Open Web Application Security Project

http://www.owasp.org/testing/

NSA to Back Private Security Testing

http://www.info-sec.com/OSsec/OSsec_072397a.html-ssi

Reality Check

http://www.fcw.com/fcw/articles/2001/0416/tec-ryan-04-16-01.asp

Cookies—Trick or Treat

http://www.fcw.com/fcw/articles/2000/0619/tec-ryan-06-19-00.asp

Quotes

"The only normal people are the ones you don't know very well."

Joe Ancis

"A friendship founded on business is better than a business founded on friendship."

John D. Rockefeller Jr.

"All programmers are playwrights and all computers are lousy actors."

Unknown

"Always do right. This will gratify some people and astonish the rest."

Mark Twain (1835 - 1910)

"The difference between the right word and the almost right word is the difference between lightning and a lightning bug."

Mark Twain (1835 - 1910)

"That you may retain your self-respect, it is better to displease the people by doing what you know is right, than to temporarily please them by doing what you know is wrong."

William J. H. Boetcker

"Lazy hands make a man poor, but diligent hands bring wealth."

Proverbs 10:4, The Bible

"Associate yourself with men of good quality if you esteem your own reputation for 'tis better to be alone than in bad company."

George Washington

Questions From the e-Mail Bag

Q: "Why does an organization need an Independent Testing Group?"

A: There are several reasons independent testing is needed

1) Developers get tunnel vision from working on the same thing for an extended period of time. It's like writing an article and missing your own errors.

2) Developers can be good testers - IF they have a good process and management support. However, there is a very strong temptation to shortcut testing when the deadline starts to press in.

3) Independent testers can test from a larger perspective, such as the integration with other applications, and from the end-user perspective.

4) Independent testers can give an objective assessment of the state of the software, unless they report to the development manager.

5) Independent testers can build a reusable base of test plans and test cases that can sometimes also be used on other projects.

Here's another perspective. As a consultant, I've seen management build up and tear down QA efforts and it is never, ever, productive. All it does is build business for

(Continued on Page 5)

Questions from the Mail Bag (Continued from Page 4)

consultants and trainers like me. These companies lose all of their investments in people and testware.

There are some downside risks, such as the "us vs. them" situation and the "throw it over the wall" scenario, but these can be dealt with. I am a proponent of both strong developer testing for structural unit testing especially, and for independent testing for functional testing, integration and user views.

I know I'm tooting my own horn here, but we wrote the *Surviving the Top Ten Challenges of Software Testing* book as an easy read for senior management to understand these kinds of issues. I recommend that you order some copies and pass around to your management team.

Q: "How does one get started in the a career of testing? What background is required?"

A: That's a good question. People come in from different backgrounds (developer, user, trainer, etc.) and a technical background is not required, although computer literacy is needed.

Most test managers I know look for attributes such as the ability to work in team, dependability, patience, tenacity, positive attitude, etc., and then they will train their team on specific testing skills.

For books, I recommend:

Software Testing by Ron Patton, and *Surviving the Top Ten Challenges of Software Te*sting by William E. Perry and yours truly.

You can get real good prices on those at www.booksamillion.com.

You can put the concepts into practice on your own and you can test any software on your own PC to get experience. Some people even hire themselves out as contract testers. Look for companies that have large projects going and contact them. Also, once you get a little experience, contact some recruiters in your area. They always seem to be looking for testers. Don't forget the web job sites, such as monster.com and dice.com. I also have a place to post a resume on my site in the Careers section.

If you have a question for Randy, e-mail him at rrice@riceconsulting.com.

"Most test managers I know look for attributes such as the ability to work in team, dependability, patience, tenacity, positive attitude, etc., and then they will train their team on specific testing skills."

Am I Getting Through to You? (Continued from Page 3)

Task 4 - Define the view of testing

This is where you define if testing will be performed from the external, black-box (zero-knowledge) test and/or the internal, white-box (full-knowledge) perspective.

Step 2 - Test Planning

In this step you define "how" the penetration test will be performed and what resources will be needed for the test. The tasks in this step include:

Task 1 - Understand the system to be tested (Discovery)

The extent of this task depends on the view of testing you define in the test strategy. Even with zero-knowledge attacks, "footprinting" or intelligence gathering can be done in advance of the test. Ways to understand the system include using the web to mirror a site using wget or Teleport Pro, Whois databases which list the owners and contact information of a specific site, and network scanning tools.

Task 2 - Drill deeper into the infrastructure (Enumeration)

This task discovers specific network addresses, user names, and application profiles.
Task 3 - Map vulnerabilities

These are based on known vulnerabilities. Publicly available sources of vulnerability information include Bugtraq, Computer Emergency Response Team (CERT) advisories and vendor security alerts.

Task 4 - Design the attacks

This is the most detailed level of test planning and is based on the vulnerabilities, risks, history and intuition. These tests can be defined using a framework of test controls, input, expected output, and procedures.

Step 3 - Perform the test

The performance of the test depends on the degree of test planning. For penetration testing, you need to have done the same homework an attacker would have done to scan and understand your system. As we mentioned earlier, appropriate people need to be notified when and how the test will be performed.

Task 1 - Set-up

In this task you plan and schedule the test, notify security and network administrators, and get the tools in place, depending on the type of penetration test you plan to perform

Task 2 - Performance

In this task you use security test cases to perform the tests, while at the same time observing the test results. The documentation of the test can include screen prints and server logs.

Step 4 - Report the results

In this step, the results of penetration testing is reported to management. You should:

- Make it relevant - the report should deal with real-life conditions as opposed to highly theoretical ones.
- Make it easily understood - avoid technical jargon and extreme detail. Use graphics and demos to illustrate points.
- Show the potential impacts, such as what would be the impact of the release of sensitive data, the denial of service, and the loss or destruction of data.

(Continued on Page 6)

Am I Getting Through to You? (Continued from Page 5)

Links and Resources

The following organizations and links contain information valuable to people designing and performing penetration testing:

Bugtraq - http://www.bugtraq.com/

Computer Emergency Response Team (CERT) - http://www.cert.org/

Fping - http://packetstorm.securify.com/

Gnit - http://security.ellicit.org/programs

Icmpenum - www.nmrc.org/files/sunix/icmpenum-1.1.1.tgz

Nessus - The Nessus Project - http://www.nessus.org/

Netcat - http://packetstorm.securify.com/UNIX/utilities/nc110.tgz

Nmap - www.insecure.org/nmap

Penetration Testers List - http://www.securityfocus.com/

SAINT - www.wwdsi.com/saint

Teleport Pro Tenmax - www.tenmax.com/teleport/pro/home.htm

Wget - http://sunsite.auc.dk/wget

whois sites, such as:

- www.crsnic.net/whois/
- http://www.arin.net/
- http://www.samspade.org/

Penetration Testing Articles

The following articles and links contain information valuable to people designing and performing penetration testing:

Penetration Testing Exposed http://www.infosecuritymag.com/articles/september00/features3.shtml

Penetration Testing Myths http://www.infosecuritymag.com/articles/september00/features4.shtml

Useful books:

Hacking Exposed, Third Edition by McClure, Scambray and Kurtz

Counter Hack by Ed Skoudis

Hack Attacks Revealed by John Chirillo

The Role of the Test Team Leader in Facilitating Change

(Continued from Page 3)

Instead, look for areas you have in common, such as the desire to deliver a quality system.

3. Leaders must never make the trip alone – they must connect with the people.

This also goes along with "The Law of Buy-in" from John Maxwell's 21 Irrefutable Laws of Leadership, which says that the people buy-in to the leader before they buy into the leader's vision. This implies that a leader for change must have credibility and clout in an organization.

4. Be careful about talking too much about how something worked great someplace else.

People can be sensitive about the uniqueness of their culture. If a new person comes in and starts to talk about transforming the organization into someplace they have been before, people start to erect mental defenses. Think about the all-too-common example of the new CIO that comes on board and tries to do the same thing they did in their previous organization. Many times these attempts are unsuccessful because: a) people don't like to change and b) if you can get people to change, they don't like to change too quickly.

5. There is an interesting paradox about change. Once you make the "big change" successfully, a lot of smaller changes will follow. However, you must make small changes to allow the big change to happen.

An example of this is when an organization starts to perform reviews. The ultimate goal is to remove defects most effectively by performing organized and rigorous inspections. Once inspections are a reality in an organization, people see the value and other smaller changes for improvement can happen – if management leads the way. However, jumping into inspections immediately will likely cause people to reject the entire approach because of time and resource concerns. If people start with less formal methods and see success, they will be more likely to go to the next step of formality.

This leads me to a key point of leadership. That is, the number one job of a leader is to define reality. This can be a challenge because people have varying perceptions of reality. The leader's job is to objectively as possible sort through all of the facts and bring people to the point of reality.

The leader may discover that he or she is part of the problem. The leader may also start to ask why things are the way they are. This is a place to start changing, but eventually people will need to be brought to a point of decision about whether or not to make the change. This is a critical step.

(Continued on Page 7)

> ***"The leader's job is to objectively as possible sort through all of the facts and bring people to the point of reality."***

The Role of the Test Team Leader in Facilitating Change

(Continued from Page 6)

Without a firmly defined point of decision, the journey of change is fuzzy and the leader's authority is easily undermined.

You might think of this point of decision as "laying it on the line." True leaders know that when you do something is more important that what you do. Timing is everything in leadership (and a lot of other things as well).

How Do You Know When To "Lay it On the Line"?

1 – you have defined reality
2 – you have identified the issues - don't take down the fence until you know why it was put up
3 – you've engaged the influencers in the process
4 – you've received counsel and support from the influencers (feedback)
5 – you've cast the vision
6 – you have achieved a few victories defeat a few average foes before giants (e.g., David killed a lion and a bear before Goliath)
7 – you've made personal changes that will affect the outcome
8 – you have seen the influencers make changes
9 – when there is nothing in your way but the big decision

What's Next?

What changes are before you? I often advise new test or QA leaders to make a list of 8 – 10 initial goals. Then, divide that list into three parts:

- Short-term tasks that can be completed in one to three months
- Mid-term tasks that will take three to six months
- Long-term tasks that will take six months or longer

The reason I advise this approach is that the short-term tasks will build momentum by showing early successes and value. The mid-term tasks can be started immediately, but require additional time and resources to complete. The short-term tasks buys time to complete the mid-term tasks. Finally, the long-term tasks often require cultural change but management wants to see results faster than six months to a year. Once again, it is the short and mid-term tasks that build momentum. In addition, there are people that will not buy into the long-term goals until they see smaller successes.

Wherever you are in the spectrum of change, don't give up and don't change just for the sake of change. Understand that defining reality and the associated needed changes are a major part of the leader's job. Define your goals, wait for the right timing, and be ready to lead your organization in positive change!

> ***"True leaders know that when you do something is more important that what you do. Timing is everything in leadership"***

The Bit Bucket

You may be wondering why we are including a recipe in a software quality newsletter. Well, this is a great cookie recipe for those times when you want to bring a treat to the test lab (or office) that doesn't take a long time to make.

THE ULTIMATE COOKIE

2 sticks butter (no substitute)
1 c. sugar
½ c. brown sugar
1 egg
1 tsp. Vanilla
1 ½ c. sifted flour
1 tsp. Baking soda
1 tsp. Cinnamon
2 c. Nestles Mega Morsels (or chocolate chips)
2 c. pecan halves or pieces
1 ½ c. oats

Cream together butter, sugar, brown sugar until creamy. Add the egg and vanilla and beat. Add the sifted flour, baking soda and cinnamon until well mixed. Then fold in the Mega morsel chips, pecan halves and oats. Mix well and chill for 1 hour. (If left over an hour the batter will be too hard to shape) Roll into 2-inch balls and bake at 350 degrees for 12 minutes.

Humor of the Month

The Washington Post's Style Invitational asked readers to take any word from the dictionary, alter it by adding, subtracting, or changing one letter, and supply a new definition.

Here are some recent winners:

Intaxication: Euphoria at getting a tax refund, which lasts until you realize it was your money to start with.

Reintarnation: Coming back to life as a hillbilly.

Giraffiti: Vandalism spray-painted very, very high.

Sarchasm: The gulf between the author of sarcastic wit and the person who doesn't get it.

Inoculatte: To take coffee intravenously when you are running late.

Hipatitis: Terminal coolness.

Osteopornosis: A degenerate disease (this one got extra credit).

Karmageddon: It's like, when everybody is sending off all these really bad vibes, right? And then, like, the Earth explodes and it's like, a serious bummer.

Glibido: All talk and no action.

Dopeler effect: The tendency of stupid ideas to seem smarter when they come at you rapidly.

The word 'politics' is derived from the word 'poly', meaning 'many', and the word 'ticks', meaning 'blood sucking parasites'.

The Software Quality Advisor Online

April, 2002

P.O. Box 891284
Oklahoma City, OK 73189

405-793-7449
405-793-7454 Fax
rrice@riceconsulting.com

"Test everything. Hold onto the good."
I Thessalonians 5:21

We're on the Web!
www.riceconsulting.com

May 2002 Issue:

The Science of Software Testing
by Randall W. Rice

Secrets of Successful User Acceptance Testing by Randall W. Rice

Book Review—Peer Reviews by Karl Weigers, Reviewed by Randall W. Rice

Coming to Chicago!

May 8—10, 2002

PMG

RCS
Consulting Excellence!

A Three-day course in Web Testing Techniques

Presented by Process Management Group, Ltd. (www.pmgltd.com), the Midwest's Premier Provider of IT Quality and Software Testing Services, and Rice Consulting Services, Inc. (www.riceconsulting.com), a world recognized leader in Quality and Testing Training.

See details and register at
www.riceconsulting.com/chicagoq2_2002.htm

Calendar of Events

A Three-day Course in Web Testing, Chicago, IL, May 8—10

Sponsored by the Process Management Group, Ltd. And Rice Consulting Services, Inc.

www.riceconsulting.com

Pacific Northwest Software Quality Conference (PNSQC) Seminar Series

Randy will be presenting a one-day version of his popular tutorial, Becoming an Effective Test Team Leader.

May 13, 2002—Beaverton, OR

May 14, 2002—Bellevue, WA

www.pnsqc.org

KCQAA Spring Conference

Kansas City, Mo, June 10—12, 2002

Randy will be presenting a three-day program on *User-Oriented Methods for Software Quality*

www.kcqaa.org

We hope to see you at one of these events!

If you have a group of 12 or more people in your city that would like to sponsor a training event, contact Randy Rice at rrice@riceconsulting.com to find out how to book a special presentation.

User-oriented Practices for Delivering Quality Software, Chicago, IL, August 14—16

Sponsored by the Process Management Group, Ltd. And Rice Consulting Services, Inc.

www.riceconsulting.com