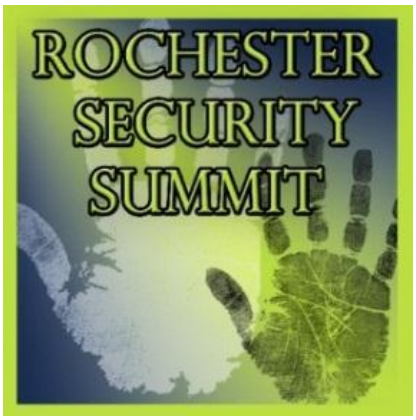
March 2013 Newsletter

Next Meeting: Thursday, April 18
Golisano Hall at RIT 5:30 pm
Joint with ISSA and OWASP
Topic: Ethical Hacking and Penetration Testing
Speaker: Ralph Durkee
RSVP: www.RocISSA.org

Ralph will briefly discuss Ethical Hacking (EH) and Penetration Testing (PT), why they are important and how they differ. He will talk about the ethical hacking mindset and the ethical hacking process and why it's important as a professional penetration testing meta-technique. The presentation will then apply the EH process with audience participation on exploiting sample vulnerabilities of both servers and clients. The examples will cover several specific, yet basic tools and techniques that continue to be effective in the exploitations of systems, applications and clients. Of course he'll also briefly discuss how to defend against these attacks. Although the cool tools and sexy exploits tend to get much of the attention when it comes to penetration testing, the focus will be on the ethical hacking as a meta-technique and how it can be applied to maximize the usefulness of the results to the hiring organization. The presentation will also cover some common misconceptions, mistakes, ethical issues and unprofessional-'isms' that continue to trouble the profession.

Biography

Ralph Durkee is the principal security consultant and president of Durkee Consulting, Inc. since 1996. Ralph founded the OWASP Rochester, NY chapter and has served on the board since 2004. Ralph served on the ISSA chapter board to start the Rochester ISSA chapter as well as starting the annual Rochester Security Summit. He has served as the ISSA chapter president since 2010. He performs a variety of network and application penetration tests, software security assessments and secure software development consultations for clients. His expertise in penetration testing, incident handling, secure software development and secure Internet and web applications is based on over 30 years of both hands-on and technical training experience. He has developed and taught a wide variety of professional security seminars including custom web application security training, and SANS SEC401 & SEC504 - Hacker Techniques and Incident Handling and CISSP bootcamp courses since 2004. Ralph also regularly consults on the development and implementation of a wide variety of security standards such as web application security, database encryption, Windows and Linux security. Ralph also has done security consulting for compliance with the Payment Card Industry Data Security Standard, and holds the following certifications CISSP, CRISC, GSEC, GCIH, GSNA, GCIA, and GPEN.



Rochester Security Summit 2013

Tuesday and Wednesday, October 22 - 23
www.rochestersecurity.org

Hyatt Regency
www.rochester.hyatt.com

Look for us on Facebook!

Call for Speakers is open!

Track Topics: Audit/Compliance, Technical, Business, InfraGard/Cybercrime

Proposals may be submitted to
present2013@rochestersecurity.org

RSS 2013 Keynote Speakers

Bruce Schneier

Bruce Schneier is an internationally renowned security technologist and author. Described by *The Economist* as a "security guru," he is best known as a refreshingly candid and lucid security critic and commentator. When people want to know how security really works, they turn to Schneier.

His first bestseller, *Applied Cryptography*, explained how the arcane science of secret codes actually works, and was described by Wired as "the book the National Security Agency wanted never to be published." His book on computer and network security, *Secrets and Lies*, was called by Fortune "[a] jewel box of little surprises you can actually use." *Beyond Fear* tackles the problems of security from the small to the large: personal safety, crime, corporate security, national security. *Schneier on Security*, offers insight into everything from the risk of identity theft (vastly overrated) to the long-range security threat of unchecked presidential power. His latest book, *Liars and Outliers*, explains how societies use security to enable the trust that they need to survive.

Regularly quoted in the media -- and subject of an Internet meme -- he has testified on security before the United States Congress on several occasions and has written articles and op eds for many major publications.

Schneier also publishes a free monthly newsletter, Crypto-Gram, and a blog, Schneier on Security, with a combined 250,000 readers. In more than ten years of regular publication, Crypto-Gram has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. As head curmudgeon at the table, Schneier explains, debunks, and draws lessons from security stories that make the news.
Schneier is the Chief Security Technology Officer of BT.

http://www.schneier.com/

Lance Spitzner

Mr. Lance Spitzner is an internationally recognized leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books, and has published over thirty security whitepapers. Mr. Spitzner started his security career with Sun Microsystems as a senior security architect, helping secure Sun's customers around the world. He is founder of the Honeynet Project; an international, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public.

Mr. Spitzner has spoken to and worked with numerous organizations, including the NSA, FIRST, the Pentagon, the FBI Academy, the President's Telecommunications Advisory Committee, MS-ISAC, the Navy War College, the British CESG, the Department of Justice, and the Monetary Authority of Singapore. He has consulted around the world, working and presenting in over 20 countries on six different continents. His work has been documented in the media through outlets such as CNN, BBC, NPR, and The Wall Street Journal. He serves on the Distinguished Review Board for the Air Force Institute of Technology, Technical Review Board for CCIED, and the Information Assurance Curriculum Advisory Board at DePaul University. Before working in information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois-Chicago.

www.spitzner.net
www.securingthehuman.org

Continuing Education Units (CEU)

There are many opportunities to get CEU for security certifications like CISSP or CISA.

- Attend an ISSA chapter meeting
- Speak at RSS or chapter meeting
- Volunteer for a committee
- Write a journal article

Upcoming Events:

Educational Technology Day
Ithaca College
March 21, 2013
http://www.ithaca.edu/edtechday/

ISACA, Western New York Chapter
Control and Compliance 2013
April 23, 2013
Rochester Plaza, 6 CPE
http://www.isacawny.org/

Digital Rochester
2013 Technology Woman of the Year Award Breakfast
Thursday, April 25, 2013
7:30 am – 10:00 am
http://digitalrochester.com/

CISSP 5 Day Bootcamp
Rochester, NY
May 13 to 17, 2013
https://ssl.durkee.us/cissp/

16th Annual New York State Cyber-Security Conference / 8th Annual Symposium on Information Assurance. It will be held June 4 & 5, 2013 in the Empire State Plaza in Albany, NY.
http://www.dhses.ny.gov/ocs/awareness-training-events/conference/2013/

What we're reading…

'Jailed for Jailbreaking'
http://www.networkworld.com/columnists/2013/013013-gearhead.html

2013 Rochester Chapter Officers

President – Ralph Durkee
Vice President – Rich Savacool
Secretary – Jackie Stewart
Communication Officer – Holly Turner
Treasurer – Phil LaGraff
Membership Director – Joel Cort
Web Administrator – Susan Casserino
Accountant – Jim Pierce

About our Chapter

The Information Systems Security Association (ISSA) is a not for profit business association comprised of information security professionals and practitioners. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government. The Rochester Chapter was the 101st official chapter of the international Information Systems Security Association.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

In 2006 Rochester ISSA members hosted the first annual Rochester Security Summit. The Summit is a community focal point for education and awareness in collaboration with higher education and business and industry partners, held during National Cyber Security Awareness Month. Speakers and panels provide education opportunities for executives, CFOs, CIOs/CSOs, business managers, IT managers, security professionals, technical specialists and developers.

Interested in Membership?
Visit www.RocISSA.org for more information.

Links:

www.issa.org

https://www.owasp.org/index.php/Rochester

http://www.rit.edu/programs/information-security-and-forensics
https://www.facebook.com/RITInfosec

http://www.isacawny.org/

http://www.infragard.net/chapters/rochester/index.php

ISC2 Central NY Chapter – Utica, NY
https://www.isc2.org/

http://digitalrochester.com/