Hackers and Auditors, can't we all just get along?

Dan Anderson CISA, CRISC, CBCLA, C|EH, PCIP, ITIL
President ISACA Utah Chapter
Mentor Weasel

What happens when you put IT Audit together with Hackers?

How did this topic come about?

- Hacker Halted, Miami 2012, Halloween
- Discussion with focus group on topics of infosec
- Chris Silvers, expert Social Engineer
- Rob Jorgensen, Infosec Professor, Utah Valley University
- I mentioned that concept of having hackers understand what Auditors do and vice versa, having Auditors understand hackers.
- I said “What would an IT Audit person ever talk about to a group of hackers like this?”.—game on!

What can hackers do?

http://youtu.be/Ow7M3nFN1ho

What are the elements?

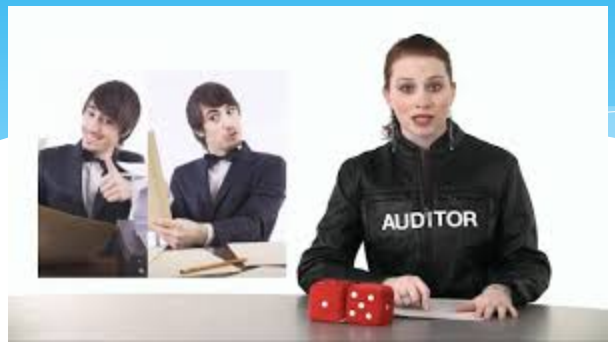
The Mindset of an IT Auditor

* Professional skepticism is the term used to describe the mindset of an auditor in critically assessing the audit evidence obtained during an audit.
* It means asking the right questions, following up when things don't make sense and not accepting what management tells you without corroboration.

The Mindset of a Hacker

A **hacker** is a knowledgeable person with a mindset fit to crack any challenge. He or she might even enjoy the challenge more than the end product. In general a hacker is creative, not destructive. A hacker will never let his challenge go without a real fight. A hacker is an inquisitor, sometimes that could mean breaking things, sometimes that could mean creating things. And last but not least, a hacker has a lot of fun.

In Audit: There are three main objectives being pursued by audit firms, standards bodies, and others to respond to the challenge of professional skepticism:



1. Improving individual auditor training.
2. Increasing awareness of where auditing standards give particular emphasis on the need to exercise professional skepticism during an audit.
3. Strengthening documentation procedures (show me the evidence!) to make sure that the auditor's thought process, not just conclusions from the work done, are explicitly set out in the audit file.

Hacking: Fixing, modifying, or making something do something it was not designed to do. This is the stereotypical definition of hacking.

Hacking is not limited to computer related stuff. This is an important note. However, the word hacking, today, is mostly used for the idea of computer-hacking.

Of the five most sought-after internal auditor skills by global recruiters, only one covers a technical area:--
IIA Audit Executive Center 2012 Global Pulse of the Internal Audit Profession survey

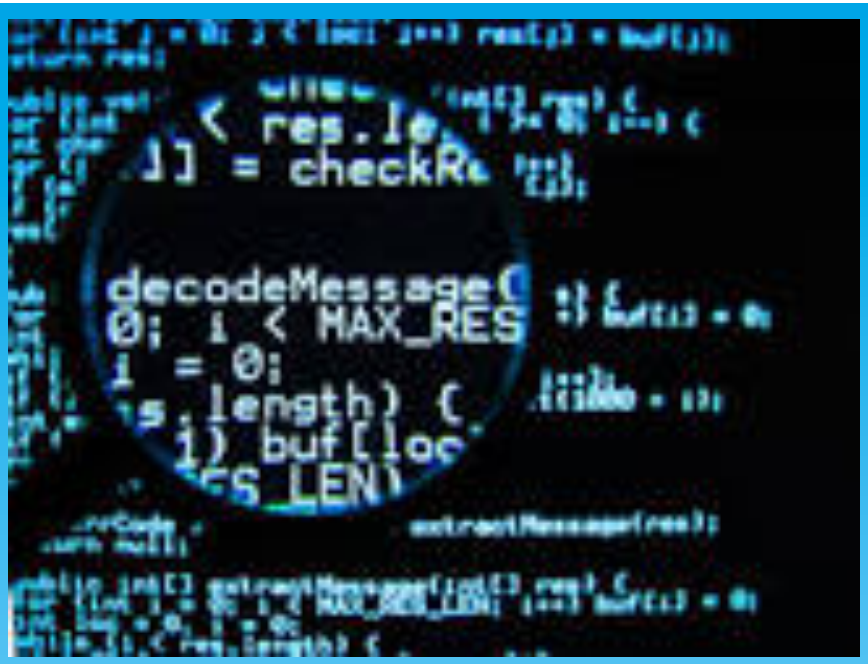
1. Analytical and critical thinking (72 percent)
2. Communication skills (57 percent)
3. IT general skills (49 percent)
4. Risk management (49 percent)
5. Business acumen (43 percent)

Software exploitation is hacking because you are making the software do something it was not designed, expected, and/or intended to do.

Web-application exploitation is hacking because you are making the software run in a way the designer did not intend or perhaps expect.

The results of the 2012 Global Pulse of the Internal Audit Profession survey conducted by The IIA's Audit Executive Center deliver dramatic confirmation of how much the requisite skills for internal auditors have changed!

Chief audit executives are no longer lined up at the doors of their local universities to bid for newly minted accounting graduates.
Instead, today's internal audit job postings are apt to look for people with nontraditional skills to fill vacant positions.



Reverse engineering could be seen as hacking because programs are not designed to be decompilable.

Each year, Protiviti's Internal Audit Capabilities and Needs Survey Report identifies the personal skills and capabilities
internal audit professionals want to improve:

1. Presenting (public speaking)
2. Developing board committee relations (beyond audit committee)
2. Developing outside contacts/networking (tie)
3. Persuasion
3. Using/mastering new technology and applications (tie)
4. Negotiation
Dealing with confrontation (tie)

Social engineering is hacking because you are making people do something they would not have done without modification of the situation.

The 7 habits of highly effective IT Auditors

* Integrity
* Relationship Building
* Partnering
* Teamwork
* Communications
* Continuous Learning
* Diversity

"Soft skills are the new hard skills"-----Larry Harrington, Chief Audit Executive, Raytheon Company

- Natural inquisitiveness
- Persuasiveness
- Change management proficiency
- A service orientation
- An ability to recognize and respond to diverse thinking styles, learning styles, and cultural qualities
- A global mindset

The Three Hats in Hacking

1) **White Hats**
2) **Grey Hats**
3) **Black Hats**

http://youtu.be/R9vDzaBwD_k

True Confessions of hackers circa 2001

http://youtu.be/R9vDzaBwD_k

"The 5 principles of the hacker mindset"…Eric Raymond Editor in Chief, from the *Jargon File*

1. The world is full of fascinating problems to be solved.
2. No problem should ever have to be solved twice.
3. Boredom and drudgery are evil.
4. Freedom is good.
5. Attitude is no substitute for competence.

The ongoing experiment

How to get started:

1. As an IT Auditor, begin by studying hackers or as a hacker, spend time with IT Auditors.
2. Familiarize yourself with local communities (hacker spaces such as 801 Labs), ISACA, ISSA, ISC^2
3. Become a C|EH, CISSP, CISA, CRISC, etc.
4. Attend Security Seminars and industry forums such as DefCon, Blackhat, Hacker Halted, Bsides, ISACA CACS, etc.
5. Become part of the hacking community and/or the IT Audit community.

The ongoing experiment

As an Auditor, you may end up with a monkey on your head. This is good. Watch out for the Sweedes!—Blackhat Vendor event Caesar's Pool party 2013.

The Benefits:

Auditors

* Learn from Hackers and be able to answer "why"
* Think about how to audit differently and/or more thoroughly
* Defense!
* Know your adversary
* Learn to use some valuable tools
  * Scanners
  * Log file manipulation
* Social Engineering

Hackers

* Understand Audit process and techniques—for future exploits
* Networking
* Understand the value proposition of why an audit can be effective in organizations
* How to engage differently with the C-Suite
* Obtain consulting gigs

What are some possible common traits shared by both Auditors and Hackers?

1. A natural curiosity and healthy skepticism
2. Work ethic
3. Integrity
4. Relationship Building
5. Partnering
6. Communication
7. Teamwork
8. Diversity
9. Continuous learning
10. Desire to make the world a better place

‘The Hacker Way’ — Mark Zuckerberg

An approach to building that involves continuous improvement and iteration.

* *Hackers believe that something can always be better, and that nothing is ever complete.*
* *They just have to go fix it – often in the face of people who say it’s impossible or are content with the status quo.*

In Summary

As Auditors adopt the hacker way, they too enjoy continuous improvement and understanding. Automation is the key to removing the drudgery and long spreadsheet hours.

As Hackers understanding processes, tools, and techniques of Auditors can help make you more efficient, more stealthy, and more thorough.

Working together we have much to gain, and also, much to share, to improve the security in our systems, in our communities, and in our people.

References

1. Mark Zuckerberg's letter to investors: 'The Hacker way'
   http://www.wired.com/2012/02/zuck-letter/
2. IIA Pulse of the Profession 2012 Global Insights:
   https://na.theiia.org/services/cae-resources/Public%20Documents/The%20Pulse%20of%20the%20Profession_2012%20Global%20Insights.pdf
3. Exploiting Software Exploit Format Strings with Python:
   http://hakin9.org/exploiting-software-0211-exploit-format-strings-with-python-2/comment-page-12/
4. Protiviti Internal Audit Capabilities and Needs Survey:
   http://www.protiviti.com/en-US/Pages/IA-Capabilities-and-Needs-Survey.aspx
5. The 7 Habits of Highly Effective Internal Auditors: Richard Chambers and Paul McDonald:
   https://global.theiia.org/news/Documents/7%20Attributes%20of%20Highly%20Effective%20Internal%20Auditors.pdf

Questions?

ISACA
Trust in, and value from, information systems
Utah Chapter

Dan K Anderson, CEO Cybereleven.com
CISA, CRISC, CBCLA, C|EH, PCIP, ITIL
Dan.anderson@cybereleven.com
Http://www.cybereleven.com

CYBER ELEVEN

ISACA®
Serving IT Governance Professionals

IT GOVERNANCE INSTITUTE®
LEADING THE IT GOVERNANCE COMMUNITY