

[Full-Disclosure] Re: [ISN] Book Review: Forensic Discovery

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0711.html>

From: Anthony Zboralski (*bcs2005_at_bellua.com*)

Date: 01/20/05

Date: Thu, 20 Jan 2005 19:37:50 +0700

To: InfoSec News <isn@c4i.org>

On 19 Jan 2005, at 14:55, InfoSec News wrote:

- > <http://books slashdot.org/books/05/01/18/2110235.shtml>
- >
- > [<http://www.amazon.com/exec/obidos/ASIN/020163497X/c4iorg> - WK]
- >
- > *Author: Dan Farmer & Wietse Venema*
- > *Pages: 198*
- > *Publisher: Addison Wesley Professional*
- > *Rating: 10*
- > *Reviewer: Ben Rothke*
- > *ISBN: 020163497X*
- > *Summary: Forensic Discovery overview*
- >
- > *Security luminaries Dan Farmer and Wietse Venema wrote one of the*
- > *first vulnerability scanners (SATAN) almost 10 years ago; SATAN was*
- > *the precursor to ISS Scanner, Retina and nmap. Venema wrote such*
- > *well-known security applications as the TCP Wrapper program and the*
- > *Postfix mail server. Farmer and Venema's new book Forensic Discovery*
- > *is a valuable book that grounds a computer-savvy reader in the world*
- > *of digital forensics.*

Source: <http://hert.org/story.php/58>

After reading the review of Dan Farmer and Wietse's Forensic Discovery, you should hear about

The Grugq who got fired from @stake after writing a Phrack Article in which he exposed numerous flaws in The Coroner's Toolkit by Dan & Wietse.

Before you read this book, check out the video (bittorrent) of The Grugq on The Art of Defiling and see how to defeat "industry grade" forensic tools and techniques .

Full-Disclosure: [Full-Disclosure] Re: [ISN] Book Review: Forensic Discovery

You can also meet him at a hacker convention near you (in March at BCS2005 in Jakarta, in April at Black Hat in S'pore and Amsterdam and at HITB2005 Bahrain.

Video of the Grugq's Speech, The Art of Defiling:
<http://www.hert.org/z/grugq.torrent> (Courtesy of HITB2004)

Presentation Slides:
<http://packetstormsecurity.com/hitb04/hitb04-grugq.pdf> (from HITB2004)

Phrack article:
<http://www.phrack.org/show.php?p=59&a=6> (Phrack 59)

Grugq's Profile:
<http://www.bellua.com/bcs2005/asia05.speakers.html#grugq>

The Grugq has been researching anti-forensics for almost 5 years. He has presented to the UK's largest forensic practitioner group where he scared Scotland Yard.

Grugq has worked to secure the networks and hosts of global corporations, and he's also worked for security consulting companies. His work as a security consultant was cut short temporarily following the publication of an article on anti-forensics.

P.S. Is it illegal to talk about anti-forensics under the Patriot Act?

gaius

--

Bellua Cyber Security Asia 2005 - <http://www.bellua.com/bcs2005>
21-22 March - The Workshops - 23-24 March - The Conference
bcs2005@bellua.com - Phone: +62213918330 HP:+628159102495

Full-Disclosure - We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>